aan	Autoriteit Persoonsgegevens Via st-mkb@autoriteitpersoonsgegevens.nl
ons kenmerk	SPF20260806
datum	6 augustus 2026
onderwerp	Consultatie *lijst DPIA-uitzonderingen*, aangekondigd op https://www.autoriteitpersoonsgegevens.nl/actueel/ap-vraagt-reacties-op-lijst-dpia-uitzonderingen

Geachte heer/mevrouw,

Graag maakt Stichting Privacy First (hierna: 'Privacy First') gebruik van de mogelijkheid om aan deze consultatie inzake het voorstel voor de *lijst DPIA-uitzonderingen*, het *Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor geen gegevensbeschermings-effectbeoordeling (DPIA) verplicht is*, (hierna: 'het ontwerpbesluit') deel te nemen.

Privacy First heeft begrip voor de behoefte van veel kleine organisaties om op voorhand duidelijkheid te hebben of de verplichting uit de AVG voor het uitvoeren van een 'data protection impact assessment' (DPIA) van toepassing is op hun voorgenomen verwerking. Het ontwerpbesluit kan daarbij behulpzaam zijn. Tegelijkertijd is Privacy First bezorgd dat de adequate bescherming van de belangen van betrokkenen afbrokkelt als bepaalde organisaties voor specifieke verwerkingen op voorhand een vrijstelling krijgen van de verplichting om een DPIA uit te voeren. De huidige ontwerplijst bevat diverse openingen voor verwerkingen die een hoog risico voor het leven van betrokkenen kunnen inhouden. Dergelijke verwerkingen zouden DPIA-plichtig moeten zijn conform de tekst en de strekking van de AVG.

Aandachtspunt is voorts dat juist bij klein(er)e organisaties de kennis inzake gegevensbescherming onvoldoende is en onvoldoende aandacht wordt besteed aan leveranciers- en productkeuze.

Stichting Privacy First
John M. Keynesplein 10
1066 EP Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KvK 34298157
ANBI erkend

Algemene aanbevelingen

Het ontwerpbesluit is een aanvulling op het besluit uit 2019 van de AP [1], waarin de AP aangeeft in welke situaties een DPIA verplicht is. Dat maakt het er voor degenen die de regels willen raadplegen niet makkelijker op. Verder valt ons op dat zowel bij het besluit uit 2019 als in het onderhavige ontwerpbesluit niet-toegelichte begrippen voorkomen en de voorwaarden summier worden beschreven.

Commentaar Privacy First

- Kunt u toelichten waarom gekozen is voor een apart ontwerpbesluit, in plaats van herziening van het besluit uit 2019, zo mogelijk met een toegankelijke opbouw en indeling?

- Kan aan het besluit van 2019 en het ontwerpbesluit (zo mogelijk samengevoegd) een toelichting worden toegevoegd, zoals bij dit soort besluiten vaker gebeurt? Dat zal de bruikbaarheid voor de praktijk vergroten.

- Als gekozen wordt voor een apart besluit, maak dan in de aanhef melding van het besluit uit 2019.

- Verduidelijk de voorwaarden voor de vrijstelling van de DPIA op een wijze die voor kleine organisaties met beperkte AVG-kennis te begrijpen is.

Het is belangrijk om te beseffen dat de impact van een verwerking op het persoonlijke leven van betrokkenen niet afhangt van de omvang van de organisatie van de verwerkingsverantwoordelijke. Daarom is het essentieel om in een lijst van DPIA-vrijstellingen te borgen dat inherente risicofactoren categorisch worden uitgesloten van een vrijstelling. Daartoe volgen hierna een aantal aanbevelingen die op meerdere typen verwerkingen uit het ontwerpbesluit van toepassing zijn.

Commentaar Privacy First

- Vermijd bijvoeglijke naamwoorden zoals “systematisch”, “stelselmatig” en “grootschalig”. Deze termen zijn relatieve begrippen afkomstig uit de AVG. In de praktijk leiden die tot niet-eenduidige interpretaties en daarmee tot onduidelijkheid voor zowel verwerkingsverantwoordelijken als betrokkenen. Voor kleine organisaties is deze onduidelijkheid onwenselijk en draagt niet bij aan de bescherming van de rechten en vrijheden van betrokkenen.

---

[1] *Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is,* Autoriteit Persoonsgegevens, Staatscourant 27 november 2019, https://wetten.overheid.nl/BWBR0042812/.

Het is van belang om in de aanhef van het ontwerpbesluit dan wel in de toelichting te benadrukken dat ook activiteiten die als zodanig normaal zijn en geen DPIA behoeven (zoals in nr. 1 de reguliere verwerking van persoonsgegevens van werknemers en andere werkzame personen), er wel wordt verondersteld dat de gebruikelijke AVG-regels worden nageleefd. Voorbeeld: als werknemers via een digitaal portaal toegang krijgen tot het personeelsdossier, hoort de leverancier van het portaal geen persoonsgegevens van de werknemer aan advertentiebedrijven (Google, Facebook c.s.) te verschaffen. De werkgever dient zich te realiseren dat een mooi contract niet voldoende is en dat de werkgever verantwoordelijk is voor een juiste leverancierskeuze en voor monitoring of de leverancier de overeengekomen regels nakomt.

In sommige onderdelen wordt als voorwaarde gesteld dat de persoonsgegevens niet met derden worden gedeeld (onder andere in nr. 3). Dat dient een algemene voorwaarde voor de toepasselijkheid van de vrijstelling te zijn.

Ook komt het verbod op doorgifte naar derde landen in sommige onderdelen voor, met de tekst 'systematisch'. In noot 11 wordt alleen naar de EU verwezen, terwijl de AVG ook in de EER geldt. Wij adviseren het verbod als algemene eis te stellen.

Commentaar Privacy First

- Verduidelijk - in de aanhef of de toelichting - dat de AVG-regels voor het overige moeten worden nageleefd, waarbij een goede leverancierskeuze en controle van de leverancier een centrale rol speelt. Geef ook aan dat het vaak niet nodig is om gegevens in de cloud of op een server van derden op te slaan, wat de gegevensbeschermingsrisico's beperkt.

- Neem op dat niet-delen van de persoonsgegevens met derden (dat wil zeggen anderen dan leveranciers die zich ertoe verplicht hebben de gegevens uitsluitend voor de opdrachtgever te verwerken) altijd voorwaarde is voor toepasselijkheid van de vrijstelling. Daarvan zijn alleen wettelijke verplichtingen tot gegevensverstrekking uitgezonderd (zoals werkgevers die personeelsgegevens aan de fiscus moeten verschaffen).

- Neem het niet-doorgeven aan landen die niet tot EU of EER behoren als algemene eis voor vrijstelling op, ook als het eenmalig gebeurt.

De reikwijdte van het ontwerpbesluit

Op pagina 2 bovenaan wordt vermeld dat het ontwerpbesluit van toepassing is op: "*verwerkingsverantwoordelijken die beroepsbeoefenaar zijn of een andere natuurlijke persoon zonder dienstverband, of werkgever zijn met maximaal 250 werknemers, en die op*

het grondgebied van het Europese deel van Nederland (hierna: Europees Nederland) hun werkzaamheden uitvoeren".

Het begrip '*beroepsbeoefenaar*' wordt door u niet nader toegelicht, terwijl activiteiten die voorheen door natuurlijke personen werden verricht (zoals bijvoorbeeld belastingadvies) tegenwoordig ook door rechtspersonen kunnen worden uitgeoefend. Een BV die belastingadviezen geeft kan heel goed meer dan 250 mensen in dienst hebben. Misschien dat u doelt op een beroepsbeoefenaar die natuurlijke persoon is, nu er daarna staat: "*of een andere natuurlijke persoon zonder dienstverband*" (onderstreping door ons). Als het u om beroepsbeoefenaren die natuurlijke persoon zijn gaat, geldt voor hen hetzelfde als wat hierna over andere natuurlijke personen zonder dienstverband wordt opgemerkt. Het begrip "*natuurlijke persoon zonder dienstverband*" is volgens Privacy First evenmin een adequate omschrijving, aangezien bij grote organisaties (zoals grote accountants- en advocatenkantoren) voorkomt dat de partners die werkzaamheden uitvoeren geen dienstverband hebben (= geen werknemer van de organisatie zijn). Door "*verwerkingsverantwoordelijken die beroepsbeoefenaar zijn of een andere natuurlijke persoon zonder dienstverband*" uit te zonderen, kunnen grote organisaties onder de DPIA-plicht uitkomen.

De passage "*werkgever zijn met maximaal 250 werknemers*" dient ook te worden aangepast, nu er organisaties zijn waarin een grote groep mensen niet als werknemer actief is.

Commentaar Privacy First

- Pas de passage inzake "*verwerkingsverantwoordelijken die beroepsbeoefenaar zijn of een andere natuurlijke persoon zonder dienstverband*" zodanig aan dat tot uitdrukking wordt gebracht dat deze verwerkingsverantwoordelijken niet actief zijn in een grote organisatie, ongeacht de rechtsvorm.

- Vervang de passage "*werkgever zijn met maximaal 250 werknemers*" door "*een organisatie zijn waarin maximaal 250 personen werkzaam zijn, al dan niet in dienstverband*".

Aanbevelingen ten aanzien van specifieke verwerkingen

Hieronder wordt de nummering aangehouden uit het ontwerpbesluit.

1. Verwerking van persoonsgegevens van werknemers

Wij adviseren de volgende verduidelijkingen:

Commentaar Privacy First

- "*bijzondere persoonsgegevens*" vervangen door "*bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, eerste lid, AVG*".
- "*systematisch monitoren*" vervangen door "*monitoren*".

2. Verwerking van klantgegevens in verband met zakelijke activiteiten

Het begrip 'zakelijke activiteiten' is een zeer ruime categorie, waarbij geen rekening wordt gehouden met de verschillende soorten ondernemingen die er zijn. Zo kan een marketingbedrijf andere bedrijven als cliënt hebben ('de afnemer'). Dat marketingbedrijf zal persoonsgegevens van de klanten van de afnemer ('derden') verwerken. Op basis van de tekst zou kunnen worden verondersteld dat de persoonsgegevens van die derden vallen onder de uitzondering.

Wij attenderen u er op dat de huidige tekst er toe zou kunnen leiden dat de vele ondernemingen die witwasbestrijdingsverplichtingen op grond van de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft) en (in de toekomst) de Europese antiwitwasverordening 'AMLR' [2] hebben, denken dat geen DPIA nodig is, terwijl voormelde regelgeving veronderstelt dat zeer gevoelige gegevens worden verwerkt die ook nog langdurig moeten worden bewaard (tot vijf jaar na het einde van de zakelijke relatie, wat bij sommige ondernemingen lang kan duren, bijvoorbeeld bij kleine banken). Verduidelijkt dient te worden dat het klantenonderzoek op grond van Wwft en AMLR niet onder de uitzondering valt.

---

[2] *Verordening (EU) 2024/1624 van het Europees Parlement en de Raad van 31 mei 2024 tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering,* https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32024R1624.

Voorts zijn diverse begrippen onhelder en loopt de tweede volzin ("*Mits de persoonsgegevens …*") niet goed.

Commentaar Privacy First

- Verduidelijk dat de uitzondering niet geldt voor de verwerking van persoonsgegevens van derden die bij de 'bestaande klanten' betrokken zijn.

- Verduidelijk dat de doeleinden van de verwerking helder afgebakend moeten zijn, dus geen beroep op 'gerechtvaardigd belang' zonder verdere uitleg,

- Verbeter de tekst van de tweede volzin, met name de passage "*klanten hebben ingestemd met de ontvangst ervan*". Het is onduidelijk waar dit betrekking op heeft. Gaat dit om de ontvangst van nieuwsbrieven?

- Verduidelijk wat met "*verwerkingen niet op grote schaal*" wordt bedoeld. Het is onduidelijk wat dit is. Gaat dit om het aantal klanten waarvan de gegevens worden verwerkt ongeacht de soort verwerking? Dat is arbitrair en niet risico-gerelateerd. Wij adviseren in ieder geval deze voorwaarde op te nemen: "*mits de persoonsgegevens niet met derden worden gedeeld*".

- Wij adviseren "*systematische monitoring van klanten*" te vervangen door "*monitoring van klanten*" en te verduidelijken dat verwerking van persoonsgegevens in verband met het klantenonderzoek op grond van de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft) en (in de toekomst) de Europese antiwitwasverordening 'AMLR' niet onder de uitzondering vallen, dus geen "*Verwerking van klantgegevens in verband met zakelijke activiteiten*" zijn. (Het klantenonderzoek valt wellicht onder "*evaluatie, scoring of monitoring*", maar wordt mogelijk door betreffende ondernemingen niet als zodanig herkend.)

- Geef in het ontwerpbesluit een toelichting op het begrip "*kwetsbare betrokkenen*". In de AVG is dat begrip niet gedefinieerd.

3. Verwerkingen die verband houden met websitebezoeken

Wij stellen enige verduidelijkingen voor. Zo is onduidelijk wat met "*een enkel klantbezoek*" wordt bedoeld – is dat een eenmalig klantbezoek? Dit begrip laat zich verder verduidelijken en beperken door de toevoeging dat de website het niet mogelijk maakt noch verlangt dat bezoekers een account aanmaken en registreren voor de website noch dat de website op

een afgeleide wijze probeert het gedrag en de bezoeken van bezoekers van de website te volgen.

Commentaar Privacy First

- Wij adviseren "*een enkel*" uit de eerste volzin te verwijderen. Verder stellen wij voor de tekst te verduidelijken door de toevoeging dat de website het niet mogelijk maakt noch verlangt dat bezoekers een account aanmaken en registreren voor de website noch dat de website op een afgeleide wijze probeert het gedrag en de bezoeken van bezoekers van de website te volgen.

- Licht toe hoe snel al sprake is van delen met derden, bijvoorbeeld door het gebruik van Google Analytics of het embedden van Youtube video's.

- Ook hier: geef in het ontwerpbesluit een toelichting op het begrip "*kwetsbare betrokkenen*". In de AVG is dat begrip niet gedefinieerd.

4. Verwerkingen uitgevoerd door een solistisch werkende zorgverlener

Wij vragen ons af waarom kleinschalige activiteiten in zorg en onderwijs niet een eigen behandeling krijgen. Nu staat in nr. 4 een tekst over de "*solistisch werkende zorgverlener*", terwijl dit ook een beroepsbeoefenaar zonder dienstverband kan zijn (nr. 5) en een mkb-bedrijf dat cameratoezicht uitoefent (nr. 6).

Aangezien in de zorg sprake is van kwetsbare personen en zeer grote gegevensbeschermingsrisico's, denken wij dat het beter is om de vrijstellingen voor kleine zorgverleners in een aparte bepaling specifiek gericht op de zorg te regelen. Voorts speelt hier dat de praktijk in de zorg is dat de IT-systemen zo worden vormgegeven dat de zorgverlener niet kan beslissen wie wanneer waartoe toegang heeft (terwijl er wel mooie woorden worden gesproken over het beroepsgeheim en de regie van de zorgverlener). Het is daarom belangrijk dat in de voorwaarden inzake de uitwisseling met andere zorgverleners en -instellingen tot uitdrukking wordt gebracht dat de solistisch werkende zorgverlener ook op technisch niveau de regie heeft.

Zie over "*systematische* doorgiften naar derde landen" (wij stellen voor het te vervangen door "doorgiften naar derde landen") de algemene opmerkingen.

Commentaar Privacy First

- Wij stellen voor "*delen/ matchen van patiëntgegevens door twee of meer individuele personen …*" algemener te formuleren, namelijk als volgt: "*delen/matchen van patiëntgegevens met enige andere zorgverlener, tenzij dit voor de behandeling nodig is*".

Verder adviseren we toe te lichten wat er met "delen/matchen" van persoonsgegevens wordt bedoeld.

- Toegevoegd dient te worden dat de vastlegging van patiëntgegevens in een elektronisch patiëntendossier waar derden mogelijk toegang toe hebben, alsmede de verwerking van genetische gegevens (DNA-gegevens) en overige biometrische gegevens als bedoeld in artikel 9 lid 1 AVG, is uitgesloten van de DPIA-vrijstelling.

- Aangezien solistisch werkende zorgverleners in verband met hun gezondheidsdiensten vaak in contact staan met andere zorgverleners en -instellingen, waarbij gebruik wordt gemaakt van IT-systemen, dient als voorwaarde te worden toegevoegd dat de gebruikte systemen voldoen aan de in de zorg gebruikelijke eisen op het gebied van informatiebeveiliging (onder andere NEN 7510) en - voor zover van toepassing - gecertificeerd en geaudit zijn.

- Verder dient aan de IT-systemen ten behoeve van de uitwisseling als voorwaarde te worden gesteld dat die systemen er voor zorgen dat bescherming van persoonsgegevens van de cliënten/patiënten van de solistisch werkende zorgverlener adequaat is gewaarborgd, mede met het oog op het beroepsgeheim van de solistisch werkende zorgverlener, wat betekent dat de solistisch werkende zorgverlener ook op technisch niveau beslist [1] wie er bij andere zorgverleners en -instellingen toegang heeft tot die persoonsgegevens; [2] welke persoonsgegevens het betreft; en [3] wanneer de toegang wordt verleend en weer ingetrokken. De solistisch werkende zorgverlener dient in staat te worden gesteld om periodiek te verifiëren of aan de hiervoor vermelde voorwaarde wordt voldaan.

5. Verwerkingen door beroepsbeoefenaar zonder dienstverband

Het is ons niet duidelijk waarom 'de beroepsbeoefenaar' die gereguleerd is, in het ontwerpbesluit een aparte behandeling krijgt (zie ook ons commentaar aan het begin) en waarom deze problematiek niet in nr. 2. wordt geregeld.

Wij begrijpen verder niet wat er wordt bedoeld met de voorwaarde inzake juristen ("*er geen sprake is van het gebruik van verwerkers voor verwerkingen van cliëntgegevens of het delen/matchen van cliëntgegevens door twee of meer individuele advocaten of notarissen … binnen Nederland valt*"). Voorts hebben wij geen idee wat er onder "*andere wettelijke beëdigde beroepsbeoefenaar*" en "*enige andere beëdigde beroepsbeoefenaar die onder een wettelijk toezichtregime … valt*" wordt verstaan.

Commentaar Privacy First

- Zie over de beroepsbeoefenaar zonder dienstverband wat wij aan het begin van dit commentaar hebben opgemerkt. Zoals vermeld stellen wij voor zorgprofessionals alleen onder 4. te behandelen. Zie over *"systematische doorgiften naar derde landen"* onze eerdere opmerkingen.

- Wellicht kan het hele onderdeel worden verwijderd.

Als het onderdeel zou blijven bestaan:

- Verwijder de passage "*of enige andere beëdigde beroepsbeoefenaar die onder een wettelijk toezichtregime … valt*".

- Verduidelijk wat wordt bedoeld met de voorwaarde inzake delen/matching van cliëntgegevens. Neem in ieder geval op dat de cliëntgegevens niet met enige andere derde partij mogen worden gedeeld.

- Vermeld dat deze uitzondering niet van toepassing is op solistisch werkende zorgverleners (daarvoor geldt alleen nr. 4) en het onderwijs (daarvoor geldt alleen nr. 7).

6. Cameratoezicht door MKB-bedrijven en verenigingen van eigenaren

Wij horen dat in de praktijk zeer onveilig wordt omgegaan met cameratoezicht, zo kregen wij van iemand deze reactie:

> *Staande praktijk is nu dat er niet naar privacy wordt gekeken bij het instellen van cameratoezicht. Iedere club hangt zomaar goedkope camera's op met app en cloud abonnement waarin in de voorwaarden staat dat deze cloudpartij de beelden voor eigen doeleinden mag gebruiken (Ring, Nest, Arlo, dozijn Chinese leveranciers), bijvoorbeeld AI trainen, gezichtsherkenning toepassen, doorverkopen aan "carefully selected business partners" en dat degene die ze ophangt maar even toestemming moet zien te krijgen van iedereen die in beeld komt. Dit gebeurt op hele grote schaal en hier is nu al geen enkele handhaving op. Het afschaffen van een DPIA-plicht gaat dit probleem nog eens flink verergeren.*

Wij adviseren de voorwaarden duidelijker te formuleren, om misverstanden te voorkomen.

Commentaar Privacy First

- Wij adviseren de passage "*geen verwerkingen op grote schaal*" te vervangen door "*camera-registraties niet langer dan 28 dagen worden bewaard en automatisch worden gewist*".

- Voorts adviseren wij "*grootschalige en stelselmatige gezichts- en stemherkenning van natuurlijke personen*" te vervangen door "identificatie van natuurlijke personen".

- Tevens dient te worden toegevoegd als voorwaarde dat er geen stemmen en andere audio worden geregistreerd en dat periodieke controle plaatsvindt of nog steeds aan de voorwaarden wordt voldaan (belangrijk na updates van de software en dergelijke).

- Wij bevelen aan om in de toelichting te verduidelijken dat er veel camera's zijn die niet aan de AVG-eisen voldoen en te verwijzen naar nadere informatie over camera's die wel AVG-*proof* zijn.

Voor deze verwerkingen gelden ook de eerder genoemde voorwaarden dat er niet wordt doorgegeven buiten EU/EER en dat er niet met derden wordt gedeeld. Een controle dat leveranciers hun verplichtingen naleven is belangrijk.

7. Verwerkingen door onderwijsinstellingen

Zoals hiervoor al onder 4. is vermeld, denken wij dat het verstandig is om de regels die relevant zijn voor onderwijsinstellingen zoveel mogelijk bij elkaar te brengen.

Commentaar Privacy First

- "*Hierbij geldt dat de voorwaarde …*" – Het woord "dat" dient te vervallen voor een leesbare zin.

- "*geen andere bijzondere categorieën van persoonsgegevens*" – na deze voorwaarde de volgende voorwaarde toevoegen: "*deze verwerking is gescheiden van de verwerking van algemene gegevens van leerlingen en wordt niet gedeeld met derden.*"

- In de toelichting kan worden opgenomen dat het is aan te bevelen dat onderwijsinstellingen zoveel mogelijk samenwerken als het om AVG- en DPIA-problematiek gaat. Nu gebeurt dat voor zover wij weten vooral bij diensten van de grote Amerikaanse leveranciers (Google/Microsoft e.d.). Wij adviseren te verduidelijken dat dit bij alle soorten inkoop de voorkeur verdient, dus ook bij kleinere IT-leveranciers.

8. Verwerkingen door kindcentrum

Hier hebben wij geen oordeel over.

9. Verwerkingen door verenigingen en stichtingen

De praktijk leert dat verenigingen en stichtingen soms teveel persoonsgegevens van hun leden, respectievelijk donateurs verwerken, om betrokkenen te kunnen profileren ten behoeve van marketing activiteiten van verenigingen/stichtingen (om aan donaties en inkomsten van derden zoals sponsors te komen). Er zijn verenigingen en stichtingen die persoonsgegevens van leden/donateurs met derden delen, waarvan de tennisbond zaak een bekend voorbeeld is (zie onder meer ECLI:NL:RBAMS:2022:5565). Leden van verenigingen en donateurs van stichtingen horen er op te kunnen rekenen dat hun gegevens niet met derden worden gedeeld.

Op het gebied van goede doelen is de stichting Donateursbelangen (https://www.donateursbelangen.nl/) actief die pleit voor een betere omgang door goede doelen met persoonsgegevens.

Uiteraard geldt het verbod op doorgifte buiten EU/EER en delen met derden ook hier.

Commentaar Privacy First

- Wij adviseren als voorwaarde toe te voegen dat andere gegevens dan nodig voor de relatie met de organisatie, zoals de naam en het contactmiddel (bijvoorbeeld e-mail of telefoonnummer) alleen verwerkt mogen worden als daar een aangetoonde noodzaak voor is. Dus geen verwerking van de geboortedatum. Bij donateurs dient niet om het adres te worden gevraagd.

Tot slot

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur