

# Nationale Richtlijn Employment Screening 2024-2029



Vereniging  
Beveiligingsprofessionals  
Nederland



# Voorwoord

Dit is de vierde versie van de Nationale Richtlijn Employment Screening 2024-2029. Deze richtlijn dient als handreiking voor HR-, facility- en security professionals, alsook bestuurders die bij het onderwerp screening betrokken zijn, om invulling te geven aan het proces van ‘betrouwbaarheidsonderzoeken’.

Deze herziene versie is bijgewerkt met de huidige stand van zaken met betrekking tot wet- en regelgeving en de praktische uitvoering van achtergrondonderzoeken van personen.

Deze richtlijn vormt een eerste stap in een doorlopend proces van aanpassing en verbetering, bedoeld om een evenwicht te vinden tussen veiligheid, inclusiviteit en flexibiliteit binnen onze arbeidsmarkt.

De Nederlandse arbeidsmarkt ondergaat momenteel ingrijpende veranderingen en uitdagingen. De toenemende krapte op de arbeidsmarkt dwingt organisaties om breder te kijken naar potentiële kandidaten, inclusief statushouders. De integratie van statushouders in het arbeidsproces bevordert niet alleen de inclusiviteit, maar biedt tevens een kans om arbeidstekorten te verminderen.

De dreiging van buitenlandse actoren, zowel statelijke als niet-statale, neemt gestaag toe. Dit vraagt om een heroverweging van onze traditionele screeningmethoden, aangezien de betrouwbaarheid en integriteit van individuen niet altijd adequaat vastgesteld kan worden. Vooral voor kennisinstellingen, organisaties binnen de vitale infrastructuur en organisaties met kwetsbare processen zal het gebruik van geavanceerde technologieën, psychologische evaluaties en internationale samenwerkingen cruciaal zijn om deze nieuwe uitdagingen aan te gaan en een evenwicht te vinden tussen nationale veiligheid en het bieden van kansen aan kwetsbare groepen binnen de arbeidsmarkt.

De herziening van deze richtlijn is uitgevoerd op verzoek van de Vereniging Beveiligingsprofessionals Nederland (VBN) door de werkgroep Insider Threat.

Mijn bijzondere dank gaat uit naar de volgende deelnemers van de werkgroep:

- **Veerle de Beurs**, rechercheur en adviseur Security Risico Management bij Levent Group B.V.
- **Lois Retèl**, criminoloog en onderzoeker bij Levent Group B.V.
- **Drs. Edwina Egger**, data protection officer (DPO / FG), adviseur informatiebeveiliging en data privacy
- **Berndt Riff, MSc, MBA**, afdelingshoofd Bureau BVA en Landelijke Beveiligingsautoriteit Rechtspraak bij Raad voor de rechtspraak
- **Mr. Marcus Draaisma**, advocaat arbeidsrecht bij Palthe Oberman Advocaten, bestuurslid bij de Nationale Sollicitatie Commissie
- **Mr. Hélène Minderman**, branchemanager Techniek Nederland – Vakcommissie Beveiliging

Deze richtlijn is tot stand gekomen dankzij hun inzet en specialistische bijdragen.

**René Reijenga**

Voorzitter VBN werkgroep  
Insider Threat

# Inleiding

Het screenen van medewerkers is cruciaal om potentiële schade te voorkomen, vooral als het gaat om kandidaten die mogelijk niet de beweerde competenties bezitten of de gewenste waarden en normen missen. Deze richtlijn, herzien door VBN en de werkgroep Insider Threat, ondersteunt uw organisatie bij het ontwikkelen en implementeren van een effectief en proportioneel screeningsbeleid binnen de wettelijke kaders.

Het doel is niet alleen het optimaliseren van het screeningsproces, maar ook het bevorderen van dialoog en bewustwording over screenings binnen uw organisatie.

## Leeswijzer

De nationale richtlijn is verdeeld in drie delen:

**Deel 1** bevat een introductie over het screenen, waarin wordt uitgelegd wat screenen is en de toegevoegde waarde ervan.

**Deel 2** biedt een format voor het opstellen van een eigen screeningsbeleid. Dit format kan worden overgenomen en naar eigen idee worden aangepast en gebruikt.

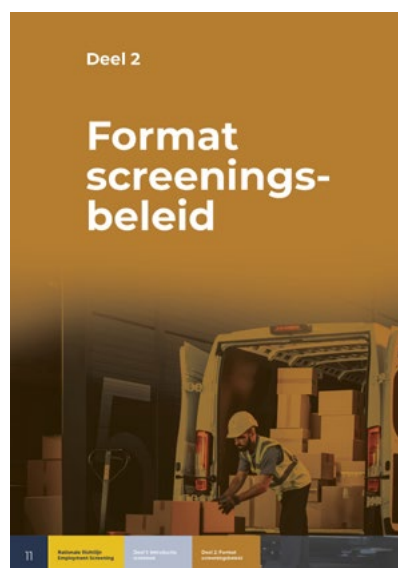
**Deel 3** geeft een uitgebreide toelichting op het screeningsbeleid uit deel 2 en bespreekt de onderwerpen die aan bod zijn gekomen.

## Onafhankelijkheid werkgroep

*De leden van de werkgroep hebben onafhankelijk gehandeld, gemandateerd door de VBN, en waren vrij van financiële belangen in het onderwerp van de richtlijn. Het concept van de richtlijn is ter goedkeuring voorgelegd aan het bestuur van de VBN.*

## Disclaimer

*Hoewel deze tekst zorgvuldig is samengesteld, kunnen de VBN en de leden van de werkgroep niet aansprakelijk worden gesteld voor de juistheid en volledigheid van de informatie. De teksten mogen vrij worden gebruikt, mits met bronvermelding.*



# Inhoudsopgave

## Voorwoord

### Inleiding

Leeswijzer

Onafhankelijkheid werkgroep | Disclaimer

## Deel 1: Introductie screenen

- 1.1 Wat is een screening?
- 1.2 Waarom screenen?
- 1.3 Wat is integriteit?
- 1.4 Wat is een kwetsbaarheid?
- 1.5 Is een VOG een screening?
- 1.6 Wat zijn de effecten van screenen?
  - 1.6.1 Cijfers
  - 1.6.2 Verdere voordelen
    - 1.7 Is deze richtlijn voor mijn bedrijf van toepassing?
- 1.8 Wat is de inhoud van een screening?
  - 1.8.1 Pre-employment
  - 1.8.2 In-employment
  - 1.8.3 Post-employment
- 1.9 Hoe ziet het screeningsproces eruit?

## Deel 2: Format screeningsbeleid

- 2.1 Inleiding
  - 2.1.1 Doel van de screening
  - 2.1.2 Scope
- 2.2 Definities
- 2.3 Juridische en ethische overwegingen
- 2.4 Risicobeoordeling en risicoprofiel
- 2.5 Screeningsprocedure
  - 2.5.1 Voorafgaande informatie
  - 2.5.2 Uitvoering van de screening
  - 2.5.3 Beoordeling
  - 2.5.4 Rollen en verantwoordelijkheden
  - 2.5.5 Bezwaar- en klachtenprocedure
- 2.6 Kwaliteitsborging
- 2.7 Herziening van het screeningsbeleid

## Deel 3: Toelichting screeningsbeleid

- 3.1 Formuleren doelstelling
- 3.2 Opstellen en uitvoeren van het screeningsbeleid
- 3.3 Wet- en regelgeving
  - 3.3.1 Algemene Verordening Gegevensbescherming (AVG)
  - 3.3.2 Nationale sollicitatiecode NVP
  - 3.3.3 Particulier Onderzoeksbureau Vergunning
- 3.4 Kaderbepalingen
  - 3.4.1 Waarom wordt een screening ingezet?
  - 3.4.2 Wanneer wordt een screening ingezet?
  - 3.4.3 Hoe wordt een screening uitgevoerd?
- 3.5 Dreigingsanalyse / Risicoprofiel opstellen
  - 3.5.1 Opstellen functiebeschrijvingen
  - 3.5.2 Opstellen risicoprofiel
- 3.6 Onderdelen van een screening
- 3.7 Uitslag beoordelen
  - 3.7.1 Uitslag pre-employment-screening
  - 3.7.2 Uitslag In-employment-screening

## Afsluiting

### Bibliografie

### Begrippenlijst

Deel 1

# Introductie screenen



# Deel 1: Introductie screenen

## 1.1 Wat is een screening?

Een 'screening' is in feite een grondige analyse van de achtergrond van een (potentiële) werknemer, bedoeld om de integriteit van de persoon in te schatten. Volgens de Autoriteit Persoonsgegevens omvat dit het verzamelen en verifiëren van relevante informatie. Deze informatie kan variëren van financiële gegevens tot opleidingshistorie en eerdere werkervaringen, waarbij soms gebruik wordt gemaakt van OSINT-technieken om gegevens uit openbare bronnen te verkrijgen (OSINT staat voor Open Source Intelligence). Dergelijke screenings kunnen plaatsvinden in verschillende fasen van het dienstverband: vóór indiensttreding (pre-employment), tijdens het dienstverband voor periodieke controles (in-employment) en zelfs na uitdiensttreding (post-employment). De meest voorkomende screening is de pre-employmentscreening, die vaak wordt ingezet voor zowel interne als externe sollicitaties. Het specifieke karakter van een screening wordt bepaald door de geïdentificeerde risico's, een aspect dat in deze richtlijn verder wordt uitgediept.

### CASUS

*Een energieleverancier, actief in de vitale infrastructuur, ontving een sollicitatie van Lisa. Gedurende het screeningsproces toonde zij zich uitermate coöperatief door alle vereiste documenten tijdig naar het screeningbureau te sturen en het bedrijf proactief te informeren over de status van haar Verklaring Omtrent het Gedrag (VOG). Tijdens de achtergrondcheck ontdekte het screeningbureau via mediabronnen verontrustende informatie. Lisa werd in verschillende nieuwsartikelen beschreven als verdachte in een grote terrorismezaak. Bronnen meldden dat ze al geruime tijd onder surveillance stond vanwege tekenen van radicalisering en mogelijke voorbereidingen op een terroristische aanslag. De combinatie van haar leeftijd en geboorteplaats in deze artikelen bevestigde dat het om de sollicitante ging.*

*Op Lisa's CV was geen melding gemaakt van een werkonderbreking tijdens de periode waarin zij volgens de media in hechtenis was in afwachting van haar proces. Een grondiger onderzoek van haar werkgeschiedenis onthulde echter onjuistheden in de opgegeven werkperiodes; er was wel degelijk een onderbreking geweest. Lisa wachtte in vrijheid op de uitspraak van haar zaak.*

*In een vervolgesprek erkende Lisa haar betrokkenheid bij de rechtszaak en gaf ze toe dat de kans klein was dat ze een VOG zou ontvangen. Gezien de ernst van de aanklacht en het potentiële imagoverlies voor de energieleverancier, werd besloten om haar sollicitatieprocedure onmiddellijk te beëindigen.*

## 1.2 Waarom screenen?

Uw organisatie bezit waardevolle elementen zoals gebouwen, goederen, financiële middelen, informatie, medewerkers, klanten/cliënten en relaties. Deze activa verdienen bescherming tegen externe en interne dreigingen. Schendingen kunnen niet alleen materiële schade veroorzaken maar ook de reputatie van uw organisatie, en soms zelfs van een hele sector, beschadigen met verstrekkende gevolgen. Het is daarom cruciaal om beschermende maatregelen te implementeren, wat soms zelfs wettelijk of contractueel verplicht is.

Pre-employment screening biedt inzicht in de achtergrond van potentiële werknemers: zijn er uit het verleden of heden omstandigheden die een integere functievervulling in de weg kunnen staan? Aan de hand van deze informatie wordt bepaald of en welke maatregelen nodig zijn om eventuele schade te voorkomen.

### Voorbeelden ter illustratie:

- Een persoon die veroordeeld is voor fraude en in een schuldsaneringstraject zit, moet niet in een financiële functie zonder toezicht worden geplaatst.
- Iemand die recent ontslagen is wegens grensoverschrijdend gedrag, is niet geschikt als leidinggevende van een kwetsbare groep medewerkers.
- Een medewerker zonder de vereiste diploma's of certificaten mag bepaalde functies niet vervullen.

Ervaring toont aan dat veel veiligheids- en integriteitsrisico's achteraf voorkomen hadden kunnen worden met een adequate screening. Een zorgvuldige afweging is daarbij essentieel. Een (jeugd)zonde hoeft niet noodzakelijkerwijs een belemmering te zijn, mits de betrokkene transparant is, ervan heeft geleerd en passende maatregelen zijn overeengekomen.

### 1.3 Wat is integriteit?

Screening biedt inzicht in het al dan niet integer functioneren van een (toekomstige) werknemer. Maar wat houdt integriteit in? Personen die als integer worden beschouwd, worden vaak gezien als eerlijk, betrouwbaar en te vertrouwen. Echter, de termen integriteit en betrouwbaarheid worden vaak door elkaar gebruikt. Voor de duidelijkheid definiëren we deze begrippen binnen ons screeningsbeleid als volgt:

- **Betrouwbaarheid** duidt op de consistentie en voorspelbaarheid van iemands gedrag en acties. Een betrouwbaar persoon komt beloften na, respecteert afspraken en deadlines, en wordt beschouwd als verantwoordelijk. Dit begrip toont aan of een persoon in staat is om taken uit te voeren en verantwoordelijkheden te dragen.
- **Integriteit** betreft eerlijkheid, eerbaarheid en ethische standaarden. Iemand met integriteit leeft volgens ethische principes, zelfs buiten het zicht van anderen. Deze persoon vermijdt oneerlijk gedrag en schendt geen waarden. Integriteit duidt op de mate waarin iemand zich houdt aan de ethische normen van de organisatie en eerlijk en integer handelt wanneer dat nodig is.

Samenvattend, betrouwbaarheid betekent consistentie en verantwoordelijkheid in het naleven van afspraken, terwijl integriteit betrekking heeft op eerlijkheid en ethisch gedrag, zelfs als er geen direct toezicht is. Beide eigenschappen zijn essentieel voor een positieve werkomgeving en organisatiecultuur. Echter, integriteit kan worden beïnvloed door bepaalde kwetsbaarheden, die verder worden uitgediept in de volgende sectie.

### 1.4 Wat is een kwetsbaarheid?

Het concept van kwetsbaarheid in relatie tot integriteit verwijst naar situaties waarin individuen worden uitgedaagd in hun vermogen om ethische normen te handhaven. Externe druk, verleidingen, en groepsdruk kunnen tot gedragingen leiden die in strijd zijn met persoonlijke waarden en integriteit. Voor organisaties is het essentieel om deze kwetsbaarheden te herkennen en preventieve maatregelen te implementeren, zodat de risico's geminimaliseerd worden. Hieronder volgen twee casussen die voorbeelden van dergelijke kwetsbaarheden illustreren.

#### **Frauderende verzekeringsman kreeg tweede kans, maar ging weer in de fout en verduisterde 1,9 ton**

| 4 dec. 2023 | RTV oost |

Nadat hij een eerste keer in de fout was gegaan bij een verzekeringskantoor in zijn eigen woonplaats Holten, kreeg hij een tweede kans. Maar de 41-jarige verzekeringsman sluisde andermaal geld weg. Deze keer een kleine 1,9 ton.

#### CASUS

*Jan, een medewerker van een verzekeraar, heeft toegang tot uitgebreide persoonsgegevens. Door persoonlijke financiële problemen ervaart hij aanzienlijke stress; hij worstelt om maandelijks rond te komen terwijl hij schulden aflost. Jan is vader van twee kinderen, voor wie hij al lang geen cadeaus meer heeft kunnen kopen. Hoewel hij verwacht binnen een jaar schuldenvrij te zijn, ontvangt hij op een dag een anoniem verzoek om persoonlijke gegevens te verstrekken. Deze gegevens kan hij uit zijn werkdata halen. Het delen van deze informatie zou hem genoeg geld opleveren om zijn schulden volledig af te betalen. Hoewel Jan weet dat het delen van de gegevens ongeoorloofd is, voelt hij de druk om zijn financiële situatie snel te verbeteren voor het welzijn van zijn familie. Deze casus illustreert de kwetsbaarheid van werknemers voor externe invloeden, voortkomend uit persoonlijke omstandigheden.*

#### CASUS

*Elsa werkt bij een softwarebedrijf, een organisatie die veel vertrouwelijke informatie verwerkt. Ze is vorig jaar vanuit een autoritair regime naar Nederland gevlucht, een regime dat bekend staat om zijn spionageactiviteiten en het uitoefenen van druk op expats en hun families. Recent ontving Elsa anonieme berichten waarin werd bedreigd met gevaar voor haar familie, tenzij zij gevoelige bedrijfsinformatie zou delen met de zender. De berichten waarschuwden haar ook tegen het inlichten van anderen, zoals haar werkgever of de politie. Nooit had Elsa voorzien dat zij in zo'n situatie terecht zou komen, en ook haar werkgever had dit risico niet met haar besproken. Nu staat Elsa voor een dilemma: het delen van de informatie druist in tegen haar principes, maar ze maakt zich ernstige zorgen over de veiligheid van haar familie. Deze casus onderstreept het belang voor bedrijven om zich bewust te zijn van de persoonlijke situaties van werknemers en om beschermende maatregelen te overwegen.*

## 1.5 Is een VOG een screening?

De Verklaring Omtrent het Gedrag (VOG) is een bekend screeningsinstrument, uitgegeven door het Ministerie van Justitie en Veiligheid, via dienst Justis. De VOG beoordeelt het justitiële verleden van een individu: bestaat er een strafblad? Justis beoordeelt of antecedenten uit de laatste vier jaar relevant zijn voor de functie in kwestie, gebaseerd op de functietitel en het door de werkgever aangeduide risicoprofiel, en besluit vervolgens de VOG te verlenen of te weigeren. In 2022 werd 15,61% van de VOG-aanvragen goedgekeurd ondanks bekende antecedenten, terwijl slechts 0,18% werd afgewezen.

Screening omvat het verzamelen van informatie uit diverse bronnen, waarbij verder gekeken wordt dan alleen naar strafbare feiten. Zo kan iemand die grensoverschrijdend gedrag op de werkvloer vertoonde, zonder dat dit heeft geleid tot een geregistreerd strafbaar feit. Deze informatie kan naar voren komen tijdens gesprekken met de kandidaat of diens referenties. Hoewel een VOG een waardevol onderdeel van een screening kan zijn, biedt het geen compleet overzicht.

### CASUS

*Frans solliciteert naar de functie van facilitair manager bij een mediabedrijf en moet een VOG overleggen. Hoewel hij een veroordeling voor pedofilie heeft, acht Justis dit niet relevant voor zijn beoogde functie en verleent derhalve de VOG. Frans begint met zijn nieuwe baan. Justis weet echter niet dat het mediabedrijf zich in een groot complex bevindt waar ook een kinderdagverblijf gevestigd is voor de kinderen van alle medewerkers in het complex. Dit illustreert hoe het verlenen van een VOG niet per se alle risico's uitsluit.*

## 1.6 Wat zijn de effecten van screenen?

De implementatie van een screeningsbeleid reikt verder dan alleen de overweging van tijd en financiën. Screening, soms vereist door wettelijke of contractuele verplichtingen, biedt significante intrinsieke waarde voor een organisatie. Een zorgvuldige screening ondersteunt de bescherming van bedrijfscultuur, imago, en integriteit.

De volgende secties zullen deze voordelen verder uitdiepen, onderbouwd met gegevens van diverse screening- en fraudepreventieorganisaties.

### 1.6.1 Cijfers

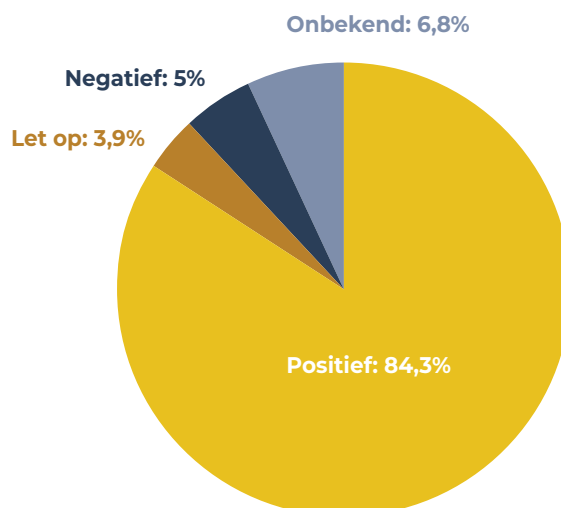
Een Nederlandse screeningsorganisatie heeft in 2022 en 2023 in totaal 11.000 dossiers behandeld. Bij 84,3% van deze screenings zijn geen feiten of omstandigheden aangetroffen die een risico vormden voor de aanstelling van de kandidaat.

In 3,9% van de gevallen kwam informatie naar boven die een potentieel risico aanduidde, maar niet direct een beletsel vormde voor aanstelling. In deze situaties is het essentieel dat de werkgever met de kandidaat in gesprek gaat om aanvullende maatregelen te treffen die de risico's minimaliseren.

Bij 5% van de screenings, ofwel 550 gevallen, werd een ernstige dreiging of risico voor de organisatie geïdentificeerd. Gevonden dreigingen omvatten onder andere vervalste informatie over arbeidshistorie of opleiding, ongewenst gedrag bij eerdere werkgevers en (online) gedrag dat imagoschade kan veroorzaken. Ook waren er gevallen waarbij de invloed van statelijke actoren een significant risico vormde, resulterend in een negatief advies.

Bijna 7% van de screenings heeft een onbekende uitslag. Dit kan zijn omdat de kandidaat niet wilde meewerken aan de screening, de resultaten niet wilde delen met de werkgever of de sollicitatieprocedure voortijdig beëindigde. De reactie en houding van een kandidaat tijdens de screening kunnen inzicht bieden in zijn of haar potentiële gedrag tijdens een dienstverband.

### Resultaten van 11.007 uitgevoerde screenings in 2022





## 1.6.2 Verdere voordelen

### • Voorkomen van omzetverlies

Screening helpt de kosten te verlagen die gerelateerd zijn aan frauduleuze activiteiten. Het vermindert de kans dat individuen met oneerlijke intenties toetreden tot de organisatie en verhoogt de kans op het ontdekken van dergelijk gedrag. Het bestaan van een screeningsproces kan op zichzelf al potentiële sollicitanten met oneerlijke bedoelingen afschrikken.

### • Verhoogde werkstandaard

Onwaarheden of leugens over vaardigheden en professionele geschiedenis worden snel onthuld tijdens een grondige screening, waardoor de kans kleiner wordt dat deze personen worden aangenomen. Dit bevordert hogere werkstandaarden en effectiviteit binnen de organisatie. Een nauwkeurige bevestiging van de competenties beschreven in het cv en tijdens selectiegesprekken verkleint de kans op tekortschieten door onbekwaamheid. Investerings in training en inwerkprogramma's worden daarmee waardevoller, wat leidt tot lagere personeelsverloop en besparingen op werving en opleiding.

### • Veiligheidsbewustzijn op de werkvloer

Door medewerkers zorgvuldig te screenen, onderstreept een organisatie het belang van een veilige werkomgeving. Weten dat collega's niet alleen op hun vaardigheden maar ook op hun integriteit zijn beoordeeld, versterkt het gevoel van veiligheid onder het personeel. Dit bevordert motivatie en draagt bij aan een positieve en veilige bedrijfscultuur.

## 1.7 Is deze richtlijn voor mijn bedrijf van toepassing?

Ondermijning, cyberaanvallen, spionage, hackers, phishing, datalekken, terrorismedreiging, en toenemend extremisme zijn termen die vaak in het nieuws verschijnen. Hoewel deze voor velen ver van hun bed lijken, zijn ze uiterst relevant voor alle organisaties. Overheidsinstellingen zoals de AIVD, NCTV, en MIVD onderstrepen dit belang.

Aan het einde van 2023 verhoogde het NCTV het nationale dreigingsniveau voor terrorisme van 'aanzienlijk' (3) naar 'substantieel' (4), wat wijst op een reële kans op een aanslag in Nederland. Deze dreiging komt niet alleen vanuit jihadistische groeperingen, maar ook vanuit rechts-extremisme en anti-institutioneel extremisme. Bovendien mengen criminele

onderwereldactiviteiten zich steeds meer met de legale bovenwereld, variërend van het misbruiken van vrachtvervoer voor het transporteren van illegale goederen tot datadiefstal. Het is cruciaal om niet alleen te weten wie uw organisatie binnenkomt, maar ook de kwetsbaarheden van uw bedrijfsvoering te identificeren. Een dreigingsanalyse (zie 3.5) stelt u in staat deze kwetsbaarheden vast te stellen en passende screeningpakketten te ontwikkelen.

De dreiging van buitenlandse actoren, zowel statelijk als niet-staatelijk, is eveneens in opkomst. De traditionele methoden zijn vaak ontoereikend om de betrouwbaarheid en integriteit van individuen in deze context vast te stellen. Er zijn nieuwe benaderingen nodig om veiligheid te waarborgen en tegelijkertijd kansen te bieden aan kwetsbare groepen in de arbeidsmarkt. In deze complexe afweging kan professionele ondersteuning door gespecialiseerde experts van cruciaal belang zijn.

Hoewel niet iedereen die betrokken is bij de genoemde activiteiten noodzakelijkerwijs kwade intenties heeft, kan de associatie met dergelijke activiteiten het imago van uw bedrijf schaden. Daarom is een effectief screeningsbeleid essentieel voor elk bedrijf, ongeacht grootte of sector.

## CASUS

*Een organisatie, gespecialiseerd in het verzamelen van informatie over Nederlandse bedrijven, heeft een vacature in de sector Informatieveiligheid. David, een jonge IT-professional, is een van de kandidaten.*

*Tijdens de screening ontdekt het screeningsbureau dat David, naast zijn IT-werk, eigenaar is van drie autohandellocaties, een feit dat hij niet had vermeld in zijn sollicitatie en onbekend was bij de organisatie. David ziet deze activiteiten als een passieve inkomstenbron en een hobby, en begrijpt niet hoe deze een risico kunnen vormen voor de organisatie. Echter, er zijn zorgen over hoe deze autohandels gefinancierd zijn en waarom David investeerde in een sector waar hij geen affiniteit mee heeft.*

*Hoewel de organisatie wist dat David nevenactiviteiten ondernam en mede-eigenaar was van een bedrijf, waren ze niet op de hoogte van de aard van deze activiteiten of dat hij de enige eigenaar was. Deze elementen roepen vragen op over mogelijke integriteitsrisico's en de potentie van ondermijning in Davids ondernemingen. Het is essentieel voor de organisatie om te overwegen of zij bereid is het risico te accepteren dat dergelijke praktijken hun organisatie beïnvloeden.*

### **Ambtenaar stal voor ruim een ton aan telefoons en laptops van ministerie**

| AD | 21 februari 2024 |

Het Openbaar Ministerie eist een celstraf van twee jaar, waarvan een half jaar voorwaardelijk, tegen een ambtenaar van het ministerie van Economische Zaken en Klimaat vanwege de diefstal van 191 iPhones, negen iPads en vijf MacBooks.

### **Helpt medewerkers maakt geen melding van integriteitsschending**

| 6 december 2023 | Consultancy.nl |

Vier op de tien medewerkers heeft het afgelopen jaar een vorm van integriteitsschending meegemaakt op de werkvloer, zo blijkt uit onderzoek van KPMG.

Integriteitsschending op de werkvloer kan vele vormen aannemen. Denk aan het onzorgvuldig omgaan met geheime of persoonlijke informatie, het schenden van de privacy, pesten, het creëren van een vijandige werksfeer of het lastigvallen van een collega of ondergeschikte.

## 1.8 Wat is de inhoud van een screening?

### 1.8.1 Pre-employment

Tijdens de pre-employmentscreening wordt de sollicitant getoetst aan het functieprofiel waarop hij/zij solliciteert. Dit proces richt zich op het uitsluiten van kwetsbare kandidaten waarvan de risico's niet effectief kunnen worden beperkt.

### 1.8.2 In-employment

Bij een in-employment screening worden bepaalde aspecten van de initiële screening herhaald. Dit stelt werkgevers in staat om op de hoogte te blijven van wijzigingen in de financiële situatie van werknemers of hun eventuele betrokkenheid bij activiteiten buiten het werk. Als er bij aanvang geen screening heeft plaatsgevonden, kan een gecombineerde pre- en in-employment screening worden uitgevoerd.

### 1.8.3 Post-employment

De post-employmentscreening concentreert zich op een correcte beëindiging van de arbeidsrelatie. Het doel is om potentiële risico's die een ex-werknemer voor de organisatie kan vormen na zijn of haar vertrek te beoordelen, zoals het risico op verlies of misbruik van vertrouwelijke informatie, of betrokkenheid bij externe fraude.

## 1.9 Hoe ziet het screeningsproces eruit?

Het uitvoeren van een screening is een gestructureerd en doordacht proces. Hieronder beschrijven we de zes algemene stappen die worden doorlopen:

- 1. Kaderbepaling:** in deze initiële fase wordt vastgesteld welk type screening wordt uitgevoerd en welke specifieke onderdelen daarbij horen. Dit is afhankelijk van de functie, het risiconiveau en de specifieke vereisten van de organisatie.
- 2. Informatieverzameling:** nadat het kader is bepaald, wordt de benodigde informatie voor de screening verzameld. Dit kan gaan om persoonsgegevens, documentatie en andere relevante data.
- 3. Analyse van de informatie:** de verzamelde gegevens worden nauwkeurig geanalyseerd. Hierbij wordt onder andere gekeken naar de echtheid van documenten, de consistentie in verstrekte gegevens en of er essentiële informatie ontbreekt.
- 4. Beoordeling en advies:** op basis van de grondige analyse wordt de informatie beoordeeld. Uit deze beoordeling volgt een advies. Dit advies is gebaseerd op de bevindingen en kan bijvoorbeeld een aanbeveling zijn om een kandidaat wel of niet aan te nemen.
- 5. Besluitvorming:** de organisatie of de verantwoordelijke persoon neemt een besluit op basis van het gegeven advies. Dit kan leiden tot een positieve of negatieve uitkomst voor de betrokken persoon of situatie.
- 6. Vastlegging van het besluit:** het uiteindelijke besluit wordt gedocumenteerd, ongeacht de uitkomst. Dit zorgt voor transparantie en is cruciaal voor toekomstige referenties of audits.

Dit zorgvuldig gestructureerde proces garandeert dat screenings grondig en consistent worden uitgevoerd, wat bijdraagt aan de betrouwbaarheid en veiligheid van de organisatie.

Deel 2

# Format screenings- beleid



# Deel 2: Format screeningsbeleid

*Beschrijf hier kort een inleiding op het screeningsbeleid. Zorg ervoor dat het aansluit bij de organisatie en tot de verbeelding spreekt.*

**Belang van screening:** leg uit wat het belang van screening in sector/ uw organisatie voor (bijvoorbeeld) veiligheid, betrouwbaarheid en naleving van de wet.

**Doelstellingen en reikwijdte:** geef een afbakening van de doelen en de reikwijdte van het screeningsbeleid.

Neem **een definitie** op van de belangrijke termen in het screeningsbeleid.

Zorg dat uw beleid niet in strijd is met de geldende wet- en regelgeving. Hiernaast staan voorbeelden van deze **wet- en regelgeving**. Win advies in als hier onduidelijkheid over bestaat (zie ook 3.3).



Dit hoofdstuk bevat een voorbeeld van een beknopt screeningsbeleid, voor het fictieve bedrijf 'PES Koeriers'. In de marge vindt u algemene toelichtingen die u kunt gebruiken als leidraad of checklist voor het aanpassen en toetsen van uw eigen screeningsbeleid. Uitgebreide achtergrondinformatie over de verschillende onderdelen vindt u in hoofdstuk 3, 'Toelichting screeningsbeleid'.

Let op dat dit een voorbeeld is van een screeningsbeleid. U kunt het beleid aanpassen op basis van de specifieke behoeften en omstandigheden van uw organisatie.

## Voorbeeld screeningsbeleid PES-koeriers

### 2.1 Inleiding

Voor PES Koeriers is het belangrijk betrouwbaar personeel te selecteren en in dienst te hebben. Onze organisatie heeft waarde: gebouwen, voertuigen, financiële middelen, informatie, medewerkers, klanten, de goederen die wij vervoeren, een uitstekende reputatie, etc. Deze waarde verdient bescherming tegen dreigingen van buitenaf en van binnenuit. Dit screeningsbeleid legt uit hoe en waarom we screenings uitvoeren.

#### 2.1.1 Doel van de screening

De doelstelling van het screeningsbeleid is het opstellen en structureren van het proces 'screening'.

Het doel van screening van (nieuwe) interne en externe medewerkers is het beperken van risico. We moeten ons personeel kunnen vertrouwen. Onze medewerkers zijn vaak verantwoordelijk voor waardevolle goederen en werken zelfstandig. Met een screening is er inzicht in de persoon die onze organisatie binnenkomt: zijn er omstandigheden uit het verleden of het heden die integer functioneren in de weg staan? Een (nieuwe) medewerker wordt er zich zo ook van bewust dat integriteit belangrijk is voor onze organisatie. Medewerkers kunnen erop vertrouwen dat nieuwe collega's dezelfde screening hebben ondergaan. Screening wordt ook ingezet bij medewerkers die al in dienst zijn, bijvoorbeeld bij een functieverandering of bij uitbreiding van verantwoordelijkheden.

#### 2.1.2 Scope

Dit screeningsbeleid is van toepassing op alle (nieuwe) interne en externe medewerkers. Het is niet mogelijk om functiegroepen uit te sluiten. Ook is het niet mogelijk om door middel van andere maatregelen te zorgen voor de zekerheid van betrouwbaar personeel en een geaccepteerd risiconiveau. De zwaarte van de screening is afhankelijk van de functie (zie 2.4).

## 2.2 Definities

|   |   |   |
|---|---|---|
| <b>AVG en UAVG</b>  | <b>Medewerker</b>   | <b>Screening</b>  |
| De Algemene Verordening Gegevensbescherming (AVG) is de wet voor de omgang met persoonsgegevens. Dit is een Europese verordening. In Nederland is daarnaast de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) van kracht. | In het kader van dit screeningsbeleid: de medewerker die een nieuwe functie krijgt of een uitbreiding van verantwoordelijkheden.  | Het systematisch onderzoeken of de verstrekte informatie door een kandidaat in overeenstemming is met de werkelijkheid en of er geen relevante gegevens zijn achtergehouden. Dit kan in de vorm van een persoonsgericht of achtergrondonderzoek..                                   |
| <b>Kandidaat</b>  | <b>Risicoprofiel</b>  | <b>Verklaring Omtrent het Gedrag (VOG)</b>  |
| De sollicitant die door het selectieproces is gekomen en aan die akkoord is met de geboden arbeidsvoorwaarden.  | Een risicoprofiel identificeert en evalueert de kwetsbare aspecten van verschillende functies binnen een organisatie. Dit profiel bepaalt de diepgang en zwaarte van de vereiste screening, rekening houdend met de mate van risico en kwetsbaarheid geassocieerd met elke functie. | Een door het ministerie van Justitie en Veiligheid (Justis) verstrekte verklaring waaruit blijkt dat een natuurlijk persoon of een rechtspersoon wel of geen strafblad heeft en zo ja, of dit bezwaarlijk is voor de uit te voeren functie (Ministerie van Justitie en Veiligheid). |

## 2.3 Juridische en ethische overwegingen

PES Koeriers respecteert de geldende wet- en regelgeving. Bij het opstellen van dit screeningsbeleid houden we rekening met de volgende regelgeving en kaders.

- **AVG en UAVG:** wetgeving die de verwerking van persoonsgegevens reguleert, waarborgt privacy en gegevensbescherming.
- **Antidiscriminatiewetgeving:** voorkomt discriminatie op basis van geslacht, ras, leeftijd of andere kenmerken tijdens het screeningsproces.
- **Wet op de Ondernemingsraden:** biedt richtlijnen voor medezeggenschap en inspraak van werknemers bij beleidsvorming, inclusief screeningsbeleid.
- **Wetboek van Strafrecht en Burgerlijk Wetboek:** regelt aspecten van persoonlijke levenssfeer en privacy, voorkomt ongeoorloofd handelen tegen individuen.
- **Art. 10 GW en Art. 8 EVRM:** beschermen het recht op persoonlijke levenssfeer en privacy van het individu.
- **Arbeidsomstandighedenwet:** legt de werkgever de verplichting op te zorgen voor een veilige en gezonde werkomgeving, inclusief aspecten gerelateerd aan screenings.
- **BW Boek 7 Artikel 658:** legt aansprakelijkheid bij de werkgever voor het waarborgen van een veilige werkomgeving.
- **NVP-sollicitatiecode:** biedt ethische en professionele richtlijnen voor het wervings- en selectieproces.

Specifiek voor de AVG geldt dat een organisatie een goede grondslag moet hebben om persoonsgegevens te verwerken voor het screenen. Op basis van het eerder omschreven doel (betrouwbaarheid van personeel en beperken van risico's) heeft de organisatie een 'gerechtvaardigd belang' om vooraf en bij verandering van functie/uitbreiding verantwoordelijkheden, kandidaten en werknemers te screenen.

Onze organisatie houdt rekening met de gevoeligheid van het screeningsproces. Er worden immers veel gegevens verzameld en geïnterpreteerd. Maar: er wordt niet meer gevraagd en onderzocht dan nodig is om aangeleverde gegevens te verifiëren en we kijken en oordelen objectief. Hier is het screeningsproces goed op ingericht.

**Het inzetten van screening moet proportioneel zijn:** daarom is het van belang om vooraf een risico-inventarisatie te doen en per functie te bepalen op welke punten moet worden gescreend. Bekijk 3.5 voor praktische voorbeelden. Uiteraard is dit geheel vrij te bepalen: nevenstaande tekst is slechts een voorbeeld.

## 2.4 Risicobeoordeling en risicoprofiel

PES Koeriers houdt rekening met alle functiespecifieke elementen om te komen tot het juiste type screening. Elke functie binnen onze organisatie wordt geëvalueerd op specifieke risico's. Op basis van deze evaluatie is bepaald welk niveau van screening nodig is voor de verschillende functies.

De inhoud van de screening is als volgt opgebouwd:

### Screenpakket A

- a. controle van de identiteit
- b. onderzoek naar de opleidingen van de kandidaat
- c. onderzoek naar het arbeidsverleden van de kandidaat, inclusief het benaderen van referenten
- d. opvragen VOG
- e. onderzoek naar antecedenten

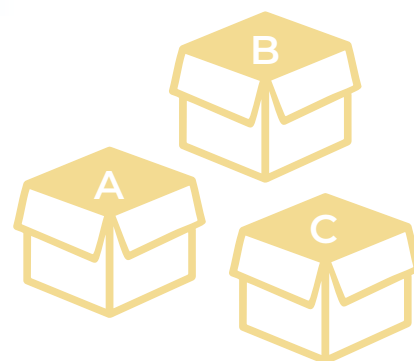
### Screenpakket B

- a. controle van de identiteit
- b. onderzoek naar de opleidingen van de kandidaat
- c. onderzoek naar het arbeidsverleden van de kandidaat, inclusief het benaderen van referenten
- d. opvragen VOG
- e. onderzoek naar antecedenten
- f. onderzoek naar de financiële situatie van de kandidaat

### Screenpakket C

- a. controle van de identiteit
- b. onderzoek naar de opleidingen van de kandidaat
- c. onderzoek naar het arbeidsverleden van de kandidaat, inclusief het benaderen van referenten
- d. opvragen VOG
- e. onderzoek naar antecedenten
- f. onderzoek naar de financiële situatie van de kandidaat
- g. onderzoek naar de kandidaat in open bronnen

| Functie                   | Pakket A | Pakket B | Pakket C |
|---------------------------|----------|----------|----------|
| Koerier                   | ✓        |          |          |
| Koerier waardetransporten |          | ✓        |          |
| Ondersteunend personeel   | ✓        |          |          |
| Financiële functies       |          |          | ✓        |
| Directie                  |          |          | ✓        |



**Beschrijf hier hoe u de kandidaat informeert, welke stappen worden genomen en hoe de beoordeling verloopt.**

**Beschrijf ook wie (rollen, afdelingen) verantwoordelijk is voor het screeningsbeleid en wie belast is met de uitvoering (zie 3.2).**

**Benoem de bewaartermijn en -plek.** Worden de screenrapportages opgenomen in het personeelsdossier? Wat is de procedure als iemand uiteindelijk toch niet in dienst treedt? Hoe lang worden de rapportages bewaard? (zie 3.3).

**Benoem hoe de gegevens worden beveiligd.** Indien gebruik wordt gemaakt van applicaties, beschrijf dan de autorisaties (wie mag wat zien/wijzigen/verwijderen). Indien gebruik wordt gemaakt van een externe partij voor screening, geef dan aan wie de rapporten ontvangt.

**Kwaliteitsborging:** beschrijf aan welke kwaliteitsnormen het screenproces moet voldoen en hoe dit door de organisatie wordt gecontroleerd en geborgd.

## 2.5 Screeningsprocedure

De screening vindt plaats voordat de kandidaat in dienst komt. De screening moet positief zijn afgerond voordat de aanstelling wordt geformaliseerd. Stapsgewijs ziet de procedure er uit zoals hieronder beschreven:

### 2.5.1 Voorafgaande informatie

- In de vacaturetekst nemen we op dat screening onderdeel is van het selectieproces. We beschrijven heel kort waarop we screenen.
- Tijdens sollicitatiegesprekken vertellen we over de screeningsprocedure. We geven de sollicitant een informatieformulier waarin wordt uitgelegd waarom onze organisatie screent, hoe het proces verloopt, wat er van de kandidaat verwacht wordt en wat zijn/haar rechten zijn tijdens het proces. Wat betreft de rechten: een kandidaat mag het resultaat van de screening inzien, heeft het recht om foutieve gegevens te corrigeren en mag het screenrapport laten verwijderen (bij een verzoek om verwijdering zal indiensttreding helaas niet mogelijk zijn).
- Wij melden vooraf dat we gekozen hebben voor een externe, onafhankelijke partij om de screening uit te voeren (indien van toepassing).
- Tijdens het arbeidsvoorwaardengesprek benadrukken we dat een positief afgeronde screening een voorwaarde is voor indiensttreding.

### 2.5.2 Uitvoering van de screening

- Afhankelijk van het screeningspakket dat bij de functie hoort, levert de kandidaat de benodigde stukken aan.
- Voor de precieze invulling van de screeningswerkzaamheden verwijzen we naar de interne procesbeschrijving (het voert voor dit voorbeeld te ver om dit hier op te nemen).

### 2.5.3 Beoordeling aan de hand van de verkregen informatie

- Voor de screening moet de kandidaat informatie aanleveren. Als de kandidaat niet of onvoldoende medewerking verleent, leidt dit tot een negatief screenrapport. Een kandidaat met een negatief screenrapport komt niet in dienst.
- Voor het afgeven van een positief screenrapport moeten alle onderdelen goed zijn afgerond, of er is een duidelijke verklaring gegeven door de kandidaat over een gevonden inconsistentie.
- Er zullen tijdens een screening bevindingen zijn die zonder meer tot een negatieve uitkomst leiden. Denk bijvoorbeeld aan een diploma dat is vervalst of een vermelding op een opsporingslijst. Een kandidaat met een negatief screeningsrapport komt niet in dienst.
- Er zijn ook bevindingen die extra weging vragen. Denk hierbij aan een minder positieve referentie, een erg 'uitgerekte' werkzame periode bij een vorige werkgever, een niet-vermelde nevenfunctie of een recent faillissement dat niet is genoemd. Hiervoor geldt dat de kandidaat de mogelijkheid krijgt om te reageren op de bevinding. Het is aan de afdeling HR en de lijnmanager om te bepalen of dit leidt tot afwijzing of dat aanvullende schriftelijke afspraken moeten worden gemaakt om het risico te mitigeren.

### 2.5.4 Rollen en verantwoordelijkheden

- In eerste instantie is de afdeling Compliance verantwoordelijk voor het screeningsbeleid. Bij afwezigheid van Compliance is de afdeling HR verantwoordelijk voor het screeningsbeleid.
- De afdeling HR is verantwoordelijk voor de correcte uitvoering van de screeningsprocedure.
- Bij screening van directieleden is de RVC verantwoordelijk voor de uitvoering van de screeningsprocedure.
- De externe screenorganisatie werkt in opdracht van de directeur HR en onder diens verantwoordelijkheid (indien van toepassing).

### 2.5.5 Bezwaar- en klachtenprocedure

- Het is mogelijk dat een kandidaat het niet eens is met de uitslag van de screening. Als er sprake is van een onjuistheid in het screenrapport, mag de kandidaat dat onderbouwd aangeven en - indien gevalideerd - worden onjuistheden gecorrigeerd.
- Als de kandidaat ook na correctie niet tevreden is over het screenrapport, kan eventueel hierover een gesprek plaatsvinden, waarbij de directeur HR zal aansluiten.
- Als er over het screeningsproces of het screenrapport een formele klacht komt, dan wordt deze neergelegd bij de directeur HR.

## 2.6 Kwaliteitsborging

Onze organisatie stelt hoge eisen aan de kwaliteit van het screeningsproces.

Dit zijn punten waaraan moet worden voldaan:

- Het screeningsproces moet binnen drie weken worden afgerond. Een langere doorlooptijd moet voorzien van achtergrondinformatie worden gerapporteerd aan de directeur HR.
- Kandidaten moeten tevreden zijn met het verloop van de screening. Eventuele klachten moeten worden gerapporteerd aan de directeur HR.
- Er mag geen aanstelling plaatsvinden voordat de kandidaat een positieve screening heeft doorlopen. Indien om een reden hiervan wordt afgeweken, is dit alleen mogelijk na accordering door de directeur HR.
- De informatievoorziening aan de kandidaat wordt jaarlijks gecontroleerd door de privacy officer.
- Jaarlijks wordt in opdracht van de directeur HR een audit uitgevoerd om de integriteit en effectiviteit van het screeningsproces te waarborgen.

## 2.7 Herziening van het screeningsbeleid

Het screeningsbeleid wordt jaarlijks herzien om de effectiviteit te garanderen en eventueel aan te passen aan veranderende omstandigheden en eisen.



Deel 3

# Toelichting screenings- beleid



# Deel 3: Toelichting screeningsbeleid

## 3.1 Formuleren doelstelling

Het is raadzaam de doelstelling van de screening(en) te documenteren in het screeningsbeleid. Deze doelstelling is afgeleid van een recent opgesteld dreigingsbeeld van de organisatie.

## 3.2 Opstellen en uitvoeren van screeningsbeleid

Het screeningsbeleid moet worden opgesteld door een of meerdere inhoudsdeskundige medewerkers. Die moeten onbevoegd menselijk handelen, dat voortkomt uit persoonsgebonden kwetsbaarheden, inzichtelijk kunnen maken in een risicoanalyse.

Deze medewerkers moeten ook in staat zijn om dreigingen te vertalen naar adequate beheersmaatregelen. Een effectief screeningsbeleid vereist inzicht in 'insider threats' en het herkennen van mogelijke dreigingsscenario's die de organisatie kunnen beïnvloeden. In het tijdperk van globalisering is het cruciaal dat de verantwoordelijke functionaris begrijpt hoe (buitenlandse) inlichtingendiensten, terroristische groeperingen en criminele netwerken kunnen infiltreren en personeel kunnen werven.

Screening moet worden uitgevoerd door gekwalificeerde functionarissen of door een gespecialiseerd extern bureau, mits de organisatie instemt met het openbaar maken van interne kwetsbaarheden. De verantwoordelijke medewerkers moeten beschikken over de vereiste competenties. Het screeningsbeleid moet speciëren welke documenten en systemen, inclusief open bronnen, beschikbaar moeten zijn voor de medewerker die de screening uitvoert. Het is cruciaal om alle belanghebbenden binnen het screeningsproces te identificeren en op te nemen in het beleid. De volgende afdelingen zijn typisch betrokken bij het ontwikkelen en uitvoeren van het screeningsbeleid:

- Compliance
- Human Resources (HR)
- Juridische zaken
- Beveiliging

Het is belangrijk dat er één verantwoordelijke afdeling - een specifieke lijnmanager - wordt aangewezen als verantwoordelijke voor het screeningsproces. Als de betreffende lijnmanager geen inhoudelijk kennis heeft van een recent dreigingsbeeld of recente risicoanalyse zal het risico geaccepteerd moeten worden dat de getroffen maatregelen de daadwerkelijke dreigingen die zich in de samenleving voordoen niet afdekken. De competenties van de proceseigenaar, inclusief noodzakelijke opleiding en werkervaring, dienen ook vastgelegd te zijn in het screeningsbeleid.

Het is cruciaal dat een specifieke afdeling of lijnmanager als verantwoordelijk wordt aangewezen voor het screeningsproces. Indien deze lijnmanager niet voldoende op de hoogte is van de actuele dreigingsbeelden of risicoanalyses, zal het risico geaccepteerd moeten worden dat de geïmplementeerde maatregelen mogelijk niet alle bestaande bedreigingen afdekken. Daarom moeten de vereiste competenties van de proceseigenaar, waaronder de benodigde opleiding en ervaring, duidelijk gedocumenteerd worden in het screeningsbeleid.

## 3.3 Wet- en regelgeving

Wet- en regelgeving bepalen de grenzen van het screenen. Volgens de Arbowet is de werkgever verplicht een veilige werkomgeving voor haar werknemers te garanderen. Screenen mag niet in strijd zijn met de anti-discriminatiewetgeving, die geldt voor zowel bestaande als toekomstige arbeidsverhoudingen (Noot: Algemene Wet Gelijke Behandeling, artikelen 7:646 e.v., artikel 3 Arbowet). Hierbij is het essentieel dat noch interne noch externe kandidaten gediscrimineerd of grensoverschrijdend behandeld worden. Bij het screenen is de erkenning van de persoonlijke levenssfeer van de kandidaten en de personen die bij werving en selectie betrokken zijn, van groot belang. Hierbij dienen de normen van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG gevolgd te worden. Verder heeft de ondernemingsraad wettelijke rechten in het wervings- en selectieproces, zoals het adviesrecht bij de benoeming van bestuurders en het groepsgewijs werven of inlenen van arbeidskrachten.

Als 'soft law' kan de NVP Sollicitatiecode genoemd worden, die richtlijnen stelt voor het sollicitatieproces. Werkgevers wordt aangeraden om een solide eigen werving- en selectiebeleid te hanteren, in overeenstemming met de wetgeving, om het werving- en selectieproces transparant en voorspelbaar te maken en zo de reputatie van de werkgever te versterken.

### 3.3.1 Algemene Verordening Gegevensbescherming (AVG)

Bij een screening worden veel persoonsgegevens verzameld, soms ook bijzondere persoonsgegevens. Werkgevers moeten daarom de Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG) zorgvuldig naleven. De belangrijkste eisen uit de AVG en UAVG zijn:

- **Gerechtigd belang.** De werkgever moet een gerechtvaardigd belang voor de screening aantonen. Dit belang, vaak de noodzaak van integriteit en betrouwbaarheid van werknemers, moet grondig worden gedocumenteerd en verdedigbaar zijn. In bepaalde gevallen, zoals bij kinderopvang, is screening wettelijk verplicht en hoeft het belang niet aangetoond te worden.
- **Juridische grondslag.** De grondslag 'toestemming' is geen geldige basis voor een screening. De kandidaat of werknemer staat in een afhankelijke positie ten opzichte van de (toekomstige) werkgever. Zij kunnen door deze afhankelijke positie druk ervaren om toestemming te geven. Hierdoor is dus geen sprake van in vrijheid gegeven toestemming. Toestemming is wel de goede grondslag bij het invullen van een sollicitatieformulier: iemand kan natuurlijk in vrijheid beslissen om wel of niet te solliciteren!
- **Proportionaliteit.** De diepgang van de screening moet proportioneel zijn aan de privacy-inbreuk. Intensieve achtergrondcontroles zijn alleen toegestaan voor functies waarbij deze strikt noodzakelijk zijn voor de veiligheid of integriteit.
- **Subsidiariteit.** De screening moet noodzakelijk zijn; de werkgever moet aantonen dat het doel niet op een minder ingrijpende manier bereikt kan worden.
- **Informatievoorziening.** Sollicitanten of werknemers moeten grondig geïnformeerd worden over het screeningsproces, het doel ervan en de relevantie. Ook moeten ze ingelicht worden over hun rechten onder de AVG, waaronder het recht op inzage en correctie van hun gegevens.

### Overige voorwaarden screening

Daarnaast moet u aan de volgende voorwaarden voldoen uit de (U)AVG:

- De werkgever gebruikt de gegevens die uit de screening zijn verkregen niet voor een ander doel.
- De gegevens worden niet langer bewaard dan noodzakelijk is voor het doel van de screening.
- De gegevens uit de screening zijn toereikend, ze doen ter zake en de organisatie verzamelt niet meer gegevens dan nodig.
- De gegevens zijn goed beveiligd.
- De werkgever beoordeelt of er een data protection impact assessment (DPIA) moet worden uitgevoerd. Screenen is namelijk een gegevensverwerking met een hoog privacyrisico.

### Data Protection Impact Assessment

Onder de AVG kunnen organisaties verplicht zijn om een Data Protection Impact Assessment (DPIA) uit te voeren. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerkende handeling in kaart te brengen, om daarna maatregelen te kunnen nemen met het doel de risico's te verkleinen c.q. te beperken. Het is zeer aan te raden om voor screening een DPIA uit te voeren.

Er zijn verschillende methodes om een DPIA uit te voeren. De basisvereisten zijn dat in de DPIA in ieder geval het volgende moet worden opgenomen:

- Een systematische beschrijving van de gegevensverwerking en de doeleinden hiervan. Beroept de werkgever zich op een gerechtvaardigd belang als grondslag voor de verwerking? Neem dit dan ook op in de beschrijving.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerking.
- Een beoordeling van de privacyrisico's voor de sollicitanten/medewerkers.
- De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat de organisatie aan de AVG voldoet.

Op de website van [de Autoriteit Persoonsgegevens](#) staat meer informatie over de DPIA.

### Vragen stellen versus informatie vastleggen

Het is een misvatting dat bepaalde vragen door de AVG verboden zijn. In het kader van risicoanalyses kan het essentieel zijn om specifieke vragen te stellen. Neem bijvoorbeeld iemand die uit China naar Nederland is verhuisd en werkt in de vitale infrastructuur; het kan relevant zijn om te vragen of er overheden zijn die druk op deze persoon kunnen uitoefenen. Voordat dergelijke vragen gesteld worden, moet de werkgever een heldere beoordeling en beleid formuleren over de noodzaak en relevantie van deze vragen. Antwoorden moeten uiterst zorgvuldig worden behandeld, waarbij alleen de strikt noodzakelijke informatie wordt vastgelegd.

### Bewaartermijnen vaststellen

Gegevens verkregen uit de screening mogen niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de screening. Dit vereist een duidelijk beleid over bewaartermijnen, in lijn met het principe van dataminimalisatie onder de AVG.

### 3.3.2 Nationale sollicitatiecode NVP

De Sollicitatiecode van de Nederlandse Vereniging voor Personeelsmanagement en Organisatieontwikkeling (NVP) geeft heldere regels over werving en selectie en de te respecteren belangen van de kandidaat.

De uitgangspunten met betrekking tot screening zijn als volgt:

- Alle informatie verkregen van de sollicitant wordt vertrouwelijk en zorgvuldig behandeld, waarbij de privacy van de sollicitant altijd wordt gerespecteerd;
- Het wervingsprofiel of de vacaturetekst moet naast de relevante kenmerken van de vacature, ook de sollicitatieprocedure, de deadline voor solliciteren, en de vereiste informatie van sollicitanten (zoals opleiding, diploma's, arbeidsverleden, en ervaring) duidelijk vermelden. Indien toepasselijk, moet het ook eventuele aanvullende selectieprocedures of -instrumenten specificeren, zoals psychologische tests, assessments, aanstellingskeuringen of verplichte antecedentenonderzoeken;
- Zowel de sollicitant als de organisatie dienen zich bewust te zijn van de potentiële onbetrouwbaarheid van informatie verkregen uit open bronnen zoals internet of derden. Dergelijke informatie moet met de sollicitant worden besproken onder vermelding van de bron, en de organisatie moet transparant zijn over hoe deze informatie is verkregen;
- Indien referenties bij derden worden opgevraagd of nader onderzoek nodig is, wordt vooraf toestemming aan de sollicitant gevraagd, behalve wanneer de wet deze toestemming niet vereist.

### 3.3.3 Particulier Onderzoeksbureau Vergunning

Bij inschakeling van een extern screeningsbureau is het van belang dat dit bureau voldoet aan de geldende wet- en regelgeving en in het bezit is van een Particulier Onderzoeksbureau (POB) vergunning, uitgegeven door het ministerie van Justitie en Veiligheid.





## CASUS

*Tom solliciteerde voor een docentenpositie bij een onderwijsinstelling die een grondige screening uitvoert als onderdeel van hun aannamebeleid, inclusief een referentiecheck. Tom gaf zijn ex-werkgever op als referent zonder deze te informeren over het aanstaande onderzoek. Aanvankelijk was de ex-werkgever terughoudend en leek onwillig om mee te werken. Hij gaf aan afstand te willen nemen van de situatie rond Tom. Echter, na verdere navraag en uitleg over het belang van de referentiecheck, kwam naar voren dat er ernstige zorgen waren over Toms gedrag op de werkvloer. Verschillende vrouwelijke collega's en studenten hadden aangegeven zich oncomfortabel en onveilig te voelen door Toms gedrag, waarvan meerdere incidenten waren vastgelegd.*

*Deze ontdekking onderstreept het belang van een grondige achtergrondcontrole en het verkrijgen van duidelijke redenen voor vertrek bij vorige werkgevers. Zonder deze referentie-informatie zou de onderwijsinstelling onbewust zijn gebleven van Toms gedrag, aangezien deze meldingen intern waren en niet extern gedocumenteerd. Het zorgvuldig vragen stellen en toepassen van geschikte gesprekstechnieken leidde ertoe dat de referent belangrijke informatie deelde die cruciaal was voor de aannamebeslissing. Deze casus illustreert het cruciale belang van een uitgebreide referentiecheck in het aannameproces.*

## 3.4 Kaderbepalingen

Het stellen van duidelijke kaders bepaalt de reikwijdte van het screeningsproces, waaronder het tijdstip en de omstandigheden waarin screening plaatsvindt, welke informatie wordt opgevraagd, en het specifieke doel van de screening.

### 3.4.1 Waarom wordt een screening ingezet?

Screening dient om te beoordelen of een (nieuwe of tijdelijke) medewerker of leverancier geen risico's oplevert, zoals geïdentificeerd in de risicoanalyse. Het doel is niet om de geschiktheid van een persoon voor een functie te bepalen; die beoordeling is de verantwoordelijkheid van de toekomstige lijnmanager en de afdeling Personeelszaken.

### 3.4.2 Wanneer wordt een screening ingezet?

Screeningstools voor pre-employment en in-employment worden gebruikt aan het einde van de (interne) wervings- en selectieprocedure. Post-employment screenings worden uitgevoerd bij het beëindigen van het dienstverband. Screenings vinden plaats vóór in- of uitdiensttreding, vóór een medewerker een nieuwe functie aanvaardt, of voor het einde van de proeftijd.

### 3.4.3 Hoe wordt een screening uitgevoerd?

Voordat een screening wordt uitgevoerd, moeten eerst specifieke voorbereidingen worden getroffen. Er moet een helder kader worden vastgesteld dat de betrouwbaarheid, integriteit en loyaliteit van de (nieuwe) medewerker beoordeelt. De basis voor de screening wordt gevormd door de bedreigingen en risico's die zijn geïdentificeerd in een dreigingsbeeld en/of risicoanalyse. Deze beoordeling bepaalt of een persoon een potentiële dreiging vormt. Voor een accurate evaluatie van de betrouwbaarheid, integriteit en loyaliteit moet bij voorkeur een periode van ten minste vijf jaar voorafgaand aan de sollicitatie worden onderzocht. Als dit niet haalbaar is, moet expliciet worden aangegeven welke risico's of dreigingen niet zijn onderzocht, gevolgd door een risicoafweging.

Afhankelijk van de functie die de persoon zal vervullen, wordt meer diepgaande informatie verzameld en gebruikt om te bepalen of de persoon geschikt is om de functie te aanvaarden of te behouden. De omvang en diepte van het onderzoek hangen af van het risiconiveau dat is vastgesteld voor de functie. De conclusie

over de betrouwbaarheid van een persoon is gebaseerd op verleden en huidig gedrag en vormt een momentopname (op de datum van afronding van het onderzoek).

De privacyimpact van de screening moet geminimaliseerd worden en voldoen aan relevante wet- en regelgeving, met nadruk op proportionaliteit en subsidiariteit. Alle screeninggegevens en het personeelsdossier moeten zorgvuldig worden behandeld en bewaard, ter bescherming van de veiligheid en privacy van de kandidaat.

### 3.5 Dreigingsanalyse / Risicoprofiel opstellen

Om te waarborgen dat een screening proportioneel en subsidiair is, is een analyse vereist die uitwijst welke persoonlijke kwetsbaarheden mogelijke risico's voor onbevoegd handelen met zich meebrengen. Deze kwetsbaarheden kunnen leiden tot onbevoegde acties door een (ingehuurde) medewerker of adviseur, hetzij uit eigen beweging door interne druk, hetzij omdat externe partijen druk uitoefenen. Beide gevallen vallen onder de noemer 'insider threats'. De Association of Certified Fraud Examiners (ACFE) publiceert om de twee jaar een rapport dat wereldwijd geanalyseerde incidenten beschrijft waarbij persoonlijke kwetsbaarheden tot onbevoegd handelen leidden. Ook veiligheidsdiensten zoals de AIVD brengen brochures uit over hoe externe partijen persoonlijke kwetsbaarheden exploiteren om druk uit te oefenen.

Uit een dreigingsanalyse, die de basis vormt voor de inzet van screeningsinstrumenten, moet duidelijk worden met welke risico's de organisatie rekening moet houden (voorstelbare scenario's). Daarnaast moet blijken dat zonder de inzet van deze instrumenten geen veilige werkomgeving gewaarborgd kan worden, zoals vereist door het Burgerlijk Wetboek.



#### 3.5.1 Opstellen functiebeschrijvingen

Een functiebeschrijving moet duidelijk de taken, verantwoordelijkheden en bevoegdheden van een functie vastleggen. Het moet specifiek aangeven welke activiteiten een medewerker uitvoert, waar deze zelfstandig kan opereren, en welke controlemechanismen er zijn om onbevoegde handelingen te voorkomen. Een gedetailleerde functiebeschrijving is essentieel voor het opstellen van een accuraat risicoprofiel en voor het rechtvaardigen van de noodzaak van een screening en de daarmee gepaard gaande privacy-impact.

Uit een functiebeschrijving - waar taken, verantwoordelijkheden en bevoegdheden van een functie in beschreven worden - moet blijken welke werkzaamheden een functionaris exact uitvoert. Een functiebeschrijving dient ook duidelijkheid te geven over de vraag waar een functionaris zelfstandig kan werken en of er controlemechanismen zijn om onbevoegde handelingen te voorkomen. Zonder goede functiebeschrijving is het vrijwel onmogelijk om een risicoprofiel op te stellen en kan ook geen antwoord gegeven worden op de vraag waarom er met een screening inbreuk gemaakt wordt op de privacy van een medewerker.

#### 3.5.2 Opstellen risicoprofiel

Elke functie bevat elementen die bepaalde kwetsbaarheden met zich meebrengen. De mate van kwetsbaarheid wordt beïnvloed door diverse factoren, waaronder de aard van de organisatie en de geografische locatie. Afhankelijk hiervan kunnen externe entiteiten zoals buitenlandse inlichtingendiensten, terroristische groepen, of criminele netwerken geneigd zijn medewerkers te dwingen tot onbevoegde acties of het lekken van waardevolle informatie. Dergelijke informatie kan ook worden onttrokken uit procedurele details of uit inzicht in de timing van interne of externe audits.

Iedere functie heeft kwetsbare functie-elementen. Er zijn verschillende factoren die de (mate van) kwetsbaarheid van die elementen bepalen. Afhankelijk van het soort organisatie en de vestigingslocatie zal een (buitenlandse) inlichtingendienst, een terroristische organisatie of een crimineel samenwerkingsverband bereid zijn medewerkers onder druk te zetten om onbevoegde (uitvoerende) handelingen te verrichten of om informatie te verstrekken die handelsperspectief geeft.

Handelingsperspectief kan ook verkregen worden uit informatie over procedures of uit kennis wanneer (interne of externe) controles gaan plaatsvinden.

Voor elke functie moet, op basis van de dreigingsanalyse en functiebeschrijving, worden vastgesteld of medewerkers potentiële doelwitten zijn voor externe kwaadwillenden om te benaderen of onder druk te zetten. Bij het opstellen van een risicoprofiel moeten de volgende vragen worden overwogen:

- In hoeverre is er sprake van omgang met geldzaken in de functie? *Denk hierbij aan budgetverantwoordelijkheid of het beschikken over contanten of girale gelden.*
- In hoeverre is er sprake van omgang met goederen in de functie? *Denk hierbij aan het aanschaffen, verkopen of beheren van goederen.*
- In hoeverre is het mogelijk om zelfstandig zakelijke overeenkomsten af te sluiten? *Denk hierbij aan het verlenen c.q. leveren of inhuren van diensten tegen betaling.*
- In hoeverre is het mogelijk invloed uit te oefenen op de uitvoering van (operationele) diensten? *Denk hierbij aan diensten zoals advies, beveiliging, schoonmaak of onderhoud.*
- In hoeverre is er sprake van controle of kan er solistisch gehandeld worden in de functie? *Denk hierbij bijvoorbeeld aan het plannen of annuleren van controles.*
- In hoeverre is er toegang tot (bedrijfs)informatie in de functie? *Denk hierbij aan kennis van veiligheidssystemen, besturingssystemen of controlemechanismen.*
- In hoeverre kunnen processen, zonder dat dit meteen opvalt, beïnvloed worden? *Denk hierbij aan werkzaamheden aan vitale processen.*
- In hoeverre betreft het een invloedrijke positie? *Denk hierbij aan het uitoefenen van invloed op personen en het organisatiebeleid.*

Hoe meer risicofactoren aanwezig zijn in een functie (of hoe belangrijker deze factor is voor de functie), des te crucialer het is om in het werving- en selectieproces aandacht te besteden aan persoonlijke kwetsbaarheden die misbruikt kunnen worden. Het aantal elementen en de mate van kwetsbaarheid bepalen de diepgang en intensiteit van een screening. Het is belangrijk te onthouden dat vaste medewerkers doorgaans loyaler zijn aan de organisatie dan niet-vaste medewerkers. Externen, vanwege een verondersteld hoger risico door minder loyaliteit, moeten eveneens worden gescreend. Wanneer tijdelijke medewerkers, ingehuurde krachten, adviseurs en leveranciers die onder hetzelfde risicoprofiel vallen niet gescreend worden, is het moeilijk te rechtvaardigen waarom eigen medewerkers wel worden gescreend, wat juridische vraagstukken omtrent privacy-inbreuk kan opleveren.



|                                       | Vragen over functionarissen   | Risico's  | Voorbeelden van functies   |
|---------------------------------------|---|---|--|
| <b>1. Vertrouwelijke informatie</b>   | Hebben ze de beschikking over vertrouwelijke of strategische informatie?  | Doorspelen/ verkopen van informatie, wijzigingen, manipuleren of misbruik ervan maken | Systeembeheerder, personeelsadviseur, communicatie-medewerker                        |
| <b>2. Omgaan met geld</b>             | Houden ze zich bezig met ontvangen, declareren, uitgeven of toekennen van geld?                                 | Fraude, diefstal, verduistering, omkoping, belangenverstrengeling                     | Kassier, medewerker inkoop, buschauffeur, medewerker burgerzaken                     |
| <b>3. Machts- en monopoliepositie</b> | Kunnen ze op basis van status/ deskundigheid invloed uitoefenen op besluitvorming of personen?                  | Machtsmisbruik  | Leidinggevende functies  |
| <b>4. Rechten en bevoegdheden</b>     | Kennen ze rechten of bevoegdheden toe aan personeel of burgers?   | Misbruik van bevoegdheden, fraude, omkoping   | Systeembeheerder, vergunningverstrekker, medewerker Sociale Dienst                   |
| <b>5. Beoordelen en adviseren</b>     | Kennen ze rechten of bevoegdheden toe aan personeel of burgers?   | Misbruik van bevoegdheden, fraude, omkoping   | Systeembeheerder, vergunningverstrekker, medewerker Sociale Dienst                   |
| <b>6. Goederen en diensten</b>        | Schaffen ze goederen of diensten aan, doen ze aanbestedingen?   | Diefstal, fraude, omkoping  | Projectleider, medewerker inkoop, medewerker projectbureau                           |
| <b>7. Handhaven</b>                   | Houden ze toezicht op de naleving van de regels?  | Omkoping  | Parkeercontroleur, milieu-agent, gemandateerd toezichthouder, accountant, inspecteur |
| <b>8. Sollistisch handelen</b>        | Voeren ze alleen of zeer zelfstandig kwetsbare handelingen uit of nemen ze besluiten zonder dat er controle is? | Omkoping, machtsmisbruik, misbruik van bevoegdheden, fraude                           | Directeur, opzichter, medewerker buitendienst, tolk/ vertaler, taxichauffeur         |
| <b>9. Invloedsfeer</b>                | Werken ze direct met burgers en bedrijven waardoor ze beïnvloed kunnen worden?                                  | Diverse vormen van belangenverstrengeling   | Medewerker buitendienst, loketfunctie  |
| <b>10. Kwetsbare groepen</b>          | Gaan ze om met kwetsbare personen zoals kinderen, ouderen of zieken?  | Misbruik, aanslagen, maatschappelijke schade  | Leraar, medewerker jeugdvereniging en kinderopvang, zorgverlener                     |
| <b>11. Toegang</b>                    | Hebben ze toegang tot bepaalde ruimtes, systemen en stoffen?  | Misbruik van bevoegdheden, fraude, omkoping   | Medewerker laboratorium, ziekenhuis, kernfysische dienst, infrastructuur             |

Bron: brochure *Screening van personeel, Justis*.





### 3.6 Onderdelen van een screening

Een screenpakket bestaat uit verschillende onderdelen, ofwel 'screentools'. Deze hebben betrekking op verschillende thema's. Per thema zijn vaak nog verschillende niveaus aan te brengen. De screentools samen vormen het screenpakket dat proportioneel is voor de functie.

In het screeningsbeleid moeten deze screenpakketten vermeld worden. Hierbij dient ook aangegeven te worden waarom deze screentools binnen de screenpakketten zijn gekozen. Voor de specifieke invulling van de screentools en mogelijkheden verwijzen wij u naar een externe partij die gespecialiseerd is in het uitvoeren van screenings. Hieronder staan een aantal voorbeelden van screentools:

- Controle van de identiteit;
- Onderzoek naar de financiële situatie van de kandidaat;
- Verificatie van de opleidingen van de kandidaat;
- Onderzoek naar het arbeidsverleden van de kandidaat, inclusief het benaderen van referenten;
- Onderzoek in open bronnen;
- Onderzoek naar antecedenten van de kandidaat.

### CASUS

*Onlangs plaatste een grote telecomprovider een vacature voor een financieel analist, waarop talrijke reacties binnenkwamen. Mark, met een masterdiploma in financiën van een prestigieuze universiteit, viel direct op tussen de sollicitanten. De telecomprovider voerde een uitgebreide pre-employment screening uit, waarbij documenten werden geverifieerd, referenties gecheckt en achtergrondonderzoeken uitgevoerd. Hoewel Mark een uittreksel van Dienst Uitvoering Onderwijs (DUO) en zijn diploma had ingediend, miste het DUO-uittreksel de gebruikelijke beveiligingskenmerken. Een verificatie bij de universiteit toonde aan dat het diploma vals was. Hierop werd Mark's sollicitatieprocedure onmiddellijk gestaakt.*

*De telecomprovider wilde geen persoon aannemen die in een vroeg stadium het vertrouwen al had geschonden door zijn academische kwalificaties te vervalsen. De zaak werd gemeld bij de relevante instanties, en zowel de universiteit als DUO deden aangifte van valsheid in geschrifte. Dit incident benadrukt het belang van een grondige pre-employment screening, en toont aan dat sommige kandidaten bereid zijn te frauderen om hun carrièrekansen te verbeteren. Dit roept de vraag op: als iemand bereid is een diploma te vervalsen, wat mag men dan nog meer verwachten van deze persoon in een professionele context?*

### 3.7 Uitslag beoordelen

Een screening kan leiden tot bevindingen die een positieve of negatieve uitslag geven. Hoe moet de organisatie met deze uitslag omgaan?

#### 3.7.1. Uitslag pre-employmentscreening

De resultaten van een pre-employment screening worden samengevat in een rapport, waarbij soms ook advies wordt gegeven door de uitvoerende partij. Echter, de organisatie die de werknemer overweegt in dienst te nemen, moet zelf besluiten over de aanname van de kandidaat. Het is essentieel om van tevoren duidelijk te hebben welke uitkomsten screenings kunnen hebben en wat de implicaties zijn. Een positief advies kan leiden tot indiensttreding van de kandidaat, terwijl een negatief advies kan leiden tot het einde van de sollicitatieprocedure, tenzij de organisatie besluit het advies verder te evalueren.

Wanneer er tijdens de screening bezwaren worden gevonden, kan worden overwogen of er maatregelen zijn om de risico's te verkleinen, zoals het invoeren van controlemechanismen voor de taken van de nieuwe medewerker. Besluiten moeten altijd op feiten gebaseerd zijn, niet op veronderstellingen, en vaststellen wie beslissingsbevoegd is, is cruciaal.

#### 3.7.2 Uitslag In-employmentscreening

In-employmentscreening betreft periodieke screening van eigen werknemers of eigen werknemers die (willen) overstappen naar een andere functie binnen de organisatie. Arbeidswetgeving en duidelijk werkgeversbeleid reguleren een eerlijke en transparante uitvoering van deze screenings, ondersteund door de norm van goed werkgeverschap. Het fundamentele principe is dat werknemers niet benadeeld mogen worden door de screening, tenzij de screening informatie onthult die zo ernstig is dat voortzetting van de arbeidsrelatie onredelijk zou zijn. Het is van belang dat is vastgelegd welke procedures moeten worden gevolgd als de arbeidsrelatie vanwege de screeningresultaten niet kan worden voortgezet.

### CASUS

*Bij een in-employmentscreening bij een zorginstelling is aan het licht gekomen dat een medewerker twee jaar geleden is veroordeeld voor mishandeling en bedreiging. Deze medewerker heeft toelichting en aanvullende documentatie verschaft na het verzoek hierom. Volgens zijn verklaring ontstond het incident uit een burenruzie, waarbij een overbuurman agressief op hem afliep. De medewerker reageerde door een voorwerp te gooien en bedreigingen te uiten, wat leidde tot een aangifte door de overbuurman. Het onderzoek onthulde dat de medewerker deze kwestie niet bij zijn werkgever had gemeld en zijn taakstraf buiten werktijden voltooide, waardoor dit onopgemerkt bleef. Verder blijkt uit zijn personeelsdossier dat hij ook op het werk vaak in conflicten verwickeld raakt.*

*Het is cruciaal dat werkgevers tijdig geïnformeerd worden over zulke situaties om passende maatregelen te kunnen nemen en escalatie op de werkvloer te voorkomen. De werkgever heeft de verantwoordelijkheid om een veilige werkomgeving te waarborgen; snel agressief gedrag van een medewerker kan deze veiligheid ondermijnen.*



Afsluiting

# Bibliografie Begrippen- lijst

# Afsluiting

De implementatie van gedegen pre-, in-, en post-employment screeningprocessen is essentieel voor elke organisatie die streeft naar het behoud van een sterke reputatie en het garanderen van een veilige werkomgeving.

Deze richtlijn is ontworpen om uw organisatie te beschermen tegen potentiële risico's die kunnen ontstaan door onvoldoende gescreende medewerkers. Door het systematisch toepassen van deze screeningsmethoden kan (imago)schade aanzienlijk worden beperkt en kan de integriteit van zowel uw personeelsbestand als uw organisatie als geheel worden versterkt.

## Advies

Het is cruciaal om deze screeningsprocedures correct en consistent toe te passen. Als uw organisatie niet over de vereiste kennis of capaciteit beschikt om een effectief screeningsbeleid te implementeren, wordt het sterk aanbevolen om samen te werken met externe gespecialiseerde bureaus. Deze bureaus beschikken over uitgebreide ervaring en expertise op het gebied van screening en kunnen waarborgen dat de procedures niet alleen voldoen aan de wettelijke eisen, maar ook op een ethisch verantwoorde manier worden uitgevoerd.

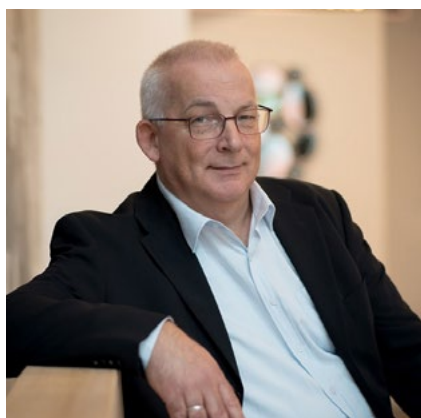
De Vereniging Beveiligingsprofessionals Nederland (VBN) kan adviseren over gekwalificeerde partijen die u kunnen ondersteunen bij het ontwikkelen en implementeren van een screeningsbeleid. Daarnaast biedt VBN voortdurende ondersteuning en advies om ervoor te zorgen dat uw screeningsprocessen actueel blijven en aanpassen aan veranderende wet- en regelgeving.

## Tot slot

Wij hopen dat deze richtlijn u de nodige inzichten heeft geboden en u in staat stelt om met vertrouwen de juiste stappen te zetten op het gebied van screening.

## René Reijenga

*Voorzitter VBN werkgroep Insider Threat*



# Bibliografie

- Autoriteit Persoonsgegevens. (z.d.). *Voorwaarden voor screening*. Geraadpleegd op 23 januari 2024, van <https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/screening/voorwaarden-voor-screening>
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2023, 11 mei). *Jaarverslagen. AIVD*. Geraadpleegd in februari 2024, van <https://www.aivd.nl/onderwerpen/jaarverslagen>
- Ministerie van Defensie. (2023, 24 april). *Jaarverslag MIVD 2022. Jaarverslag | Defensie.nl*. Geraadpleegd in februari 2024, van <https://www.defensie.nl/downloads/jaarverslagen/2023/04/19/jaarverslag-mivd-2022>
- Justis. (z.d.). *Screening van personeel*. Geraadpleegd op 23 januari 2024, van <https://justis.nl/justis/screening-van-personeel>
- Ministerie van Justitie en Veiligheid. (2023, 18 december). *Dreigingsbeeld Terrorisme Nederland. Nationaal Coördinator Terrorismebestrijding en Veiligheid*. Geraadpleegd op 5 februari 2024, van <https://www.nctv.nl/onderwerpen/dtn>
- NVP, netwerk voor HR-Professionals. (z.d.). *Sollicitatiecode - NVP*. Geraadpleegd op 5 februari 2024, van <https://www.nvp-hrnetwerk.nl/nl/sollicitatiecode>

# Begrippenlijst

## Algemene Verordening Gegevensbescherming (AVG)

De AVG bevat de belangrijkste regels voor de verwerking van persoonsgegevens in Nederland, en is de Nederlandse implementatie van de Europese GDPR.

## Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens.

## Betrouwbaarheid van informatie

Betreft de betrouwbaarheid van de informatie die door en over een kandidaat is aangeleverd.

## Betrouwbaarheid van personen

Gaat na of de persoon in kwestie betrouwbaar is.

## Data Protection Impact Assessment (DPIA)

Een essentieel instrument om privacyrisico's verbonden aan gegevensverwerking vooraf te identificeren en te beperken.

## Dreiging

Scenario waarin een criminele organisatie of insider gemotiveerd en in staat is om de belangen van een organisatie te schaden.

## Dreiging, concrete

Dit is de meest directe vorm van dreiging. Het is gebaseerd op specifieke, actuele informatie die aangeeft dat er een dreiging bestaat die zeer waarschijnlijk is en binnenkort kan plaatsvinden.

## Dreiging, voorspelbare

De voorspelbare dreiging wordt voorzien door het analyseren van trends en patronen in historische gegevens en ervaringen. Het gaat om dreigingen die in de toekomst waarschijnlijk kunnen voorkomen op basis van eerdere gebeurtenissen, hoewel ze op dit moment niet onmiddellijk zijn.

## Dreiging, voorstelbare

De voorstelbare dreiging is gebaseerd op theoretische scenario's en bekende informatie, maar is niet direct of waarschijnlijk. Het betreft mogelijke dreigingen die nog niet zijn voorzien, maar door vooruit te denken en dergelijke scenario's te identificeren, kunnen maatregelen worden genomen om ze te voorkomen.

## Dreigingsbeeld

Het dreigingsbeeld beschrijft de potentiële risico's van ongeoorloofd handelen die een organisatie kan voorzien en moet adresseren om een veilige werkomgeving te garanderen, conform artikel 658 Boek 7 van het Burgerlijk Wetboek. (Zie ook de begrippen voorstelbare en voorspelbare dreigingen hierboven.)

## Dreigingsinventarisatie

Identificatie, analyse en evaluatie van voorstelbare bedreigingen.

## Dreigingsprofiel

Identificeert en analyseert dreigingen die een organisatie kan ondervinden, inclusief aard, omvang en waarschijnlijkheid.

## Functiebeschrijving

Omschrijft de verantwoordelijkheden en bevoegdheden verbonden aan een functie.

## In-employment screening

Periodieke achtergrondcontroles van bestaande medewerkers om een beeld te krijgen op basis van huidige en verleden informatie, vooral bij veranderingen in functie-elementen.

## Integriteit

Handelen met openheid, eerlijkheid, en betrouwbaarheid, waarbij de waarden en normen van de organisatie worden gerespecteerd en nageleefd.

### Kwetsbare functies

Functies die gevoelig zijn voor dreigingen door misbruik van persoonlijke kwetsbaarheden door kwaadwillenden.

### Kwetsbare functie-elementen

Factoren die de kwetsbaarheid van elementen binnen een functie beïnvloeden.

### NVP - Netwerk voor HR Professionals

De NVP publiceert regelmatig een sollicitatiecode die gedragsregels voor werkgevers en sollicitanten omvat.

### Onderzoek

Het systematisch onderzoeken of de verstrekte informatie over een kandidaat in overeenstemming is met de werkelijkheid en of er geen relevante gegevens zijn achtergehouden. Dit kan in de vorm van een persoonsgericht- of achtergrondonderzoek.

### OSINT

Open Source Intelligence: informatie verzameld uit publiek toegankelijke bronnen (open bronnen).

### Post-employment screening

Screening van personeel dat de organisatie verlaat om na te gaan of zij zich aan contractuele afspraken zoals geheimhouding houden.

### Pre-employment screening

Het uitvoeren van een achtergrondonderzoek bij aantreden van een nieuw personeelslid in de organisatie.

### Risico

Risico verwijst naar de evaluatie van het te beschermen belang, de voorstelbare dreiging en de bestaande weerstand. Als de beschikbare en toegepaste screeningsmaatregelen niet voldoende zijn om de voorstelbare dreiging te verminderen, moet het resterende risico worden geaccepteerd. Hierdoor neemt de kans toe dat het risico zich daadwerkelijk manifesteert.

### Risico-inventarisatie

Het overzicht van geïdentificeerde (rest)risico's naar aanleiding van de weging belang-dreigingweerstand.

### Risicoprofiel

Een functieprofiel gebaseerd op de kwetsbare risicovolle elementen uit de functiebeschrijving. Het beschrijft de impact van geïdentificeerde dreigingen, vooral als de weerstand ontoereikend is.

### Risicovolle functies

Risicovolle functies betreffen functiegebonden (fysieke) dreigingen waarmee de persoon in deze functie te maken kan krijgen. Deze functies staan los van persoonlijke kwetsbaarheden.

### Risicovolle functie-elementen

Aspecten van een functie die een verhoogd risico met zich meebrengen. Voorbeelden hiervan zijn de zichtbaarheid van een functionaris en de impact van diens beslissingen op anderen.

### Screening

Zie 'onderzoek', hierboven.

### Verklaring Omtrent het Gedrag (VOG)

Een door het ministerie van Justitie en Veiligheid (Justis) verstrekte verklaring die aangeeft of een persoon een strafblad heeft dat relevant is voor de uit te voeren functie.

# Colofon

Deze richtlijn is een uitgave van  
Vereniging Beveiligingsprofessionals  
Nederland (VBN), werkgroep  
Insider Threat, o.l.v. René Reijenga.

U kunt contact opnemen met de  
werkgroep via [secretaris@devbn.nl](mailto:secretaris@devbn.nl)