

Whitepaper

Gegevenssoevere initeit en HR

In deze gids ontdek je alles wat je nodig hebt om een effectief beleid voor background screening van kandidaten en werknemers op te stellen en te implementeren. Je vindt er praktische tips, de nieuwste trends en een handige checklist om je op het juiste spoor te houden. Met deze inzichten ben je helemaal klaar voor 2026!

Screeninggids
Inhoudsopgave

Invoering 03

Waarom de privacy van kandidaten een heroverweging van HR-gegevenspraktijken vereist 04

De noodzaak tot naleving: GDPR en verder 05

Uitdagingen op het gebied van gegevenssoevereiniteit voor HR-teams 06

Privacybezwaren van kandidaten bij werving en selectie 07

Strategische implicaties voor het samenstellen van teams 08

Checklist voor screeningsbeleid 09

Maak kennis met PESCHECK 11

Definitielijst 12

Invoering

In 2026 is data zowel een troef als een risico voor HR-teams in heel Europa. De opkomst van digitale recruitmenttools, cloudopslag en AI-gestuurde wervingsmethoden heeft de manier waarop kandidaatinformatie wordt verzameld, verwerkt en opgeslagen, getransformeerd. Tegelijkertijd vereisen regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) en de groeiende nadruk op datasoevereiniteit dat HR-teams opnieuw bekijken waar data zich bevindt, wie er controle over heeft en hoe er onder verschillende rechtsstelsels toegang toe kan worden verkregen. Het negeren van deze realiteit is niet langer alleen een kwestie van compliance, maar ondermijnt ook het vertrouwen van kandidaten, het werkgeversimago en de rechtszekerheid.

> "Het respecteren van kandidaatgegevens draait om mensen. Wanneer organisaties laten zien dat ze erom geven waar en hoe persoonlijke informatie wordt bewaard, geven ze een duidelijke boodschap af: we waarderen u, uw privacy en uw vertrouwen."
>
> Serhat Elban, CEO PESCHECK

Het begrip gegevenssoevereiniteit in de EU-context begrijpen

Datasoevereiniteit verwijst naar het concept dat digitale informatie onderworpen is aan de wetten en bestuurskaders van het gebied waar deze wordt gecreëerd of opgeslagen. Dit gaat verder dan alleen de locatie van gegevensopslag; het omvat wie de wettelijke controle over de gegevens heeft en welke wetgeving van toepassing is. In de EU is datasoevereiniteit nauw verbonden met privacybescherming die individuen uitgebreide rechten geeft over hun persoonlijke gegevens, waaronder wervings- en personeelsgegevens.

De locatie waar kandidaatgegevens worden opgeslagen of verwerkt, kan van invloed zijn op het toepasselijke rechtsstelsel. Als de persoonsgegevens van een EU-kandidaat bijvoorbeeld op servers buiten de EU worden gehost, kunnen deze onder buitenlandse wetgeving vallen die in strijd is met de EU-privacywetgeving. Deze discrepantie kan leiden tot lacunes in de soevereiniteit, waardoor organisaties worden blootgesteld aan juridische procedures en de transparantie voor betrokkenen afneemt.

Waarom de privacy van kandidaten een heroverweging van HR-gegevenspraktijken vereist

Werving en selectie brengt inherent grote hoeveelheden persoonsgegevens met zich mee, variërend van cv's, contactgegevens, aantekeningen van sollicitatiegesprekken en resultaten van background check tot resultaten van psychometrische tests en beoordelingsgegevens. Al deze gegevens vallen onder de bescherming van de AVG.

Zelfs bij de dagelijkse gang van zaken rondom werving en selectie, zijn kandidaten steeds gevoeliger voor de manier waarop hun persoonsgegevens worden behandeld. Studies tonen aan dat een aanzienlijk deel van de werkzoekenden zich zorgen maakt over hoe organisaties hun persoonlijke informatie beheren, en dat slechte gegevensbeschermingspraktijken het vertrouwen in potentiële werkgevers direct ondermijnen. Bijvoorbeeld::

- ✓ Onderzoek wijst uit dat 62% van de kandidaten zich zorgen maakt over hoe hun gegevens worden beheerd, en dat een onjuiste omgang met privacy kan leiden tot reputatieschade en het verlies van talent.
- ✓ Bedrijven die te maken krijgen met datalekken kunnen binnen zes maanden tot wel 25% van hun potentiële kandidaten verliezen, omdat sollicitanten organisaties mijden die als onveilig worden beschouwd met betrekking tot persoonsgegevens.

Voor HR-teams betekent dit dat privacybeleid proactief, transparant en kandidaatgericht moet zijn. Het is niet langer voldoende om te voldoen aan de AVG; organisaties moeten duidelijk communiceren hoe gegevens worden verzameld, opgeslagen en beschermd, en ervoor zorgen dat kandidaten zich gedurende het hele wervingsproces veilig voelen. Zo verandert privacy van een wettelijke verplichting in een concurrentievoordeel in de strijd om talent.



De noodzaak tot naleving: GDPR en verder

De Algemene Verordening Gegevensbescherming (AVG) blijft de basis voor de verwerking van persoonsgegevens van kandidaten en werknemers in de hele EU. In 2026 gaat de naleving echter verder dan het voldoen aan wettelijke vereisten; het vereist continue verantwoording, transparantie en de mogelijkheid om te allen tijde aan te tonen dat er correct met gegevens wordt omgegaan.

In de kern vereist de AVG dat persoonsgegevens rechtmatig, eerlijk en transparant worden verwerkt. Voor HR-teams betekent dit dat privacy in elke fase van het wervingsproces moet worden geïntegreerd en dat er moet worden overgestapt van reactieve naleving naar proactief gegevensbeheer.

In de praktijk moeten organisaties duidelijk uitleggen welke gegevens worden verzameld, waarom deze nodig zijn en hoe lang ze worden bewaard, terwijl ze strikte principes van gegevensminimalisatie toepassen. Ze moeten ook een gedocumenteerde wettelijke basis voor de verwerking hebben en ervoor zorgen dat kandidaten gemakkelijk hun rechten kunnen uitoefenen, zoals inzage, correctie of verwijdering van hun gegevens.

Wat is belangrijk?

- ✓ **Duidelijke communicatie over het gebruik en de bewaring van gegevens is essentieel voor transparantie**
  Kandidaten moeten begrijpen wat er met hun gegevens gebeurt vanaf het moment dat ze solliciteren. Door duidelijk aan te geven hoe informatie wordt gebruikt, opgeslagen en hoe lang, wordt onzekerheid verminderd en wordt direct vertrouwen in het proces gewekt.
- ✓ **Het minimaliseren van gegevens vermindert zowel het nalevingsrisico als de bezorgdheid van kandidaten**
  Door alleen de strikt noodzakelijke gegevens te verzamelen, wordt het risico op datalekken of misbruik beperkt. Het geeft kandidaten bovendien de zekerheid dat de organisatie hun privacy respecteert en onnodige inbreuken op hun privacy voorkomt.
- ✓ **Gedocumenteerde juridische grondslagen garanderen verantwoording in geval van audits**
  Een duidelijke en vastgelegde rechtvaardiging voor de verwerking van persoonsgegevens toont aan dat beslissingen weloverwogen en conform de regelgeving zijn genomen. Dit ondersteunt niet alleen audits door toezichthouders, maar versterkt ook de interne governance en consistentie.
- ✓ **Het waarborgen van de rechten van kandidaten vergroot het vertrouwen en versterkt de eerlijkheid**
  Door kandidaten eenvoudig toegang te geven tot hun gegevens en hen de mogelijkheid te bieden deze te corrigeren of te verwijderen, toon je respect voor hun zeggenschap over persoonlijke informatie. Wanneer deze rechten efficiënt worden beheerd, versterkt dit de perceptie van een eerlijk en betrouwbaar wervingsproces.

Uitdagingen op het gebied van gegevenssoevereiniteit voor HR-teams

Grensoverschrijdende gegevensstromen

Wereldwijde HR-systemen centraliseren vaak recruitmenttechnologie, analyses en cloudopslag over verschillende regio's. Hoewel dit de efficiëntie kan verbeteren, maakt het de naleving van regelgeving ook complexer. Als kandidaatgegevens worden opgeslagen in een rechtsgebied buiten de EU, kunnen lokale wetten buitenlandse autoriteiten of dienstverleners toegangsrechten verlenen die in strijd zijn met de EU-privacywetgeving. Dit brengt soevereiniteitsrisico's met zich mee die verder reiken dan alleen de AVG.

Risico's van leveranciers en derden

Recruitmenttechnologie werkt zelden op zichzelf. HRIS-platformen, ATS-systemen, salarisverwerkers, assessmenttools en leveranciers van background screening fungeren allemaal als gegevensverwerkers. Hoewel de AVG HR-teams verantwoordelijk stelt als gegevensbeheerders, kan een datalek of niet-naleving door een derde partij nog steeds leiden tot boetes en reputatieschade voor de wervende organisatie. Actief leveranciersbeheer, gegevensverwerkingsovereenkomsten (DPA's) en beveiligingsbeoordelingen zijn daarom essentieel.

Rechten en verwachtingen van kandidaten

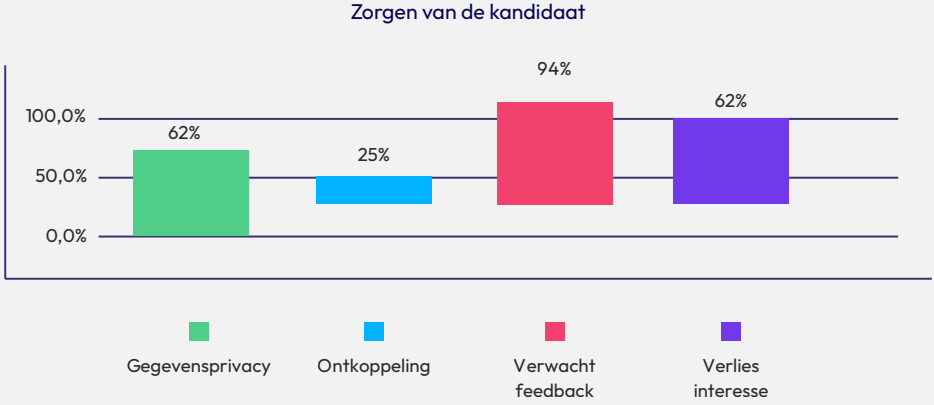
Volgens de AVG hebben kandidaten uitgebreide rechten met betrekking tot hun persoonsgegevens, waaronder inzage, correctie, verwijdering (met bepaalde wettelijke uitzonderingen) en bezwaar tegen de verwerking. Het misbruiken van deze rechten, zoals het niet tijdig reageren op inzageverzoeken of het weigeren van een rechtmatig verwijderingsverzoek, kan op zichzelf al een schending van de AVG zijn.

> "Mensen willen weten dat hun persoonlijke gegevens veilig en gerespecteerd worden. Wanneer kandidaten het gevoel hebben dat ze controle hebben over hun gegevens en begrijpen hoe deze worden gebruikt, groeit het vertrouwen in het wervingsproces vanzelf."
>
> Serhat Elban, CEO PESCHECK

Privacybezwaren van kandidaten bij werving en selectie

Wereldwijde HR-systemen centraliseren vaak recruitmenttechnologie, analyses en cloudopslag over verschillende regio's. Hoewel dit de efficiëntie kan verbeteren, maakt het de naleving van regelgeving ook complexer. Als kandidaatgegevens worden opgeslagen in een rechtsgebied buiten de EU, kunnen lokale wetten buitenlandse autoriteiten of dienstverleners toegangsrechten verlenen die in strijd zijn met de EU-privacywetgeving. Dit brengt soevereiniteitsrisico's met zich mee die verder reiken dan alleen de AVG.

Belangrijkste gegevenspunten:



62% van de kandidaten maakt zich zorgen over hoe hun persoonlijke gegevens worden beheerd

25% van de gekwalificeerde kandidaten haakt af na een datalek

94% van de kandidaten verwacht feedback na hun sollicitatie

62% van de kandidaten verliest interesse als ze binnen twee weken geen reactie ontvangen

Deze cijfers tonen aan dat privacy, transparantie en communicatie nauw met elkaar verbonden zijn. Wanneer kandidaten het gevoel hebben dat hun gegevens niet verantwoord worden behandeld of dat de communicatie tekortschiet, neemt het vertrouwen af en daarmee ook de betrokkenheid.

Strategische implicaties voor het samenstellen van teams

Het heroverwegen van dataopslag en privacy binnen HR gaat niet alleen over compliance; het gaat ook over het opbouwen van vertrouwen, duurzaamheid en concurrentievoordeel. Organisaties die strategieën hanteren die rekening houden met datasoevereiniteit, profiteren op verschillende manieren:

- ✓ **Verbeterd zelfvertrouwen bij de kandidaten**
  Transparante en lokale controlemechanismen geven kandidaten de zekerheid dat hun gegevens veilig zijn en vallen onder bekende wettelijke beschermingsmaatregelen.
- ✓ **Verminderde juridische risico's**
  Het minimaliseren van risicovolle grensoverschrijdende overdrachten en het proactief implementeren van robuuste kaders voor gegevensbeheer beperken nalevingsrisico's.
- ✓ **Verbeterde merkreputatie**
  Het tonen van een principieel beheer van persoonsgegevens getuigt van professionaliteit en respect voor de rechten van kandidaten.

Als reactie op deze trends lanceren sommige HR-technologieleveranciers EU-soevereine cloudoplossingen waarmee organisaties HR-gegevens volledig binnen de EU-grenzen kunnen opslaan en verwerken, onder controle van de klant. Dit biedt een oplossing voor zowel wettelijke als strategische soevereiniteitsvraagstukken en maakt tegelijkertijd AI-integratie en -analyse mogelijk.



Checklist voor screeningsbeleid

Wil je aan de slag met het ontwerpen van een screeningsbeleid? Gebruik deze checklist om de controle en het overzicht te behouden.

Omvang en doel

- Definieer het doel van het screeningsbeleid.
- Identificeer welke functies een screening vóór en tijdens het dienstverband vereisen.
- Specificeer de situaties die een screening tijdens het dienstverband in gang zetten (promoties, detacheringen, klantvereisten).

Wettelijke naleving

- Zorg voor afstemming met de AVG, lokale arbeidswetgeving en grensoverschrijdende regelgeving.
- Definieer de soorten vragen en controles die wettelijk zijn toegestaan.
- Neem procedures op voor het verkrijgen van geïnformeerde toestemming van werknemers/kandidaten.

Soorten cheques

- Integriteitsverklaring
- Identiteitsverificatie + biometrie voor digitale onboarding
- Controle op recht om te werken
- PEP-, sanctie- en watchlistcontrole
- Controle op negatieve media-aandacht
- Werkreferentie-CV-controle
- Controle van kwalificaties / diploma-controle
- Kredietcontrole
- Verzoek van het Internationaal Strafregister / VOG 1 2
- Uploaden + Validatie van het Internationale Strafregister / VOG 3
- Adrescontrole
- CV-vergelijking

Werkwijze en verantwoordelijkheden

- Wijs de verantwoordelijkheid voor de screening toe (HR, externe dienstverlener of een combinatie hiervan).
- Definieer de stappen voor screening voorafgaand aan en tijdens de indiensttreding.
- Beschrijf hoe resultaten worden beoordeeld, geïnterpreteerd en veilig worden opgeslagen.

Medewerkerscommunicatie

- Leg het doel van de screening uit aan kandidaten/werknemers.
- Geef duidelijke richtlijnen over toestemming, privacy en gegevensverwerking.
- Vermeld een contactpersoon voor vragen of opmerkingen over de screening.

Besluitvorming

- Definieer hoe de screeningsresultaten van invloed zijn op aanwervingen, promoties of toewijzingen.
- Stel regels op voor het omgaan met afwijkingen of negatieve bevindingen.
- Zorg ervoor dat beslissingen consistent, eerlijk en niet-discriminerend zijn.

Overzicht en updates

- Plan periodieke herzieningen van het beleid in om rekening te houden met wijzigingen in wetgeving, technologie of organisatorische risico's.
- Actualiseer de procedures voor internationale werving, digitale controles en opkomende risicogebieden.

Heeft u hulp of advies nodig bij het opstellen van het screeningsbeleid?

Heinoud en Serhat ondersteunen dagelijks veel HR-professionals bij het background screening. Ze delen graag hun kennis over het opstellen en implementeren van beleid met u. Neem gerust contact met ons op en we helpen u graag de juiste stappen te zetten.

Maak kennis met PESCHECK

De basis leggen voor vertrouwen

Wij zijn PESCHECK®, Europa's vertrouwde aanbieder van background screening, met een sterke dekking in de Benelux en de DACH-regio, met name Nederland en Duitsland. Sinds 2015 helpen we organisaties, van mkb's tot internationale ondernemingen, om zelfverzekerde wervings- en zakelijke beslissingen te nemen door geavanceerde technologie te combineren met lokale expertise.

Onze aanpak levert snelle, betrouwbare en volledig conforme screenings (GDPR, ISO 27001, PI-licentie), die nauwkeurige, bruikbare inzichten bieden om vertrouwen op te bouwen bij het onboarden van medewerkers, het verifiëren van partners of het beveiligen van gevoelige omgevingen zoals hightech, defensie, financiën en consultancy.

Bij PESCHECK geloven we dat vertrouwen groeit door openheid. Onze schaalbare, kandidaatgerichte oplossingen maken verificatie eenvoudig, veilig en efficiënt, waardoor vertrouwen een katalysator voor groei wordt.

Een afspraak inplannen?

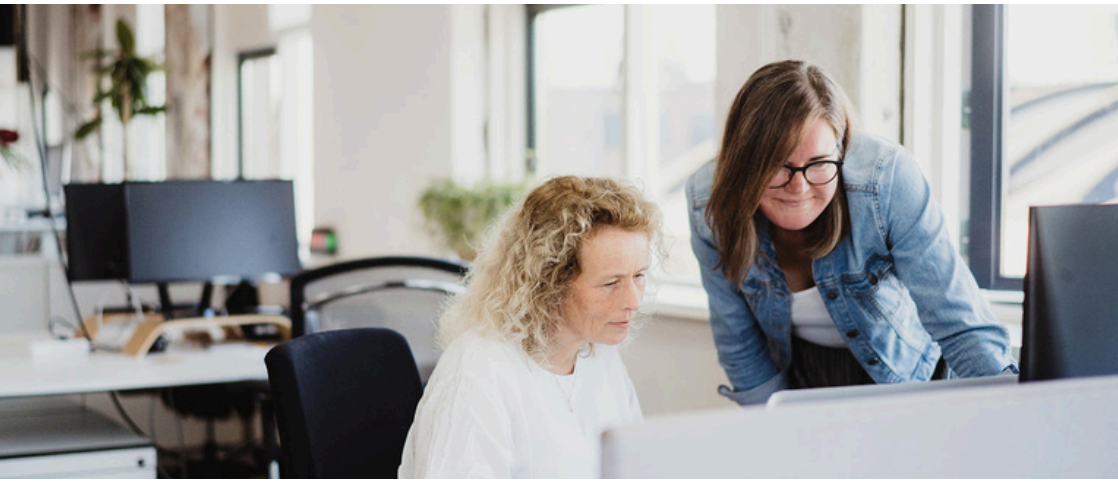
Een kennismakingsgesprek is altijd vrijblijvend en altijd met de bedoeling u te helpen. Wilt u meer weten over het opstellen van een polis of het uitvoeren van een background screening? Neem contact met ons op of boek direct een afspraak via onze website: Book a Demo.

bsi ISO/IEC 27001 Information Security Management CERTIFIED

GDPR

PBSA PROFESSIONAL BACKGROUND SCREENING ASSOCIATION

Ministerie van Justitie en Veiligheid
POB 1551



PESCHECK Definitielijst

Integriteitsverklaring	9 integriteitsgerelateerde vragen of een aanpasbare integriteitsverklaring ter verificatie.
Identiteitsverificatie + biometrie voor digitale onboarding	Verifieert de identiteit van een kandidaat aan de hand van officiële documenten en biometrische gegevens (beschikbaar in 160 landen).
Recht op werk	Bevestigt het wettelijke recht van een kandidaat om in een bepaald land te werken door werkvergunningen, visa of verblijfsstatus te verifiëren.
PEP-, sanctie- en watchlistcontrole	Kandidaatgegevens worden vergeleken met wereldwijde databases van criminelen, terroristen en wetshandhavers om potentiële risico's in te schatten.
Controle op negatieve media-aandacht	Analyseert de online aanwezigheid van de kandidaat, inclusief openbare profielen en relevante verbanden met zoekwoorden of reputatierisico's.
Werkreferentie-CV-controle	Controleert de arbeidsgeschiedenis door contact op te nemen met maximaal 3 werkgevers in de afgelopen 5 jaar, waarbij de functies en werkprestaties worden nagegaan.
Controle van kwalificaties / diploma-controle	Controleert de hoogst behaalde academische kwalificatie van de kandidaat. Nederlandse diploma's worden gecontroleerd via DUO; internationale diploma's doorlopen een breder verificatieproces. Inclusief verificatiekosten tot € 25 incl. btw (of equivalent). Eventuele extra kosten van derden of instellingen kunnen apart in rekening worden gebracht, tenzij schriftelijk anders is overeengekomen.
Kredietcontrole	Biedt een financiële beoordeling van de kandidaat door hun kredietgeschiedenis te controleren, beschikbaar in de EMEA- en APAC-regio's.

Verzoek van het Internationaal Strafregister / VOG 1	Vraagt het internationale strafblad of het Verklaring omtrent Gedrag (VOG) van de kandidaat op en verifieert dit, afhankelijk van de betreffende regio.
Uploaden + Validatie van het Internationale Strafregister / VOG 3	Uploaden + Validatie van het Internationale Strafregister / VOG 3
Adrescontrole	Controleert het huidige of vroegere adres van de kandidaat door de verstrekte gegevens te vergelijken met betrouwbare of officiële bronnen.
CV-vergelijking	De juistheid van het cv van de kandidaat wordt handmatig gecontroleerd door de op het platform verstrekte gegevens te vergelijken met het daadwerkelijk door de kandidaat ingediende CV.

pescheck

Trust grows in the light of openness

pescheck

Headquarters
Capitool 10, 7521 PL
Enschede, Netherlands
(0)85 060 8999

Germany Office
Franz-Joseph-Str. 11
80801 Munich
Bavaria, Germany

Follow Us
X
Facebook
LinkedIn