NATIONALE RICHTLIJN PRE-, IN- EN POST-EMPLOYMENT SCREENING

Vereniging
Beveiligingsprofessionals
Nederland

VERSIE 3.0
2018 - 2023

Disclaimer:
De Vereniging Beveiligingsprofessionals Nederland (VBN), de auteurs en gebruikte bronnen van dit document kunnen niet instaan voor de juistheid, volledigheid en actualiteit van de geboden informatie en zijn niet aansprakelijk voor enige schade, van welke aard en hoegenaamd ook, die geleden wordt door welke persoon dan ook als gevolg van enig gebruik van dit document door die persoon of door een andere persoon.

Lees goed de toelichting en maak keuzes op grond van uw eigen inventarisatie. Het is belangrijk dat de inhoud van het beleidsplan aansluit op systemen en procedures die u daadwerkelijk heeft geïmplementeerd binnen uw onderneming.

Voorwoord

Voor u ligt de derde versie van de Nationale richtlijn pre-, in- en post-employment screening. Deze derde versie komt in opvolging van de Nationale richtlijn pre-employment screening 2012-2017 en is voorzien van de huidige stand van zaken met betrekking tot wet- en regelgeving en de praktische uitvoering van achtergrondonderzoeken van personen. Het herschrijven van de richtlijn heeft plaatsgevonden op verzoek van de Vereniging Beveiligingsprofessionals Nederland (VBN) en is opgedragen aan de werkgroep Insider Threat van deze vereniging.

Mijn dank gaat uit naar de deelnemers van de werkgroep Insider Threat, te weten de heer Cees van der Giessen CPP, adviseur strategisch risk management, mevrouw mr. Helene Minderman RSA, beleidsmedewerker van Transport en Logistiek Nederland, Rosa Kascha, onderzoeker bij Levent Bedrijfsrecherche en deskundige op het gebied van security management en de heer mr. Marcus Draaisma, advocaat bij advocatenkantoor Palthe Oberman en lid van de Nationale Sollicitatie Commissie.

Zeer trots ben ik dat, met hun onophoudelijke steun en specialistische inbreng, ik de Nationale richtlijn pre-, in- en post-employment screening 2018-2023 aan u mag presenteren.

René Reijenga

Voorzitter werkgroep Insider Threat

Inhoudsopgave

Definitielijst

Autoriteit Persoonsgegevens (AP)	De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens (AP, 2018).
Algemene Verordening Gegevensbescherming (AVG)	De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de AVG. Dit is de vertaling van *de General Data Protection Regulation* (GDPR) van de Europese Unie (AP, 2018).
Betrouwbaarheid	In hoeverre de gegevens vrij zijn van toevallige fouten // de precisie en nauwkeurigheid van een meetprocedure (Verhoeven, 2014).
Basisregistratie Personen (BRP)	De benaming voor de door de gemeente geregistreerde persoonsgegevens (Rijksoverheid).
Dreigingsbeeld	Stand van zaken omtrent de dreigingen voor de organisatie.
Data Protection Impact Assessment (DPIA)	Een instrument om vooraf de privacyrisico's van de gegevensverwerkende handelingen in kaart te brengen en de risico's te mitigeren (AP).
Eigen Verklaring (EV)	De Eigen Verklaring is een verklaring waarin de kandidaat zelf aangeeft of deze binnen een bepaalde periode in aanraking is geweest met de politie in het kader van een misdrijf en eventueel of de kandidaat bepaalde zaken verzwegen heeft tijdens de sollicitatie die van belang kunnen zijn voor de functie van de kandidaat.
Functiebeschrijving	De beschrijving van de verantwoordelijkheden en bevoegdheden van een functie.
In-employment screening	Het periodiek uitvoeren van een screening voor personeelsleden die veranderen van functie en/of bevoegdheden binnen de huidige organisatie.
Integriteitsverklaring (IV)	De Integriteitsverklaring is een uitgebreidere versie van de Eigen Verklaring waarin vragen gesteld worden over de integriteit van de kandidaat en eventuele risicodragende kenmerken.
Kwetsbare functie-elementen	Verschillende factoren die de (mate van) kwetsbaarheid van die elementen bepalen binnen een functie.
Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling (NVP)	De NVP geeft periodiek een sollicitatiecode uit waarin de gedragsregels voor werkgevers en sollicitanten beschreven staan (NVP).
OSINT	Open Source Intelligence: informatie afkomstig uit open bronnen.
Pre-employment screening	Het uitvoeren van een screening bij aantreden van een nieuw personeelslid in de organisatie.
Post-employment screening	Het uitvoeren van een screening en exit-briefing bij uitdiensttreding van een personeelslid.
Risico-inventarisatie	Een lijst met alle risico's in uw bedrijf en een plan voor het oplossen ervan.
Risicoprofiel	Een profiel dat is opgesteld aan de hand van de in de functiebeschrijving voorkomende kwetsbare functie-elementen.
Screening	Het systematisch onderzoeken of de verstrekte informatie over een kandidaat in overeenstemming is met de werkelijkheid en of er geen relevante gegevens zijn achtergehouden.
Verklaring Omtrent het Gedrag (VOG)	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).

Inleiding

Door niet te screenen, lopen ondernemers een grote kans op potentiële schade. Iemand aannemen die mogelijk niet over de beweerde competenties beschikt of niet de gewenste waarden en normen hanteert (of gehanteerd heeft), kan zeer nadelige gevolgen hebben.

Deze richtlijn zal u helpen een gedegen screeningsbeleid in uw organisatie te implementeren en screeningsonderzoeken op een gedegen manier, binnen wettelijke kaders uit te voeren. Deze richtlijn is tot stand gekomen met behulp van de werkgroep Insider Threat naar aanleiding van de gelijknamige workshop die gegeven is tijdens de Security Summit 2018. Het doel van deze richtlijn is om organisaties bij te staan bij het (her)ontwikkelen en implementeren van een screeningsbeleid.
Deze richtlijn is primair ontwikkeld ten behoeve van functionarissen die binnen de organisatie verantwoordelijk zijn voor bijvoorbeeld:

- Human Resources (HR) / Personeelszaken;
- Security Management;
- Facility Management;
- Juridische Zaken;
- Kwaliteitsmanagement.

De richtlijn is bedoeld om daar waar nodig te helpen om tot een goed en adequaat screeningsbeleid te komen, dan wel om de bestaande screeningsprocessen te optimaliseren.

Deze richtlijn biedt tevens ondersteuning aan de betrokken personen bij het bespreekbaar maken c.q. bewustmaken van alle betrokkenen binnen een organisatie.

Onafhankelijkheid werkgroep

De werkgroepleden hebben onafhankelijk, gemandateerd door de VBN, gehandeld en waren vrij van financiële belangen betreffende het onderwerp van de richtlijn. Het concept van de richtlijn, zoals opgesteld door deze werkgroep, is ter becommentariëring voorgelegd aan het bestuur van de VBN.

Leeswijzer

Deze richtlijn bestaat uit vier onderdelen:

Opstellen van een screeningsbeleid
Dit onderdeel schetst de kaders waarbinnen geadviseerd wordt om het screeningsbeleid te schrijven en welke punten uitgeschreven dienen te worden om tot een compleet screeningsbeleid te komen.

Procesbeschrijving screening
In dit onderdeel is het screeningsproces per processtap uitgewerkt.

Verantwoording
In het onderdeel 'Verantwoording' staat beschreven waarom iedere organisatie een screeningsbeleid zou dienen te hebben en wat de *Unique Selling Points* (USP's) van screenen zijn.

Infographic screenen
Tot slot is een *infographic* opgesteld waarin beschreven staat waaruit een screeningsbeleid bestaat en uit welke stappen een screening bestaat.

Opstellen screeningsbeleid

Dit onderdeel schetst de kaders waarbinnen geadviseerd wordt om het screeningsbeleid te schrijven en welke punten uitgeschreven dienen te worden om tot een compleet screeningsbeleid te komen.

De volgende punten komen terug in een screeningsbeleid en zullen in dit hoofdstuk behandeld worden. In Bijlage 3: Template 'screeningsbeleid' vindt u een template voor het opstellen van een screeningsbeleid.

- Afbakening screeningsbeleid
    - Doelstelling formuleren
    - Doelgroep vaststellen
    - Definities uitwerken
    - Eigenaarschap bepalen
    - Kaders uitwerken
        - Operationele randvoorwaarden screening
            - Opstellen van functiebeschrijvingen
            - Opstellen van een risicoprofiel
        - Juridische randvoorwaarden screening
            - Belangrijke verwijzingen
            - Juridisch speelveld
            - Verzamelen en bewaren van persoonsgegevens
        - Tactische randvoorwaarden screening
    - Beschrijving screentools
    - Financiën
    - Kwaliteitsborging

Afbakening

Doelstelling formuleren

Wij bevelen aan om het doel van het screeningsbeleid en de screening vast te leggen in het screeningsbeleid, voortvloeiend uit een recent dreigingsbeeld van de organisatie. Hieronder volgt een voorbeeld van een dergelijke doelstelling.

Voorbeelduitwerking(en)

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

Doelstelling screening
De doelstelling van het screeningsproces is het vaststellen of een natuurlijk en/of rechtspersoon voldoende betrouwbaar is, afgezet tegen de uit het risicoprofiel voortvloeiende bedreigingen, om werkzaamheden voor of bij <naam organisatie> te mogen uitvoeren.

Doelgroep vaststellen

Het screeningsbeleid zal geschreven worden door een (aantal) functionaris (-sen) die binnen de organisatie verantwoordelijk is/zijn voor de onderdelen security, veiligheid en recruitment. De screening zelf kan worden uitgevoerd door een functionaris van een van deze afdelingen of door een extern gespecialiseerd screeningsbureau. Deze functionarissen dienen te beschikken over een aantal competenties en toegang te hebben tot bepaalde systemen en documenten. Deze gegevens dienen vastgelegd te worden in het screeningsbeleid. Het is belangrijk om de belanghebbenden van het proces te identificeren- en te benoemen in het beleid. De volgende afdelingen zijn van belang bij het opstellen en uitvoeren van een screeningsbeleid:

- Human Resources (HR) / Personeelszaken
- Security / Facility
- Juridische afdeling
- Overige eventueel relevante afdelingen, zoals kwaliteitsmanagement, lijnmanagers en de afdeling Financiële Zaken.

Definities uitwerken

Het is belangrijk dat de definities duidelijk worden omschreven. Dit onderdeel maakt deel uit van het beleidsplan.

Eigenaarschap bepalen

De eerdergenoemde belanghebbende afdelingen hebben mogelijk verschillende belangen bij het (ontwikkelen en implementeren van een) beleid omtrent pre-, in- en/of post-employment screening. Derhalve is het belangrijk dat er één verantwoordelijke afdeling inclusief contactpersoon wordt aangewezen die het proces in goede banen kan leiden en het aanspreekpunt is voor de verschillende afdelingen (CPNI, 2015). Alvorens de verantwoordelijke afdeling en contactpersoon worden aangewezen, zullen de competenties beschreven dienen te worden. Ook wordt in dit onderdeel bepaald welke systemen en documenten nodig zijn voor het uitvoeren van een screening. Het wordt geadviseerd om te beschikken over een recent dreigingsbeeld en/of een risico-inventarisatie van de organisatie.

Kaderbepaling

Tevens wordt geadviseerd om de kaders te schetsen waarbinnen de screening gaat plaatsvinden. Bij het uitvoeren van een screeningsonderzoek zijn een aantal randvoorwaarden van belang. Deze zijn onder te verdelen in operationele, juridische en tactische randvoorwaarden. Allereerst dient het proces 'screening' afgebakend te worden. Aan de hand van de volgende voorbeeldUitwerkingen kan een omschrijving geformuleerd worden.

Voorbeelduitwerking(en)

Omschrijving
Onder 'screening' wordt verstaan: Het proces dat het mogelijk maakt om periodiek onderzoek te doen of een natuurlijke en/of rechtspersoon die werkzaamheden gaat uitvoeren of al uitvoert voor <naam organisatie> voldoet aan de door <naam organisatie> voor die functie gestelde eisen van betrouwbaarheid.

Kaders
Het proces 'screening' wordt ingezet om: ▪ Vast te stellen of een (nieuwe/tijdelijke) medewerker en/of toeleverancier voldoende betrouwbaar is en geen (toekomstige) dreiging en/of niet-mitigeerbaar risico oplevert voor <naam organisatie>. ▪ Vast te stellen of door een leverancier voor of bij <naam organisatie> te werk gestelde (nieuwe) medewerker voldoende betrouwbaar is en geen (toekomstige) dreiging en/of niet-mitigeerbaar risico oplevert voor <naam organisatie>. ▪ Vast te stellen of een (nieuwe) leverancier die voor of bij <naam organisatie> werkzaamheden gaat uitvoeren voldoende betrouwbaar is en geen (toekomstige) dreiging en/of niet-mitigeerbaar risico oplevert voor <naam organisatie>.
Het proces 'screening' wordt niet ingezet voor: ▪ Het doen van een uitspraak over de geschiktheid van een persoon voor een functie. Deze taak valt onder de verantwoordelijkheid van de toekomstige lijnmanager en de afdeling Personeelszaken (of een soortgelijke afdeling).

Vervolgens zijn de volgende operationele, juridische en tactische randvoorwaarden van belang. Deze worden hieronder beschreven.

Operationele randvoorwaarden
Binnen de screening zijn een aantal randvoorwaarden van belang. Deze operationele randvoorwaarden zijn hieronder beschreven. Geadviseerd wordt om deze te waarborgen voordat het screeningsbeleid in werking treedt. Deze randvoorwaarden bestaan uit het opstellen van functiebeschrijvingen en risicoprofielen.

Opstellen van functiebeschrijvingen
Door het opstellen van functiebeschrijvingen waarin de taken, verantwoordelijkheden en bevoegdheden van die functie beschreven worden, kan aan de start van de screening een risicoprofiel opgesteld worden waarmee de kaders van de screening bepaald kunnen worden. Een functiebeschrijving bestaat uit ten minste de volgende componenten:

- Omschrijving taakuitvoering
- Verantwoordelijkheden
- Bevoegdheden

Opstellen van een risicoprofiel
Iedere functie binnen een organisatie heeft andere verantwoordelijkheden en bevoegdheden. Hierdoor bevat iedere functie eigen kwetsbare functie-elementen. Er zijn verschillende factoren die de (mate van) kwetsbaarheid van die elementen bepalen. Deze factoren zijn hieronder opgesomd. Met behulp van de onderstaande opsomming van risicofactoren kan onderzocht worden welke elementen voorkomen in welke functies en welke functies dienen te worden geïdentificeerd als kwetsbaar.

Hoe meer risicofactoren voorkomen in een functie (of hoe belangrijker deze factor voor de functie is), hoe belangrijker het is dat al in het werving- en selectieproces aandacht wordt besteed aan integriteit. Het aantal elementen en de mate van kwetsbaarheid bepalen tevens de diepgang/zwaarte van de screening.

! Belangrijk: om het screeningsproces te waarborgen, zal gedetacheerd personeel/inhuurpersoneel eveneens gescreend dienen te worden binnen het juiste risicoprofiel.

In de volgende tabellen is opgesomd welke categorieën kwetsbare functie-elementen er zijn. Een uitgebreide omschrijving van deze risico-elementen staat beschreven in Bijlage 1: Kwetsbare functie-elementen.

	Functie	**Werkzaamheden**
A	***Basis (voor iedere functie)*** *Aankruisen onderdelen wanneer deze NIET van toepassing zijn.*	○ Controle identiteitsdocument ○ Controle Tewerkstellingsvergunning ○ Adresverificatie ○ Controle internationale sanctielijsten en waarschuwingsregisters ○ Verklaring Omtrent het Gedrag (VOG) ○ Integriteitsverklaring (IV)
B	***Omgang met personen***	○ Is er sprake van dat de zorg en het welzijn van mensen en/of dieren aan de kandidaat worden toevertrouwd? ○ Is er sprake van dat de kandidaat wordt belast met de zorg voor personen die in een afhankelijkheidssituatie verkeren?
C	***Omgang met geldzaken***	○ De kandidaat kan beschikken over contanten en/of girale gelden ○ Is de kandidaat budgetverantwoordelijk? ○ Is de budgetverantwoordelijkheid hoger dan tien procent van het netto bedrijfsresultaat?
D	***Omgang met goederen***	○ Beheren van goederen ○ Aanschaffen/verkopen goederen ○ Verstrekken goederen ○ Laden/lossen/inpakken/transport/*warehousing* ○ Samenstellen en/of bewerken en/of vervaardigen. ○ Bewaken van productieproces ○ Kan de kandidaat beschikken over stoffen, goederen e.d. die bij oneigenlijk of onjuist gebruik een risico vormen voor de veiligheid en het welzijn van mens en/of dier?
E	***Afsluiten van zakelijke overeenkomsten***	○ Is de kandidaat zelfstandig bevoegd te beslissen of hij/zij diensten tegen betaling kan verlenen c.q. leveren of inhuren?
F	***Verlenen van diensten***	○ Zal de kandidaat diensten verlenen op het gebied van advies, beveiliging, schoonmaak, catering, onderhoud e.d.?
G	***Solistisch handelen***	○ Voert de kandidaat zeer zelfstandig besluiten en/of kwetsbare handelingen uit?

	Organisatie	**Werkzaamheden**
H	***Omgang met bedrijfsinformatie***	○ Gaat om met vertrouwelijke informatie ○ Kan zonder directe controle vertrouwelijke (vitale) bedrijfsgegevens raadplegen ○ Heeft kennis van veiligheidssystemen ○ Heeft kennis van controlemechanismen ○ Heeft kennis van verificatieprocessen ○ Heeft toegang tot besturingssysteem
I	***Omgang met procesonderdelen***	○ De kandidaat verricht fysieke werkzaamheden aan onderdelen van bedrijfsvitale processen ○ De werkzaamheden vallen onder door de overheid benoemde vitale infrastructuur (gas, water, elektra, telecom e.d.)
J	***Leidinggevende functies***	○ Personen die vanuit hun functie mensen en/of een organisatie (of een deel daarvan) aansturen

Juridische randvoorwaarden
De werkgever of opdrachtgever die een kandidaat wil screenen voordat hiermee een samenwerking wordt aangegaan, zal zoveel mogelijk willen weten over deze kandidaat om te bepalen of de kandidaat voor het bedrijf of de instelling een risico vormt. De te bekleden functie bepaalt de noodzakelijkheid en diepgang van de gewenste screening. De speelruimte van de werkgever of opdrachtgever heeft een juridisch kader ter bescherming van de belangen van een kandidaat, doorgaans de economisch gezien zwakkere partij. De kandidaat wil graag de baan of de opdracht en heeft daarnaast recht op privacy. De werkgever of opdrachtgever wil graag een kandidaat van onbesproken gedrag die geen bedreiging vormt voor het bedrijf of de instelling. Dat wil overigens niet zeggen dat een persoon in dienst van het bedrijf of de instelling later wel een bedreiging kan vormen. Om dit laatste risico te beperken, kan de werkgever of opdrachtgever werknemers of opdrachtnemers van tijd tot tijd onderwerpen aan een in-employment screening.

Extern screenbureau
Bij gebruik van een extern screenbureau is het van belang dat deze voldoet aan de vigerende wet- en regelgeving en dat deze beschikt over een Particulier Onderzoeksbureau (POB) vergunning.

Belangrijke verwijzingen
De VOG van Dienst Justis – Dienst Justis is de screeningsautoriteit van het ministerie van Justitie en Veiligheid. Justis heeft inzicht in de strafrechtelijke gegevens van kandidaten en voert derhalve de VOG-aanvragen uit. Tevens heeft de dienst een brochure uitgegeven over de uitvoering van het screenen van kandidaten conform de bestaande maatschappelijke behoefte. De link naar het pdf-bestand vindt u in het hoofdstuk 'Handige informatie'.

De Sollicitatiecode van de NVP (NVP, 2016) - De Sollicitatiecode van de 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 van de sollicitant verkregen informatie wordt vertrouwelijk en zorgvuldig behandeld en in alle gevallen wordt de privacy van de sollicitant gerespecteerd;
- Een wervingsprofiel/vacaturetekst vermeldt naast de relevante kenmerken van de vacature de wijze van solliciteren en de termijn waarbinnen dient te worden gesolliciteerd, de door de sollicitant te verschaffen informatie (zoals opleiding, diploma's, arbeidsverleden en ervaring) en indien van toepassing: aanvullende selectieprocedures/-middelen (zoals psychologisch onderzoek en/of assessment), een aanstellingskeuring en/of een verplicht antecedentenonderzoek;
- De sollicitant en de organisatie zijn zich ervan bewust dat beschikbare informatie van open bronnen, zoals internet en informatie via derden verkregen, niet altijd betrouwbaar is. De verkregen informatie zal onder vermelding van de bron met de sollicitant worden besproken en de organisatie is transparant over de verkregen informatie;
- Indien een referentie wordt opgevraagd bij derden of indien nader onderzoek noodzakelijk is, wordt daartoe aan de sollicitant vooraf om toestemming gevraagd, tenzij deze toestemming op grond van de wet of nadere regelgeving niet is vereist.

Juridisch speelveld
Het juridische speelveld ter bescherming van de kandidaat of werknemer wordt bepaald door de volgende regels:

- Grondrechten (artikel 10 GW en 8 EVRM) die het recht op de persoonlijke levenssfeer waarborgen;
- De Algemene Verordening Gegevensbescherming (AVG), die op Europees niveau de verwerking en bescherming van verwerkte persoonsgegevens regelt;
- De antidiscriminatiewetgeving, waarin regels staan over verboden discriminatie bij selectie en tijdens het dienstverband;
- Civiel recht vanuit het Burgerlijk Wetboek;
- Wet op de ondernemingsraden, waarin regels staan over wanneer de OR instemmingsrecht heeft ten aanzien van reglementen (beleidsregels) over werving en selectie, veiligheid en de beoordeling van werknemers;
- Strijdig handelen met de hiervoor genoemde regels, dan wel handelen in strijd met in het Wetboek van Strafrecht en het Burgerlijk Wetboek opgenomen regels over handelingen die leiden of hebben geleid tot handelen in strijd met de persoonlijke levenssfeer van een persoon, kunnen ook onrechtmatig zijn, waardoor er grond ontstaat voor schadevergoeding (onrechtmatige daad).

Verzamelen van persoonsgegevens
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 (AP).

De verwerking dient altijd te voldoen aan de AVG en er dient te worden nagegaan of er voor de verwerking een geldige grondslag is. Is er geen geldige grondslag, dan mogen de persoonsgegevens niet worden verwerkt, ongeacht de uitkomsten van een eventuele DPIA.

Uitgangspunt van de AVG is steeds dat er voor het verzamelen van informatie over een kandidaat of een werknemer een legitiem doel dient te zijn. Er dienen bijvoorbeeld bepaalde veiligheids- en/of integriteitseisen te gelden om bepaald diepgaand onderzoek te doen naar de achtergrond van een kandidaat. Dit kan ook door specifieke regelgeving worden voorgeschreven, bijvoorbeeld voor de financiële sector. Als een kandidaat toestemming geeft informatie over hem/haar te verzamelen, zal de (potentiële) werkgever dit mogen doen. Het gaat dan om het geven van toestemming uit vrije wil. Onder bepaalde omstandigheden kan getwijfeld worden aan de vrije wil van deze toestemming, omdat de kandidaat of de werknemer in een economisch afhankelijke positie is ten opzichte van de (potentiële) werkgever. Deze afhankelijkheid zal weer afhangen van de specifieke situatie, waaronder de opleiding en ervaring van de kandidaat, zijn bekendheid met de gevolgen van zijn toestemming, de zwaarte van de eisen voor de betreffende functie en de omvang van het risico.

Van belang is steeds of de kandidaat van tevoren bekend is met de screening bij deze werkgever. Wanneer de werkgever op de website en bij openstaande vacatures over het eigen wervings- en selectiebeleid duidelijk aangeeft dat er gescreend wordt op integriteit en het risicoprofiel van de kandidaat, is de kandidaat daar vooraf mee bekend. Wanneer hij/zij dan solliciteert naar een functie bij dit bedrijf geeft hij/zij impliciet toestemming voor de screening. Wanneer hij/zij het sollicitatieformulier daadwerkelijk invult, zal hij/zij schriftelijk wederom toestemming geven voor de screening als het formulier van de werkgever daar duidelijk over is.

Als blijkt dat de kandidaat geschikt is, zal de werkgever aangeven dat er nog een nadere uitleg volgt met uitleg over waarop gescreend wordt. Wordt de screening door een extern bureau gedaan, dan zal de kandidaat toestemming dienen te verlenen voor afgifte van de screeningsconclusies aan de werkgever. Een kandidaat heeft dan drie keer toestemming gegeven. In de Nationale richtlijn pre-, in- en post-employment screening geldt dit als blijk van het feit dat de kandidaat werkelijk vrij zijn toestemming in de zin van de AVG heeft gegeven.

! 3 x toestemming:

1. Keuze voor sollicitatie waarbij screening vooraf is aangegeven.
2. Uitdrukkelijke toestemming voor screenen, waarbij wordt aangegeven wat de screening inhoudt.
3. Uitdrukkelijke toestemming om de screeningsresultaten met de werkgever te delen.

Bewaartermijnen van persoonsgegevens

Bewaartermijnen worden met inachtneming van de privacywet- en regelgeving, de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) vastgesteld. Op grond van de AVG is dataminimalisatie een van de uitgangspunten. Het is belangrijk dat wordt vastgesteld waarom gegevens bewaard worden (in bijvoorbeeld het personeelsdossier).

- De bewaartermijn van screeningsuitkomsten dient te worden vastgesteld. De gegevens worden niet langer bewaard dan noodzakelijk is voor het doel van de screening.
- Ook bewaartermijnen van onderliggende documenten worden vastgesteld. Er geldt een bewaartermijn van vier weken zonder toestemming van de betreffende kandidaat, bijv. sollicitatiebrief, sollicitatieformulier, correspondentie inzake sollicitatie, getuigschriften, VOG. Met toestemming van de sollicitant kan een bewaartermijn van een jaar worden gehanteerd. De ingangsdatum van de bewaartermijn vangt aan na beëindiging van de sollicitatieprocedure of na beëindiging van het dienstverband.
- Wanneer wordt afgeweken van de genoemde termijnen dient er een goede reden met daarbij een heldere omschrijving te zijn waarom een langere bewaartermijn wordt gehanteerd. Bijvoorbeeld in de situatie dat een cv van een persoon met een dienstverband langer wordt bewaard kan een goede reden zijn dat er een (latere) check van gevolgde opleidingen volgt (is er daadwerkelijk een diploma behaald) en dat het vaststellen van de werkervaring op een later tijdstip gedaan wordt. In de situatie dat er later twijfel ontstaat over onderdelen van het cv en er een controle dient te worden uitgevoerd, kan het cv een bruikbaar instrument zijn. Het is verstandig om een termijn te stellen en in ieder geval maximaal een jaar na beëindiging van het dienstverband het document te vernietigen.

Tactische randvoorwaarden

Het wordt geadviseerd om een aantal uitgangspunten op te nemen in het screeningsbeleid waar de organisatie zich reeds aan gecommitteerd heeft. In de volgende tabel worden deze randvoorwaarden genoemd.

Tactische randvoorwaarden
▪ De tool pre-, in- en post-employment screening wordt ingezet ter afsluiting van de (interne) wervings- en selectieprocedure en/of uitdiensttreding. ▪ De tool pre-, in- en post-employment screening wordt niet gebruikt om de geschiktheid van een kandidaat voor een functie vast te stellen. Dit is een verantwoordelijkheid van de lijnmanager en/of de afdeling Personeelszaken (of soortgelijke afdeling). ▪ Het screeningsproces vindt plaats vóór de in-/uitdiensttreding van de betrokkene en in ieder geval vóór het einde van de proeftijd (behalve in het geval van een in-employment screening). ▪ De betrokkene wordt in de vacaturetekst al geïnformeerd over het screeningsonderzoek. ▪ Het screeningsproces wordt pas in gang gezet nadat alle benodigde informatie door de betrokkene, de afdeling Personeelszaken en/of de lijnmanager bij de afdeling/ medewerker die de screening uitvoert, is aangeleverd. ▪ Het wegingskader om te bepalen of er voldoende waarborgen zijn voor de betrouwbaarheid, integriteit en loyaliteit van een (nieuwe) medewerker staat op schrift. ▪ Voordat wordt overgegaan tot de inzet van een pre-, in- en post-employment screening dient duidelijk te zijn tegen welke onderkende bedreigingen de inzet van de screeningstool weerstand moet bieden (= uitkomst dreigingsbeeld en/of risico-inventarisatie). ▪ Het vaststellen of een natuurlijk en/of rechtspersoon een dreiging en/of risico oplevert, gebeurt aan de hand van vastgestelde indicatoren die in het dreigingsbeeld en/of de risico-inventarisatie zijn vastgesteld. ▪ Om een gefundeerde uitspraak te kunnen doen over de (toekomstige) betrouwbaarheid, integriteit en loyaliteit van een (nieuwe) medewerker dient een periode van minimaal vijf jaar voorafgaand aan de sollicitatie te kunnen worden onderzocht. ▪ Als deze periode niet kan worden gehaald, dient op heldere wijze aangegeven te worden welke risico's en/of dreigingen niet konden worden onderzocht en vindt vervolgens risicoafweging plaats. ▪ De betrokkene die onderwerp van het onderzoek is, dient voorafgaand aan de inzet van de pre- en in-employment screening schriftelijk toestemming te geven voor de uitvoering van het onderzoek en eventuele latere periodieke herhaalonderzoeken.

- De betrokkene die onderwerp van het onderzoek is, dient een (screenings)formulier te ondertekenen en te verklaren dat hij/zij in het verleden niet met politie en/of justitie in aanraking is geweest en dat de verstrekte informatie juist en volledig is.

- Afhankelijk van de functie die de betrokkene gaat uitvoeren of uitvoert, zal met meer diepgang informatie worden ingewonnen en gebruikt voor het maken van de risicoafweging of de betrokkene voor of bij <naam organisatie> de functie mag gaan of blijven uitvoeren.

- Een interview maakt deel uit van de screeningsprocedure, zeker als er belastende informatie is gevonden, zodat de betrokkene in staat is aanvullende informatie te verstrekken, een nadere toelichting te geven en/of de informatie te corrigeren als deze onjuist is.

- De omvang en de diepgang van het onderzoek zijn gerelateerd aan het vastgestelde risiconiveau voor de functie waarin de betrokkene wordt of is tewerkgesteld.

- Bij het niet kunnen vaststellen van de betrouwbaarheid van de betrokkene kunnen er door de betrokkene in die functie geen werkzaamheden bij of voor <naam organisatie> worden verricht.

- De doorlooptijd van een screening is maximaal 15 werkdagen gerekend vanaf het moment dat alle voor het onderzoek benodigde informatie bij de (risk)manager is aangeleverd.

- De uitspraak over de betrouwbaarheid van een natuurlijk persoon en/of rechtspersoon is gebaseerd op gegevens uit het verleden en heden (houding en gedrag) en vertegenwoordigen een ''tijdsopname'' (= datum afsluiting onderzoek).

- De inbreuk op de privacy van een natuurlijk persoon en/of rechtspersoon die aan de inzet van de tool verbonden is, dient tot een minimum beperkt te blijven en te voldoen aan ter zake vigerende wet- en regelgeving, waarbij gekeken dient te worden naar de proportionaliteit en subsidiariteit.

- De gegevens van het screeningsonderzoek en het personeelsdossier dienen te allen tijde op een zorgvuldige manier behandeld en bewaard te worden met het oog op de veiligheid en privacy van de kandidaat.

De impact van de bovengenoemde tactische beleidsuitgangspunten dienen voor de organisatie te worden uitgewerkt in het beleidsplan pre-, in- en post-employment screening, de toetsingscriteria betrouwbaarheid in het kader van pre-, in- en post-employment screening en een wegingskader betrouwbaarheid in het kader van pre-, in- en post-employment screening.

Beschrijving screentools

Hieronder kan een keuze gemaakt worden welke screentools worden ingezet afhankelijk van het soort screening (pre-, in- of post-employment screeningen) en de zwaarte van de screening. Het is van belang om de screeningsmaatregelen en -methoden/-werkwijze te vermelden die u toepast.

Hieronder worden de verschillende screentools opgesomd. Een uitgebreide beschrijving van de toepassing van de verschillende tools staat vermeld in Bijlage 2: Toelichting screentools.

Nr.	Screentools	Omschrijving
1.	**Vaststellen identiteit**	Het bepalen of de identiteit van de kandidaat overeenkomt met bekende gegevens met behulp van een identiteitskaartencontrole en een controle van het BRP middels officiële overheidsdocumenten, zoals de VOG.
2.	**Financieel onderzoek**	Het toetsen op negatief betaalgedrag van de kandidaat middels een (aantal) database(s).
3.	**A. Integriteit: VOG**	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).
	B. Integriteit: EV	Een verklaring waarin de kandidaat zelf aangeeft of deze binnen een bepaalde periode in aanraking is geweest met de politie in het kader van een misdrijf en eventueel of de kandidaat bepaalde zaken verzwegen heeft tijdens de sollicitatie die van belang kunnen zijn voorde functie van de kandidaat. Dit is een aanvulling op de VOG.
	C. Integriteit: IV	Een uitgebreidere versie van de Eigen Verklaring waarin vragen gesteld worden over de integriteit van de kandidaat en eventuele risicodragende kenmerken. Dit is een aanvulling op de VOG.
4.	**Check juistheid curriculum vitae (cv)**	Het controleren van de juistheid van het cv door middel van verschillende *crosschecks.* Het cv wordt vergeleken met open bronnen over de kandidaat, de uitkomsten van referentenonderzoeken, een interview met de kandidaat, aangeleverde certificaten, getuigenschriften en de handmatig ingevulde gegevens over de gevolgde opleidingen, financiële gegevens en arbeidshistorie.
5.	**Check opleidingen en diploma's**	Het controleren van de echtheid van de door de kandidaat opgegeven opleidingen en diploma's.
6.	**Referentenonderzoek**	Het bevragen van (oud-)leidinggevenden over het arbeidsverleden van de kandidaat aan de hand van de beschikbare informatie.
7.	**Integriteitsinterview**	Het bevragen van de kandidaat over het arbeidsverleden aan de hand van de beschikbare informatie.
8.	**A. Open bronnen onderzoek**	Het gebruik van open bronnen om informatie te vinden over de kandidaat.

Financiën
In dit onderdeel is het van belang dat de budgettering wordt opgenomen in het beleidsplan en dat dit in samenspraak met de financiële afdeling gedaan wordt. Zie tevens het hoofdstuk ' Verantwoording'.

Kwaliteitsborging
Het wordt geadviseerd om een paragraaf op te nemen in het beleidsplan waarin kwaliteitsnormen en doelen vastgesteld zijn. Ook wordt aanbevolen om te beschrijven wanneer en op welke wijze metingen van de (effectiviteits)kwaliteit zullen plaatsvinden.

Personeelsdossier:
Het wordt geadviseerd om het uiteindelijke screeningsrapport met de resultaten van de screening op te nemen in het personeelsdossier voor eventuele audits en vervolgscreeningen. Daarnaast is het verstandig om de documenten van de VOG en de EV/IV hierin op te nemen.

Procesbeschrijving screening

In dit onderdeel wordt het screeningsproces per processtap nader uitgewerkt. In Bijlage 4: Template 'procesbeschrijving screening' vindt u de template voor het uitwerken van de processtappen.

Soorten screeningen

Bij iedere soort screening wordt naar aanleiding van het opgestelde risicoprofiel een keuze gemaakt over de zwaarte van de screening. De zwaarte heeft invloed op het aantal en de soort screentools die ingezet worden.

Pre-employment

Bij een pre-employment screening is het belangrijk dat de kandidaat op basis van het risicoprofiel gescreend wordt. Het doel van een pre-employment screening is het voorkomen van het binnenlaten van risicodragende kandidaten waarvan de risico's niet voldoende gemitigeerd kunnen worden.

In-employment

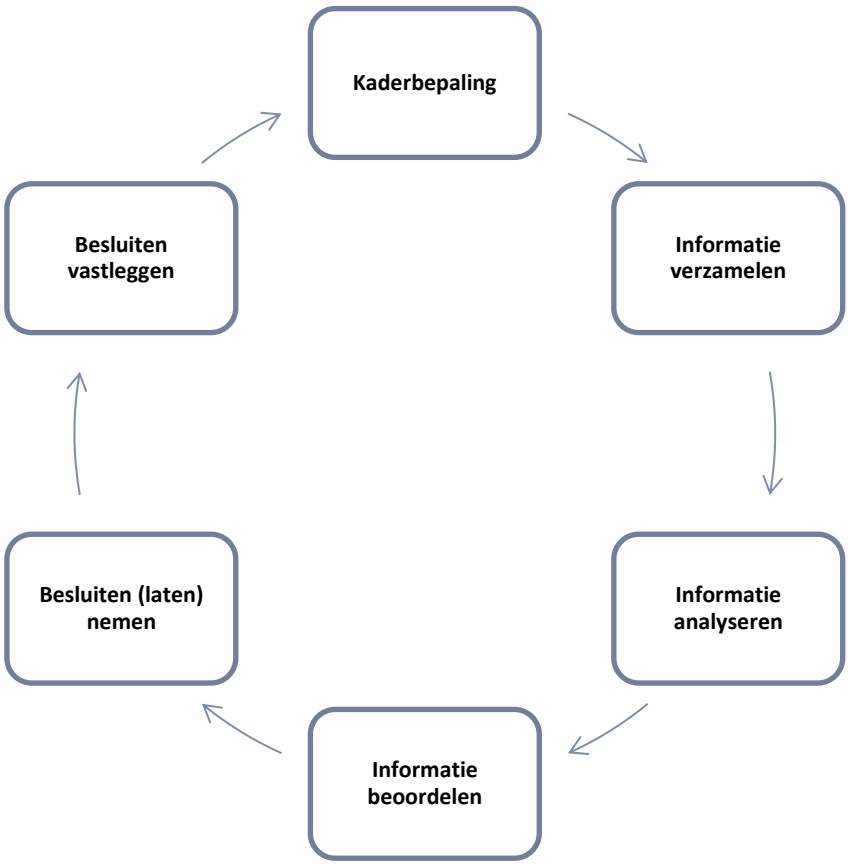
Bij een in-employment screening zijn niet alle zaken van een pre-employment screening relevant. Bij een in-employment screening is het van belang dat er concreet beleid door de werkgever is opgesteld. De waarborging van privacy van de werknemer is cruciaal.
Binnen iedere soort screening kan de doelstelling verschillen. Dit is afhankelijk van het risicoprofiel van de betrokkene in het screeningsonderzoek en de opdracht vanuit de opdrachtgever. De gemene deler in de doelstelling is: het voorkomen van interne fraude en criminaliteit door werknemers.

Post-employment

Bij een post-employment screening ligt de focus op het zorg dragen voor een nette arbeidsafsluiting van de kandidaat waarbij gekeken wordt of de kandidaat een risico kan vormen voor de organisatie na uitdiensttreding. Het doel hierbij is om verlies en/of misbruik van vertrouwelijke informatie, externe fraude en criminaliteit door voormalige medewerkers te voorkomen.

Procesbeschrijving

Een screening bestaat over het algemeen uit de volgende zes stappen:



Figuur 1: procesbeschrijving screening

Kaderbepaling

Binnen het proces 'Kaderbepaling' wordt bepaald voor wie welk soort screening (pre-, in- of post-employment screening en laag-gemiddeld of hoog risico) uitgevoerd gaat worden. Aan de hand van de functiebeschrijving is eerder al een risicoprofiel opgesteld waarin de kwetsbare functie-elementen zijn geïdentificeerd. De in te zetten screentools dienen de risico's die naar voren komen in het risicoprofiel te kunnen identificeren en eventueel mitigeren. Zie hiervoor het hoofdstuk ' Opstellen screeningsbeleid'.

Informatie verzamelen

In de procesbeschrijving 'Informatie verzamelen' wordt beschreven wat het doel van het proces is, wie dit proces uitvoert en welke methode gehanteerd wordt in het proces.

Een uitgebreide beschrijving van de toepassing van de verschillende tools is beschreven in Bijlage 2: Toelichting screentools.

Methode pre-employment

Voor een pre-employment screening worden bij voorkeur diverse tools in combinatie ingezet. Door het combineren van verschillende tools en de daaruit voortvloeiende resultaten kunnen verbanden tussen de resultaten onderzocht worden in de stap 'Informatie analyseren'.

Screentools

Binnen de pre-employment screening kunnen de volgende tools ingezet worden:

Nr.	Screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
5.	Check opleidingen en diploma's
6.	Referentenonderzoek
7.	Integriteitsinterview
8.	Open bronnen onderzoek

! Het verdient aanbeveling om afhankelijk van de sector ook specifieke sectorale screentools mee te nemen. Deze vallen onder de tool 'Integriteit'. Voorbeeld: waarschuwingsregisters van diverse branches.

Methode in-employment

Wanneer de kandidaat een in-employment screening dient te ondergaan, is het van belang dat een aantal screentools opnieuw uitgevoerd worden. Als de kandidaat bij indiensttreding geen screening heeft ondergaan, wordt geadviseerd om een aangepaste screening uit te voeren waarbij de pre- en in-employment screening worden gecombineerd.

Door het combineren van verschillende screentools en de daaruit voortvloeiende resultaten kunnen verbanden tussen de resultaten onderzocht worden.

Screentools

Binnen de in-employment screening kunnen de volgende tools ingezet worden:

Nr.	Screentools
2.	Financieel onderzoek
3.	A. Integriteit: VOG (elke 5 jaar)
	B. Integriteit: EV (elke 5 jaar)
	C. Integriteit: IV (elke 5 jaar)
7.	Integriteitsinterview
8.	Open bronnen onderzoek

Methode post-employment

Post-employment screeningen zijn vooral bedoeld voor medewerkers die onrechtmatig gevoelige informatie kunnen meenemen en daarmee uw bedrijf schade kunnen berokkenen. Binnen een post-employment screening wordt een exitgesprek gevoerd met de betrokkene waarbij nagegaan wordt of de betrokkene geen bedrijfsgevoelige en geheime informatie, klanten of bezit meeneemt.

Bij functies met een commercieel en strategisch karakter zijn risico's op ongewild verlies van bedrijfs-, geheime en strategisch gevoelige informatie aanwezig. Voor werkgevers is dit vaak een lastig gespreksonderwerp. De werknemer kan ten onrechte de indruk krijgen dat hij/zij niet vertrouwd wordt. Daarnaast is het over het algemeen voor werkgevers moeilijk vast te stellen of de risico's gelopen worden, dan wel al gelopen zijn. Door het onderzoek door een externe onafhankelijke partij te laten uitvoeren, voorkomt u emotionele en soms lastige, juridische situaties.

Het is van belang om dit gesprek in een vroeg stadium, vóór vertrek van de medewerker uit te voeren: hoe eerder, hoe beter. Zodra de werknemer zijn of haar ontslag heeft gemeld, kan in feite de post-employment screening starten. Zolang de werknemer nog in loondienst is, heeft u grip op de situatie en kunt u nog sturing geven. U kunt het zien als de correcte, passende afsluiting van de arbeidsovereenkomst, waarmee u het risico tot een minimum beperkt. Er kunnen dan eventueel aanvullende afspraken worden gemaakt en onduidelijkheden, maar ook juridische processen, worden voorkomen.

Bespreek met de werknemer een aantal zaken, zoals welke bedrijfsinformatie en/of goederen hij/zij in bezit heeft, maar ook het concurrentie- en relatiebeding.

Screentools
Binnen de post-employment screening kunnen de volgende tools ingezet worden:

Nr.	Screentools
7.	Integriteitsinterview
8.	Open bronnen onderzoek

Informatie analyseren
Binnen dit onderdeel wordt de verzamelde informatie dusdanig bewerkt dat deze geschikt is om een uitspraak te kunnen doen over de mate van betrouwbaarheid van de betrokkene.

In de procesbeschrijving 'Informatie analyseren' dient te worden beschreven wat het doel van het proces is, wie dit proces uitvoert en welke methode gehanteerd wordt in het proces.

Informatie beoordelen
Nadat aan de hand van de vooraf vastgestelde uitgangspunten en dreigingsindicatoren de verzamelde informatie is geanalyseerd, kan een advies opgesteld worden met betrekking tot de (toekomstige) betrouwbaarheid van de betrokkene.

In de procesbeschrijving 'Informatie beoordelen' dient te worden beschreven wat het doel van het proces is, wie dit proces uitvoert en welke methode gehanteerd wordt in het proces.

Risico's
Tijdens het analyseren en beoordelen van informatie is van belang dat er rekening wordt gehouden met een aantal zaken:

- Subjectiviteit en vooroordelen, dit is (deels) te ondervangen met behulp van bijvoorbeeld het gebruik van het vierogenprincipe;
- Informatie die gevonden is in een open bron, zoals *social media.* Deze dient niet zomaar als juist beoordeeld te worden. Het is belangrijk dat er te allen tijde gebruik wordt gemaakt van *crosschecks* tussen meerdere verschillende soorten bronnen;
- Betrokkenen die frauduleuze informatie verstrekken met als doel om te misleiden.

! Besluiten dienen te allen tijde gebaseerd te zijn op feiten, de zogenaamde 'harde informatie', en nimmer op aannames.

Besluiten (laten) nemen

Na het opstellen van een conceptadvies over de (toekomstige) betrouwbaarheid van de betrokkene en de eventuele dreiging/het risico die/dat daarvan voor de organisatie kan uitgaan, dient een beslissing genomen te worden door de verantwoordelijke lijnmanager over het dreigingsniveau van de betrokkene.

In de procesbeschrijving ‘Besluiten (laten) nemen’ dient te worden beschreven wat het doel van dit proces is, wie dit proces uitvoert en welke methode gehanteerd wordt in het proces.

Proportionaliteit en subsidiariteit

De screeningsprocedures dienen toegepast te worden met inachtneming van proportionaliteit en subsidiariteit. Dit betekent o.a. dat wanneer er minder belastende tools mogelijk zijn om hetzelfde doel te bereiken er gekozen wordt voor deze tools.

Besluiten vastleggen

Binnen deze processtap wordt managementinformatie over het screeningsproces gegenereerd.
In de procesbeschrijving ‘Besluiten vastleggen’ dient te worden beschreven wat het doel van het proces is, wie dit proces uitvoert en welke methode gehanteerd wordt in het proces.

Informatie omtrent de bewaartermijnen van personeelsgegevens vindt u in het hoofdstuk ‘Opstellen screeningsbeleid’ onder 'Juridische randvoorwaarden'.

Verantwoording

In dit onderdeel is beschreven waarom iedere organisatie een screeningsbeleid zou dienen te hebben, oftewel: wat zijn de Unique Selling Points (USP's) van screenen? Dit hoofdstuk is geschreven om op strategisch niveau uw organisatie te overtuigen van het screenen van personeel.

Screenen is een serieuze en vaak complexe zaak. Gezien de vele verschillende belangen die in het geding kunnen zijn, is het van groot belang dat een screening zorgvuldig wordt uitgevoerd, zowel binnen het wettelijk kader als binnen de organisatiestructuur.

Het screenen van personeel en leveranciers binnen Europa en zeker binnen Nederland is nog geen vanzelfsprekendheid. In de financiële sector maar ook bij bedrijven in de vitale infrastructuur zijn de afgelopen jaren wel een aantal screenprocessen ingericht, maar dit gebeurde vaak op basis van wettelijke voorschriften. Ook bij het verkrijgen van bepaalde certificeringen wordt vaak een screeningsbeleid voorgeschreven. Exporterende bedrijven hebben te maken met landelijke regelgeving (bijvoorbeeld *US Customs Trade Partnership Against Terrorism, Authorised Economic Operator* en de luchtvrachtverordening) welke vereist dat er een gedegen screenbeleid wordt uitgevoerd om zo de kans op risico's en sanctieblokkades te beperken.

Door bewustwording (en de negatieve publiciteit met betrekking tot niet-gekwalificeerd of niet-integer personeel) begint thans de noodzaak van personele screening binnen bedrijven meer basis te krijgen en is de visie dat pre-employment screening steeds meer een standaard onderdeel wordt bij de afsluiting van een wervings- en selectietraject.

De onbekendheid van de screenmogelijkheden zorgt voor een onvolledig beeld van een individu en heeft het risico in zich dat zowel een positieve als negatieve uitkomst wordt gebaseerd op slechts enkele aannames en/of veronderstellingen. Bijvoorbeeld: vaak wordt aangenomen dat een screening door middel van een VOG afdoende is en dat daarmee de risico's in kaart zijn gebracht en onderzocht. Het tegengestelde is echter waar. De VOG biedt een beperkte inzage in eventuele risico's op basis van strafrechtelijke veroordelingen, maar biedt zeer zeker geen compleet beeld van de betrouwbaarheid, integriteit en eventuele kwetsbare functie-elementen van een medewerker, sollicitant of leverancier.

De *Unique Selling Points* van screenen

Op strategisch en tactisch niveau kan er verschil in inzicht bestaan omtrent de noodzaak en/of uitvoering van gedegen screeningen. Het is belangrijk om bij het ontwikkelen, implementeren en uitvoeren van het screeningsbeleid niet alleen te denken aan de investering van tijd en kosten, maar ook aan de *Unique Selling Points* (USP's) - in financiële zin, maar ook op vlakken als bedrijfscultuur en imago. Hieronder zijn enkele cijfers opgenomen van verschillende organisaties die zich bezighouden met screenen en fraude.

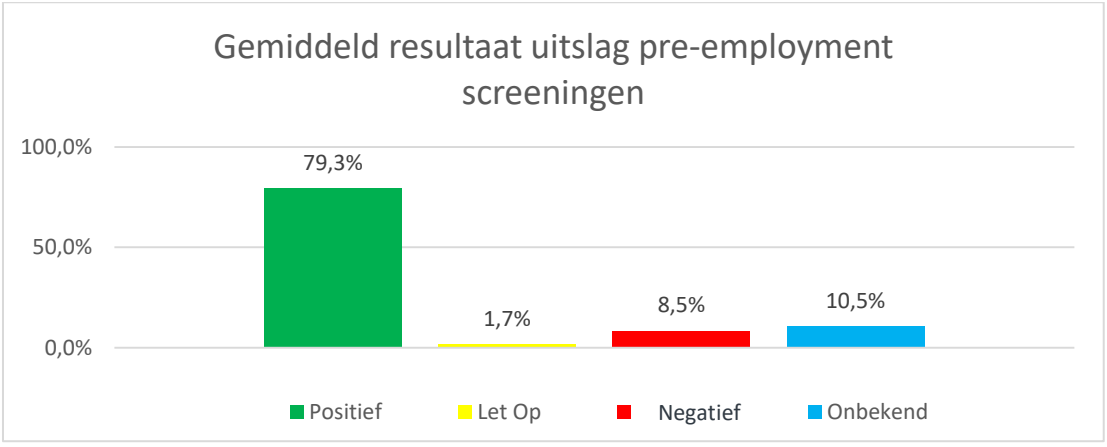
Cijfers screenen

Bij de analyse van de in 2016 en 2017 uitgevoerde pre-employment screeningen binnen een screeningsorganisatie in Nederland werden van de duizenden screeningen bij **79,3 procent** van de onderzochten personen geen feiten of omstandigheden aangetroffen welke een risico zouden vormen bij de aanstelling.

Bij **1,7 procent** werd aangegeven dat er informatie bekend was geworden welke mogelijk een risico met zich zou kunnen meebrengen, maar geen beletsel hoefde te zijn voor een aanstelling (bijvoorbeeld incassovorderingen, faillissementen, schuldsanering e.d., maar ook onjuistheden met betrekking tot opleiding en/of werkhistorie). In dit geval is de werkgever met de kandidaat daarover in overleg gegaan.

Bij **8,5 procent** werd informatie aangetroffen welke een ernstige bedreiging c.q. risico zou vormen voor de organisatie. Vaak betrof het hier het opzettelijk verstrekken van vervalste c.q. onjuiste informatie (liegen), zoals arbeidshistorie, behaalde opleidingen vervalste diploma's en cijferlijsten, maar ook een lidmaatschap van organisaties welke een imago risico zou kunnen vormen voor de werkgever. Bij **drie** onderzoeken werd vastgesteld dat het een poging tot infiltratie betrof vanuit crimineel en/of terroristisch oogmerk.

10,5 procent van de screeningsonderzoeken werd afgesloten met een onbekend resultaat. In de meeste gevallen betrof het hier screeningsdossiers die door de werkgever werden ingetrokken onder opgave dat de kandidaat tijdens het screeningsproces was afgehaakt. In een groot aantal gevallen bleek dat de kandidaat de sollicitatie niet wenste voort te zetten omdat deze zelf verwachtte niet door de screening heen te komen.



Figuur 2: Gemiddeld resultaat pre-employment screeningen (Levent Bedrijfsrecherche, 2018)

Cijfers fraude

De *Association of Certified Fraud Examiners* (ACFE) brengt periodiek een *Report to the Nations* uit. Bij een uitvoerige analyse van 2690 fraudezaken tussen 2016-2017 in 125 landen kwam naar voren dat in **97 procent** van de gevallen geprobeerd werd om de fraude te verbergen door (valse) informatie te creëren, wijzigen of verwijderen. De meest voorkomende manieren van het verbergen van fraude waren:

- Het creëren van frauduleuze (fysieke) documenten;
- Het wijzigen van frauduleuze (fysieke) documenten.

Binnen het domein van screenen is dit goed nieuws: dit betekent dat in een groot deel van deze fraudezaken bewijs, zoals vervalste documenten, was te vinden door een gedegen screeningsonderzoek in te stellen. Denk hierbij aan het vervalsen van diploma's, cijferlijsten en het creëren van een onjuist cv met arbeidshistorie en opleidingen.

Bron: (ACFE, 2018).

Overige USP's

Het screenen van individuen bij het wervings- en selectietraject (pre-employment), maar ook periodiek tijdens het dienstverband (in-employment) en zelfs bij het beëindigen van het dienstverband (post-employment) draagt bij aan de bewustwording en geeft een duidelijk signaal af dat er waarde wordt gehecht aan een veilige en betrouwbare werkomgeving. Juist die bewustwording, het weten dat de nieuwe collega niet alleen op zijn competenties, maar ook op zijn betrouwbaarheid is getoetst, zorgt voor een gevoelsmatige veiligheid, werkt motivatieverhogend en draagt bij aan een gezonde bedrijfscultuur.

Individuen die onjuistheden of zelf leugens vertellen over hun competenties en werkverleden maken veel eerder kans om tijdens een screening door de mand te vallen en zullen eerder niet dan wel worden aangenomen. Dat dit zijn uitwerking heeft op een verhoogde kwaliteit, effectiviteit en kwaliteit van werken mag duidelijk zijn. Immers zal de deskundigheid op basis van het cv en de selectiegesprekken worden bevestigd. De kans dat dan de nieuwe medewerker (moet) afhaken op in

de praktijk bewezen ongeschiktheid wordt substantieel kleiner, en de kosten die gepaard gaan met de inwerkperiode en eventuele aanvullende opleidingen zijn een goede investering. Er zal een lager verloop van personeel zijn, hetgeen zich vertaalt in het reduceren van wervings-, selectie- en opleidingskosten.

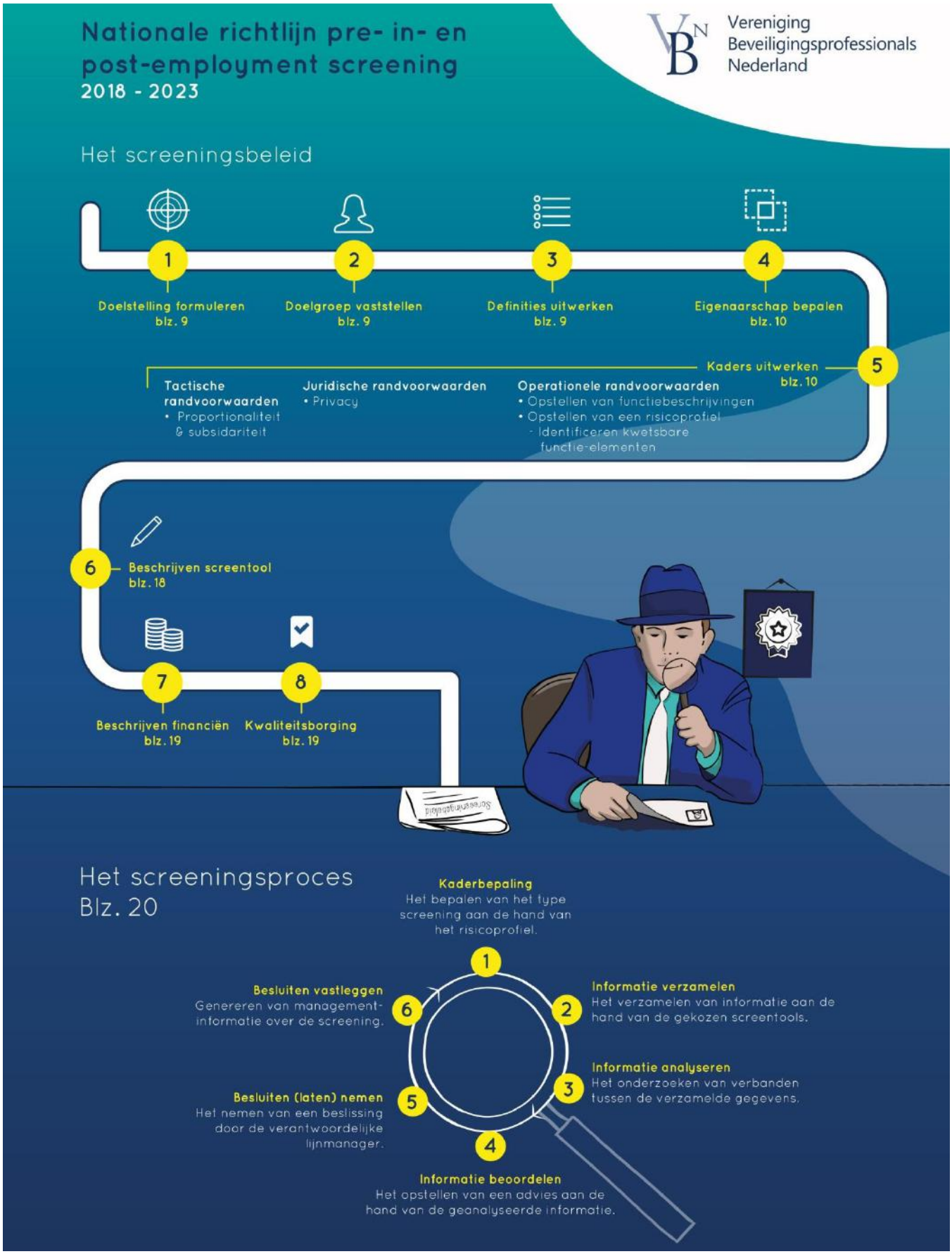
Het verlagen van dervingskosten ten gevolge van frauduleuze praktijken neemt af. De kans om de organisatie binnen te komen met oneigenlijke bedoelingen wordt verkleind en de kans op ontdekking wordt vergroot. Vaak is het screenen aan de voordeur al een preventieve maatregel die individuen doen besluiten de sollicitatieprocedure te stoppen.

Het is niet de bedoeling om iedereen aan wie iets mankeert een kans op een baan op de arbeidsmarkt te ontzeggen - integendeel. Maar het is belangrijk om te beseffen welke risico's u in huis haalt. Deze dienen afgewogen te worden tegen de belangen van de organisatie. Bij de risicoafweging worden die factoren in ogenschouw genomen welke een bedreiging zouden kunnen vormen voor de organisatie en haar medewerkers. Wat zijn de mogelijke effecten/gevolgen en wat zijn de kansen als het risico zou optreden? Wanneer dat risico, al dan niet met aanvullende afspraken, acceptabel en aanvaardbaar is, kan alsnog besloten worden om tot aanstelling over te gaan.

USP's samengevat

Wel screenen	***Niet screenen***
Bijdrage aan kwaliteit van personeel	Toename kosten ten gevolge van fraude
Motivatie verhogen	Toename kosten werving en selectie
Bewustzijn op gang brengen	Afnemende effectiviteit
Bedrijfscultuur	Minder efficiëntie
Minder schadeclaims	Niet-renderende opleidingskosten
Verhogen rendement	Schuldsanering trajecten (loonbeslagen hebben een enorme impact op de arbeidsmotivatie)
Certificatie	Hoger ziekteverzuim
Onderscheiden van de concurrent	Kans op verlies van klanten ten gevolge van ontevredenheid
Effectiviteit	Hoge(re) verzekeringskosten
Efficiëntie	Ondermijning bedrijfscultuur
Imago	Afnemend imago
Voldaan aan wettelijke controleplicht / audits	
Voldoen aan certificeringseisen	
Minder fraude, criminaliteit	

Infographic richtlijn



Handige informatie

- Sollicitatiecode – NVP https://nvp-plaza.nl/sollicitatiecode
- Brochure screening van personeel – Dienst Justis https://www.justis.nl/binaries/Screening%20van%20personeel%20december%202017_tcm34-295972.pdf
- Screeningsprofiel VOG bepalen – Dienst Justis https://www.justis.nl/producten/vog/vog-aanvragen/naar-welke-gegevens-wordt-gekeken/screeningsprofielen.aspx
- *Report to the Nations* 2018 – *Association of Certified Fraud Examiners* (ACFE) https://www.acfe.com/report-to-the-nations/2018/

Bibliografie

ACFE. (2018). *Report of the Nations.*

AP. (2018). *Verstrekken en bewaren van persoonsgegevens*. Opgehaald van Autoriteit persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/verstrekken-van-persoonsgegevens

AP. (sd). *Data Protection Impact Assessment (DPIA)*. Opgehaald van https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

Centre for the Protection of National Infrastructure. (2015). *Pre-employment screening - A Good Practice Guide.* Verenigd Koninkrijk.

Levent Bedrijfsrecherche. (2018).

Ministerie van Justitie en Veiligheid . (2017). *Screening van personeel.* Den haag: Ministerie van Justitie en Veiligheid (Rijksoverheid).

Ministerie van Justitie en Veiligheid. (sd). *Wat is een VOG?* Opgehaald van Dienst Justis: https://www.justis.nl/producten/vog/

NVP. (2016). *Sollicitatiecode.* Nijkerk.

NVP. (sd). *Over NVP*. Opgehaald van NVP: https://nvp-plaza.nl/over-nvp

Rijksoverheid. (sd). *Basisregistratie Personen (BRP)*. Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/basisregistratie-personen-brp

Rijksoverheid. (sd). *Wettenbank*. Opgehaald van Overheid: https://wetten.overheid.nl

Verduijn, N. (2016). *Masterthesis Tilburg Universiteit.*

Verhoeven. (2014). Praktijkboek voor methoden en technieken.

Bijlagen

Bijlage 1: Kwetsbare functie-elementen
Bijlage 2: Toelichting screentools
Bijlage 3: Template ‘screeningsbeleid’
Bijlage 4: Template ‘procesbeschrijving screening’

Bijlage 1: Kwetsbare functie-elementen

A. Basis (voor iedere functie)

De basisscreening geeft u een eerste inzicht in de integriteit van uw kandidaat. Er worden een aantal controles uitgevoerd die u helpen met het vaststellen van de betrouwbaarheid van de kandidaat.

Elk screeningsdossier bestaat uit een minimaal aantal screentools, waaronder de controle van het identiteitsbewijs en de eventueel daarbij behorende 'Tewerkstellingsvergunning', die u dient op te nemen in het personeelsdossier. Met deze controle voldoet u aan de wettelijke eisen die daaraan gesteld worden en beperkt u het risico bij controle van de arbeidsinspectie op een boete. Voorbeelden hiervan zijn:

- De identiteitscontrole
- Werkvergunningscontrole (alleen nodig voor kandidaten van buiten de Europese Unie)
- Adresverificatie
- Check van waarschuwingsregisters (diverse sectoren beschikken over een waarschuwingsregister: transport en logistiek (WLS), de detailhandel (FAD) etc.)

Daarnaast kan een VOG worden aangevraagd bij het ministerie van Justitie en Veiligheid en dient de kandidaat eveneens gevraagd te worden om een EV of IV te ondertekenen. Niet iedere strafzaak leidt tot een veroordeling en soms is de zaak nog in onderzoek of onder de rechter. In dat geval zal een VOG niet toereikend zijn en door de EV/IV van de kandidaat wordt dit risico ook uitgesloten. Mocht later blijken dat de kandidaat in dezen niet de juiste informatie heeft gegeven, dan kunt u met de EV/IV een ontbindingsprocedure opstarten.

Nr.	Minimale screentools
1.	Vaststellen identiteit
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV

B. Omgang met personen

Uw kandidaat is belast met de zorg en het welzijn van kwetsbare personen. Kwetsbare personen zijn minderjarigen en hulpbehoevenden, zoals ouderen en gehandicapten. De kandidaat heeft vaak een voorbeeldfunctie en vertrouwenspositie. Hij/zij kan in een een-op-een relatie komen te verkeren met minderjarigen die aan zijn/haar zorg zijn toevertrouwd. Ook kan de kandidaat invloed uitoefenen op de aan hem/haar toevertrouwden door middel van gedragingen, waardoor bijvoorbeeld vermogensdelicten en overtredingen van de Opiumwet niet met de functie zijn te verenigen. In deze relatie kan sprake zijn van een (tijdelijke) afhankelijkheid. Het is dan ook van belang dat uw kandidaat zeer integer is in de omgang met personen.

Risicofactoren: vermogensdelicten, overtredingen van de Opiumwet, machtsmisbruik, zeden- en geweldsdelicten, afpersing of chantage, misbruik van bevoegdheden.

Nr.	Minimale screentools
1.	Vaststellen identiteit
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
2.	Financieel onderzoek
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

C. Omgang met geldzaken

Uw kandidaat heeft in de functie beschikking over bedrijfsgelden en/of heeft budgetbevoegdheden. Denk hierbij bijvoorbeeld aan contant geld of waardepapieren. Het is van groot belang dat de kandidaat verantwoord omgaat met geld en geen misbruik maakt van zijn/haar positie. Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen indien men in een functie of bezigheid de beschikking heeft over geld. Onder dit risicogebied valt het omgaan met contante en/of girale gelden en/of (digitale) waardepapieren en het hebben van budgetbevoegdheden.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

D. Omgang met goederen

Uw kandidaat zal in zijn/haar functie toegang hebben tot goederen en/of productieprocessen. Hierdoor ontstaat het risico van bijvoorbeeld diefstal en verduistering, of vernieling en sabotage. Door vernieling of sabotage bestaat het risico dat bedrijfsprocessen worden ontregeld waardoor de (economische belangen) van bedrijven kunnen worden geschaad.

Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen bij het bewaken van productieprocessen en het beschikken over goederen. Onder dit laatste wordt ook verstaan het laden en lossen, inpakken en opslaan van goederen.

Verder valt onder dit risicogebied het voorhanden hebben van stoffen, objecten of voorwerpen die bij oneigenlijk of onjuist gebruik een risico vormen voor mens en dier. Bij het bewaken van productieprocessen kunnen risico's zich verwezenlijken door het onzorgvuldig omgaan met voedingsmiddelen, chemicaliën of andere stoffen, hetgeen een risico voor de volksgezondheid betekent.

Om dit te voorkomen is het van belang dat u vooraf gedegen inzicht heeft in de integriteit van de kandidaat. Een uitgebreide screening draagt hieraan in grote mate bij.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, milieudelicten, oneigenlijk of onjuist gebruik van stoffen, voorwerpen of objecten kan de veiligheid en het welzijn van mensen en dieren in gevaar brengen.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

E. Afsluiten van zakelijke overeenkomsten

Uw kandidaat is in de beoogde functie bevoegd om zelfstandig te beslissen of er tegen betaling diensten worden verleend. Hierbij is het van belang dat de kandidaat niet vatbaar is voor omkoping, verduistering en chantage waarbij bedrijfs- of beroepsgeheimen kunnen worden gestolen en informatie kan worden gelekt.

Het risicogebied beoogt de maatschappelijke risico's in kaart te brengen die zich kunnen voordoen bij het aangaan en onderhouden van zakelijke contacten. Dit risicogebied omvat onder andere overleg over offertes, advisering en bemiddeling, het voeren van onderhandelingen en het afsluiten van contracten.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, verlies van vertrouwelijke bedrijfsinformatie.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

F. Verlenen van diensten

Uw kandidaat zal in de beoogde functie diensten verlenen als advisering, beveiliging, schoonmaak, catering en dergelijke. Het is van belang dat de kandidaat geen misbruik zal maken van de kennis en bevoegdheden die voortvloeien uit de dienstverlening.

Het risicogebied 'diensten' beoogt de risico's in kaart te brengen die zich kunnen voordoen indien kennis en bevoegdheden die voortvloeien uit deze dienstverlening worden misbruikt.

Dienstverlening als advisering, beveiliging, schoonmaak, catering en onderhoud vallen onder dit risicogebied.

Afhankelijk van de aard en de locatie van de dienstverlening kan het risico van verduistering, diefstal, milieudelicten of het misbruik van vertrouwelijke informatie aanwezig zijn. Indien er sprake is van klantcontact bestaat tevens het risico van gewelds- en zedenmisdrijven.

Het verlenen van diensten in de persoonlijke leefomgeving valt ook onder dit risicogebied. Hierbij vindt het klantcontact in de persoonlijke woon- en leefomgeving plaats.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, milieudelicten, verlies van vertrouwelijke bedrijfsinformatie, geweld en zedenmisdrijven.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

G. Solistisch handelen

Medewerkers voeren alleen of zeer zelfstandig kwetsbare handelingen uit of nemen alleen of zeer zelfstandig besluiten waarbij de kwaliteit van de besluitvorming en de controle op uitgevoerde handelingen onvoldoende is gewaarborgd.

Risico: omkoping, machtsmisbruik, misbruik van bevoegdheden, fraude etc. (alle vormen van integriteitschendingen (of de schijn daarvan) zijn mogelijk doordat iemand alleen opereert, besluiten neemt en er geen controle of direct toezicht plaatsvindt).

Voorbeeld van functies: directeur, medewerker buitendienst.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

H. Omgang met bedrijfsinformatie

Uw kandidaat heeft toegang tot bedrijfssystemen en/of vertrouwelijke bedrijfsinformatie en is in staat deze te wijzigen. Het is van belang dat de kandidaat integer omgaat met de systemen en informatie en hier geen misbruik van maakt.

Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen indien men in een functie of bezigheid toegang heeft tot systemen dan wel tot informatie. Onder dit risicogebied valt ook het omgaan met gevoelige dan wel vertrouwelijke informatie.

Voorts betreft dit het toegang hebben tot of het hebben van kennis over veiligheidssystemen, controlemechanismen en verificatieprocessen.

Indien men het beheer heeft over of bijzondere bevoegdheden heeft bij systemen bestaat het risico dat deze systemen misbruikt worden. Bij het omgaan met gevoelige dan wel vertrouwelijke informatie kan deze informatie misbruikt worden, bijvoorbeeld om iemand te chanteren. Bedrijfs- of beroepsgeheimen kunnen worden gestolen of informatie kan worden gelekt. Bedrijfsprocessen kunnen worden ontregeld door bijvoorbeeld vernieling of sabotage.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, verlies van vertrouwelijke bedrijfsinformatie, omkoping, vernieling, sabotage.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

I. Omgang met procesonderdelen

Uw kandidaat heeft toegang tot vitale bedrijfsprocessen. Denk hierbij aan werkzaamheden als onderhoud en bediening van machines, apparaten en voertuigen, maar ook het vervoer van goederen en/of personen. Hierdoor ontstaat het risico van sabotage en vernieling van bedrijfsprocessen, maar ook gevaar voor de veiligheid van personen en kans op diefstal van goederen.

Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen indien macht over processen wordt misbruikt. Onder dit risicogebied vallen werkzaamheden als het onderhouden, ombouwen en bedienen van (productie)machines, apparaten en voertuigen.

Daarnaast valt onder dit risicogebied het (rijdend) vervoer van goederen, productie, post en pakketten en personen anders dan het interne transport binnen het bedrijf.

Als gevolg van sabotage en vernieling kunnen vitale bedrijfsprocessen worden ontregeld. De veiligheid van personen en goederen kan hierdoor in gevaar worden gebracht.

Bij het rijdend vervoer van grondstoffen en producten en het bezorgen van post en pakketten bestaat het gevaar van diefstal, verduistering en verkeersgerelateerde delicten.

Bij het vervoer van personen bestaat de mogelijkheid dat personen in gevaar worden gebracht door bijvoorbeeld het overschrijden van de maximumsnelheid, rijden onder invloed van o.a. drugs en alcohol, agressief rijgedrag of overige verkeersgerelateerde delicten.

Bij het vervoer van personen is tevens het risico aanwezig van diefstal en gewelds- en zedendelicten.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, verlies van vertrouwelijke bedrijfsinformatie, omkoping, vernieling, sabotage, gewelds- en zedendelicten, verkeersgerelateerde delicten.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

J. Leidinggevende functies

Uw kandidaat zal in de beoogde functie verantwoordelijk zijn voor het aansturen van medewerkers en/of het aansturen van (een deel van) de organisatie. In deze functie bestaat het risico van afpersing, diefstal, verduistering en valsheid in geschrifte.

Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen indien macht over organisaties en de daaraan verbonden personen wordt misbruikt. Dit risicogebied omvat het aansturen van medewerkers en het aansturen van de organisatie. Managers, bedrijfsleiders, filiaalhouders en procuratiehouders vallen onder dit risicogebied.

Door de positie van deze functionarissen in de organisatie bestaat het gevaar van misbruik van bevoegdheden zoals afpersing, diefstal, verduistering en valsheid in geschrifte.

Als gevolg van een onjuiste of onzorgvuldige bedrijfsvoering kunnen de veiligheid en het welzijn van personen in gevaar gebracht worden.

Risicofactoren: vermogensdelicten, afpersing of chantage, misbruik van bevoegdheden, valsheid in geschrifte, verlies van vertrouwelijke bedrijfsinformatie, omkoping, vernieling, sabotage, geweld en zedendelicten, verkeersgerelateerde delicten.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
6.	Referentenonderzoek
8.	Open bronnen onderzoek

Optioneel

Nr.	Minimale screentools
5.	Check opleidingen en diploma's
7.	Integriteitsinterview

K. Invloedrijke positie (macht)

Uw kandidaat heeft in zijn/haar functie veel macht, zowel intern als extern. Het is dan ook van groot belang dat de kandidaat uw bedrijf geen schade toebrengt met een negatief imago. Om dit te waarborgen, dient een uitgebreide screening uitgevoerd te worden waarbij onder andere een bronnenonderzoek over ten minste de afgelopen tien jaar wordt gedaan. Denk hierbij aan uitingen in de media, zoals de traditionele pers maar ook opinieblogs en *social media*. Zowel de uitingen over de kandidaat als van de kandidaat worden meegenomen in het onderzoek. Op basis hiervan krijgt u een gedegen inzicht in de achtergrond van de kandidaat.

Het risicogebied beoogt de risico's in kaart te brengen die zich kunnen voordoen indien macht over organisaties en de daaraan verbonden personen wordt misbruikt. Dit risicogebied omvat het uitoefenen van invloed en/of macht op medewerkers en de organisatie. Leden van de raad van bestuur, raad van commissarissen, raad van toezicht, algemeen procuratiehouders en politieke ambtsdragers vallen onder dit risicogebied.

Door de positie van deze functionarissen in de organisatie bestaat het gevaar van misbruik van bevoegdheden, zoals afpersing, diefstal, verduistering, corruptie en omkoping. Als gevolg van ongewenst gedrag kunnen de veiligheid en het welzijn van personen en het imago van de organisatie in gevaar gebracht worden.

Nr.	Minimale screentools
1.	Vaststellen identiteit
2.	Financieel onderzoek
3.	A. Integriteit: VOG
	B. Integriteit: EV
	C. Integriteit: IV
4.	Check juistheid cv
5.	Check opleidingen en diploma's
6.	Referentenonderzoek
7.	Integriteitsinterview
8.	Open bronnen onderzoek

Bijlage 2: Toelichting screentools

Nr.1 Vaststellen identiteit

Volgens wettelijke bepalingen heeft een werkgever de plicht om identiteitsbewijzen van medewerkers te controleren op juistheid en om te controleren of er geen wettelijke bezwaren bestaan dat er werk verricht mag worden.

De adresverificatie is een onderdeel van de crosscheck en geeft zekerheid omtrent de inschrijving in het BRP.

Controle op de nationale en internationale waarschuwings- en sanctielijsten wordt uitgevoerd om signalering door opsporingsautoriteiten, bijvoorbeeld in verband met zware criminaliteit en betrokkenheid bij terroristische activiteiten, uit te sluiten. (Bijvoorbeeld de lijsten van de EU, VN en VS, Interpol en de FBI, maar ook beschikbare nationale waarschuwingslijsten.) LET OP: controle van het FAD-register maakt hiervan geen onderdeel uit.

Inhoud:

- Controle identiteitsdocument;
- Controle VIS-registratie van vermiste en/of gestolen identiteitsdocumenten;
- Controle Tewerkstellingsvergunning *= controle op naleving Wet arbeid vreemdelingen;*
- Adresverificatie;
- Controle nationale en internationale waarschuwingslijsten.

Voordelen:

- Er wordt vastgesteld dat het identiteitsbewijs geldig is en daadwerkelijk aan de kandidaat is afgegeven;
- De check bewijst dat diegene is wie hij/zij zegt te zijn;
- Voldoen aan de Wid - Wet op de identificatieplicht (Wid 1993);
- Voldoen aan Wav - Wet arbeid vreemdelingen (art.2 Wav 1994);
- Bij inspectie door controlerende instituten geen kans meer op boetes;

Toelichting:

Voor werkgevers valt de identificatieplicht ten aanzien van werknemers uiteen in vier gedeelten:

- **Verificatieplicht,** controleren van origineel identiteitsdocument bij aanname nieuwe werknemer.
- **Bewaarplicht,** kopiëren van deze documenten, in administratie opnemen en tot minstens vijf jaar na einde dienstverband bewaren.
- **Zorgplicht,** werknemers erop wijzen om tijdens werkzaamheden een origineel identiteitsbewijs bij zich te dragen.

- **Toonplicht,** verstrekken van inlichtingen bij controle door de Arbeidsinspectie, Vreemdelingendienst, Belastingdienst etc. Zowel de Arbeidsinspectie als de Belastingdienst voert steeds strengere controles uit.

Met andere woorden: de werkgever, maar ook de inlenende partij, is verplicht om bij indiensttreding/aanvang van de werkzaamheden de identiteit te controleren aan de hand van een geldig identiteitsdocument en dit op echtheid en geldigheid te controleren. Daarnaast is de werkgever verplicht om een kopie van het controleerde document, inclusief BSN en pasfoto, op te nemen in de loonadministratie. De werknemer heeft op de werkvloer de verplichting om bij controle van bijvoorbeeld de Inspectie SZW het identiteitsbewijs te tonen.

Nr. 2 Financieel onderzoek

- Een meerderheid van alle interne fraudegevallen heeft als oorzaak een financieel probleem in de privésituatie (ACFE, 2018);
- Loonbeslagen hebben een enorme impact op de arbeidsmotivatie;
- Inschatten risico's bij financiële problemen (risico's) wordt hierdoor mogelijk;
- Middels een controle op financiële fraude-incidenten wordt nagegaan of er sprake is van betrokkenheid bij oplichting, valsheid in geschrifte, online oplichtingpraktijken etc.

Verzwaard financieel onderzoek:

- Onderzoek naar inkomsten en uitgaven;
- Beoordeling van de financiële positie;
- Onderzoek naar bezittingen;
- Onderzoek naar financiële deelnemingen (bedrijven e.d.).

Inhoud:

- Controle op registratie van lopende incassovorderingen;
- Controle op registratie schuldsaneringtraject;
- Controle op registratie lopend faillissement/surseance van betalingen;
- Controle op lopende gerechtelijke invorderingsprocedures;
- Fraudedetectie.

Toelichting:

Bedenk daarnaast dat iemand met financiële problemen simpelweg een risico voor de onderneming kan betekenen. Door middel van een financiële toets of onderzoek naar de financiële omstandigheden kunnen eventuele risico's, zoals verlies van geld of goederen door frauduleuze activiteiten of de kans op imagoschade, worden onderkend.

Het aantal consumenten met betalingsachterstanden, die de eindjes niet meer aan elkaar kunnen knopen, is groot. Denk hierbij aan achterstanden in betalingen aan postorder- en telecombedrijven, de Belastingdienst, woningcorporaties, nutsbedrijven, zorgverzekeraars etc. Een opvallend groot aantal maar ook recente incassovorderingen, deurwaardersexploten e.d. kunnen een indicatie zijn dat de financiële huishouding niet op orde is.

Hoe groot is de kans dat er binnen afzienbare tijd of misschien wel direct na indiensttreding loonbeslag wordt gelegd, wat weer een hoop extra administratieve handelingen met zich meebrengt? Daarnaast is gebleken dat medewerkers met ernstige (financiële) problemen deze ook tijdens de werkzaamheden met zich meedragen, hetgeen invloed heeft op de kwantiteit en kwaliteit van de uit te voeren werkzaamheden. Door als werkgever op de hoogte te zijn, kunt u hierop sturen en afspraken maken in de arbeidsovereenkomst.

Bij bepaalde functies is het eveneens raadzaam om bij het financieel onderzoek niet alleen te kijken naar risicovolle schulden, maar ook naar de inkomsten en bezittingen. Voor financiële en directiefuncties waarin de kandidaat zelfstandig bevoegd is om financiële transacties te doen, is het

van belang te weten dat die persoon zijn financiële huishouding op orde heeft, om niet in verleiding te komen.

Vraag kan bijvoorbeeld zijn of zijn/haar levenspatroon in verhouding is met de inkomsten. Een groot verschil daartussen kan wijzen op ongeoorloofd gedrag of andere inkomsten. Het kan bijvoorbeeld wijzen op nevenactiviteiten waarmee u liever niet in verband wilt worden gebracht - denk aan drugshandel, de porno-industrie of gokken. Ook kan het zo zijn dat de kandidaat er een baan naast heeft, een nevenfunctie die niet te rijmen is met de functie bij uw bedrijf.

Een financieel onderzoek kan bij beide partijen zorgen voor een goede start: u kunt naar aanleiding van het onderzoek een gesprek aangaan over mogelijk problemen en de werknemer kan daarover uitsluitsel geven.

Voordelen:

- Directe kostenbesparing door minder loonbeslagen;
- Zicht op financiële problemen van nieuwe medewerkers;
- Terugdringen van interne fraude;
- Terugdringen van overheadkosten;
- Terugdringen van schade ten gevolge van fraude.

Nr. 3 Integriteit

Verklaring Omtrent het Gedrag (VOG)
Een VOG wordt door Dienst Justis van het ministerie van Justitie en Veiligheid afgegeven indien blijkt dat gedrag in het verleden, ook als het om strafbare feiten gaat, geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving.

De VOG kan op twee manieren worden aangevraagd:

1. Een aanvraag kan door de werkgever digitaal worden ingediend, waarna de kandidaat door de dienst Justis zal worden geïnformeerd en begeleid bij het verkrijgen van de VOG. De VOG zal naar het officiële woonadres van de kandidaat worden gestuurd.
2. De aanvraag kan worden gedaan door de kandidaat bij de afdeling Burgerzaken van de gemeente waar hij/zij woonachtig is.

De VOG wordt afgegeven indien de kandidaat (over het algemeen) de voorgaande vier jaar niet is veroordeeld voor een delict dat relevant is voor de werkzaamheden of de omgeving van de functie.

Voordelen:

- Dienst Justis geeft een verklaring af dat de betrokkene geen strafrechtelijke veroordelingen heeft die relevant kunnen zijn voor de functie die vervuld gaat worden.
- Sollicitanten met een veroordeling op hun naam die een risico vormt voor de beoogde functie haken tijdens het wervings- en selectietraject al af bij de mededeling dat de VOG een aanstellingseis is.

Eigen Verklaring (EV)
Laat de kandidaat een formulier 'Eigen verklaring omtrent het gedrag' ondertekenen. Hij/zij verklaart de afgelopen vijf jaar niet met de politie en/of justitie in aanraking te zijn geweest. Deze verklaring kan worden opgenomen in het personeelsdossier.

Integriteitsverklaring (IV)
Laat de kandidaat een integriteitsverklaring (een uitgebreide EV) invullen en ondertekenen. Hij/zij verklaart :

- al dan niet ooit veroordeeld/vervolgd te zijn voor overtreding van een wettelijk voorschrift met een financieel economisch karakter;
- en/of onderwerp te zijn van een strafrechtelijke of disciplinair onderzoek;
- en/of ooit veroordeeld te zijn voor een misdrijf;
- en/of de afgelopen vijf jaar onderwerp te zijn geweest van publicaties;
- en/of ooit bestuurder of senior manager te zijn geweest van een onderneming of stichting die failliet is gegaan;
- en/of onder toezicht te zijn geweest van een toezichthouder;
- en/of een conflict te hebben gehad met een werkgever of zakelijke relatie;
- en/of er ooit arbeidsrechtelijke sancties aan hem/haar zijn opgelegd;

! Let op:

Het aanvragen van een VOG is een stap in de goede richting, maar het probleem is dat alleen een VOG niet zoveel zegt. Een VOG wordt namelijk afgegeven indien gedrag in het verleden, ook als het om strafbare feiten gaat, geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving. Het zegt niets over hoe diegene zich de afgelopen jaren verder gedragen heeft. Nieuwe medewerkers die eerder fraude hebben gepleegd maar niet tegen de lamp gelopen zijn, kunnen ondanks die verklaring dus een potentieel risico vormen. In de praktijk blijkt dat een VOG over het algemeen wordt verstrekt en dat slechts een zeer klein deel van de aanvragen wordt geweigerd (0,29 procent in 2017) (Dienst Justis, 2017).

De EV en IV zijn daarom een aanvulling op de VOG en kijken verder dan alleen de delicten waarvoor iemand is veroordeeld. De EV en IV kunnen dienen als bewijsstuk bij een eventuele ontslagprocedure. Wanneer later blijkt dat de kandidaat hierin geen juiste verklaring heeft afgelegd, kan dit document dienen ter ondersteuning van een ontslagprocedure.

Nr. 4 Check juistheid cv

Binnen deze check wordt gecontroleerd of het cv overeenkomt met de overige verstrekte gegevens en of er inconsistenties worden waargenomen in het cv. Hierbij wordt onder meer gekeken naar de volgende punten:

- Is de opbouw logisch en correct;
- Tijdlijn opleiding en werkervaring;
- Consistentie;
- Beschikbaarheid referenten;
- Eventuele tegenstrijdige belangen.

Toelichting:

Onjuistheden vermelden of zelfs liegen tijdens een sollicitatiegesprek komt regelmatig voor en kan grote problemen opleveren, zowel voor de sollicitant als voor uw organisatie. Denk aan het opgeven van zelfstandigheid of van studies die helemaal niet zijn gevolgd of afgerond. Het vervalsen van diploma's of certificaten is zelfs een misdrijf en daarmee ontstaat de kans op juridisch vervolging. Naast beschadiging van het imago van de sollicitant kunnen leugens ook zeer schadelijk zijn, al was het alleen al vanwege de oneerlijke concurrentie tegenover de andere sollicitanten. Wat kunt u doen tegen leugens en de bijbehorende mogelijke schade aan uw organisatie door toekomstige medewerkers?

Lees het cv zorgvuldig. Is dit logisch van opbouw? Zet een tijdlijn op en controleer of de tijd tussen opleidingen en werkervaring verklaarbaar is. Ga na of de 'gaten' in de tijdlijn verklaard kunnen worden en controleer dit zorgvuldig. Let goed op als er een sabbatical periode wordt vermeld: wees dan kritisch en vraag hier bij de kandidaat speciaal op door (een sabbatical wordt vaak gebruikt om negatieve aspecten te verdoezelen, bijvoorbeeld een detentieperiode of een werkgever waarmee een incident heeft plaatsgevonden). Zijn er weinig referenten of worden die niet vermeld? Let dan extra goed op! En controleer tenslotte of er informatie over de opleiding en het arbeidsverleden op internet terug te vinden is. Vraag de sollicitant om originele en relevante diploma's te tonen.

De vraag dient zich aan of de verzwegen of gelogen informatie van belang is voor de functie die de werknemer zal gaan vervullen. Dat is ter afweging aan de organisatie, maar u kunt zich natuurlijk wel afvragen of de sollicitant die belangrijke zaken verzwijgt, onjuist weergeeft of daadwerkelijk verzint in de toekomst een betrouwbare en integere werknemer zal zijn.

Voordelen:

- Eventuele achtergehouden informatie wordt zichtbaar;
- Onduidelijkheden of onregelmatigheden worden opgehelderd;
- Verschillen tussen het cv en informatie die wordt verstrekt ten behoeve van het onderzoek komen naar voren;
- Kosten voor het werven en inwerken van uiteindelijk niet gekwalificeerd personeel worden beperkt.

Nr. 5 Check opleidingen en diploma's

Het komt erg vaak voor dat een kandidaat geen diploma kan overhandigen. Veelgehoorde excuses zijn: tijdens de scheiding zoekgeraakt, er is brand geweest of het ligt nog bij mijn ouders en die wonen ver weg etc. In de meeste gevallen wordt het de kandidaat niet lastig gemaakt omwille van de goede verstandhouding. Het probleem is echter dat het steeds vaker voorkomt dat een diploma nooit is behaald of simpelweg is gekocht/gefraudeerd.

Inhoud:

- Controle studieduur en periode opleiding;
- Check op echtheid diploma / cijferlijst /certificaten;
- Check op diploma Mills;
- Check op ranking opleidingsinstituut;
- Check op EFQ level van buitenlands diploma*.

Aanvullende controles per beroepsgroep, zoals:

- Check geldig rijbewijs;
- BIG-registratie (of andere beroepsgebonden registraties).

Voordelen:

- Voldoen aan de functie-eisen;
- Enorme risicoverlaging als het gaat om functies waarbij hoge of specialistische opleidingen vereist zijn.

*Toelichting EFQ level:

Indien noodzakelijk voor de functie is het mogelijk een vergelijking te laten plaatsvinden van een internationaal diploma/getuigschrift ten opzichte van de Nederlandse equivalent. Het Nuffic is het expertisecentrum in Nederland op het gebied van diplomawaardering van in het buitenland gevolgd algemeen voortgezet en hoger onderwijs. Voor de waarderingscriteria bij het maken van diplomawaarderingen worden de criteria en procedures gehanteerd die in de Lissabon Erkenningsconventie worden aangemerkt als *good practice*.

Het onderzoek naar de waardering van het opleidingsinstituut zal zich specifiek richten op de reputatie van de vereiste opleidingen. Indien mogelijk zal er bij elk onderzoek naar de reputatie van het opleidingsinstituut worden gekeken, waaronder welke gewogen ranking dit wereldwijd en in Europa heeft en of er omstandigheden bekend zijn die de reputatie van het instituut of zijn opleidingen twijfelachtig maken.

Nr. 6 Referentenonderzoek

Referenties worden zoveel mogelijk als laatste onderdeel van het onderzoek benaderd. Bij de opgegeven referenties zal gericht informatie worden gevraagd over de kandidaat. Hierdoor wordt een beeld verkregen van de mate van integriteit van de kandidaat en zijn/haar wijze van functioneren.

Inhoud:

- Vaststellen tijdsduur dienstverband;
- Vaststellen rol en verantwoordelijkheid van de functie;
- Navraag betrouwbaarheid en integriteit.

Voordelen:

- Betrouwbaarheid/integriteit wordt bevestigd of ontkracht;
- Geen vertrouwensbreuk doordat de referenten na toestemming benaderd worden;
- Er wordt altijd getracht minimaal twee referenten te benaderen;
- Gegevens uit het cv worden bevestigd of ontkracht;
- Eventuele achtergehouden informatie wordt bekend;
- Onduidelijkheden of onregelmatigheden worden opgehelderd;
- De kosten voor het werven en inwerken van uiteindelijk niet gekwalificeerd personeel zijn erg hoog, en een referentenbevraging maakt beter inzichtelijk wie u in huis haalt;
- Richtlijnen in Nederland beletten dat voormalige werkgevers negatieve informatie over hun ex-werknemers verstrekken. Let op: dit zijn richtlijnen. Specialistische ondervragingstechnieken zijn nodig om gewenste informatie te krijgen.

! Let op:

Niet alle opgegeven referenten zijn altijd geschikt om een onafhankelijk oordeel te geven over een kandidaat. Denk hierbij aan familie, vrienden etc. Bedenk of een referent wel altijd eerlijk is geweest in zijn antwoorden. Kan hij/zij bepaalde vragen wel beantwoorden?

Het is sowieso niet raadzaam om af te gaan op wat één referent vertelt over een kandidaat. Een negatieve referentie betekent trouwens zeker niet dat de kandidaat dan ook een negatief advies krijgt. Bij een goed uitgevoerde screening wordt gecheckt of de negatieve elementen daadwerkelijk gebaseerd zijn op feiten en niet op aannames en veronderstellingen. Een referent kan een totaal ongefundeerde mening hebben; ook dan gaat het gaat erom de feiten te objectiveren en dus een gewogen oordeel te geven op basis van feiten.

Nr. 7 Integriteitsinterview

Binnen dit interview worden de onderzoeksresultaten besproken met de kandidaat. Daar waar nodig kan de kandidaat aanvullende informatie verstrekken. Tevens worden algemene integriteitsissues besproken aan de hand van diverse casussen. Specialistische ondervragingstechnieken zijn nodig om gewenste informatie te krijgen.

Voordelen:

- Werving en selectie kan beperkt blijven tot de competenties en geschiktheid voor de functie;
- Kritische vragen met betrekking tot integriteit en betrouwbaarheid worden door een deskundige onafhankelijke derde gesteld;
- Geen vertrouwensbreuk doordat de vragen met betrekking tot integriteitvraagstukken door een onafhankelijke partij gesteld worden;
- Geeft een onafhankelijkheid beeld van de verwachte integriteit.

Toelichting:

Een integriteitsinterview is iets heel anders dan een sollicitatiegesprek. En het verdient aanbeveling om dit door een onafhankelijke medewerker of een externe partij te laten uitvoeren die gewend is om met integriteitsvraagstukken om te gaan. Het gaat hier niet meer over het competentievraagstuk. Bij een integriteitsinterview draait het uitsluitend om risico's en integer gedrag. Door casussen te schetsen, kan inzicht worden verkregen in hoe de kandidaat in een bepaalde situatie zou handelen.

Het integriteitsinterview kan worden toegepast om die vragen te laten stellen die bijvoorbeeld de recruiter of HR-medewerker tijdens een sollicitatiegesprek liever niet stelt omdat ze de net opgebouwde goede vertrouwensverstandhouding met de sollicitant zouden kunnen verstoren. Het vraagt van de interviewer dat hij/zij kritisch is en durft door te vragen. Let tijdens het interview op eventueel non-verbaal gedrag. Zodra de kandidaat zich 'ongemakkelijk' voelt of wanneer bij de interviewer 'onderbuikgevoelens' opspelen, dienen eventuele twijfels te worden weggenomen. Maak dit bespreekbaar. De antwoorden op de vragen kunnen een basis vormen voor het referentenonderzoek.

Nr. 8 Open bronnen onderzoek

Een open bronnen onderzoek is voornamelijk gericht op zoeken op het internet. Het is de manier om gegevens te verzamelen op het openbaar toegankelijke web.

Het internet biedt een schat aan informatie die openbaar toegankelijk is. Veel informatie is beschikbaar in geheel vrij toegankelijke bronnen, zoals Google, Facebook, LinkedIn, Twitter etc. Daarnaast is veel interessants te vinden in bronnen waarvoor een (gratis of betaalde) registratie nodig is. Om optimaal informatie in die schat aan informatie te vergaren, is het nodig dat u goed kunt zoeken.

"Zoeken op internet is meer dan alleen een zoekopdracht via Google"

Een open bronnen onderzoek kan een al dan niet geringe inbreuk op het recht op privacy opleveren. Het handmatig op het internet rondkijken vanuit een controlefase zal in principe geen inbreuk op het recht op privacy opleveren. De handelingen zijn niet stelselmatig. (Verduijn, 2016)

Doordat de juridische aspecten van open bronnen onderzoek op internet nog nauwelijks in kaart zijn gebracht, is het niet mogelijk om een uitputtende analyse te geven van alle juridische aandachtspunten.

! Let op:

Wanneer er gebruik wordt gemaakt van geautomatiseerde systemen met een hoge intensiteit en het gebruik van datamining omvangrijk is, kan een (geringe) inbreuk op het recht op privacy worden aangenomen. In het geval van gebruik van een beperkte hoeveelheid metadata die geen concreet (of uitgebreid) beeld van het leven van een persoon oplevert, zal een inbreuk niet worden aangenomen of zal slechts een geringe inbreuk worden aangenomen. Dit zal over het algemeen bij een pre- en in-employment screening niet van toepassing zijn.

Inhoud (variërend in zwaarte van onderzoek):

- Controle zoekmachines
- Controle *social media*-websites
- Controle nieuwsbronnen
- Controle openbare registers
- Controle waarschuwingsregister (div. branches) (semi-openbare bron);
- Controle sanctielijsten.

Voordelen:

- Eventuele achtergehouden informatie wordt zichtbaar;
- Verstrekte informatie kan worden gevalideerd;
- Onduidelijkheden of onregelmatigheden kunnen zichtbaar worden.

Toelichting:
Het doel van een open bronnen onderzoek is om een zo duidelijk mogelijk beeld te schetsen van een sollicitant of een kandidaat en om te controleren of de informatie welke door hem/haar is aangeleverd, kan worden gevalideerd. Om dat beeld zo volledig mogelijk te krijgen, worden er verschillende relevante bronnen geraadpleegd. Een belangrijk onderdeel hiervan zijn openbare bronnen (zoals internet, diplomaregisters en dergelijke) en bronnen rondom de kandidaat, zoals voormalige werkgevers en andere referenten. Voor het benaderen van deze referenten dient toestemming aan de kandidaat te worden gevraagd.

Het zoeken in openbare bronnen, ook wel Open Source Intelligence (OSINT) genoemd, maakt dus deel uit van de screeningsprocedure. ***Gegevens die uit dit onderzoek naar voren komen, worden doorgaans niet in het personeelsdossier vastgelegd.*** Wel wordt in het dossier aangegeven dat deze bronnen zijn onderzocht en of er relevante informatie is aangetroffen.

Bijlage 3: Template ‘screeningsbeleid’

Afbakening screeningsbeleid

Doelstelling	
Doelgroep	
Definities	
Eigenaarschap	
Kaders*	
Screentools	
Financiën	
Kwaliteitsborging	

***Operationele randvoorwaarden screening**

Functiebeschrijvingen	
Risicoprofiel	

***Juridische randvoorwaarden screening**

Belangrijke verwijzingen	
Juridisch speelveld	
Verzamelen en bewaren van persoonsgegevens	

***Tactische randvoorwaarden screening**

Bijlage 4: Template ‘procesbeschrijving screening’

Afbakening screeningsbeleid

Proces	Screening hoog risico	Screening middelhoog risico	Etc.
Kaders bepalen o.b.v. risicoprofielen			
Informatie verzamelen			
Informatie analyseren			
Informatie beoordelen			
Besluiten (laten) nemen			
Besluiten vastleggen			