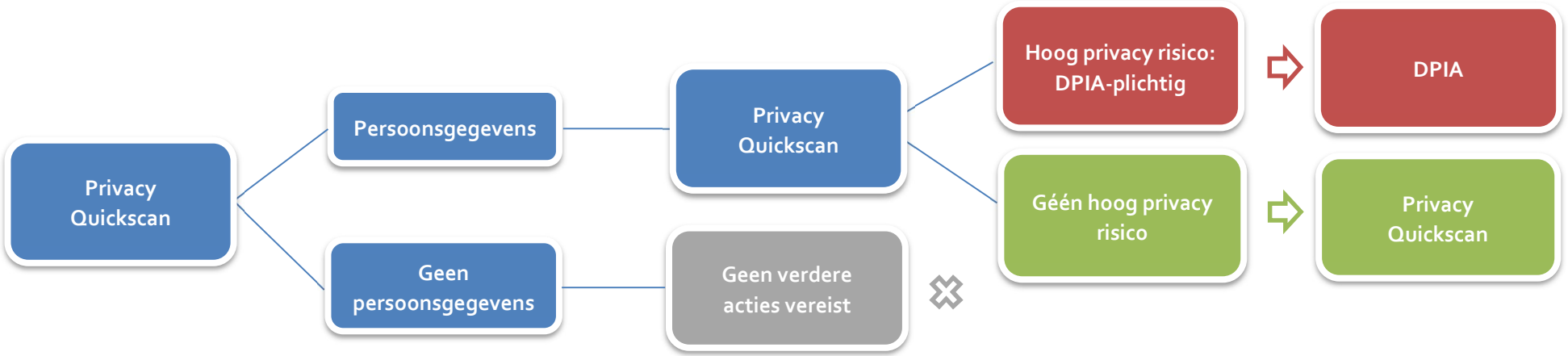
Gemeente Amsterdam

Privacy Quickscan

Deze Privacy Quickscan is een beknopt onderzoek naar de verwerking van persoonsgegevens die de gemeente wil doen. Het doel is om aan de hand van 7 vragen te toetsen of aan de beginselen van de AVG wordt voldaan en, als dat nodig is, maatregelen te nemen. Deze Quickscan bevat ook een bijlage. De bijlage 'DPIA Pre-scan' dient om te toetsen of sprake is van een hoog privacy risico en daarom een DPIA (Data Protection Impact Assessment) moet worden uitgevoerd.

Het proces voor het doorlopen van deze Privacy Quickscan ziet er als volgt uit:



- Bij constatering dat **géén** sprake is van het verwerken van persoonsgegevens (vraag 1.2) hoef je niet verder te gaan met de Privacy Quickscan, omdat de AVG niet van toepassing is.
- Blijkt uit de Privacy Quickscan dat een **DPIA verplicht moet worden uitgevoerd** (vraag 1.3), dan hoef je deze **Privacy Quickscan niet** verder in te vullen en kun je verder met het uitvoeren van een DPIA. Raadpleeg hiervoor de Privacy Officer.
- Blijkt uit de Privacy Quickscan dat een DPIA **niet** verplicht is, dan dienen de vragen **Privacy Quickscan** verder te worden ingevuld.

BEHEER EN SAMENVATTING

Cluster	DII
Directie	Data
Proces	250165 Peilingen gemeenteraadsverkiezingen 2026
Proceseigenaar	5.1, 2, e en 5.1, 2, e
Privacy Officer	5.1, 2, e

Versie	**Datum**	**Auteur(s) + rol/functie**	**Opmerkingen**
0.8	22-01-2026	5.1, 2, e Privacy Officer Directie Data	Privacy Quickscan opgesteld; nadere vragen gesteld aan 5.1, 2, e en 5.1, 2, e
0.9	23-01-2026	5.1, 2, e onderzoeker	opmerkingen beantwoord en kleine wijzigingen in tekst
1.0	27-01-2026	5.1, 2, e Privacy Officer Directie Data	Laatste aanpassingen doorgevoerd
1.1	13-02-2026	5.1, 2, e onderzoeker. 5.1, 2, e senior onderzoeker	Laatste opmerkingen beantwoord en ondertekend

Risico's en maatregelen *(na invulling van de Privacy Quickscan)*

Risico's / negatieve gevolgen voor de privacy van betrokkenen	**Maatregelen (en evt. acceptatierisico's)**	**Actiehouder + termijn**
Risico's beschreven in DPIA enquêteonderzoek	Maatregelen beschreven in DPIA enquêteonderzoek	Proceseigenaar

Akkoord proceseigenaar

Datum	**Naam (functie)**	**Handtekening**
	5.1, 2, e (senior onderzoeker)	5.1, 2, e
	5.1, 2, e (onderzoeker)	5.1, 2, e

1. PROCES EN VERWERKINGEN

1.1. **Geef een omschrijving van de verwerking (het proces, het product of de dienst).**
Leg uit wat je gaat doen met gegevens, op welk moment en wat hiervan het doel is.

Introductie:
Deze Privacy Quickscan heeft betrekking op de verwerking van persoonsgegevens door de afdeling *Onderzoek & Statistiek* (hierna: "O&S") van de gemeente Amsterdam. De uiteindelijke verwerkingsverantwoordelijke is het college van burgemeesters en wethouders (B&W).

De afdeling O&S is verantwoordelijk voor het uitvoeren van kwantitatief, kwalitatief en enquêteonderzoek voor verschillende interne en externe opdrachtgevers, evenals voor eigen onderzoek in relatie met de gemeente Amsterdam.

Deze Privacy Quickscan is bedoeld om de verwerkingen van persoonsgegevens in kaart te brengen die gepaard gaan met het uitvoeren van het onderzoek: **250165 Peilingen gemeenteraadsverkiezingen 2026**

Specifieke aspecten van het onderzoek:

Het voorliggende onderzoek vindt plaats op initiatief van O&S zelf, en wordt dus niet uitgevoerd in opdracht van een interne of externe opdrachtgever.

Voortbouwend op een eerder onderzoek uit maart 2025, voert O&S in aanloop naar de gemeenteraadsverkiezingen van 18 maart twee peilingen uit om inzicht te krijgen in de politieke voorkeuren van Amsterdammers. Deze aanpak sluit aan bij de langdurige traditie waarin O&S, soms in samenwerking met lokale media zoals het Parool en AT5, peilingen uitvoert voorafgaand aan verkiezingen.

Ter uitvoering van het voorliggende onderzoek zal O&S een vragenlijst voorleggen aan 2.500 leden van het Stadspanel verdeeld over de verschillende stadsdelen van Amsterdam. Vanwege een lagere verwachte respons, nodigt O&S relatief meer panelleden uit die woonachtig zijn in de stadsdelen Noord, Zuidoost en Nieuw-West. Onderstaand overzicht geeft de verdeling van de steekproef onder leden van het Stadspanel weer:

Stadsdeel	**Aantal**
Centrum	300
West	300
Nieuw-West	400

Zuid	300
Oost	300
Noord	400
Weesp	100
Zuidoost	400
Totaal	**2.500**

Omdat jonge Amsterdammers, Amsterdammers met een migratieachtergrond en Amsterdammers met een basisopleiding in het panelbestand zijn ondervertegenwoordigd, zet O&S hiernaast face-to-face (F2F) onderzoek in om deze groepen beter te bereiken en daarmee een veelzijdigere groep respondenten te realiseren. O&S streeft hierbij naar 150 ingevulde straatenquêtes, uitgevoerd op vergelijkbare wijze als bij een eerdere peiling uit 2018. Destijds zijn 150 enquêtes verzameld in Nieuw-West, Zuidoost, Noord en Oost, waarbij enquêteurs werden geïnstrueerd om op markten en in winkelstraten te enquêteren. O&S verwacht dat enquêteurs ongeveer 5 enquêtes per uur kunnen ophalen. Voor het uitvoeren van deze F2F-enquêtes wordt gebruikgemaakt van enquêteurs in dienst van Randstad.

De vragenlijst voor dit onderzoek bevat vragen over de stemintentie van respondenten, hun partijvoorkeuren bij de komende gemeenteraadsverkiezingen en hun partijkeuze bij de vorige gemeenteraadsverkiezingen van 2022. Daarnaast worden vragen gesteld over hoe respondenten hun stem bepalen, hoe zij vinden dat het gaat met Amsterdam, en over welke maatschappelijke vraagstukken zij zich het meeste zorgen maken in de stad. AT5 en het Parool kunnen input geven voor de vragenlijst, maar O&S in eindverantwoordelijke voor de vragenlijst. Voor de tweede peiling wordt een vraag toegevoegd over het ontvangen van de krant Amsterdam.

Om de uitslag van de peiling te kunnen duiden, worden de volgende achtergrondkenmerken gebruikt:
– Geslacht
– Opleidingsniveau
– Generatie van migratie
Van panelleden zijn deze achtergrondkenmerken reeds bekend bij O&S, omdat zij deze gegevens hebben opgegeven op het moment van aanmelding bij het Stadspanel. In de F2F-interviews zullen deze achtergrondkenmerken worden uitgevraagd door enquêteurs.

Na afloop van de dataverzameling analyseert O&S de respons op de vragenlijst en verwerkt deze in een rapportage. In deze rapportage wordt geen informatie opgenomen die herleidbaar is naar individuele respondenten.

1.2. Worden persoonsgegevens verwerkt in het proces?

Bij persoonsgegevens gaat het om alle informatie over een persoon (ook om gegevens die indirect iets over iemand zeggen). Bijvoorbeeld iemands naam, adres, e-mailadres, klantnummer, salarisstrook, foto etc. Alles wat je doet met persoonsgegevens wordt 'verwerken' van persoonsgegevens genoemd, denk hierbij aan: verzamelen, ordenen, opslaan, wijzigen, gebruiken, delen, doorsturen, inkijken, raadplegen, combineren, wissen of vernietigen van persoonsgegevens. NB: anonieme, gepseudonimiseerde, geaggregeerde en synthetische gegevens dienen te worden geverifieerd door een Privacy Officer.

In verschillende fasen van het onderzoek worden persoonsgegevens verwerkt.

Panelonderzoek

Onderdeel 1: Het selecteren van relevante panelleden van het Stadspanel Amsterdam

Het selecteren van relevante panelleden voor het voorliggende onderzoek vindt plaats in overleg tussen de betrokken onderzoeker(s) en de Data Collection Unit ("DCU") van O&S. Bij de aftrap van het onderzoek is besproken op welke kenmerken relevant zijn gezien het doel van het onderzoek. In dit geval is ervoor gekozen om een selectie te maken van 2.500 leden van het Stadspanel, verdeeld over de verschillende stadsdelen van Amsterdam. Zoals hierboven reeds uiteengezet, is een differentiatie aangebracht in het aantal personen dat per stadsdeel wordt uitgenodigd voor het onderzoek. Dit heeft te maken met verschillen in verwachte respons van geselecteerde panelleden uit verschillende stadsdelen. Naast het stadsdeel waarin de betreffende respondent woonachtig is, wordt vooraf niet gefilterd op beschikbare achtergrondkenmerken in het panelbestand.

In de steekproef krijgt elk geselecteerd panellid een uniek Respondent ID. Dit unieke nummer wordt gebruikt om de achtergrondgegevens van een geselecteerd panellid te koppelen aan voor dit onderzoek relevante achtergrondgegevens (geslacht, opleidingsniveau, generatie van migratie).

Onderdeel 2: Het aanschrijven van panelleden van het Stadspanel Amsterdam en het Stadspaspanel

Geselecteerde panelleden worden door de Data Collection Unit (DCU) van O&S per e-mail uitgenodigd om aan het onderzoek mee te doen door het invullen van een vragenlijst.

Onderdeel 3: Het binnenhalen van enquêteantwoorden van panelleden

De enquêteantwoorden van panelleden worden opgeslagen door de DCU van O&S. Hierbij geldt dat enquêteantwoorden nooit in hetzelfde bestand worden bewaard als steekproefgegevens.

Onderdeel 4: Het combineren van enquêteantwoorden van panelleden met bekende achtergrondkenmerken
De DCU van O&S combineert de enquêteantwoorden van panelleden met achtergrondkenmerken die voor het onderzoek van belang zijn (geslacht, hoogst voltooide opleiding, al dan niet in Nederland geboren, ouders al dan niet in Nederland geboren). Zoals hierboven beschreven, wordt hiervoor gebruik gemaakt van het unieke Respondent ID van elk geselecteerd panellid.
Onderdeel 5: Beschikbaar stellen gepseudonimiseerde enquêteantwoorden aan onderzoekers van O&S
De verzamelde enquêteantwoorden worden door de DCU in gepseudonimiseerde vorm aangeleverd bij de betrokken onderzoeker(s) van O&S. Dit betekent dat zij enkel toegang hebben tot de verrijkte enquêteantwoorden van respondenten, en nooit tot hun namen, (mail)adressen en telefoonnummers.

Onderdeel 6: Analyse door betreffende onderzoeker(s) van O&S
De betrokken onderzoeker(s) van O&S analyseren de gepseudonimiseerde enquêteantwoorden van respondenten en gebruiken deze gegevens voor het opstellen van de eindrapportage.

Onderdeel 7: Verwijderen van steekproefgegevens en anonimisering van enquêteantwoorden
Steekproefgegevens uit het panelbestand worden 12 maanden na afronding van het veldwerk vernietigd. Enquêteantwoorden worden 12 maanden na afronding van het veldwerk geanonimiseerd.

F2F-interviews
Bij het afnemen van F2F-interviews worden persoonsgegevens verwerkt, aangezien enquêteurs gedurende korte tijd inzicht hebben in welke antwoorden door ondervraagde voorbijgangers zijn gegeven. Vanaf het moment dat enquêteurs de antwoorden op de vragenlijst hebben verstuurd aan de DCU van O&S, zijn deze feitelijk geanonimiseerd. De opgeslagen antwoorden bevatten namelijk geen kenmerken die direct of indirect naar individuele personen zijn te herleiden.

De opgeslagen antwoorden worden door de DCU beschikbaar gesteld aan onderzoekers van O&S. Onderdelen 5 en 6 van de beschrijving voor panelonderzoek zijn van overeenkomstige toepassing op de verwerking van antwoorden die zijn gegeven in het kader van F2F-interviews.

N.B.:
Het eindrapport van het onderzoek bevat geen persoonsgegevens. Aangezien de AVG niet van toepassing is op anonieme gegevens, zal in deze Privacy Quickscan geen aandacht worden besteed aan dit onderdeel van het onderzoek.

➔ **Indien uit bovenstaande vragen blijkt dat géén persoonsgegevens worden verwerkt, dan kun je stoppen met de Quickscan en de Privacy Officer informeren. Indien er wel persoonsgegevens worden verwerkt, ga dan verder met vraag 1.3 en vul tevens het verwerkingsregister in samen met de Privacy Officer.**

1.3. **Is sprake van een verwerking van persoonsgegevens waarvoor een DPIA moet worden uitgevoerd? Vul de '*Bijlage DPIA Pre-scan*' in om te achterhalen of een DPIA verplicht is.**

Als sprake is van een hoog privacy risico voor de personen van wie gegevens worden verwerkt, moet je een DPIA uitvoeren. Je moet een DPIA uitvoeren voordat je met deze verwerking start.

Nee, zie input op Bijlage DPIA Pre-scan. In algemene zin wordt verwezen naar de DPIA enquêteonderzoek, waarin processen die worden beschreven in deze Privacy Quickscan nader zijn uitgewerkt.

➔ **Indien uit de DPIA Pre-scan blijkt dat het noodzakelijk is een DPIA uit te voeren, dan kan je hier stoppen met deze Quickscan. Raadpleeg de Privacy Officer om een DPIA uit te voeren. Indien een DPIA niet noodzakelijk is, ga dan verder met vraag 2.**

1. BETROKKENEN EN PERSOONSGEGEVENS

Vul onderstaande tabel in om inzicht te verschaffen in welke persoonsgegevens worden verwerkt van betrokkenen.

Betrokkenen • Omschrijf de groep betrokkenen, bijvoorbeeld medewerkers of burgers. • Beschrijf of sprake is van een kwetsbare groep, bijvoorbeeld minderjarigen of asielzoekers. • Benoem het aantal betrokkenen.	**Persoonsgegevens** • Vul in welke persoonsgegevens worden gebruikt. • Classificeer de gegevens: gewone persoonsgegevens, bijzondere persoonsgegevens of gevoelige persoonsgegevens.
Geselecteerde leden van het Stadspanel Amsterdam - **2.500 leden van het Stadspanel Amsterdam worden geselecteerd en uitgenodigd voor dit onderzoek, verdeeld over de verschillende stadsdelen van de stad. De gekozen verdeling is eerder in deze privacy quickscan nader uitgewerkt.** ***Deelnemers aan het F2F-onderzoek*** - **150 willekeurige voorbijgangers die deelnemen aan het F2F-onderzoek**.	*Gewone persoonsgegevens:* Steekproef- en contactgegevens van geselecteerde panelleden (niet van toepassing bij F2F-interviews) - Respondent ID - E-mailadres Achtergrondkenmerken (worden uitgevraagd in F2F-interviews, zijn al bekend bij panelleden en worden gekoppeld door DCU) - Geslacht - Hoogst voltooide opleiding - Al dan niet in Nederland geboren - Ouders al dan niet in Nederland geboren *Bijzondere persoonsgegevens:* Enquêteantwoorden waaruit de politieke opvattingen van betrokkenen blijken (zowel bij F2F-interviews als panelonderzoek): - Stemintentie bij de gemeenteraadsverkiezingen van 2026 - Partijvoorkeuren bij de gemeenteraadsverkiezingen van 2026 - Partijkeuze bij de gemeenteraadsverkiezingen van 2022 - Factoren voor stemkeuzebepaling - Mening over of het al dan niet de goede kant opgaat in Nederland - Mening over of het al dan niet de goede kant opgaat in Amsterdam - Mening over welke maatschappelijke vraagstukken de respondent het meeste zorgen baren. Uitzonderingsgrond: expliciete toestemming o.g.v. artikel 9(2)(a) AVG

2. RECHTMATIGHEID

Geef aan op basis van welke grondslag de persoonsgegevens mogen worden verwerkt en motiveer waarom die grondslag van toepassing is.

Grondslag	Toelichting
Toestemming	De verwerking van persoonsgegevens in het enquête-onderzoek vindt plaats op basis van expliciete toestemming van betrokkenen. Deelname aan het voorliggende onderzoek is volledig vrijwillig, en betrokkene wordt vooraf op een duidelijke en begrijpelijke manier geïnformeerd over de aard van het onderzoek, welke gegevens worden verzameld en met welk doel deze worden verwerkt. ***Panelonderzoek:*** - *Panelleden hebben bij hun aanmelding toestemming gegeven om door O&S benaderd te worden voor onderzoeksdoeleinden (onderdelen 1 en 2 van het panelonderzoek).* - *Toestemming voor het verwerken van enquêteantwoorden in het kader van het voorliggende onderzoek wordt gevraagd voorafgaand aan het invullen van de online vragenlijst (onderdelen 3 en verder van het panelonderzoek). Hierbij worden respondenten gewezen op het feit dat het invullen van de vragenlijst volledig vrijwillig is en dat het hen vrij staat om elke vraag waar zij geen antwoord op willen geven, over te slaan. Bovendien wordt aan respondenten gemeld dat zij hun toestemming op elk moment kunnen intrekken, en dat hun enquêteantwoorden vanaf dat moment niet meer voor het onderzoek gebruikt zullen worden.* - *Respondenten geven toestemming door middel van een keuzevakje in de online vragenlijst. Respondenten kunnen hun toestemming intrekken door een specifiek nummer te bellen of te mailen naar de helpdesk van O&S.* ***F2F-onderzoek*** *Deelnemers aan het F2F-onderzoek geven vooraf expliciet mondeling toestemming voor het verwerken van hun persoonsgegevens in het kader van het onderzoek. Enquêteurs registreren gegeven toestemming van deelnemers door middel van de beantwoording van de 'toestemmingsvraag' aan het begin van het onderzoek. Deze registratie werkt dus feitelijk hetzelfde als bij panelonderzoek. Deelnemers krijgen dezelfde informatie als deelnemers aan het panelonderzoek voordat zij toestemming geven voor de verwerking van hun persoonsgegevens. Respondenten worden erop gewezen dat er geen*

	identificerende gegevens worden opgeslagen, en dat hun antwoorden dus feitelijk geanonimiseerd zijn nadat zij worden opgeslagen.

3. DATAMINIMALISATIE

Is het nodig alle persoonsgegevens te gebruiken of kan het doel ook met minder (of geen) gegevens worden behaald?

Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Er mogen niet meer persoonsgegevens worden verwerkt dan (strikt) noodzakelijk is voor het doel.

O&S verwerkt in het enquêteproces enkel persoonsgegevens die noodzakelijk zijn voor het doel van het onderzoek. O&S verwerkt in dit proces geen additionele persoonsgegevens die niet noodzakelijk zijn voor dit specifieke doel. Onderzoekers krijgen alleen toegang tot gepseudonimiseerde enquêteantwoorden.

4. BEWAREN EN VERWIJDEREN

Geef aan welke bewaartermijnen voor de persoonsgegevens zijn vastgesteld en waarom voor die termijn is gekozen. Beschrijf hoe wordt gerealiseerd dat de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn wordt nageleefd.

Er moet een passende bewaartermijn worden bepaald en afgestemd met de Privacy Officer en maatregelen moeten worden genomen om te borgen dat de bewaartermijn wordt gehandhaafd (denk aan automatische opschoning en afspraken in een verwerkersovereenkomst). Indien nodig, neem voor het vaststellen van bewaartermijnen contact op met collega's van Informatiebeheer.

O&S bewaart de persoonsgegevens in het kader van enquête onderzoeken voor zolang dit noodzakelijk is voor het onderzoek. Concreet betekent dit:
- Steekproefgegevens uit het panelbestand worden 12 maanden na afronding van het veldwerk vernietigd.
- Enquêteantwoorden worden 12 maanden na afronding van het veldwerk vernietigd.

5. TRANSPARANTIE

Op welke manier(en) worden betrokkenen geïnformeerd over de verwerking van hun persoonsgegevens?

De gemeente moet transparant zijn over de verwerking van persoonsgegevens. Het moet voor de betrokkene inzichtelijk zijn in hoeverre en op welke manier zijn persoonsgegevens worden verwerkt. De gemeente heeft een algemene privacyverklaring gepubliceerd en er is een format voor specifieke privacyverklaringen beschikbaar.

Er is een specifieke privacyverklaring gepubliceerd op de website van de gemeente Amsterdam. Deze staat op de volgende webpagina: Privacyverklaring enquêtes. Daarnaast is er ook nog een specifieke privacyverklaring voor enquêteonderzoek Stadspanel: Privacyverklaring enquêteonderzoek Stadspanel Amsterdam.

6. DOORGIFTE VAN PERSOONSGEGEVENS

7.1 Benoem alle externe partijen die betrokken zijn bij de verwerking van persoonsgegevens.

Geef ook aan welke rol elke partij vervult (verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, verstrekker, ontvanger etc.) en welke afspraken zijn gemaakt m.b.t. de verwerking van persoonsgegevens (bijvoorbeeld: verwerkersovereenkomst, convenant, onderlinge regeling bij gezamenlijke verantwoordelijkheid, leveringsovereenkomst). Het gemeentelijk model voor deze overeenkomsten kan je hier vinden: Afspraken met derden – SAM (intranet).

Naam partij	Rol	Overeenkomst/afspraken
Randstad	Verwerker	Inhuurovereenkomst, verwerkersovereenkomst

7.2 Indien persoonsgegevens worden doorgegeven naar landen buiten de Europese Economische Ruimte (EER), geef dan aan om welke partijen en landen het gaat, welke waarborgen hiervoor zijn genomen en of de Standard Contractual Clauses (SCC) zijn gesloten en een Data Transfer Impact Assessment (DTIA) is uitgevoerd.

Doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (EER) is alleen toegestaan als het beschermingsniveau in het betreffende land adequaat is. De gemeente hanteert het beleid om zo min mogelijk gebruik te maken van (sub)verwerkers buiten de EER. Kijk eerst of er gebruik kan worden gemaakt van een (sub)verwerker die dezelfde dienst kan leveren, maar dan binnen de EER of in een land waarvoor een adequaatheidsbesluit is genomen. Bij doorgifte van persoonsgegevens buiten de EER zal in veel gevallen, naast de verwerkersovereenkomst, ook het modelcontract van de Standard Contractual Clauses moeten worden gesloten en mogelijk een Data Transfer Impact Assessment moeten worden uitgevoerd om risico's te beperken.

Naam partij	Verwerkingslocatie	Doorgiftemechanisme/waarborgen	SCC & DTIA

BIJLAGE: DPIA PRE-SCAN

Verwerkingen waarvoor een DPIA verplicht is

Als sprake is van een hoog privacyrisico voor de personen van wie gegevens worden verwerkt, moet een DPIA worden uitgevoerd voordat de verwerking wordt gestart. De Autoriteit Persoonsgegevens (AP) heeft een lijst met verwerkingen uitgegeven waarvoor de DPIA verplicht is. Deze is onderverdeeld in Lijst 1 (verwerkingen waarvoor een DPIA verplicht is) en Lijst 2.

Lijst 1: Verwerkingen waarvoor een DPIA verplicht is

De verwerkingen waarbij het uitvoeren van een DPIA verplicht is, staan hieronder beschreven. Indien bij invulling van deze lijst **één van de antwoorden met "Ja" wordt beantwoord,** dan is het verplicht om een DPIA uit te voeren en hoeft Lijst 2 niet meer te worden ingevuld. Ga dan direct door naar 'Algehele conclusie'.

	Omschrijving AP	Ja/Nee	Toelichting/argumentatie
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 rechercheburea's, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten). Een 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 DPIA te worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever).	Nee	*Grootschalig* *Om te bepalen of een verwerking grootschalig is, kijk dan naar de volgende criteria:* - *het aantal betrokkenen (de mensen van wie je gegevens verwerkt);* - *de hoeveelheid gegevens die je verwerkt;* - *de duur van de gegevensverwerking;* - *de geografische reikwijdte van de verwerking.* *Stelselmatig* *Stelselmatig of systematisch betekent ordelijk, volgens een bepaald systeem opgezet.*
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 (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).	Nee	
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).	Nee	
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.	Nee	

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).	Nee	
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).	Nee	
7.	**Gezondheidsgegevens** Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.	Nee	*Gezondheidsgegevens zijn alle gegevens die betrekking hebben op de gezondheidstoestand van een persoon en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand. Het gaat dus om meer dan alleen medische gegevens. Het gegeven dat iemand ziek is (zonder dat bekend is om wat voor ziekte het gaat) of het gegeven dat iemand de bedrijfsarts heeft bezocht, zijn ook gezondheidsgegevens.*
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 (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.	Nee	
9.	**Cameratoezicht** Grootschalige en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.	Nee	
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).	Nee	
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).	Nee	
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).	Nee	
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.	Nee	
14.	**Internet of things**	Nee	

	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).		
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.	Nee	
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.	Nee	
17.	**Biometrische gegevens** Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren. Op grond van de AVG 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 de Uitvoeringswet AVG. De verwerking van biometrische gegevens is alleen toegestaan als de verwerking strikt noodzakelijk is voor authenticatie of beveiligingsdoeleinden.	Nee	

Conclusie Lijst 1:

Op basis van Lijst 1 is een DPIA **[NIET]** verplicht.

Indien het resultaat uitkomt op "niet verplicht" → **ga dan door met Lijst 2**.
Indien het resultaat uitkomt op "wel verplicht" → neem **contact op met jouw Privacy Officer** voor het uitvoeren van een DPIA.

Let op:
- Indien je een DPIA moet uitvoeren, raadpleeg dan een Privacy Officer.
- De gemeente heeft een format voor een DPIA dat verplicht moet worden gebruikt. Deze is te vinden op de privacypagina op intranet/Sam of via de privacy officer.
- Houd er verder rekening mee dat de DPIA verplicht moet worden voorgelegd aan de interne toezichthouder van de gemeente, de Functionaris Gegevensbescherming (FG).

<u>Lijst 2</u>: Verwerkingen waarvoor *mogelijk* een DPIA verplicht is

De Europese privacy toezichthouders hebben negen (9) criteria opgesteld om te beoordelen of een voorgenomen verwerking van persoonsgegevens een hoog privacyrisico zal opleveren voor de betrokken personen. Deze criteria zijn hieronder opgenomen in Lijst 2. Als vuistregel kun je hanteren dat een DPIA verplicht moet worden uitgevoerd als de verwerking aan twee (2) of meer van de negen (9) criteria voldoet.

	Toetsing verwerking met een hoog privacyrisico	Ja/Nee	Toelichting/argumentatie
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.	Nee	*Profiling is een profiel opbouwen rond een persoon aan de hand van bepaalde gegevens. Het doel hiervan is om inzicht te krijgen in bepaalde persoonlijke kenmerken van de persoon. Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.*
2.	**Geautomatiseerde beslissingen** Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.	Nee	*Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.*
3.	**Stelselmatige en grootschalige monitoring** Het gaat hierbij om monitoring van openbaar toegankelijke ruimten.	Nee	*Bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.*
4.	**Gevoelige gegevens** Het gaat hierbij om bijzondere persoonsgegevens, Burgerservicenummer, strafrechtelijke gegevens en andere gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.	Ja	*Bijzondere persoonsgegevens zijn gegevens over iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gezondheid (lichamelijk en geestelijk), seksueel gedrag of seksuele gerichtheid, genetische gegevens (zoals DNA) en biometrische gegevens (zoals vingerafdrukken).*
5.	**Grootschalige gegevensverwerkingen** Het gaat hierbij om verwerkingen waarbij op grote schaal persoonsgegevens worden verwerkt. Om te bepalen of het grootschalig is, kijk dan naar de volgende criteria: - het aantal betrokkenen (de mensen van wie je gegevens verwerkt); - de hoeveelheid gegevens die je verwerkt; - de duur van de gegevensverwerking; - de geografische reikwijdte van de verwerking.	Nee	*Voorbeelden van grootschalige verwerkingen:* - *Een ziekenhuis dat patiëntgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.* - *Een vervoersmaatschappij die reisinformatie verwerkt van mensen die met het openbaar vervoer in een bepaalde stad reizen. Bijvoorbeeld door hen te volgen via reiskaarten.*

			- *Een verwerker die gespecialiseerd is in marktonderzoek en die in opdracht van een internationale fastfoodketen de actuele locatiegegevens van klanten verwerkt voor statistische doeleinden.* - *Een verzekeringsmaatschappij of bank die klantgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.* - *Een zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag.* - *Een telefoon- of internetprovider die gegevens verwerkt over het telefoon- en/of internetgedrag van klanten. Zoals inhoud, verkeer en locatie.*
6.	**Gekoppelde databases** Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn.	Nee	*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.*
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. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens.	Nee	*Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.*
8.	**Gebruik van nieuwe technologieën** Het gaat hierbij om innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen. Het gebruik van een nieuwe technologie kan gepaard gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacy risico's. De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen.	Nee	*Hierbij gaat het bijvoorbeeld om Internet of Things'-toepassingen die een grote impact hebben op het dagelijks leven en de privacy van mensen.*
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.	Nee	*Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.*

Conclusie Lijst 2:

Op basis van Lijst 2 is een DPIA **[NIET]** verplicht.

Indien het resultaat uitkomt op "niet verplicht" → **Ga dan verder met het invullen van de Privacy Quickscan**.
Indien het resultaat uitkomt op "wel verplicht" → neem **contact op met jouw Privacy Officer** voor het uitvoeren van een DPIA.