Autoriteit
Consument & Markt

ACM & PRIVACY
Openbaar

DPIA – VERPLICHT?

Onderwerp : Azure AD / Entra ID
Contactpersoon : Productcoördinator Digitale Werkplek (ICT)
Zaaknummer : …
Datum : 28-3-2024

Waarom dit document?

Wanneer de verwerking waarschijnlijk hoge risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, dan is het vanuit de AVG verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. Met deze scan ga je na of er sprake is van een dergelijk hoog privacyrisico. Mocht je bij het invullen van dit document vragen hebben, benader de Privacy Officer van jouw directie om je hierbij te helpen.

1. Beoordeel adhv onderstaande elementen (**I t/m IV**) of sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen.

I. Gelet op:

a) aard,
b) omvang,
c) context, en,
d) doelstellingen.

II. Situatie uit lijst AP (zie bijlage 1)

III. Minimaal twee punten uit WP29-criteria (zie bijlage 2)

III. Situatie uit afspraken Ministerraad (zie bijlage 3)

Licht toe waarom er gelet op (a) aard, (b) omvang, (c) context en/of (d) doelstellingen wel/geen sprake is van hoog risico voor de rechten en vrijheden van natuurlijke personen:

In Azure AD worden de naam, inlognaam, e-mailadres, zakelijk telefoonnummer, afdeling en functietitel opgeslagen, zodat mensen in kunnen loggen op hun laptop en (indirect, via een federatieve koppeling) op zaken als het Rijksportaal. Dat mensen een bepaalde functie hebben bij de ACM brengt geen hoog risico met zich mee voor natuurlijke personen.

IV. De ACM gaat:

1) systematisch en uitgebreid persoonlijke aspecten evalueren gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseren die gevolgen hebben voor mensen,
2) op grote schaal bijzondere persoonsgegevens verwerken of strafrechtelijke gegevens verwerken, of,
3) op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

2. Is een (of meerdere) van bovenstaande elementen (**I t/m IV**) van toepassing?

☐ **ja** → Het is wel verplicht om een DPIA uit te voeren. Ga naar het stappenplan 'checklist DPIA – Uitvoering'. En informeer de FG en de Privacy Officer van jouw directie dat er een DPIA verplicht is voor deze verwerking.

☒ **nee** → Het is niet verplicht om een DPIA uit te voeren. Je kunt er wel voor kiezen om de privacyrisico's van een verwerking gestructureerd in kaart te brengen in de vorm van een PIA.

Afsluiting

Het is van belang dat de ACM zich te allen tijden kan verantwoorden naar de relevante partijen (denk aan de Autoriteit Persoonsgegevens en de betrokkenen). Om die verantwoording te kunnen realiseren dient dit document ingevuld op te worden geslagen in het bijbehorende DOX-dossier. Maak een submap ‘Privacy’ aan of label dit document met het tabje ‘Intern - Privacy’ in het DOX-dossier. Zo leg je vast waarom er wel / niet een DPIA is uitgevoerd. Informeer de Privacy Officer van jouw directie na het invullen van dit stappenplan door een e-mail te sturen met de betreffende link naar de ingevulde versie in DOX.

BIJLAGE 1: AP-lijst van verwerkingen waarvoor een DPIA verplicht is

Valt je verwerking onder één van de volgende zeventien typen? Dan moet er hoe dan ook een DPIA worden uitgevoerd. Je hoeft dan dus ook niet meer naar de criteria in bijlage 2 te kijken.

Nr.	Typen	ja	nee
1.1	*Heimelijk onderzoek* Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld met onderzoek, zonder de betrokkene daarvan vooraf op de hoogte te stellen. Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek voor fraudebestrijding en onderzoek op internet voor bijvoorbeeld online handhaving van auteursrechten. Een DPIA is ook verplicht bij heimelijk cameratoezicht door werkgevers om diefstal of fraude door werknemers te bestrijden. Hierbij moet soms ook een DPIA worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen werknemer en werkgever.	☐	☒
1.2	*Zwarte lijsten* Verwerkingen waarbij persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden. Bijvoorbeeld zwarte lijsten of waarschuwingslijsten, zoals verzekeraars, horecabedrijven, winkelbedrijven en telecomproviders die gebruiken. En ook zwarte lijsten die gaan over onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus.	☐	☒
1.3	*Fraudebestrijding* Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens voor fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.	☐	☒
1.4	*Creditscores* Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.	☐	☒
1.5	*Financiële situatie* Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.	☐	☒
1.6	*Genetische persoonsgegevens* Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses om persoonlijke kenmerken in kaart te brengen, bio-databanken	☐	☒
1.7	*Gezondheidsgegevens* Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars en onderzoeksinstituten), waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid. Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.	☐	☒
1.8	*Samenwerkingsverbanden*	☐	☒

	Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen, zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.		
1.9	*Cameratoezicht* Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.	☐	☒
1.10	*Flexibel cameratoezicht* Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.	☐	☒
1.11	*Controle werknemers* Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht voor diefstal- en fraudebestrijding.	☐	☒
1.12	*Locatiegegevens* Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.	☐	☒
1.13	*Communicatiegegevens* Grootschalige verwerkingen en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder of het randapparaat van de eindgebruiker.	☐	☒
1.14	*Internet of Things* Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'-toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.	☐	☒
1.15	*Profilering* Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.	☐	☒
1.16	*Observatie en beïnvloeding van gedrag* Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen wordt geobserveerd of beïnvloed, dan wel gegevens die daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.	☐	☒
1.17	*Biometrische gegevens* Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.	☐	☒

NB: Het kan zijn dat de AP de lijst met DPIA-verplichte verwerkingen aanpast of uitbreidt. Kijk op de website van de AP voor de meest actuele lijst.

Bijlage 2: WP29-criteria

Onderstaande criteria kunnen je helpen bij de beoordeling of sprake is van een verwerking met een hoog privacy-risico, waarbij een DPIA moet worden uitgevoerd. Als vuistregel geldt dat wanneer de verwerking aan 2 of meer van de 9 criteria voldoet, een DPIA dient te worden uitgevoerd.

Nr.	Criteria	ja	nee
2.1	*Beoordelen van mensen op basis van persoonskenmerken* Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.	☐	☒
2.2	*Geautomatiseerde beslissingen* Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.	☐	☒
2.3	*Stelselmatige en grootschalige monitoring* Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht.	☐	☒
2.4	*Gevoelige gegevens* Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.	☐	☒
2.5	*Grootschalige gegevensverwerkingen* De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De Europese privacytoezichthouders adviseren om met de volgende criteria te bepalen of hiervan sprake is: • de hoeveelheid mensen van wie gegevens worden verwerkt; • de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt; • de tijdsduur van de gegevensverwerking; • de geografische reikwijdte van de gegevensverwerking.	☐	☒
2.6	*Gekoppelde databases* Het gaat hierbij op gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.	☐	☒
2.7	*Gegevens over kwetsbare personen* Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan	☐	☒
2.8	*Gebruik van nieuwe technologieën* De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie.	☐	☒
2.9	*Blokkering van een recht, dienst of contract*	☐	☒

	Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen: • een recht niet kunnen uitoefenen of; • een dienst niet kunnen gebruiken of; • een contract niet kunnen afsluiten.		

Bijlage 3

In 2013 heeft de Ministerraad afgesproken dat binnen de Rijksoverheid voor de volgende situaties ook een DPIA verplicht is:

Nr.	Situatie	ja	nee
3.1	*Ontwikkeling van beleid en regelgeving* Een DPIA moet binnen de Rijksoverheid uitgevoerd worden bij de ontwikkeling van beleid en regelgeving als deze betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien. Is hiervan sprake?	☐	☒
3.2	*Groot politiek-bestuurlijk en maatschappelijk vraagstuk* Een DPIA moet binnen de Rijksoverheid uitgevoerd worden als de gegevensverwerking raakt aan een groot politiek-bestuurlijk en maatschappelijk vraagstuk. Is hiervan sprake?	☐	☒
3.3	*Grootschalig project met ICT-component* Een DPIA moet binnen de Rijksoverheid ook uitgevoerd worden bij projecten met een ICT-component van ten minste €5 miljoen. Is hiervan sprake?	☐	☒

Let hierop bij Clouddiensten: Privacytoezichthouders wijzen overheden op vereisten bij gebruik clouddiensten | Autoriteit Persoonsgegevens