STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 64418
27 november 2019

Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens

Besluit

De Autoriteit Persoonsgegevens,

gelet op artikel 35, vierde lid, in samenhang bezien met artikel 57, eerste lid, onder k, van de Algemene verordening gegevensbescherming;

gezien de "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679" d.d. 4 april 2017, laatstelijk gewijzigd en vastgesteld op 4 oktober 2017, van de European Data Protection Board (hierna: de Richtsnoeren);

overwegende:

dat in de Richtsnoeren negen criteria zijn vermeld die in aanmerking moeten worden genomen bij de beoordeling of een gegevensbeschermingseffectbeoordeling (DPIA) moet worden uitgevoerd, te weten in het geval dat sprake is van:
1. Evaluatie of scoretoekenning
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg
3. Stelselmatige monitoring
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard
5. Op grote schaal verwerkte gegevens
6. Matching of samenvoeging van datasets
7. Gegevens met betrekking tot kwetsbare betrokkenen
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen
9. de situatie waarin als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst";

dat voor alle soorten verwerkingen van persoonsgegevens die op de lijst staan, is aangegeven welk criterium uit de Richtsnoeren in aanmerking is genomen;

dat voor alle soorten verwerkingen van persoonsgegevens die op de lijst staan, onverkort geldt dat moet worden voldaan aan alle verplichtingen die de Algemene verordening gegevensbescherming stelt;

dat de lijst omschrijvingen van soorten verwerkingen bevat waarbij het uitgangspunt is dat de verwerkingsverantwoordelijke verplicht is een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren voordat met de verwerking van persoonsgegevens wordt begonnen;

dat de lijst niet uitputtend is en dat het kan zijn dat een verwerking van persoonsgegevens niet op de lijst staat, maar gelet op de aard, de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen en aldus een gegevensbeschermingseffectbeoordeling (DPIA) moet worden gedaan;

dat de Autoriteit Persoonsgegevens op grond van artikel 35, zesde lid, van de Algemene verordening gegevensbescherming het in artikel 63 van de Algemene verordening gegevensbescherming bedoelde coherentiemechanisme heeft toegepast;

dat dit coherentiemechanisme heeft geleid tot toevoeging van een extra categorie van verwerkingen van persoonsgegevens, te weten biometrische gegevens, alsmede tot enkele tekstuele wijzigingen;

stelt vast

dat voor de volgende verwerkingen van persoonsgegevens een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is:

1. Heimelijk onderzoek

Grootschalige verwerkingen van persoonsgegevens en-of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen (bijvoorbeeld: heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten). Een gegevensbeschermingseffectbeoordeling (DPIA) is ook verplicht in geval van heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een gegevensbeschermings-effectbeoordeling (DPIA) te worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever)). [3], [5], [7]

2. Zwarte lijsten

Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden (artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming)(zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus). [4], [6], [7], [8]

3. Fraudebestrijding

Grootschalige verwerkingen van (bijzondere) persoonsgegevens en-of stelselmatige monitoring in het kader van fraudebestrijding (bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars). [3], [4], [5], [9]

4. Creditscores

Grootschalige gegevensverwerkingen en/of stelselmatige monitoring die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore. [1], [2], [3], [4], [5], [9]

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). [3], [4], [5]

6. Genetische persoonsgegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens (bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, biodatabanken). [3], [4], [5]

7. Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratie-bedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid (let wel: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de Algemene verordening gegevensbescherming uitgezonderd van de verplichting een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren). [4], [5], [7]

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgege-vens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen, bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten. [6], [7], [8]

9. Cameratoezicht

Grootschalige en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones. [3], [5]

10. Flexibel cameratoezicht

Grootschalig en/of stelselmatig gebruik van flexibel cameratoezicht (camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten). [3], [5]

11. Controle werknemers

Grootschalige verwerking van persoonsgegevens en-of stelselmatig monitoring van activiteiten van werknemers (bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding). [3], [5], [7]

12. Locatiegegevens

Grootschalige verwerking 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). [3], [5]

13. Communicatiegegevens

Grootschalige verwerking 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. [3], [5]

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 ('internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etcetera). [3], [5], [8]

15. Profilering

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag. [1], [3]

16. Observatie en beïnvloeding van gedrag

Grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd of beïnvloed, dan wel gegevens daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld. [1], [5]

17. Biometrische gegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.
Op grond van de Algemene verordening gegevensbescherming is de verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijk persoon, in beginsel verboden. In Nederland zijn aanvullende voorwaarden gesteld in artikel 29 van de Uitvoeringswet Algemene verordening gegevensbescherming. Enkel als de verwerking strikt noodzakelijk is voor authenticatie of beveiligingsdoeleinden, is de verwerking van biometrische gegevens toegestaan. [3], [5], [8]

Den Haag, 19 november 2019

Autoriteit Persoonsgegevens,
A. Wolfsen
Voorzitter