



Samenvatting

1 Inleiding en aanleiding van het onderzoek

De openbaarheid van persoonsgegevens in openbare registers staat onder toenemende druk in het digitale tijdperk. Waar vroeger de fysieke toegankelijkheid van informatie een natuurlijke bescherming bood, hebben ontwikkelingen op het gebied van digitalisering, automatisering en kunstmatige intelligentie deze barrières grotendeels weggenomen, waardoor persoonsgegevens gemakkelijker te verzamelen, combineren en hergebruiken zijn.

Openbare registers gedefinieerd als registers die zijn ingesteld bij of krachtens de wet, en raadpleegbaar zijn voor eenieder (oftewel ongeacht je hoedanigheid of belang), vervullen belangrijke maatschappelijke functies, zoals het waarborgen van rechtszekerheid, transparantie van bestuur en bescherming van economische belangen. De toegenomen toegankelijkheid leidt echter tot spanning tussen deze openbaarheid en het recht op gegevensbescherming.

Deze spanning is verder toegenomen door uitspraken van het Hof van Justitie van de EU, waaronder het zetten van een streep door het openbare karakter van het UBO-register, en door zorgen geuit door de Autoriteit Persoonsgegevens (AP) en registerbeheerders over misbruikrisico's, variërend van identiteitsfraude tot intimidatie.

In reactie op deze zorgen gaf het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) opdracht voor dit onderzoek (projectnummer 3457). Het doel was om de openbaarheid van persoonsgegevens in dertien specifieke openbare registers te toetsen aan het Europese gegevensbeschermingsrecht en om privacybeschermende maatregelen te identificeren die deze registers in overeenstemming kunnen brengen met de regels of toekomstbestendig kunnen maken in het licht van technologische ontwikkelingen.

2 Onderzoeksvraag en methodologie

De centrale vraag in dit onderzoek luidt:

Is de openbaarheid van de persoonsgegevens in de onderzochte openbare registers in overeenstemming met het gegevensbeschermingsrecht? En welke privacybeschermende maatregelen zijn nodig om deze registers in overeenstemming te brengen en/of te houden?

Voor de beantwoording hebben we een toetsingskader ontwikkeld op basis van jurisprudentie en relevante regelgeving, bestaande uit vier kernvragen:

1. **Voorzienbaarheid en voorspelbaarheid:** Is er een duidelijke wettelijke grondslag voor de openbaarheid?
2. **Doelstelling en passendheid:** Dient het register een erkend algemeen belang en is openbaarheid een geschikt middel?
3. **Subsidiariteit:** Zijn er minder ingrijpende alternatieven mogelijk?
4. **Proportionaliteit:** Is de praktische toegankelijkheid evenredig en zijn er voldoende waarborgen?

De onderzoeksaanpak combineert juridisch-dogmatisch onderzoek met praktijk-gerichte methoden. Voor elk register zijn interviews met beheerders afgenomen, is deskresearch uitgevoerd, en zijn waar mogelijk kwantitatieve gegevens over gebruik en toegang verzameld en geanalyseerd. Het onderzoek werd begeleid door een begeleidingscommissie om onder meer de wetenschappelijke kwaliteit te borgen.

3 Hoofdbevindingen uit het onderzoek

Na analyse van de dertien onderzochte registers kan worden geconcludeerd dat twee van de dertien registers in het geheel niet openbaar zouden moeten zijn.

Bij de Lijst vergunninghouders Wpbr ontbreekt de grondslag voor de openbaarheid van het register in het geheel, en bij het Centraal Gezagsregister is deze grondslag er wel, maar blijkt uit het onderzoek onvoldoende dat openbaarheid überhaupt kan bijdragen aan de verwezenlijking van het doel van het register. Daarnaast is tevens niet aangetoond waarom openbaarheid in dit geval een subsidiair middel is en er niet gewerkt zou kunnen worden met beperkte toegang voor vooraf gedefinieerde groepen met een aantoonbaar belang, en gelet op het feit dat het hier gaat om persoonsgegevens van zowel ouders maar juist ook kinderen is de brede toegankelijkheid disproportioneel vanwege de inherente veiligheidsrisico's voor deze kwetsbare groep.

De overige elf registers voldoen grotendeels aan de vereisten die het gegevens-beschermingsrecht stelt aan openbaarmaking, maar schieten op sommige punten (ernstig) tekort. **Bij zeven van de elf overgebleven registers ontbreekt een grondslag voor de openbaarmaking van één of meerdere persoonsgegevens die in het register zijn opgenomen.** Bij alle vier de onderzochte registers binnen het Centraal Insolventieregister (faillissement, surseance, WSNP en WHOA) ontbreekt de grondslag voor de publicatie van bepaalde persoonsgegevens. Voor de WHOA betreft dit zeer beperkte en niet bijzonder gevoelige gegevens. Bij zowel het register van faillissementen als dat van surseance van betaling gaat het echter om de publicatie van faillissementsverslagen die vol persoonsgegevens kunnen staan, ook van gevoeligere aard. Ook bij het WSNP-register ontbreekt in sommige gevallen de grondslag voor de

publicatie van geboorteplaats en woonadres. Voor het Centraal Curatele- en Bewindregister ontbreekt eveneens de grondslag voor openbaarmaking van de geboorteplaats. Bij het Register beëdigde tolken en vertalers (Wbtv-register) lijkt een schakelbepaling te ontbreken, waardoor de publicatie van gegevens op de zogenoemde uitwijklíst juridisch niet is toegestaan. Dit terwijl openbaarmaking wel de bedoeling lijkt te zijn en in de praktijk ook gebeurt.

Bij alle elf van deze overgebleven registers zijn tekortkomingen geconstateerd in de privacybeschermende maatregelen, ook al voldoen zij grotendeels aan de vereisten voor openbaarmaking. Het gaat om het algehele gebrek aan adequate logging van de raadplegingen, maar ook om enkele specifieke aandachtspunten, zoals gebrekkige technische waarborgen tegen bulktoegang, inconsistente toegangsprocedures tussen rechtbanken, het opnemen van onnodige gegevens zoals aanhef of geboorteplaats, onduidelijkheid over gebruikersgroepen en verwarring over het geven van toestemming voor openbaarmaking van sommige gegevens waar deze feitelijk verplicht is en het geen keuze betreft.

4 Toetsingsresultaten per register

Líst vergunninghouders Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr)

Doel en functie: Dit register bevat de namen van organisaties die een vergunning hebben om op te treden als particuliere beveiligingsorganisatie of recherchebureau. Het is bedoeld om derden te informeren over de vergunningsstatus van deze bedrijven.

Conclusie: Niet in overeenstemming met het gegevensbeschermingsrecht.

Kernprobleem: Voor de openbaarmaking ontbreekt een wettelijke grondslag. Hoewel het formeel om bedrijfsnamen gaat, bevatten veel daarvan persoonsgegevens, en zegt het al dan niet hebben van een vergunning ook iets over de natuurlijke persoon achter de onderneming. Het register maakt daarmee ook persoonsgegevens openbaar. Aan de grondslag wordt op dit moment gewerkt, maar deze bestaat nog niet.

Het register vervult een praktische behoefte in de markt. Zodra er een deugdelijke grondslag is gerealiseerd, bevelen wij daarnaast de volgende verbeteringen aan.

Aanbevelingen:

- Beperk de toegankelijkheid van het register door bulkverstrekkingen niet standaard toe te staan, tenzij hiervoor een afzonderlijke en expliciete onderbouwing is opgenomen in de wettelijke grondslag of toelichting daarop.
- Verwijder verouderde pdf-lijsten die nog beschikbaar zijn op de website.
- Formuleer een eenduidig beleid over het (al dan niet) vermelden van adresgegevens.

Nederlands Register Gerechtig Deskundigen (NRGD)

Doel en functie: Het NRGD is een kwaliteitsregister waarin forensische deskundigen worden opgenomen die voldoen aan vastgestelde standaarden. Strafrechtelijke ketenpartners, zoals het OM en de rechterlijke macht, zijn vaak verplicht om deskundigen uit dit register te gebruiken.

Conclusie: Het NRGD is in overeenstemming met het gegevensbeschermingsrecht, maar er zijn wel enkele aandachtspunten.

Kernpunten: De wettelijke grondslag is duidelijk en de openbaar gemaakte gegevens zijn beperkt van aard. Het NRGD heeft voorts goed het beginsel van minimale gegevensverwerking doorgevoerd als het gaat om de aanduiding van het geslacht van de deskundige: dit wordt *alleen* weergegeven bij een categorie van deskundigen waarbij dit relevant is.

Aandachtspunt: Deskundigen geven bij registratie zogenaamd 'toestemming' voor openbaarmaking, terwijl die verplicht is. Dit kan verwarring wekken over de vrijwilligheid ervan.

Aanbeveling: Schrap de verkapte toestemming voor het openbaar maken van de gegevens. Vervang dit door duidelijke bewoordingen over de gevolgen van registratie van bepaalde gegevens. Met andere woorden: informeer de deskundigen.

Centraal Insolventieregister – Faillissementen

Doel en functie: Het register informeert het publiek over faillissementsprocedures en relevante proceshandelingen, met als doel transparantie te waarborgen voor schuldeisers en het economisch verkeer.

Conclusie: Het CIR – Faillissementen is deels in strijd met het gegevensbeschermingsrecht.

Kernpunten:

- Er ontbreekt een wettelijke grondslag voor de publicatie van faillissementsverslagen.
- Bij natuurlijke personen (zonder onderneming) is de publicatie van onder andere woonadres en geboortedatum mogelijk onevenredig.
- Informatie wordt zowel in het CIR als in de Staatscourant gepubliceerd, zonder duidelijke rechtvaardiging voor deze dubbele verstrekking.

Aanbevelingen:

- Schort publicatie van faillissementsverslagen op totdat er een wettelijke basis is gerealiseerd.
- Stop met de publicatie van gegevens zoals geboortedatum/-plaats en woonadres zolang er niet is voorzien in een adequate grondslag.
- Er dient nader onderzoek te worden uitgevoerd naar de noodzaak om persoonsgegevens in de Staatscourant te publiceren, met bijzondere aandacht voor gevallen van publicatie inzake natuurlijke personen die failliet zijn verklaard.
- De registratie en het gebruik van geboortedatum/-plaats en woonadres kan gehandhaafd blijven en gebruikt worden als verificatievraag. Deze gegevens hoeven echter niet vervolgens ook allemaal getoond te worden in de registratie, met name het adres kan hier achterwege blijven.

Centraal Insolventieregister – Surseance van betaling

Doel en functie: Dit register bevat informatie over surseanceprocedures, waarin aan een ondernemer uitstel van betaling wordt verleend onder toezicht van een bewind-voerder. Het doel is het informeren van schuldeisers en andere belanghebbenden over de status en voortgang van de procedure.

Conclusie: Het CIR – Surseance is deels in strijd met het gegevensbeschermingsrecht.

Kernpunten:

- Voor de publicatie van surseanceverslagen ontbreekt een wettelijke grondslag.

- Bij natuurlijke personen (met onderneming) worden persoonsgegevens openbaar gemaakt — zoals woonadres en geboortedatum — terwijl de evenredigheid daarvan discutabel is.
- Ook hier vindt dubbele publicatie plaats in het CIR én de Staatscourant, zonder onderbouwing van de noodzaak.

Aanbevelingen:

- Staak de publicatie van surseanceverslagen zolang er geen wettelijke grondslag voor bestaat.
- Schrap de publicatie van specifieke persoonsgegevens zoals geboortedatum en woonadres, tenzij hiervoor een expliciete en toereikende grondslag aanwezig is.
- Beperk de openbaarmaking van het woonadres van natuurlijke personen, tenzij dit ook het officiële postadres betreft.
- Bied natuurlijke personen die hun onderneming vanuit huis voeren de mogelijkheid om een alternatief postadres te registreren.
- Voer een onderzoek uit naar de noodzaak van dubbele publicatie in de Staatscourant en het CIR, met bijzondere aandacht voor de positie van natuurlijke personen.

Centraal Insolventieregister – WSNP (Wet schuldsanering natuurlijke personen)

Doel en functie: Dit register bevat gegevens over personen die zijn toegelaten tot het wettelijke schuldsaneringstraject. De openbaarheid van het register is bedoeld om schuldeisers en andere belanghebbenden te informeren over de status van deze procedure.

Conclusie: Het CIR – WSNP is deels in strijd met het gegevensbeschermingsrecht.

Kernpunt: Bij de openbaarmaking van persoonsgegevens van natuurlijke personen die deelnemen aan de WSNP-procedure ontbreekt in sommige gevallen een duidelijke noodzaak.

Aanbevelingen:

- Schrap het standaard openbaar maken van de geboorteplaats en het woonadres van natuurlijke personen. De registratie daarvan kan gehandhaafd blijven en ook gebruikt worden ten behoeve van het lokaliseren van de specifieke natuurlijk persoon, maar deze gegevens hoeven niet getoond te worden bij raadpleging van het register.

- Er dient een nader onderzoek te worden uitgevoerd naar de noodzaak om persoonsgegevens in de Staatscourant te publiceren, met bijzondere aandacht voor gevallen van schuldsanering.

Centraal Insolventieregister – WHOA (Wet homologatie onderhands akkoord)

Doel en functie: De WHOA-procedure biedt ondernemingen in financiële problemen, met inbegrip van natuurlijke personen die een zelfstandig beroep of bedrijf uitoefenen, de mogelijkheid om buiten faillissement om tot een akkoord met schuldeisers te komen. Het Centraal Insolventieregister maakt meldingen over openbare WHOA-procedures inzichtelijk, onder andere voor schuldeisers, rechtbanken en marktpartijen.

Conclusie: Het CIR – WHOA is in grote lijnen in overeenstemming met het gegevensbeschermingsrecht, met enkele noodzakelijke verbeterpunten.

Kernprobleem: Tot op heden zijn uitsluitend gegevens gepubliceerd over rechts-personen, zoals BV's en NV's. Daarmee zijn de meeste privacyrisico's beperkt. Echter, binnen het register worden ook persoonsgegevens van functionarissen zoals de observator en deskundige gepubliceerd (inclusief naam, adres en telefoonnummer), zonder dat hiervoor een expliciete wettelijke grondslag aanwezig is.

Daarnaast is het volledige WHOA-register zonder drempels toegankelijk via een centrale website, zonder gebruik van verificatievragen of toegangslimieten. Dit maakt bulkverstrekkingen mogelijk en legt druk op de proportionaliteit van de openbaarheid, zeker indien op termijn ook natuurlijke personen (die een zelfstandig beroep of bedrijf uitoefenen) onder de regeling gaan vallen.

Aanbeveling: Tref voorzieningen voor het geval de WHOA ook natuurlijk personen die handelen in zelfstandig beroep of bedrijf gaat bevatten ten aanzien van de toegankelijkheid. Maak het register niet in zijn geheel toegankelijk via de website, maar voer een zoekfunctionaliteit in, voorzien van de nodige waarborgen om bulkverstrekking, of veelvoudige incidentele verstrekkingen, te voorkomen.

Huwelijksgoederenregister (HGR)

Doel en functie: Dit register bevat informatie over huwelijkse voorwaarden, goederenscheidingen en andere afspraken die van invloed zijn op het vermogen tussen (ex-)partners. Het register dient twee doelen: het stelt echtgenoten in staat hun huwelijksvermogensrechtelijke situatie kenbaar te maken aan derden, en beschermt derden tegen de gevolgen van niet-geregistreerde huwelijkse

voorwaarden. Inschrijving is niet verplicht, maar zonder inschrijving kunnen huwelijkse voorwaarden niet tegen onwetende derden worden ingeroepen.

Conclusie: Het huwelijksgoederenregister is in grote lijnen in overeenstemming met het gegevensbeschermingsrecht, maar de effectiviteit van het register staat onder druk.

Kernpunten:

- De openbaarmaking zelf vindt plaats onder voorwaarden: om het register te raadplegen moeten de achternamen van beide partners én de datum van huwelijk of geregistreerd partnerschap worden ingevoerd. Deze verificatie vormt een belangrijke privacybeschermende maatregel. Tegelijkertijd is er kritiek in de literatuur dat juist deze vereiste een te hoge drempel opwerpt, waardoor het register onvoldoende wordt geraadpleegd.
- Ook is onduidelijk wie het register daadwerkelijk raadpleegt: in 2023 werden circa 490.000 verzoeken geregistreerd, maar vanwege het ontbreken van gebruikersinformatie is niet vast te stellen of dit afkomstig is van een brede doelgroep of grotendeels van professionele partijen zoals notarissen.
- Verder biedt het register enkel de mededeling dát huwelijkse voorwaarden zijn geregistreerd; de inhoud is uitsluitend toegankelijk voor een beperkte groep (zoals de betrokkenen, notarissen en bepaalde instanties). Vanuit de literatuur is de vraag opgeworpen of deze beperkte inzage wel voldoet aan de wettelijke bedoelingen, en of deze werkwijze — die met het oog op de AVG is ingevoerd — de effectiviteit van het register niet verder belemmert.

Aanbeveling: Implementeer een systeem waarbij het mogelijk wordt om categorieën van raadplegers te onderscheiden, op basis waarvan de effectiviteit van het register gemeten kan gaan worden.

Boedelregister

Doel en functie: Het boedelregister bevat informatie over boedelbeschikkingen en nalatenschappen. Het register is bedoeld om belanghebbenden, zoals erfgenamen, notarissen of schuldeisers, inzicht te geven in lopende boedel-procedures. De registers worden decentraal gehouden bij de griffies van de rechtbanken.

Conclusie: De openbaarheid van de persoonsgegevens in het boedelregister is grotendeels in overeenstemming met het gegevensbeschermingsrecht. Wel is de wijze van toegang tot het register niet overal conform de wettelijke eisen en ontbreekt uniformiteit tussen rechtbanken.

Kernpunt: Er bestaat een verschil tussen de werkwijze van de verschillende rechtbanken, die niet allemaal in overeenstemming zijn met de wet. Zo verlangt de Rechtbank Amsterdam ten onrechte een kopie van een identiteitsbewijs bij een verzoek om informatie, en vraagt de Rechtbank Noord-Holland naar de reden van raadpleging. Beide praktijken zijn niet in overeenstemming met artikel 7 van het Besluit boedelregister en kunnen een afschrikkend effect hebben, ook op legitieme raadplegers.

Aandachtspunt: De beperkte toegankelijkheid vormt een effectieve waarborg, maar ook een praktische drempel. Voor het gebruiksgemak (en consistentie met andere registers) kan digitalisering worden overwogen, mits onder strikte voorwaarden.

Aanbevelingen:

- Het vereiste van een kopie identiteitsbewijs door de Rechtbank Amsterdam voordat het register geraadpleegd kan worden moet per direct worden geschrapt.
- Het verzoek om opgaaf van redenen voor de aanvraag door de Rechtbank Noord-Holland moet per direct worden gestopt.
- Overweeg om het boedelregister op nationaal niveau te regelen op een wijze gelijk aan het huwelijksgoederenregister, in de vorm van een verwijzindex.
- Zorg voor een uniforme wijze van raadpleging bij de verschillende rechtbanken en de vereisten die daaraan worden gesteld. Evalueer daarbij of de huidige verificatievragen echt nodig zijn of dat ze een onredelijke drempel vormen voor legitieme belanghebbenden.

Centraal Gezagsregister (CGR)

Doel en functie: Het CGR is een openbaar register waarin rechtsfeiten worden vastgelegd omtrent het gezag over minderjarigen in gevallen waarin het gezag niet van rechtswege volgt, zoals bij gezamenlijke gezagsverklaring van ongehuwde ouders of benoeming van een voogd. Het register dient om derden inzicht te geven in wie wettelijk bevoegd is namens een kind op te treden, bijvoorbeeld in situaties rond paspoortaanvragen, medische beslissingen of aansprakelijkheid.

Conclusie: Het Centraal Gezagsregister is niet in overeenstemming met het gegevensbeschermingsrecht.

Kernpunten: De brede openbaarheid van het CGR is onvoldoende onderbouwd, zeker gezien de gevoelige aard van de gegevens over minderjarigen. De actuele gezagsverhoudingen zijn slechts indirect af te leiden, wat de effectiviteit van het register beperkt. Voogdijbenoemingen worden voortijdig openbaar gemaakt, en

de toegangsprocedures verschillen per rechtbank. Dit alles roept ernstige vragen op over de proportionaliteit, subsidiariteit en doelmatigheid.

Aanbevelingen:

- Schrap het openbare karakter van het Centraal Gezagsregister en maak het register alleen raadpleegbaar voor personen met een aantoonbaar legitiem belang. Stel een limitatieve lijst op van partijen waarvoor een dergelijk belang kan worden verondersteld.
- Schrap de onmiddellijke openbaarmaking van voogdijbenoemingen voor na overlijden. Maak deze informatie pas openbaar wanneer ze rechtens relevant wordt.

Register beëdigde tolken en vertalers (Wbtv-register)

Doel en functie: Dit register bevat gegevens van beëdigde tolken en vertalers en is bedoeld om ketenpartners zoals politie, justitie en advocatuur in staat te stellen snel bevoegde professionals te vinden.

Conclusie: Het Wbtv-register is in grote lijnen in overeenstemming met het gegevensbeschermingsrecht, met enkele verbeterpunten.

Kernpunten: Er is geen formele grondslag voor het afwijken van wettelijke publicatievereisten zoals vastgelegd in de Wbtv, ondanks het toepassen van dataminimalisatie. De mogelijkheid tot vrijwillige openbaarmaking van aanvullende persoonsgegevens is juridisch kwetsbaar, omdat de beroepsregistratie verplicht is. Verder ontbreken technische maatregelen zoals logging en toegangscontrole, waardoor misbruik niet kan worden uitgesloten of opgespoord.

Aanbevelingen:

- Maak gebruik van de wettelijke mogelijkheid om via een amvb gegevens af te schermen die nu al feitelijk niet openbaar worden gemaakt.
- Overweeg om door middel van een aanvullende schakelbepaling expliciet duidelijk te maken dat de specifieke regels uit het Besluit beëdigde tolken en vertalers (met name artikel 10), betreffende de aard en omvang van persoonsgegevens die opgenomen en openbaar gemaakt mogen worden, niet alleen gelden voor het hoofdregister, maar ook voor de Uitwijklijst.

Centraal Curatele en Bewindregister (CCBR)

Doel en functie: Het CCBR geeft inzicht in de handelingsbekwaamheid en vertegenwoordigingsbevoegdheid van personen die onder curatele of bewind zijn gesteld, en vermeldt tevens wie als curator of bewindvoerder is aangewezen. Het register is bedoeld om schuldenproblematiek en rechtsonzekerheid bij derden te voorkomen.

Conclusie: Het CCBR is in grote lijnen in overeenstemming met het gegevensbeschermingsrecht, met één expliciete tekortkoming en enkele verbeterpunten.

Kernpunten: De openbaarmaking van de geboorteplaats van de betrokkene heeft geen wettelijke grondslag en is daarom niet verenigbaar met de AVG. Daarnaast zijn de contractuele bewaartermijnen voor afnemers van de Web-service relatief lang, en zijn de algemene voorwaarden van die Webservice niet van toepassing op beschermingsbewind. Tot slot ontbreekt een expliciete juridische motivering voor het verwerken van bijzondere persoonsgegevens bij curatele.

Aanbevelingen:

- Schrap het openbaar maken van de geboorteplaats in het CCBR.
- Pas de voorwaarden van de Webservice aan, zodat deze ook betrekking hebben op beschermingsbewind.
- Verkort de contractuele bewaartermijn voor afnemers van gegevens uit het register na beëindiging van curatele of bewind.
- Leg expliciet vast dat het verwerkingsverbod van artikel 9 lid 1 AVG inzake bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens, wordt doorbroken op grond van artikel 9 lid 2 sub g) AVG jo. art. 1:391 BW.

Nevenbetrekkingenregister rechterlijke organisatie – NERO (rechters)

Doel en functie: Het NERO-register geeft inzicht in nevenbetrekkingen van rechters, met als doel het waarborgen van onafhankelijkheid, onpartijdigheid en transparantie binnen de rechterlijke macht. De openbaarmaking is wettelijk verankerd in de Wvra.

Conclusie: Het NERO is in overeenstemming met het gegevensbeschermingsrecht, met enkele technische en inhoudelijke aandachtspunten.

Kernpunten: De toegankelijkheid is te ruim: het register is in bulk doorzoekbaar zonder beperkingen, wat het risico op misbruik vergroot. Daarnaast is de

toegevoegde waarde van het vermelden van aanhef (mw./dhr.) onvoldoende onderbouwd.

Aanbevelingen:

- Beperk de mogelijkheden tot bulkverstrekking door het verplicht stellen van gerichte zoekopdrachten op naam, waarbij enige foutmarge is toegestaan. Sluit het zoeken enkel op functie of gerecht uit. Dit kan wel worden gebruikt als (niet verplichte) verificatievraag.
- Schrap de aanhef (mw./dhr.), tenzij een functioneel doel kan worden aangetoond.

Nevenbetrokkenregister openbaar ministerie – NEOM (leden van het OM)

Doel en functie: Het NEOM-register is bedoeld om inzicht te bieden in nevenbetrokkeningen van officieren van justitie, ter ondersteuning van transparantie en vertrouwen in de onafhankelijkheid van het OM. Openbaarheid volgt eveneens uit de Wvra.

Conclusie: Het NEOM is niet volledig in overeenstemming met het gegevensbeschermingsrecht. De wettelijke basis is aanwezig, maar de technische implementatie en mate van inhoudelijke openheid ondermijnen de doelstelling van het register.

Kernpunten: Veel nevenfuncties zijn omschreven in vage, generieke termen. Locatiegegevens ontbreken vaak. Bovendien beperkt een technische karakterlimiet de weergave van volledige functiebeschrijvingen. Tegelijkertijd is ook hier sprake van onbeperkte doorzoekbaarheid, met risico op misbruik.

Aanbevelingen:

- Verplicht volledige en specifieke omschrijving van nevenbetrokkeningen en betrokken organisaties, tenzij sprake is van concrete veiligheidsrisico's die een meer terughoudende weergave rechtvaardigen.
- Hef de technische beperking op het aantal weergegeven tekens in de registervermelding op.
- Schrap de aanhef (mw./mevr. en dhr.).
- Beperk de mogelijkheden tot bulkverstrekking door het verplicht stellen van gerichte zoekopdrachten op naam, waarbij enige foutmarge is toegestaan. Sluit het zoeken enkel op functie of gerecht uit. Dit kan wel worden gebruikt als (niet verplichte) verificatievraag.

5 Conclusie en aanbevelingen

Dit onderzoek toont aan dat van de dertien onderzochte registers er twee geheel niet openbaar zouden moeten zijn: de Lijst vergunninghouders Wpbr vanwege het ontbreken van een wettelijke grondslag, en het Centraal Gezagsregister omdat de brede toegankelijkheid onvoldoende is onderbouwd en disproportionele veiligheidsrisico's voor minderjarigen met zich meebrengt. Van de overige elf registers ontbreekt bij zeven registers een grondslag voor de openbaarmaking van bepaalde persoonsgegevens, terwijl alle elf registers tekortkomingen vertonen in privacybeschermende maatregelen.

De openbaarheid van persoonsgegevens in registers blijft alleen verantwoord met meer aandacht voor daadwerkelijk gebruik en praktische toegankelijkheid. Technologische ontwikkelingen maken persoonsgegevens uit openbare bronnen steeds kwetsbaarder voor oneigenlijk gebruik. Het probleem is primair een vraag van toegankelijkheid geworden, niet alleen van openbaarheid. Waar vroeger praktische barrières natuurlijke bescherming boden, kunnen gegevens nu gemakkelijk massaal worden verzameld en gecombineerd.

Het onderzoek identificeert vier categorieën structurele uitdagingen: juridische grondslagen, data-georiënteerde uitdagingen zoals gebrek aan dataminimalisatie en bulktoegangsrisico's, procesgeoriënteerde uitdagingen zoals onvoldoende monitoring van het daadwerkelijke gebruik, en de noodzaak tot nader onderzoek naar de dubbele publicatie in zowel registers als de Staatscourant. Toekomstbestendige registers vereisen regelmatige evaluatie en bijstelling, zowel juridisch als technisch en organisatorisch. Zonder adequaat inzicht in wie de registers raadpleegt, blijft het moeilijk om de effectiviteit en proportionaliteit te beoordelen.

Op basis van dit onderzoek doen we de volgende aanbevelingen, gegroepeerd in vier hoofdcategorieën:

Juridische maatregelen:

- Zorg voor expliciete wettelijke grondslagen voor alle openbaar gemaakte persoonsgegevens waarvoor openbaarheid noodzakelijk is.

Data-georiënteerde maatregelen:¹

- Implementeer gelaagde toegang waar mogelijk, waarbij basisinformatie breed toegankelijk is en detailinformatie beperkt.
- Voorkom bulkverstrekkingen door gerichte zoekopdrachten te vereisen en een standaardprocedure voor legitieme bulkverzoeken in te voeren.
- Beperk de standaardweergave van persoonsgegevens tot wat strikt noodzakelijk is.
- Harmoniseer verificatievragen bij decentraal gehouden registers zoals het boedelregister.

Procesgeoriënteerde maatregelen:²

- Implementeer standaardbeschermingsmaatregelen, zoals rate-limiting en robots.txt.
- Zorg voor systematische logging en monitoring om gebruikspatronen te analyseren.
- Ontwikkel uniforme richtlijnen voor afschermingsmogelijkheden in bijzondere situaties.
- Evalueer periodiek de effectiviteit van registers en het gebruik door beoogde doelgroepen. Faciliteer eenvoudige toegang voor goed identificeerbare doelgroepen, zoals overheidsinstanties en beroepsgroepen.

Verder onderzoek

- Verricht nader onderzoek naar de noodzaak van publicatie van persoonsgegevens in de Staatscourant.

De in dit rapport geboden aanbevelingen vormen een noodzakelijk startpunt voor het aanpakken van de geconstateerde knelpunten. Een voortvarende implementatie is essentieel om de privacyrisico's te beperken zonder de maatschappelijke waarde van deze registers aan te tasten, en om zowel de rechtmatigheid als de effectiviteit voor nu en in de toekomst te waarborgen.

¹ Hierbij wordt aangesloten bij de categorisering zoals uiteengezet in de *Handleiding Privacy by Design* van het ministerie van Justitie en Veiligheid uit 2023, nu overheidsinstanties hiermee al bekend zijn. Het gaat hier om het volgende: 'De data georiënteerde strategieën richten zich op de verwerking van persoonsgegevens zelf en zijn daardoor technisch van aard. De data georiënteerde strategieën betreffen met name technische aspecten van de verwerking van persoonsgegevens' (Bennink & Drukarch 2023, p. 10).

² 'De proces georiënteerde strategieën zijn organisatorische maatregelen. Deze maatregelen zien op de organisatie en de mens daarin en niet op de technische maatregelen die kunnen worden getroffen, bijvoorbeeld het verstrekken van informatie aan betrokkenen' (Bennink & Drukarch 2023, p. 11).