Internetconsultatie Verzamelwet gegevensbescherming

Graag maken we gebruik van de mogelijkheid om te reageren op het concept wetsvoorstel Verzamelwet gegevensbescherming. In deze reactie gaan we graag in op de volgende vier punten:

1. Biometrie: duidelijkheid en rechtszekerheid (art. 29 UAVG)
2. Melding bij AP en betrokkene bij buiten toepassing laten rechten en plichten (art. 41 UAVG)
3. Toestemming jongeren (art. 5 UAVG)
4. Wegnemen van knelpunten uit de praktijk

1. Biometrie: duidelijkheid en rechtszekerheid (art. 29 UAVG)

Artikel 9(2)(g) AVG stelt dat er sprake moet zijn van een 'zwaarwegend algemeen belang', om biometrische gegevens te verwerken voor de unieke identificatie van een persoon. Het is niet de bedoeling van de wetgever om met voorliggende aanpassing van de UAVG de ruimte in te perken voor het gebruik van innovatieve toepassingen op basis van biometrische gegevens om de beveiliging en authenticatie te verbeteren.

De praktijk heeft echter wel behoefte aan nadere duidelijkheid en rechtszekerheid, in welke gevallen de uitzondering kan worden toegepast. Gewenst is dat de MvT behalve het voorbeeld van de kerncentrale ook andere voorbeelden geeft van gevallen waarop deze uitzondering kan worden toegepast. Dit is niet iets om over te laten aan de toezichthouder, maar vereist afweging vanuit het beleid. Wij denken aan de volgende toepassingen waar gebruik van biometrie, onder de nodige voorwaarden uiteraard, toegelaten zou moeten zijn, welke in de MvT verduidelijkt zou moeten worden:

- Controle op toegangsbevoegdheden op vitale, gevoelige of gevaarlijke locaties, zoals voor bedrijven en/of diensten uit de vitale infrastructuur[1] (zoals kerncentrale, telecomcentrum, beheercentrum energie-infra), aanbieders van essentiële diensten en voor digitale dienstverleners (NIS-Richtlijn), bedrijven of gebieden met veiligheidsrisico's zoals BRZO-bedrijven en lucht- en zeehavens.
- Beveiliging van vertrouwelijke informatie (waaronder persoonsgegevens) alsmede het netwerk van de organisatie. Dit gaat bijvoorbeeld over het gebruik van biometrie bij Windows Hello en biometrische toegang tot mobiele telefoons (vingerafdruk of gezichtsherkenning). Zonder deze uitzondering zou het gebruik van biometrische toegang tot laptops of mobiele telefoons van de zaak verboden zijn.
- Beveiliging van supermarkten en andere winkels. Zo heeft bijvoorbeeld 66% van de supermarkten te maken met agressie en geweld, 61% met rondreizende bendes en 40% met vernielingen. Supermarkten zijn cruciale locaties van en in de samenleving, waar iedereen samenkomt en waar veiligheid een bijzondere urgentie moet hebben. Het beveiligen van een supermarkt tegen onrechtmatige toegang door onbevoegden moet dus kwalificeren als een zwaarwegend algemeen belang.
- Controle op identiteit in het kader van de Wet Ketenaansprakelijkheid (bijv. om te voorkomen dat een ingeleende werknemer zich bijvoorbeeld laat vervangen door zijn broer of neef).

[1] https://www nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

- Beveiliging van geld of andere waardevolle zaken (bijv. een biometrisch kassasysteem om bijv. overvallen te voorkomen of stadionverboden te handhaven).

Tussen de genoemde garage en kerncentrale zit een heleboel grijs. Het is tenminste noodzakelijk om niet op voorhand de mogelijkheid van de ontwikkeling van “best practices” te verbieden, maar veeleer te ondersteunen Dat zou bedrijven ondersteunen zowel in de rechtmatige invulling van een belangrijk maatschappelijk belang, maar ook in de doorontwikkeling van privacy by design.

2. Melding bij AP en betrokkene bij buiten toepassing laten rechten en plichten (art. 41 UAVG)

Artikel 41 UAVG creëert de mogelijkheid voor een verwerkingsverantwoordelijke om bepaalde rechten en plichten buiten toepassing te laten, zoals het recht op inzage. Het voorstel is om hieraan twee vereisten te verbinden, namelijk het met een dragende onderbouwing voorzien informeren van de betrokkene en het gelijktijdig informeren van de AP.
Wij hebben bezwaren tegen deze beide verplichtingen:

<u>Informeren betrokkene</u>

De toepassing van dit artikel is met name relevant als de verwerkingsverantwoordelijke de verwerking van bepaalde persoonsgegevens (tijdelijk) geheim wil of moet houden. Te denken valt bijvoorbeeld aan een fraude onderzoek, waarbij de gegevens(verwerking) conform art. 41 lid 1 sub i UAVG in het belang van de zaak (tijdelijk) geheim moet worden gehouden jegens de betrokkene (vergelijk ook art. 14 lid 5 sub b AVG). De gevallen genoemd in artikel 41 zijn bijna zonder uitzondering gevallen waarin de zwaarwichtigheid van het doel een belangrijke rol speelt (nationale veiligheid, opsporing van strafbare feiten, etc.).

Het moeten informeren van de betrokkene over de gronden van de weigering, zoals het wetsvoorstel voorstelt, past daar niet bij. Sterker, het kan juist de voortgang van bijvoorbeeld het fraude onderzoek belemmeren wanneer de persoon daarover geïnformeerd moet worden.

<u>Informeren Autoriteit Persoonsgegevens</u>

Ook de notificatie richting de AP is problematisch, om verschillende redenen. Ten eerst is dit een zware verplichting. Immers, een gemiddelde verwerkingsverantwoordelijke of verwerker heeft vrij regelmatig te maken met verzoeken van betrokkenen, zoals inzageverzoeken, waarbij het ook regelmatig voorkomt dat dat recht enigszins moet worden beperkt, bijvoorbeeld omdat de rechten en vrijheden van anderen in het geding komen als volledige inzage zou worden gegeven (zie het huidige artikel 41, eerste lid, sub i). Dat de AP iedere keer van een dergelijke beperking op de hoogte moet worden gesteld, gaat ons inziens te ver. Het brengt extra (en onnodige) administratieve lasten met zich mee. Daarnaast bestaat er bij iedere notificatie een risico dat de AP (in het ergste geval) naar aanleiding daarvan besluit een onderzoek te starten en zelfs een boete op te leggen. De notificatie zou in dat geval dus kunnen leiden tot onbedoelde zelfincriminatie. De notificatieplicht is dan ook een te zwaar middel, als we het hebben over rechten van betrokkenen die volgens de AVG niet onder alle omstandigheden absoluut dienen te zijn.

Maar het grootste probleem is wellicht nog wel dat geen rekening wordt gehouden met partijen die in meerdere EU-lidstaten gevestigd zijn en een leidende toezichthouder hebben in een andere EU-lidstaat dan Nederland.

Omdat een dergelijke partij een vestiging heeft in Nederland, zal in het algemeen de UAVG van toepassing zijn.

Tegelijkertijd dient een dergelijke partij te profiteren van het one stop shop mechanisme onder de AVG, waar (onder andere) uit voortvloeit dat de leidende toezichthouder de enige gesprekspartner dient te zijn (zie artikel 56, zesde lid van de AVG). Dit brengt een dergelijke partij in de lastige positie. Zij zal namelijk netjes aan artikel 41 van de UAVG willen voldoen en derhalve de AP een afschrift willen sturen, terwijl dat zou betekenen dat zij niet kan profiteren van het one stop mechanisme. Als het afschrift naar de leidende toezichthouder zou worden gestuurd, is het gevolg dat de leidende toezichthouder in een andere EU-lidstaat met een Nederlandsrechtelijke verplichting te maken krijgt, hetgeen niet wenselijk is. Het lijkt erop alsof in het voorstel niet voldoende is nagedacht over deze internationale dimensie en de potentiële consequenties van het voorstel in dat kader. Hier zou in ieder geval opheldering over moeten komen.

3. Toestemming jongeren (art. 5 UAVG)

Het is positief dat in het voorstel erkend wordt dat jongeren niet afhankelijk moeten zijn van een wettelijke vertegenwoordiger om een einde te kunnen maken aan een verwerking van zijn eígen persoonsgegevens en zelf de rechten (hoofdstuk III van de AVG) uit kunnen oefenen. We vragen ons daarbij wel af of het voor de uniformiteit in de interne markt niet duidelijker is om de leeftijdsgrens van 12 jaar en ouder aan te houden in plaats van 11 jaar en ouder.

We zouden ook graag zien dat jongeren van 13, 14 en 15 jaar voor de initiële toestemming niet afhankelijk zijn van hun vertegenwoordiger. Jongeren hebben recht op privacy en op extra bescherming bij het gebruik van diensten waarbij gegevensverwerking aan de orde is. Dit wordt ons inziens niet bereikt door de leeftijdsgrens voor het geven van de initiële toestemming op 16 jaar te zetten. We mogen immers niet de ogen sluiten voor de (mogelijke) praktijk waarbij jongeren (in de puberleeftijd) - uit privacy overwegingen en drang naar zelfstandigheid - er eerder voor kiezen om een andere geboortedatum in te vullen in plaats van de benodigde toestemming te vragen van hun vertegenwoordiger, waardoor deze jongeren de waarborgen mislopen die zijn ingesteld om hen als jongere te beschermen.

We steunen dan ook nog steeds de brief van het Safer Internet Center waarin gepleit wordt voor het verlagen van de leeftijdsgrens voor toestemming van het verwerken van persoonsgegevens van 16 naar 13 jaar[2].

Daarnaast speelt het gebrek aan harmoniserende werking binnen de Europese markt een rol. Een uniforme leeftijdsgrens voor het geven en intrekken van toestemming en het uitoefenen van de rechten van een betrokkene maakt het voor zowel (mkb)bedrijven als voor jongeren en hun vertegenwoordigers overzichtelijker en werkbaarder in deze wereld van grensoverschrijdend dataverkeer. Naast een aanpassing van dit wetsvoorstel, zou het daarom goed zijn als in Europa één uniforme leeftijdsgrens van 13 jaar wordt vastgesteld.

4. Wegnemen knelpunten uit de praktijk

Tijdens de behandeling van de Uitvoeringswet AVG (UAVG) heeft minister Dekker de Tweede Kamer toegezegd om ervaringen van stakeholders met deze wet te onderzoeken.

[2] https://ecp nl/wp-content/uploads/2017/10/Brandbrief-Artikel-8-AVG-brengt-online-privacy-van-onze-jeugd-in-gevaar.pdf

En waar problemen rijzen deze zo mogelijk ook op te lossen. Via onze brief van 19 september 2018, hebben we de minister geïnformeerd over diverse knelpunten uit de praktijk.
Wij moeten helaas constateren dat een groot deel van deze knelpunten nog niet is opgelost, ook niet in onderhavig wetsvoorstel. In de bijlage vindt u deze brief.

Graag zouden wij vernemen hoe de minister denkt deze knelpunten, eventueel in samenwerking met andere departementen weg te nemen. Ook geven wij in overweging om deze wetswijziging te benutten om die knelpunten weg te nemen.

Bijlage:
Brief “inventarisatie knelpunten UAVG” van VNO-NCW en MKB-Nederland aan minister Dekker, d.d. 19 september 2018.

_____

[redacted]

VNO NCW

MKB Nederland

Zijne Excellentie

Minister voor Rechtsbescherming
Ministerie van Justitie en Veiligheid
Turfmarkt 147
2511 DP DEN HAAG

Briefnummer
[redacted]

Onderwerp
Inventarisatie knelpunten UAVG

Den Haag
19 september 2018

Telefoonnummer
[redacted]

E-mail
[redacted]

Excellentie,

Tijdens de behandeling van de Uitvoeringswet AVG (UAVG) heeft u de Tweede Kamer toegezegd om ervaringen van stakeholders met deze wet nader te onderzoeken. En waar problemen rijzen deze zo mogelijk ook op te lossen. VNO-NCW en MKB-Nederland brengen u in de bijlage graag de voornaamste van deze problemen onder de aandacht waar ondernemers dagelijks tegenaan lopen[1].

Ondernemers in de knel

Onderliggend probleem bij een aantal van de knelpunten is, dat de Autoriteit Persoonsgegevens (AP) ruimte voor uitvoering van werkgeversverantwoordelijkheden drastisch beperkt. Dat brengt ondernemers in een onwenselijke spagaat.

Werkgevers hebben in hun dagelijks werk namelijk rekening te houden met allerlei maatschappelijke belangen zoals re-integratie, openbare orde, veiligheid en gezondheid van medewerkers, arbeidsparticipatie, informatie-uitwisseling over buitenlandse werknemers in het kader van de werkvergunning, het tegengaan van fraude etc. Ondernemers zijn hier veelal bij wet verantwoordelijk voor.

Vanwege die verantwoordelijkheid moeten ondernemers ook ruimte hebben om invulling te geven aan deze maatschappelijke belangen. Daarvoor moeten zij persoonsgegevens gebruiken, soms ook bijzondere gegevens zoals medische gegevens. De (U)AVG geeft hier op hoofdlijnen ruimte voor, maar de AP kleurt deze ruimte steeds vaker uitermate restrictief in middels beleidsregels of besluiten (*soft law*).

[1] Over problemen met de AVG zelf - punten die in Brussel bij de evaluatie van de AVG in mei 2020 zouden moeten worden opgelost - sturen wij u graag binnen afzienbare termijn een aparte brief.

Gevolg is dat ondernemers in een onmogelijke spagaat komen: zij kunnen "kiezen" tussen sancties van de AP of van één van de toezichthouders van de vakdepartementen.

Aanpassingen in wetgeving of nadere uitleg wetgever noodzakelijk

Om deze knelpunten te verhelpen zijn zowel wettelijke aanpassingen nodig als een andere invulling van het toezicht door de AP. Belangrijke oplossing is het creëren van duidelijke(r) wettelijke grondslagen voor het verwerken van persoonsgegevens voor specifieke publieke belangen: de AVG geeft de nationale wetgever die ruimte ook. Dat geldt niet alleen voor hierna genoemde knelpunten, maar ook bij nieuwe wetgeving, zodat dergelijke problemen niet steeds opnieuw ontstaan.

Omdat de knelpunten beleidsinhoudelijk niet alleen op het terrein van Justitie en Veiligheid liggen, maar ook het ministerie van SZW en Financiën raken, is het belangrijk dat deze departementen samen met u tot werkbare oplossingen komen. Uiteraard denken wij daar de komende periode graag over mee.

Hoogachtend,

[redacted]

voorzitter VNO-NCW

[redacted]

voorzitter MKB-Nederland

Bijlage 1: knelpunten bedrijfsleven (U)AVG en oplossingsrichtingen

Belangrijkste knelpunten en oplossingsrichtingen
Hieronder vindt u de belangrijkste aandachtspunten voor VNO-NCW en MKB-Nederland beschreven, met per punt een mogelijke oplossingsrichting. Graag gaan wij daarover met u in gesprek. Tevens voegen we het pamflet *'Een knellend probleem: privacy versus goed werkgeverschap'* bij, met een volledig overzicht van alle specifieke deelproblemen op het vlak van sociale wetgevingen privacy (bijlage 2).

1. <u>Re-integratie van zieke werknemers (tot 6 wkn.)</u>
   De werkgever is vanaf de eerste ziekmelding verantwoordelijk voor de re-integratie van een zieke werknemer. De Wet verbetering poortwachter vraagt werknemer en werkgever samen de re-integratie vorm te geven, zonder medicalisering door een traject via de bedrijfsarts. Doet hij dat niet goed, dan kan een boete van het UWV volgen. De wet staat werkgevers dan ook expliciet toe om gezondheidsgegevens ten behoeve van re-integratie te verwerken. De Autoriteit Persoonsgegevens (AP) echter heeft middels beleidsregels verboden om zonder tussenkomst van een bedrijfsarts naar 'functionele mogelijkheden en beperkingen' te vragen (of iemand nog kan zitten, staan, of zich kan concentreren). Dit is echter belangrijke informatie die bij eerste tekenen van mogelijke uitval nodig zijn om de werknemer goed te kunnen begeleiden. Dat hindert een optimale re-integratie. Een gerelateerd knelpunt is dat de AP snel van mening is dat bepaalde gegevens of de uitwisseling ervan tussen partijen 'niet strikt noodzakelijk' is. Hoewel de UAVG het gebruik van 'noodzakelijke' gegevens toestaat, leidt deze strikte uitleg tot zeer inefficiënte processen. Enkele afgeleide knelpunten op het gebied van re-integratie vindt u in het meegezonden pamflet (bijlage).

   Mogelijke oplossingen:
   - De UAVG staat werkgevers toe (art 30, lid 1 sub b) om gezondheidsgegevens te verwerken voor zover noodzakelijk voor re-integratie. Wel moeten gegevens onder geheimhouding worden verwerkt. De AP vult dit nauw in (altijd via bedrijfsarts) waarmee zij de facto artikel 30 onklaar maakt. Bij AmvB kan geregeld worden dat een HRM-medewerker of leidinggevende ook zonder tussenkomst van de bedrijfsarts de gegevens rond re-integratie mag verwerken, mits geheimhouding is geborgd bijvoorbeeld contractueel.
   - Daarnaast kan de wetgever verduidelijken welke gegevensverwerking zij noodzakelijk acht in het kader van re-integratie. De invulling hiervan kan tot stand komen in nauw overleg met het vakdepartement en onder meer ondernemers, verzekeraars en de re-integratiebranche.

2. Bemiddeling van werknemers met een afstand tot de arbeidsmarkt
Werkgevers willen graag werknemers met een afstand tot de arbeidsmarkt aannemen. Zij schakelen daarvoor vaak een bemiddelaar - bijvoorbeeld een uitzendbureau - in. Bij de werving en selectie willen bemiddelaar en potentiële werkgever graag vroegtijdig weten of hij in aanmerking komt voor loondispensatie dan wel loonkostensubsidie. Dit mag het UWV van de AP echter niet aan werkgevers of bemiddelaars doorgeven. Een tweede obstakel voor optimale plaatsing is dat een bemiddelaar niet mag verwerken welk soort aandoening de persoon heeft, terwijl dat juist heel relevant is. Hierdoor wordt het proces van werving en selectie onnodig gefrustreerd. Volgens de AP is ook deze verwerking van gegevens niet strikt noodzakelijk, en daarmee gaat zij op de stoel van de ondernemer en de wetgever zitten.

Mogelijke oplossingen:

- Ook in deze casus beperkt de AP de wettelijke basis voor verwerking, in dit geval voor (her)intrede op de arbeidsmarkt. Bij AmvB kan geregeld worden dat cruciale schakels in de keten - bijvoorbeeld medewerkers van bemiddelaars - ook onder de wettelijke vereisten van geheimhouding vallen, indien bij overeenkomst vastgelegd.
- Daarnaast kan de wetgever verduidelijken welke gegevensverwerking zij noodzakelijk acht in het kader van optimale bemiddeling. De invulling hiervan kan tot stand komen in nauw overleg met het vakdepartement en onder meer ondernemers en bemiddelaars.

3. Alcohol- en drugstesten
Bepaalde bedrijven zijn wettelijk verplicht of voelen de noodzaak om met het oog op veiligheid en gezondheid van medewerkers en hun collega's een alcohol- en drugsbeleid te voeren. Ook wettelijk geldende alcohollimieten om taken te mogen uitoefenen (bijvoorbeeld in de zeescheepvaart) of zwaarwegende maatschappelijke belangen zoals veiligheid van direct omwonenden, continuïteit van de vitale infrastructuren en voorkoming van verontreiniging van het milieu nopen hiertoe. Om een alcohol- en drugsbeleid effectief vorm te kunnen geven, dan wel als werkgever toe te kunnen zien op de naleving van wettelijk geldende limieten, moet het testen hierop door of namens de werkgever onderdeel kunnen zijn van een alcohol- en drugsbeleid. De AP staat dit echter niet toe, omdat zij geen juridische basis voor verwerking van deze gezondheidsgegevens ten behoeve van dergelijke testen ziet, zoals die wel bestaan voor de luchtvaart en het spoor. Maar ook juist buiten die sectoren kunnen risicovolle situaties ontstaan door gebruik van alcohol, drugs of andere medicatie.

Mogelijke oplossing

- Omdat het om gezondheidsgegevens gaat, kan de werkgever geen beroep doen op zijn gerechtvaardigd belang, noch op toestemming vanwege de gezagsverhouding tussen werkgever en werknemer.

Daarmee ontbreekt in de UAVG rechtstreekse wettelijke grond voor het afnemen van alcohol- en drugstesten als onderdeel van zo'n beleid. Invoegen van een nieuw lid onder UAVG artikel 30 is nodig, mogelijk met als basis AVG art 9.2 sub b en g (wettelijke eisen, goed werkgeverschap, substantieel publiek belang).

4. Aansprakelijkheid loonheffing op grond van de WKA

Op grond van de Wet ketenaansprakelijkheid ('WKA') kan een aannemer aansprakelijk worden gesteld als zijn onderaannemer geen loonheffingen aan zijn personeel heeft betaald. Om dat te voorkomen, moet uit de administratie van de aannemer blijken wie er precies voor hem heeft gewerkt. In de praktijk geeft een onderaannemer om deze reden relevante persoonsgegevens van zijn werknemers rechtstreeks door aan de aannemer. Dat mag echter niet, omdat daarvoor geen grondslag bestaat onder de AVG. Volgens de AP wordt namelijk niet aan het noodzakelijkheidsvereiste voldaan. Wettelijk is slechts geregeld dat de onderaannemer het BSN van de werknemers door mag geven met het oog op efficiëntie en het minimaliseren van het risico op fouten.

De aannemer is daardoor genoodzaakt op de bouwplaats/plaats van het werk zelf de benodigde persoonsgegevens te verzamelen, over te schrijven en op dat moment een verwijzing naar zijn privacyverklaring aan die werknemers te verstrekken. Linksom of rechtsom komen de persoonsgegevens dus altijd in de administratie van de aannemer terecht, alleen op zeer omslachtige wijze.

Mogelijke oplossing

- De verplichting om de persoonsgegevens van werknemers door te geven aan de aannemer kan worden toegevoegd aan de wettelijke verplichting om het BSN door te geven. Ook kan ervoor worden gekozen om het noodzakelijkheidsvereiste in de AVG bij de grondslag "gerechtvaardigd belang" iets ruimer uit te leggen. Doorgifte van de persoonsgegevens in het kader van de WKA is dan op grond van de AVG mogelijk.

5. Controle en registratie in het kader van de WAV

Aannemers of inleners moeten op grond van de Wet Arbeid Vreemdelingen ('WAV') controleren of een buitenlandse werknemer van een onderaannemer of een ingehuurde arbeidskracht in Nederland mag werken. Het is niet duidelijk wat aannemer of inlener bij beoordeling hiervan wel en niet is toegestaan ten aanzien van de daarbij door de persoon te tonen documenten, zoals A1 verklaring, verblijfs- en werkvergunning en het notificatieformulier van het UWV. Onduidelijk is met name of de onderaannemer/uitlener (een kopie van) de genoemde documenten mag verstrekken of dat de aannemer dit aan de werknemer zelf moet vragen. Ook is niet duidelijk of de aannemer of inlener een kopie mag maken en bewaren, of de documenten alleen mag inzien.

Op grond van de AVG lijkt dit voor de aannemer/inlener verboden, waar hij uiteraard het liefst kopieën wil maken of vragen om zich te kunnen verdedigen tegen claims, naheffingen en boetes van overheidsinstanties.

Betrokken instanties verspreiden hierover echter andere en ook tegenstrijdige berichten. Zo valt op de website van de Inspectie SZW te lezen dat zij adviseert een kopie te bewaren van de werkvergunning, terwijl de Belastingdienst aangeeft dat je alleen de aanwezigheid van een werkvergunning mag noteren. Dit lijkt tegenstrijdig en als je alleen mag controleren, dan maakt dat bewijslevering in een later stadium vrijwel onmogelijk.

Mogelijke oplossing

- De bevoegdheid van aannemer of inlener om kopieën te maken van de benodigde documenten kan worden opgenomen in de wet. Ook kunnen doorgifte door onderaannemer en inlener en opslag van deze kopieën door de AP worden toegestaan met als grondslag het gerechtvaardigd belang van aannemer of inlener.

6. <u>Tegengaan fraude met werktijden</u>

In een aantal sectoren komt veel fraude voor met werktijden. Dit is een misdrijf dat bedrijven en de maatschappij aanzienlijke schade toebrengt. Om dit tegen te gaan vervangen werkgevers in bepaalde zeer fraudegevoelige sectoren de kaart van de prikklok door biometrie (irisscan of vingerafdruk). Dat is immers een hoogwaardige manier om vast te stellen of het inklokken ook daadwerkelijk wordt gedaan door de betreffende medewerker en niet door een collega die bijvoorbeeld twee kaarten incheckt. Eerder dit jaar heeft de staatssecretaris van SZW in antwoord op Kamervragen gezegd dat biometrie slechts gebruikt mag worden voor authenticatie voor beveiliging. Daardoor zou een wettelijke basis voor een biometrische prikklok ontbreken. Dat lijkt echter onjuist omdat de UAVG spreekt over biometrie voor authenticatie óf beveiliging. Alhoewel antwoorden op Kamervragen niet wettelijk bindend zijn, heeft deze uitspraak in de praktijk tot gevolg dat gebruikers van zo'n systeem dat nu gaan terugdraaien, en fraude niet op deze sluitende manier kan worden tegengegaan.

Mogelijke oplossing:

- De UAVG stelt dat biometrische gegevens met het oog op de unieke identificatie is toegestaan wanneer deze noodzakelijk is voor authenticatie óf beveiligingsdoeleinden. Omdat de biometrische prikklok ten doel heeft om onomstotelijk vast te stellen dat wie inklokt ook degene is wie hij zegt te zijn, is hier duidelijk sprake van authenticatie. Wij vragen u om in overleg met het departement van SZW deze uitspraak te heroverwegen, en helder te communiceren over de uitkomst.

7. Cross sectoraal fraude gegevens delen
De schade door fraude loopt jaarlijks in de miljarden euro's. Er wordt gesjoemeld met creditcards, verzekeringen en spooknota's. In navolging van de succesvolle aanpak in Engeland willen ook bedrijven in Nederland informatie over wangedrag en fraudeurs kunnen uitwisselen.
Op dit moment is dat echter niet mogelijk tussen bedrijven uit verschillende sectoren. Hoewel 'zwarte lijsten' binnen bepaalde sectoren wel zijn toegestaan, geeft de AP geen fiat voor het cross-sectoraal delen van informatie. Uw departement en ook wij zijn van mening dat de huidige wet hier voldoende ruimte voor biedt, maar ondanks vele gesprekken zien we nog geen beweging bij de AP.

Mogelijke oplossing:
- Een expliciete wettelijke grondslag voor cross-sectoraal uitwisselen van kennis over deze fraudeurs maakt klip en klaar dat dit kan en mag. De strenge AVG biedt ook ruimte voor zo'n grondslag. Uiteraard zal dat omkleed moeten zijn met de nodige waarborgen waardoor mogelijke onbedoelde schadelijke effecten voor onschuldige personen worden uitgesloten.

8. Vastleggen vermoeden van (geestelijke) ziekte of dementie
Bepaalde sectoren, bijvoorbeeld de financiële sector, wordt geconfronteerd met situaties waar sprake is van vermoedens van (geestelijke) ziektes of dementie. Verkeerde of onterechte besluiten ten gevolge van deze aandoeningen kunnen grote gevolgen hebben. Uit hoofde van de zorgplicht is het noodzakelijk dat financiële instellingen kunnen vastleggen wanneer sprake is van dergelijke vermoedens, de daarbij behorende stappen te kunnen nemen en verantwoorden. De vastlegging van deze vermoedens kan echter botsen met de beperkingen rondom de verwerking van gezondheidsgegevens.

Mogelijke oplossing
- De wens is dat de ruimte die de AVG hiervoor biedt ook wordt benut om helderheid te krijgen over de verwerking van dergelijke gegevens.

9. Geautomatiseerde besluitvorming op basis van profilering
De UAVG (art. 40) biedt een uitzondering op het verbod op geautomatiseerde individuele besluitvorming. Zo kan een bedrijf op basis van persoonsgegevens geautomatiseerd besluiten nemen over klanten of werknemers, als dit noodzakelijk is om te voldoen aan een wettelijke verplichting. Dit is echter niet toegestaan wanneer het geautomatiseerde besluit genomen wordt op basis van een profiel. Dit maakt nieuwe profiel-gebaseerde technieken om te voldoen aan wettelijke verplichtingen, zoals bijvoorbeeld zorgplicht, fraude detectie of voorkomen van witwassen of terrorisme financiering onmogelijk, terwijl de AVG die ruimte wel biedt.

Mogelijke oplossing

- Aanpassing van UAVG artikel 40 lid 1 UAVG hierop als volgt aan te passen: Artikel 22, eerste lid, van [...] de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, ~~anders dan op basis van~~ **waaronder** profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.

10. Volledige aansprakelijkheid dienstverleners

Het Rijk heeft in haar nieuwe Algemene inkoopvoorwaarden ARIV, ARVODI en ARBIT volledige aansprakelijkheid voor tekortkomingen met betrekking tot persoonsgegevens verankerd. Volledige aansprakelijkheid, voor welk soort schade dan ook wordt in aanbestedingen echter doorgaans als disproportioneel gezien, zie hiervoor ook de gids proportionaliteit: "*de aanbestedende dienst verlangt geen aansprakelijkheid die op geen enkele manier gelimiteerd is*". Ook worden boetes in de nieuwe inkoopvoorwaarden opeens als schade gekwalificeerd, zodat boetes van de AP integraal kunnen worden doorbelast aan dienstverleners. Dat is onwenselijk omdat een boete juridisch anders is dan schade. Boetes zijn punitief, en wanneer deze contractueel worden doorgeschoven is een boete geen straf meer, maar simpelweg het outsourcen van risico's.

- *Mogelijke oplossing*
  Het besluit om in de inkoopvoorwaarden de volledige aansprakelijkheid bij opdrachtnemers neer te leggen moet worden teruggedraaid en net zoals dat bij andere schades het geval is gelimiteerd worden. Het besluit om boetes door te belasten zou eveneens moeten worden teruggedraaid; de AP heeft hierover eerder ook al gezegd een boete op te willen kunnen leggen aan de 'schuldige', en dat het contractueel wegmanagen hiervan niet in orde is.

11. Journalistieke exceptie

De (U)AVG heeft niet de maximale ruimte benut die de AVG wel biedt om voor journalistieke doeleinden gegevens te verwerken. Dit leidt tot risico's in de vertrouwelijkheid tijdens de onderzoeksfase van journalistieke producties en bronbescherming. Ontoereikende journalistieke excepties kunnen ertoe leiden dat bronnen en klokkenluiders minder geneigd zijn om misstanden via de media naar buiten te brengen. Een tweede aandachtspunt is dat 'mensen op straat' de uitzonderingen die voor de journalistiek gelden niet kennen. Zo komt voor dat betrokkenen zichzelf (soms met geweld) verzetten tegen foto's op de openbare weg. Of zij proberen zich uit online archieven van digitale media te verwijderen middels het recht om vergeten te worden.

Mogelijke oplossing

- Gebruik de volle ruimte die de AVG biedt om gegevens voor journalistieke doeleinden te gebruiken. En maak via een publiekscampagne vervolgens duidelijk welke (extra) rechten en plichten nieuwsmedia hebben ten opzichte van het verwerken van persoonsgegevens.

12. Gebruik BSN

Het BSN is een nummer dat bijzondere bescherming geniet en waar de regering op een aantal vlakken (gebruik BSN in BTW nummer, verplaatsen BSN naar achterzijde paspoort) maatregelen gaat treffen om misbruik in relatie tot identiteitsfraude tegen te gaan. VNO-NCW en MKB-Nederland hechten waarde aan deze bijzondere bescherming, maar constateren tegelijkertijd dat doordat het BSN al een zo veelvuldig gebruikt nummer is, de bescherming niet langer gezocht zou moeten worden in de *beperking* van het nummer door bijvoorbeeld overheden en zorginstellingen, maar door het *gebruik van aanvullende beschermende maatregelen*. In bijvoorbeeld Portugal, Zweden en Denemarken is dit de normaalste zaak van de wereld. Ondernemingen zouden graag gebruik maken van het burgerservicenummer vanwege de unieke cijfercombinatie gekoppeld aan een individu. Dit maakt voor ondernemers onder meer een foutloze administratie mogelijk (nooit meer doublures met mogelijke privacy risico's van dien), maar registratie van het BSN kan ondernemers ook meer vertrouwen geven om klanten pas bij ontvangst van goederen te laten betalen (afterpay).

Mogelijke oplossing

- Het BSN is onder de AVG geen bijzonder persoonsgegeven meer. Gezien de enorme meerwaarde die gebruik van het BSN heeft voor allerlei administratieve processen én klantgerichte vertrouwensmodellen zoals afterpay, vragen wij artikel 46 UAVG te heroverwegen en dit nummer voor breder gebruik vrij te geven. Uiteraard moet dit geen risico's voor bijvoorbeeld identiteitsfraude opleveren, daarbij is het goed te kijken naar de sluitende oplossingen die men daarvoor bijvoorbeeld in Zweden heeft.

13. Leeftijdsvereiste rechtsgeldige toestemming

Voor sommige verwerkingen van persoonsgegevens is toestemming nodig, bijvoorbeeld voor het plaatsen van volgcookies of het installeren van een app. In Nederland kan iemand onder de 16 niet zelf toestemming geven, maar moet een ouder/voogd dit doen. Het is maatschappelijk onwenselijk en ook in de praktijk niet na te leven dat 14 en 15 jarigen voor dergelijke eenvoudige handelingen altijd toestemming moeten vragen aan hun ouders. In de praktijk zal dat niet gebeuren, en dat leidt ertoe dat een rechtsgeldige basis zal ontbreken, waarvoor ook bedrijven aansprakelijk kunnen zijn.

Mogelijke oplossing:

- In Scandinavische landen, België en Ierland is gekozen voor de leeftijdsgrens van 13 jaar. In het kader van rechtszekerheid en aansprakelijkheid vragen we de wetgever de leeftijd voor toestemming van 16 jaar naar 13 jaar te brengen. Dat is bovendien in het kader van bekwaamheid niet irreëel, bijvoorbeeld omdat voor andere – meer ingrijpende – beslissingen (zoals over de eigen gezondheid of omgang met gescheiden ouders) de leeftijd van 12 jaar wordt aangehouden.