AUTORITEIT
PERSOONSGEGEVENS

Sectorbeeld Arbeid en Sociale Zekerheid

april 2024

Uit dit sectorbeeld komt naar voren dat in de gehele sector Arbeid en sociale zekerheid het gebruik van en experimenteren met algoritmes en artificiële intelligentie (AI) toeneemt. Werkgevers gebruiken algoritmes bijvoorbeeld om werknemers nog nauwer in de gaten te kunnen houden. Ook op andere manieren willen werkgevers hun personeel controleren, zoals met personeelsvolgsystemen en alcohol- en drugstests. Bijvoorbeeld om zo voor een veilige werkomgeving te zorgen. Ook uitkeringsinstanties kunnen een nobel doel hebben, zoals mensen opsporen die een mogelijke uitkering mislopen. Bij al deze verwerkingen van persoonsgegevens is het echter uiterst belangrijk dat organisaties rekening houden met de privacy van de mensen om wie het gaat en dat zij dus – op tijd – nagaan wat er volgens de privacywetgeving wel en niet is toegestaan. De ondernemingsraad en de functionaris gegevensbescherming (FG) spelen hierbij een belangrijke rol.

1. Inleiding: de sector Arbeid en Sociale Zekerheid in beeld

De sector Arbeid bestrijkt alle sectoren in Nederland. Vrijwel iedereen in ons land heeft hiermee te maken. Of dit nu in de detailhandel, de zorg, het onderwijs of de financiële markt is. Zodra een organisatie werknemers heeft, ontkomen zij niet aan de verwerking van hun persoonsgegevens in de werksfeer. En mocht het onverhoopt zo zijn dat iemand niet (meer) kan werken, dan is er het sociale vangnet van Nederland. Uitkeringsinstanties verwerken zo mogelijk nóg meer (bijzondere) persoonsgegevens van mensen dan werkgevers doen.

In dit sectorbeeld komen de sector Arbeid en de sector Sociale zekerheid los van elkaar aan bod. De meeste aandacht gaat hierbij uit naar de sector Arbeid, omdat er in deze sector veel ontwikkelingen plaatsvinden. Bijvoorbeeld op het gebied van algoritmisch management.

We noemen de trends die we als AP waarnemen, wat daarvan de privacy risico's zijn en we geven aanbevelingen om deze risico's tegen te gaan. Daarna volgt een (zelf)reflectie vanuit de sector Arbeid en besteden we aandacht aan relevante nieuwe wet- en regelgeving voor deze sector.

2. Sector Arbeid

2.1 Trends, risico's en aanbevelingen

2.1.1 Gezondheidscontroles op de werkvloer

Trend

Er is een groeiende interesse onder werkgevers om op de hoogte te zijn van de gezondheidstoestand van hun werknemers. Denk hierbij aan het afnemen van een alcohol, drugs- of medicijnentest (ADM-test) aan de poort. Veelal komt deze interesse voort uit de plicht voor werkgevers om een veilige werkomgeving te bieden. Werkgevers willen bijvoorbeeld niet dat werknemers onder invloed van alcohol, drugs of medicijnen werken op een bedrijfsterrein met gevaarlijke (chemische) stoffen.

Voor sommige beroepen is wettelijk geregeld dat een ADM-test is toegestaan.[1] Dit zijn bepaalde beroepen die worden genoemd in de Scheepvaartwet, Spoorwegwet, Wet lokaal spoor en Wet luchtvaart. Bij andere beroepen mag een ADM-test dus niet. Het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) onderzoekt of wijziging van de Arbowet nodig is en of voor meer beroepen een ADM-test mogelijk moet worden gemaakt. Zie verder paragraaf 2.4.1.

Risico

Werkgevers hebben de verplichting om een veilige werkomgeving te bieden, maar meestal is er geen grondslag (wettelijke basis) in de Algemene verordening gegevensbescherming (AVG) voor hen om gegevens over de gezondheid van hun werknemers te verwerken. Het risico bestaat dat werkgevers die besluiten dergelijke persoonsgegevens toch te verwerken, dit onrechtmatig doen.[2] Werkgevers geven vaak aan dat het verwerken van de gezondheidsgegevens van de werknemer mogelijk is, omdat de werknemer hiervoor toestemming heeft gegeven. U dient zich te realiseren dat de grondslag uitdrukkelijke toestemming meestal niet opgaat. Dat komt omdat de hiërarchische verhouding die tussen de werkgever en de werknemer bestaat de vrijwillige (uitdrukkelijke) toestemming van de werknemer nagenoeg onmogelijk maakt. Alleen in zeer bijzondere gevallen kan hiervan wellicht sprake zijn.

Aanbeveling aan werkgevers

Bent u als werkgever van mening dat er gegevens over de gezondheid van werknemers verwerkt moeten worden? Dan kunt u gebruikmaken van de arbodienst of bedrijfsarts. Die zijn bevoegd gezondheidsgegevens van werknemers te verwerken, mits de juiste waarborgen in acht worden genomen.[3]

2.1.2 Personeelsvolgsystemen

Trend

Personeelsvolgsystemen beslaan een heel scala aan digitale toepassingen die werkgevers kunnen gebruiken om werknemers in de gaten te houden en/of te volgen. Hierbij verwerken werkgevers meestal

[1] Zie verder: Controle op alcohol, drugs of medicijnen | Autoriteit Persoonsgegevens

[2] Zie artikel 9, eerste lid, AVG, waarin is bepaald dat het verwerken van persoonsgegevens over gezondheid verboden is. Het eerste lid is echter niet van toepassing wanneer aan een van de voorwaarden van artikel 9, tweede lid, AVG, wordt voldaan.

[3] Zie ook: https://www.autoriteitpersoonsgegevens.nl/actueel/testen-op-alcohol-drugs-of-geneesmiddelen-tijdens-werktijd-alleen-met-wettelijke-regeling

uniek identificerende kenmerken van hun werknemers, ook wel biometrische persoonsgegevens genoemd. Zoals het scannen van vingerafdrukken, gezicht, iris, netvlies, vingerader, handader of oogader om in te loggen. Bovendien worden sensoren op de werkplek gebruikt om het aantal toetsaanslagen te monitoren, sensoren in bedrijfsvoertuigen om routes te monitoren, camera's op de werkplek en het gebruik van een smartwatch om fysieke prestaties te monitoren.[4]

Risico

Hoewel de verscheidene personeelsvolgsystemen in de praktijk wellicht hun nut kunnen bewijzen, is er niet altijd een grondslag voor werkgevers om met deze systemen (bijzondere) persoonsgegevens van hun werknemers te verwerken. Het gebruik van deze systemen op de werkvloer, zeker in samenhang met inzet van AI & algoritmes (zie ook paragraaf 2.3.1), kan onder meer leiden tot een hogere werkdruk onder werknemers, omdat werkgevers hen daarmee nog nauwer, constant en kostenefficiënt in de gaten kunnen houden.

Aanbeveling aan werkgevers

Ga na of er een uitzonderingsgrond is voor het verwerken van bijzondere persoonsgegevens. Bijvoorbeeld of het gebruik van biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden.[5] Verder geldt er vaak een informatieplicht naar werknemers en/of dient u instemming te vragen bij de OR voordat u een systeem invoert op de werkplek.

Aanbeveling aan ondernemingsraden

Maak gebruik van het instemmingsrecht dat u als ondernemingsraad heeft bij het introduceren van personeelsvolgsystemen door de werkgever (artikel 27 lid 1 sub k jo sub l van de Wet op de Ondernemingsraden). Het OR-privacyboekje van de AP kan u hierbij behulpzaam zijn.[6]

2.1.3 AI & Algoritmes op de werkvloer

Trend

Persoonsgegevens bevatten een bron van informatie voor (potentiële) werkgevers. Werkgevers maken meer en meer gebruik van artificiële intelligentie (AI) en algoritmes om bestaande werkprocessen te verbeteren en de productie te verhogen.[7] Ook kunnen werkgevers algoritmes gebruiken om de werving en selectie van potentiële nieuwe medewerkers te vergemakkelijken. Bijvoorbeeld door sollicitanten uit bepaalde postcodegebieden uit te sluiten.[8]

---

[4] Zie onder andere het rapport uit 2020 van het Rathenau Instituut 'Werken op waarde geschat': https://www.rathenau.nl/sites/default/files/2020-04/RAPPORT%20Werken%20op%20waarde%20geschat%20-%20Rathenau%20Instituut%202020.pdf

[5] Zie ook: https://www.autoriteitpersoonsgegevens.nl/actueel/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers
En: Biometrie | Autoriteit Persoonsgegevens

[6] OR-privacyboekje | Autoriteit Persoonsgegevens

[7] Algoritmisch management bijvoorbeeld wordt steeds effectiever dankzij innovaties in AI en het beschikbaar komen van grote hoeveelheden data.

[8] Zie onder andere het rapport van 2 september 2020 van het College voor de Rechten van de Mens: Algoritmes kunnen kans op discriminatie bij sollicitaties vergroten, maar ook verkleinen

Risico
Het gebruik van algoritmes in het sollicitatieproces (pre-employment screening) kan leiden tot discriminatie en profilering.[9] Algoritmes en AI-toepassingen zijn vaak niet transparant en accuraat, wat bijvoorbeeld het risico met zich meebrengt van vooringenomenheid.[10] Doorgaans zullen sollicitanten of werknemers er niet van op de hoogte zijn dat zij aan algoritmes worden onderworpen. Dit schuurt onder andere met het recht op informatie (artikel 13 en 14 AVG) en het recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming (profilering, artikel 22 AVG).

Aanbevelingen aan werkgevers

Als u sollicitanten screent verwerkt u hun persoonsgegevens. Dat betekent dat de AVG van toepassing is. Als werkgever bent u er verantwoordelijk voor dat screening aan alle eisen van de AVG voldoet.[11]

Vraag u als werkgever af of het gebruik van AI of een algoritme in bestaande werkprocessen noodzakelijk is. Zo ja, dan is van belang dat u weet hoe het algoritme is ingericht. En dat u hierover uitleg kunt geven aan uw werknemers.[12]

Wilt u een algoritme gebruiken in een sollicitatieproces? Check dan of het algoritme inhoudelijk is getoetst, vooral op non-discriminatoire en AVG-aspecten. Toetsing maakt de kwaliteit van het algoritme transparant en maakt het uitlegbaar richting sollicitanten. Informeer verder uw sollicitanten naar behoren.

Houd er ook rekening mee dat er nieuwe wet- en regelgeving op komst is: de Platformwerkrichtlijn en de AI-verordening. Zie verder paragraaf 2.4.

De rol van de ondernemingsraad (OR)

Werkgevers verwerken veel persoonsgegevens van hun werknemers. En sommige van die verwerkingen kunnen heel ingrijpend zijn. Het is daarom uiterst belangrijk dat werkgevers rekening houden met de privacy van hun werknemers. En dat hierover wordt gesproken binnen de organisatie. Daarbij speelt de OR een cruciale rol.

De ondernemingsraad is nauw betrokken bij afspraken over de verwerking van persoonsgegevens van personeel en bij personeelsvolgsystemen. De Wet op de Ondernemingsraden (WOR) bepaalt dat de werkgever de OR moet vragen om in te stemmen met regelingen waarvoor persoonsgegevens van werknemers worden verwerkt.[13]

Aanbeveling aan werkgevers

Is er een OR in uw organisatie aanwezig? Dan is het van belang dat de OR voldoende AVG- kennis en -bewustzijn heeft. En dat de OR goed gebruikmaakt van de rechten die de OR kan uitoefenen bij het verwerken van (bijzondere) persoonsgegevens van werknemers door de werkgever. Gebruik bijvoorbeeld het OR-

[9] Dit kan een 'chilling effect' tot gevolg hebben.
[10] Zie ook: Onvoorziene effecten van zelflerende algoritmen.pdf
[11] Zie: https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/screening/voorwaarden-voor-screening
[12] Zie ook: Rapportage AI- & algoritmerisico's Nederland (RAN) - najaar 2023 | Autoriteit Persoonsgegevens
[13] Artikel 27, eerste lid onder k en l. van de Wet op de ondernemingsraden.

privacyboekje van de AP bij het opleiden van nieuwe OR-leden.[14]

2.2 Zelfreflectie vanuit de sector

Het is lastig om over de gehele sector in zijn algemeenheid iets te concluderen over het verwerken van persoonsgegevens van werknemers door werkgevers, aangezien de sector Arbeid alle sectoren beslaat. Daarom volgen nu alleen enkele hoofdwaarnemingen van de AP, die voortkomen uit gesprekken met organisaties, Functionarissen Gegevensbescherming (FGs) en ondernemingsraden, en uit de klachten en tips die de AP heeft ontvangen.

2.2.1 Leiderschap en toezicht

De AP constateert dat er grote verschillen zijn in de privacyvolwassenheid van organisaties.

- Waar de ene organisatie bewust met privacy bezig is en dit (regelmatig) op de agenda van het bestuur staat, is het voor de andere organisatie een 'invulhokje' of nevenbezigheid.
- Opvallend is dat de ene organisatie de FG overal proactief bij betrekt en dat de FG daar optimaal kan functioneren, terwijl dat bij andere organisaties in veel mindere mate of soms helemaal niet het geval is.
- Gebleken is dat een actieve FG doorgaans een positieve invloed heeft op de organisatie, zeker als deze regelmatig verslag uitbrengt in de raad van bestuur en daar goed wordt gehoord. Ook heeft het een positieve uitwerking op OR-leden als de FG af en toe in de OR verschijnt en verslag doet.
- De AP ziet echter dat de FG vaak ook andere taken vervult. Organisaties moeten zich afvragen of de FG dan voldoende tijd heeft om de FG-taken naar behoren te verrichten.

2.2.2 Training en bewustwording/bewustzijn

Training is een belangrijk onderdeel om het privacybewustzijn van medewerkers te vergroten.

- Veel organisaties trainen hun medewerkers regelmatig en bieden hiertoe verschillende mogelijkheden via intranet, bijvoorbeeld in quizvorm. Andere organisaties besteden er echter weinig aandacht aan. Dat kan bijvoorbeeld datalekken tot gevolg hebben.
- Sommige ondernemingsraden zijn niet goed op de hoogte van de basisbeginselen van de AVG en zijn zich er niet van bewust dat het nodig is een cursus over het beschermen van persoonsgegevens te volgen. Hierdoor kunnen zij hun rechten op grond van de WOR niet goed uitoefenen.[15] Er zijn echter ook ondernemingsraden die gegevensbescherming binnen de organisatie hoog op de agenda hebben staan, en die zich regelmatig laten (bij)scholen. Dan is er sprake van maximale bewustwording.

2.2.3 Monitoren en verifiëren

Er zijn ondernemingsraden die goed monitoren met welke privacygerelateerde projecten of onderwerpen hun werkgever bezig is. Zij maken goed gebruik van hun instemmings- en adviesrecht. En ze hebben regelmatig contact met de FG. Opvallend is dat de FG in zo'n organisatie vaak een stevige positie heeft, onafhankelijk kan werken en goed toezicht kan houden.

[14] OR-privacyboekje | Autoriteit Persoonsgegevens

[15] Artikel 27, eerste lid onder k en l. van de Wet op de ondernemingsraden.

2.3 Bij de AP ingediende klachten en tips
Deze lijst toont over welke onderwerpen binnen de sector Arbeid de AP in de periode januari t/m juli 2023 klachten en tips heeft ontvangen en in welke aantallen. Een klacht gaat altijd over een inbreuk op iemands eigen persoonsgegevens. Een tip kan ook anoniem worden ingediend, over iemand anders gaan of algemeen van aard zijn.

Doorgeven persoonsgegevens aan derden	19
Rechten van betrokkene	18
Onrechtmatige verwerking	12
Beveiliging	6
Verwerken bijzondere persoonsgegevens	4
Bovenmatige verwerking	4
Cameratoezicht	4
Beeldmateriaal online	3
Niet gemelde datalekken	3
Arbeidsrelatie/solliciteren	2
Verwerking kopie ID/BSN	2
Direct marketing (post, telefoon, e-mail)	2
Totaal	77

In de periode van januari t/m juli 2023 zijn in totaal 1600 klachten en tips binnengekomen bij de AP. Het onderdeel van de sector Arbeid is dus een kleine 5%.

2.4 Nieuwe wettelijke regels in de sector

2.4.1 Wettelijke basis alcohol- en drugstesten
Sinds medio 2020 is een wijziging van de Arbeidsomstandighedenwet (Arbowet) in voorbereiding. Hiermee wordt een wettelijke basis gecreëerd om ADM-testen af te nemen. Hiervoor gelden dan wel strenge voorwaarden en het gaat ook alleen om specifieke functies die cruciaal zijn voor de veiligheid binnen Brzo[16]-bedrijven. Daarnaast wordt onderzocht of er ook een wettelijke basis kan worden gecreëerd voor andere specifieke functies met een groot veiligheidsrisico. Tot slot wordt ingezet op het versterken van deugdelijk ADM-beleid binnen ondernemingen.[17]

Op 10 mei 2022 heeft de minister van Sociale Zaken en Werkgelegenheid (SZW) de Tweede Kamer geïnformeerd.[18] In het najaar van 2023 heeft het ministerie van SZW bekendgemaakt dat er in de eerste helft van 2024 een breed onderzoek zal worden gedaan. In kaart moet worden gebracht welke problemen er bestaan en of nieuwe wetgeving die problemen eventueel kan oplossen. In de tweede helft van 2024 komt het ministerie met meer informatie.

2.4.2 Initiatiefwetsvoorstel verantwoord en duurzaam internationaal ondernemen
Het wetsvoorstel introduceert een algemene zorgplicht voor ondernemingen bij mogelijke nadelige gevolgen van hun activiteiten voor mensenrechten, arbeidsrechten of het milieu in een land buiten

[16] Bedrijven die vallen onder het Besluit risico's zware ongevallen 2015.
[17] Kamerbrief voortgang alcohol- en drugstesten op de werkvloer | Kamerstuk | Rijksoverheid.nl
[18] https://open.overheid.nl/documenten/ronl-38a66a26b4ee642bbed637575b5eef13db6463ee/pdf

Nederland. En voor een specifieke categorie van ondernemingen het principe van gepaste zorgvuldigheid in productieketens, zoals dat is neergelegd in de OESO-richtlijnen voor multinationale ondernemingen.[19]

2.4.3 Platformwerkrichtlijn

De Platformwerkrichtlijn gaat over arbeidsplatformen en mensen die via een platform werken, al dan niet als werknemer. De richtlijn geeft nieuwe regels voor geautomatiseerde monitoring en besluitvorming door platformen. Een van de doelen van de richtlijn is om duidelijkheid te scheppen over de arbeidsstatus van mensen die platformwerk verrichten. Een heet hangijzer in de onderhandelingen is de werking van het 'rechtsvermoeden' van een arbeidsovereenkomst dat met de richtlijn wordt gecreëerd.[20]

Daarnaast heeft de richtlijn tot doel om de transparantie, eerlijkheid en verantwoordelijkheid te vergroten bij het gebruik van geautomatiseerde monitorings- en besluitvormingssystemen van platformen.[21] Daartoe wordt in de richtlijn de verwerking van persoonsgegevens door platformen nader geregeld, maar wordt ook de geautomatiseerde monitoring en besluitvorming door die platformen gereguleerd.

Het Belgische voorzitterschap van de Raad van de EU, de Europese Commissie en het Europese Parlement (EP) hebben tijdens de triloog van 8 februari 2024 een nieuw voorlopig akkoord bereikt over het Richtlijnvoorstel. Lidstaten zijn hierover geïnformeerd in het Coreper van 9 februari 2024. Als de Platformwerkrichtlijn uiteindelijk van kracht wordt, zal deze binnen 2 jaar in Nederlandse wetgeving geïmplementeerd moeten worden.

2.4.4 AI-Verordening

In de AI-verordening worden AI-systemen in de werkgelegenheid, het personeelsbeheer en de toegang tot zelfstandige arbeid (inclusief AI-systemen voor werving, selectie en screening) aangemerkt als hoog risico. De AI-verordening zal onder meer van toepassing zijn op AI-systemen om beslissingen te nemen over mensen in arbeidsrelaties, bijvoorbeeld voor promotie of beëindiging van een arbeidsverband, het toekennen van taken en het monitoren van prestaties.[22] Zodra de verordening is goedgekeurd, heeft deze directe werking. Dat wil zeggen dat de verordening ingevolge artikel 288 VWEU een algemene strekking heeft, verbindend is in alle onderdelen en rechtstreeks toepasselijk is in elke lidstaat.

3. Sociale Zekerheid

3.1 Trends, risico's en aanbevelingen

Trend

In de sociale verzekeringssector/sociale domein verwerken verschillende overheidsorganisaties grote hoeveelheden (bijzondere) persoonsgegevens. Deze partijen willen vaak meer met deze gegevens doen dan wat tot hun wettelijke taken behoort. Zij hebben zich ten doel gesteld de cliënt zo goed mogelijk van dienst te zijn. Daarbij gaat het bijvoorbeeld om het koppelen/uitwisselen van persoonsgegevens om

[19] Zie voor behandeling wetsontwerp:
https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2021Z04465&dossier=35761
[20] Hoofdstuk II van de conceptrichtlijn.
[21] Artikel 1, onder 1c Raadstekst.
[22] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

burgers die een mogelijke uitkering mislopen op te sporen. Het delen en koppelen van gegevens wordt vaak gedaan wordt vanuit de juiste intenties. Hiervoor moet echter wel een juridische grondslag zijn. In de politiek en media is hiervoor veel aandacht als het gaat om het bestrijden van armoede.

Een ontwikkeling die de AP binnen het sociale domein signaleert is dat overheidsorganisaties gebruik maken van algoritmes om bijvoorbeeld burgers met een bijstandsuitkering te profileren op frauderisico. Mensen met een hoger fraudeprofiel kunnen na profilering rekenen op intensievere controle door hun gemeente. Uit recent AP onderzoek blijkt dat gemeenten de eisen die de AVG stelt aan algoritmische gegevensverwerking niet scherp in beeld hebben. Zo mogen gemeenten geen bijzondere persoonsgegevens verwerken, tenzij daarvoor een uitzondering geldt. En profilering op basis van de woonwijk waar iemand woont, of op basis van woonvorm en daarmee indirect op 'ras' (zoals het College voor de Rechten van de Mens oordeelde in de zaak over woonwagenbewoners), kan leiden tot discriminatie van mensen.

Ook experimenteert de sociale verzekeringssector/sociale domein met artificial intelligence (AI).

Risico

Mensen die zijn aangewezen op sociale zekerheid, zijn meestal verplicht hun gegevens af te staan. Vaak gaat het daarbij ook om gevoelige persoonsgegevens. Van vrijwillig gegeven toestemming voor het verwerken van hun persoonsgegevens is niet gauw sprake, omdat mensen afhankelijk zijn van een uitkeringsinstantie. Het risico bestaat dat door koppelingen/uitwisselingen zoals hierboven beschreven, de grenzen worden overschreden van wat mag op grond van de AVG en aanverwante wet- en regelgeving. Denk hierbij aan vertroebeling van de doelbinding, het ontbreken van een grondslag en het te breed uitleggen van het juridische beginsel van noodzakelijkheid.

Het werken met algoritmes en experimenteren met AI wordt vaak van te voren niet naar behoren doordacht.[23] Dit kan bijvoorbeeld komen omdat de juiste mensen niet aan tafel zitten, zoals de FG. Dan kan achteraf blijken dat zo'n algoritme niet AVG-proof is.

Aanbevelingen aan de sociale verzekeringssector/sociale domein

1. Het koppelen/uitwisselen van persoonsgegevens om bijvoorbeeld burgers op te sporen die een mogelijke uitkering mislopen, kan slechts plaatsvinden als hiervoor een juridische grondslag is. Ook al is de doelstelling nog zo nobel. Onderzoek uitgebreid met de verschillende partijen welke juridische mogelijkheden er zijn en vraag eventueel guidance aan de AP. Gaat het om een structureel probleem, breng dit dan onder de aandacht van de wetgever en vraag de wetgever een grondslag te creëren.
2. Betrek het beschermen van persoonsgegevens en vooral ook de FG van meet af aan bij een nieuw (technologisch) project waarin persoonsgegevens worden verwerkt. En laat de FG, voor zover nodig, aangehaakt blijven in het hele traject. Maak goed gebruik van een data protection impact assessment (DPIA), ook wel 'gegevensbeschermingseffectbeoordeling' genoemd, en raadpleeg zo nodig de AP.[24] Toets vooraf nadrukkelijk of de verwerking noodzakelijk is. Is er een grondslag waarop u deze verwerking kunt baseren? Is er sprake van transparantie, zeker als het om een

[23] Denk aan de inzet van algoritmes om fraude op te sporen. Daaraan zijn heel veel risico's verbonden (bias in datasets, discriminatoire effecten).
[24] Voorafgaande raadpleging op grond van artikel 36 AVG.

algoritme gaat?[25] Worden er niet teveel persoonsgegevens verwerkt? Door het van meet af aan toetsen en toepassen van alle relevante AVG-beginselen kunt u een project privacyproof maken.

3. Draag zorg voor een deugdelijk beveiligingsbeleid en voorkom datalekken. Zijn er voldoende technologische en organisatorische maatregelen waarmee de bescherming van persoonsgegevens wordt gewaarborgd? Evident is dat het zeer onwenselijk is als gevoelige persoonsgegevens van uitkeringsgerechtigden op straat komen te liggen. Uitkeringsinstanties moeten dus extra goed op hun hoede zijn om dit te voorkomen. Een deugdelijk beveiligingsbeleid draagt hieraan bij. Hierbij hoort ook regelmatige training van werknemers, bijvoorbeeld via intranet, om hun awareness te vergroten. Zo kunt u datalekken zoveel mogelijk voorkomen.

[25] Overheidsorganen kunnen hierbij (ook) gebruikmaken van een IAMA. Zie: https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf