



PRIVACY
C O M P A N Y

Handboek AVG & statistisch onderzoek

Vereniging voor Statistiek en Onderzoek

Definitief

09-12-2022

Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: "AVG") in werking getreden. Deze wet geeft regels voor de verwerking van persoonsgegevens. Het gaat hierbij om de verplichtingen welke gelden voor verwerkingsverantwoordelijken en verwerkers. Maar ook om de rechten van respondenten. Dit zijn in de regel immers natuurlijke personen over wie persoonsgegevens worden vastgelegd.

De AVG biedt ruime kaders en mogelijkheden voor het uitvoeren van statistisch, historisch en wetenschappelijk onderzoek. Een belangrijk criterium onder de AVG is dat persoonsgegevens die worden verkregen, ontvangen of verzameld verder mogen worden gebruikt als dit verenigbaar is met het oorspronkelijke doel waarvoor deze persoonsgegevens zijn verkregen. Uit de AVG volgt expliciet dat dit voor statistisch, historisch en wetenschappelijk onderzoek verenigbaar en dus rechtmatig is.¹ Hierbij is het wel van belang dat rekening wordt gehouden met de wijze waarop in de AVG statistisch onderzoek wordt gezien, namelijk als *het verzamelen en verkrijgen van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van de resultaten*.² Daarbij bestaat het resultaat van het onderzoek niet uit persoonsgegevens, maar betreffen het uitspraken over populaties en geaggregeerde gegevens. De resultaten mogen dus niet direct worden gebruikt voor maatregelen of beslissingen op individueel niveau.

Statistisch onderzoek onder de AVG betekent nog steeds dat het onderzoeksdoel wel samen moet hangen met of direct voort moet vloeien uit bijvoorbeeld de publieke taak die je als gemeente uitvoert. Voor de verenigbaarheid is het wel van belang dat je dit kunt uitleggen. Denk bijvoorbeeld aan een woningmarktonderzoek gelet op inzichten ten behoeve van vraagstukken over ruimtelijke ordening en eventuele wijzigen van een bestemmingsplan. In die zin moet het dus toch 'verenigbaar' zijn met het oorspronkelijke verwerkingsdoel en dus samenhangen met – in de regel – de publieke taak die gemeenten uitvoeren!

De AVG schrijft verder in artikel 89 specifiek voor dat er wel maatregelen moeten worden getroffen zodat in het statistisch (historisch en wetenschappelijk) onderzoek uitsluitend de voor dat onderzoeksdoel benodigde (persoons)gegevens worden gebruikt *én* er passende technische en organisatorische maatregelen zijn getroffen. Kaders hiervoor worden in dit Handboek verder uitgewerkt.

Daarnaast volgt uit artikel 44 van de Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) dat indien persoonsgegevens *uitsluitend* voor statistisch (en wetenschappelijk) onderzoek worden gebruikt *én* voldoende maatregelen zijn getroffen om dit te waarborgen, de gemeente ervoor kan kiezen het recht op inzage (art. 15 AVG), correctie (art. 16 AVG) en de beperking van de verwerking (art. 18 AVG) niet van toepassing te verklaren. Indien de gemeente hiervoor kiest, zal men moeten onderbouwen dat men voldoet aan de toepasselijke wet- en regelgeving.

Dit Handboek is opgesteld voor alle VSO-leden en biedt handzame kaders en praktische handvatten ten behoeve van statistisch onderzoek binnen de regels van de AVG. Bij het verrichten van statistisch onderzoek wordt namelijk veel met persoonsgegevens gewerkt. Het is van belang dat dit op een zorgvuldige en verantwoorde manier gebeurt, zodat er voor respondenten geen nadelige gevolgen ontstaan en de organisatie de risico's beperkt. Door het volgen van dit Handboek bij het verrichten

¹ Algemene Verordening Gegevensbescherming, overweging 50.

² Algemene Verordening Gegevensbescherming, overweging 162.

van statistisch onderzoek worden die nadelige gevolgen en de risico's zoveel als mogelijk beperkt of uitgesloten.

Leeswijzer

Dit Handboek bestaat uit vier hoofdstukken. Elk hoofdstuk behandelt een afzonderlijke onderzoeksfase. Hoofdstuk 1 gaat in op de onderzoeksfase waarin het plan voor het uitvoeren van een statistisch onderzoek wordt opgesteld. Hierbij wordt aandacht besteed aan de AVG-aspecten waar onderzoekers rekening mee moeten houden, zoals het afsluiten van Verwerkersovereenkomsten, het formuleren van een onderzoeksdoel en het informeren van respondenten. In Hoofdstuk 2 wordt de uitvoerende fase van het onderzoek besproken en wordt aangegeven waar rekening mee moet worden gehouden bij het verkrijgen van onderzoeksdata, bij het analyseren van onderzoeksdata en wat de richtlijnen zijn met betrekking tot het bewaren en vernietigen van onderzoeksdata. Vervolgens wordt in Hoofdstuk 3 aandacht besteed aan de wijze waarop onderzoeksresultaten gepresenteerd worden. Hoofdstuk 4, tot slot, behandelt het delen van onderzoeksdata, resultaten en rapportages.

Ter verduidelijking wordt in elk hoofdstuk gebruik gemaakt van voorbeelden uit de gemeentelijke praktijk. De Bijlage van dit Handboek bevat tevens een sjabloon dat door onderzoekers gebruikt kan worden om het onderzoek voor beoordeling, goedkeuring of verantwoording voor te leggen aan de Privacy Officer of de Functionaris Gegevensbescherming.

Disclaimer

Dit Handboek AVG geeft kaders en richtlijnen voor VSO-leden voor het uitvoeren van kwalitatief en kwantitatief onderzoek gelet op de AVG. Aan dit Handboek AVG kunnen geen rechten worden ontleend waarop VSO-leden zich in de praktijk op kunnen beroepen. Ieder VSO-lid is er zelf voor verantwoordelijk dat het uitgevoerde en gepresenteerde statistische onderzoek voldoet aan de AVG.

Inhoudsopgave

Inleiding	2
Leeswijzer	3
Disclaimer	3
Startnotitie	7
De do's and dont's van AVG-conform onderzoek.....	6
Hoofdstuk 1: Het plan voor het uitvoeren van een statistisch onderzoek	7
Het opdrachtgeverschap	7
Interne opdrachtgever.....	8
Externe opdrachtgever	8
Externe opdrachtnemer.....	8
Verwerkersovereenkomsten	9
Het onderzoeksdoel en de grondslag	10
Het onderzoeksdoel	10
De grondslag	10
1. Onderzoek in het kader van een wettelijke verplichting:	10
2. Onderzoek in het kader van een publieke taak van algemeen belang	11
3. Onderzoek op basis van een overeenkomst	12
4. Onderzoek op basis van gerechtvaardigd belang	12
5. Onderzoek op basis van voorafgaande toestemming:.....	12
Verdere verwerkingen	13
De voor het onderzoek noodzakelijke data.....	14
Data onder de AVG.....	14
Gewone persoonsgegevens.....	14
Bijzondere persoonsgegevens	14
Gevoelige persoonsgegevens	15
Dataminimalisatie	15
Data reeds aanwezig binnen de gemeente	15
Het gebruik van basisregistraties	16
Data uit externe bronnen.....	17
Het koppelen van verschillende databronnen	17
Maatregelen om data en analyses te beveiligen	17
Data Protection Impact Assessment.....	18
Het informeren van respondenten en de rechten van respondenten.....	19
Hoofdstuk 2: Het uitvoeren van het onderzoek.....	21
Het verkrijgen van onderzoeksdata bij Respondenten	21
Het benaderen van respondenten.....	21
Onderzoek bij respondenten op basis van panel-onderzoek	21
Onderzoek op basis van een algemeen belang of wettelijke verplichting	21
Adreslijsten	21
Het ontvangen en verwerken van de resultaten van de respondenten	22
Het verkrijgen van onderzoeksdata buiten respondenten.....	23
Interne afdelingen	23
Externe bestanden	23
Het ontvangen, bewaren en vernietigen van onderzoeksdata	23
Versleutelen	23
Bewaren en vernietigen van onderzoeksdata.....	23

Hoofdstuk 3: Het presenteren van de onderzoeksresultaten.....	25
Wijze van rapporteren.....	25
Anonimiseren, pseudonimiseren en aggregeren.....	26
Geaggregeerde persoonsgegevens	26
Pseudonimisatie door middel van hashing.....	27
Toestemming.....	28
Externe bronnen.....	29
Hoofdstuk 4: Het delen van onderzoeksdata, resultaten en rapportages	30
Onderzoeksdata.....	30
Onderzoeksresultaten en -rapportages	30
Slot	30
Bijlage 1: Startnotitie.....	31
Bijlage 2: DPIA Checklist	36
Bijlage 3: Template privacyverklaring voor respondenten.....	40
Bijlage 4: Template toestemmingsformulier interview of panelonderzoek	44

De do's and dont's van AVG-conform onderzoek

1. Werk waar mogelijk met anonieme onderzoeksdata.
2. Een statistisch onderzoek vereist dat de resultaten, analyses en rapportages op geaggregeerd niveau worden gepresenteerd.
3. De onderzoeksresultaten van een statistisch onderzoek mogen niet herleidbaar zijn tot een persoon of gebruikt worden om op individuele basis een beslissing te nemen.
4. Als een onderzoeksbureau de opdracht krijgt een statistisch onderzoek uit te voeren op basis van persoonsgegevens, zorg dan voor een juiste verwerkersovereenkomst.
5. Zonder wettelijke basis, bevoegdheid of belang (AVG-grondslag) mag je geen persoonsgegevens verwerken, ontvangen of verstrekken.
6. Identificatienummers die voortvloeien uit de wet (BSN, A-nummer, paspoortnummer en vergelijkbare nummers) mogen alleen worden verwerkt voor de uitvoering van de wet. Daarnaast moet het noodzakelijk zijn om het identificatienummer te gebruiken. In de regel is het voor onderzoek niet noodzakelijk en vereist om dergelijke identificatienummers te gebruiken!
7. Respondenten die jonger zijn dan 12 jaar hebben toestemming nodig van de wettelijke vertegenwoordiger, tenzij het kind middelbaar onderwijs volgt.
8. Respondenten die via internet deelnemen en jonger zijn dan 16 jaar hebben toestemming nodig van de wettelijk vertegenwoordiger;
9. Afwijken van de AVG, UAVG en de kaders als beschreven in dit Handboek brengt risico's met zich mee. Het is echter mogelijk af te wijken indien hiertoe door het college een afwijkingsbesluit wordt genomen waarin wordt onderbouwd waarom van de wettelijke kaders wordt afgeweken. Raadpleeg hiervoor altijd vooraf de Privacy Officer en Functionaris Gegevensbescherming.

Hoofdstuk 1: Het plan voor het uitvoeren van een statistisch onderzoek

In dit Hoofdstuk wordt beschreven waar rekening mee moet worden gehouden in de planvormingsfase van een statistisch onderzoek. Door al in deze fase van het onderzoek rekening te houden met de eisen die volgen uit de AVG kunnen problemen in latere fases van het onderzoek voor een groot deel voorkomen worden. Dit wordt ook wel Privacy by Design of Privacy by Default genoemd. Door de overwegingen die in deze fase van het onderzoek worden gemaakt goed te documenteren is het ook makkelijker om te voldoen aan een van de belangrijkste plichten uit de AVG: de verantwoordingsplicht.

Startnotitie

In het kader van de AVG is het van groot belang om aan te kunnen tonen dat er AVG-conform onderzoek wordt verricht. Deze aantoonbaarheid vereist dat overwegingen met betrekking tot persoonsgegevens die gemaakt zijn ter voorbereiding op het onderzoek goed worden vastgelegd. Dit doe je in een startnotitie. In Bijlage 1 van dit Handboek is een sjabloon Startnotitie opgenomen. Vul voor ieder nieuw onderzoek deze startnotitie in aan de hand van het Handboek en leg het voor aan de Privacy Officer en/of Functionaris Gegevensbescherming ter beoordeling, accordering of verantwoording.

Op basis van de Startnotitie kan door de Privacy Officer en/of Functionaris Gegevensbescherming, of een vergelijkbare functionaris, worden beoordeeld of het kwantitatieve of kwalitatieve onderzoek dat zal worden verricht moet worden opgenomen in het verwerkingsregister van de gemeente. De AVG vereist dat alle verwerkingen die niet incidenteel zijn worden geregistreerd in het verwerkingsregister.

Verwerkingsregister

Kortom, als het onderzoek niet incidenteel is, en dus op structurele basis zal plaatsvinden, moet dat type onderzoek dus worden opgenomen in het verwerkingsregister. Een onderzoek voor een specifiek onderzoeksdoel dat slechts incidenteel plaatsvindt, hoeft op grond van de AVG niet in het verwerkingsregister te worden opgenomen. Het advies is in het verwerkingsregister generiek de verwerking 'het verrichten van kwantitatief en kwalitatief onderzoek' op te nemen inclusief een generieke beschrijving van de voor het verwerkingsregister vereiste informatie. Hiermee zijn dan alle vormen van onderzoeken die structureel worden verricht gedekt (en beschreven), zolang de onderzoeken worden uitgevoerd binnen de beschrijving van die generieke verwerking. Indien er specifieke onderzoeken op structurele basis, meer dan eenmalig, worden uitgevoerd die afwijken van de generieke verwerking als beschreven in het verwerkingsregister, bijvoorbeeld indien hierbij bijzondere persoonsgegevens worden verwerkt, dan is het advies die verwerking apart te registreren in het verwerkingsregister.

Het opdrachtgeverschap

Onder de AVG is het van groot belang dat bepaald is wie verantwoordelijk is voor het verwerken van de persoonsgegevens. Doorgaans zal dit de gemeente zijn die het onderzoek uitvoert of laat uitvoeren. De verantwoordelijkheid voor het verwerken van persoonsgegevens brengt belangrijke verplichtingen met zich mee. Zo zal de gemeente moeten controleren en garanderen dat een door haar ingeschakeld onderzoeksbureau de AVG naleeft. De gemeente is als opdrachtgever namelijk de uiteindelijke verantwoordelijke die in het geval dat er iets fout gaat met het verwerken van persoonsgegevens ook verantwoordelijk kan worden gehouden. Door duidelijk vooraf te bepalen bij wie de verantwoordelijkheid voor het verwerken van persoonsgegevens ligt, zorg je er als

onderzoeker voor dat je weet wie waarvoor verantwoordelijk is en welke zaken extra aandacht behoeven.

Gelet op het uitvoeren van statistisch onderzoek kunnen de volgende rollen onderscheiden worden:

Interne opdrachtgever

De onderzoekers binnen een gemeente voeren een onderzoek uit op een bepaald beleidsterrein. Deze onderzoeksbehoefte is in de regel afkomstig van een bepaalde afdeling of team dat verantwoordelijk is voor de uitvoering van die gemeentelijke taken. Op grond van de AVG is het college respectievelijk de burgemeester de verantwoordelijke voor het naleven van de AVG bij het uitvoeren van het onderzoek. Indien een onderzoek afdelingoverstijgend is, dan zal afhankelijk van de ambtelijke organisatie de bevoegdheid tot het opdracht geven voor een onderzoek gegeven kunnen worden door een gemeentesecretaris, directeur of afdelingshoofd. Belangrijk is na te gaan wie waarvoor intern gemandateerd is, zoals op basis van het mandaatbesluit. Indien het een specifieke vraag is voor een onderzoek vanuit een bepaalde afdeling of een team, dan is deze afdeling (of het team) degene die intern het doel van het onderzoek bepaald. Het desbetreffende afdelingshoofd zal in dat geval logischerwijs de interne opdrachtgever zijn, voor zover in een mandaatbesluit niet anders is bepaald.

In het geval van bijvoorbeeld een opdracht vanuit de afdeling Sociaal Domein die een onderzoek wenst naar de effectiviteit van het beleid op het terrein van de Participatiewet, zijn de volgende uitgangspunten van belang. Het onderzoeksdoel wordt door de afdeling Sociaal Domein bepaald. Dit betekent dat de onderzoeker het statistisch onderzoek uitvoert voor de desbetreffende afdeling. Mede omdat het in de regel zal gaan om de (persoons)gegevens die door die afdeling bij de uitvoering worden gebruikt. Daarom is de afdeling voor wie het onderzoek verplicht, of op verzoek, wordt uitgevoerd de opdrachtgever én dus ook onder de AVG degene die intern verantwoordelijk is: *de verwerkingsverantwoordelijke*. Deze interne verantwoordelijkheid brengt de verplichting mee om te zorgen voor het juist en correct uitvoeren van het onderzoek binnen de kaders van de AVG. Een Afdeling Onderzoek (& Statistiek) of de onderzoeker binnen de gemeente is dus niet de opdrachtgever. Zorg er dan ook voor dat de intern verantwoordelijke opdrachtgever van het domein, de afdeling of het team de Startnotitie (Bijlage 1) accordeert.

Externe opdrachtgever

In de praktijk komt het voor dat een grotere gemeente of gemeente met een eigen Afdeling Onderzoek wordt gevraagd een statistisch onderzoek uit te voeren namens een andere gemeente(n). In dat geval is de uitvoerende gemeente de opdrachtnemer en zal zij onderzoeksdata van de andere gemeente(n) gaan verwerken. Als die onderzoeksdata ook bestaan uit persoonsgegevens treden de gemeenten die de opdrachtgever zijn op als *verwerkingsverantwoordelijken* onder de AVG. De uitvoerende gemeente treedt in dat geval als opdrachtnemer op als *verwerker*. In dit geval ben je als gemeenten, zowel opdrachtgever als opdrachtnemer, verplicht een verwerkersovereenkomst te sluiten.

Externe opdrachtnemer

Als de gemeente een extern onderzoeksbureau in wil schakelen voor het uitvoeren van een statistisch onderzoek en de onderzoeksdata ook persoonsgegevens bevatten, dan kwalificeert deze externe opdrachtnemer als een *verwerker*. Dit betekent dat de gemeente vooraf moet controleren of het desbetreffende onderzoeksbureau de opdracht uit kan voeren binnen de regels van de AVG. Naast deze controle moet bij gebleken geschiktheid met het onderzoeksbureau een verwerkersovereenkomst worden gesloten. Deze verwerkersovereenkomst moet feitelijk voorafgaand aan het onderzoek zijn ondertekend. In de verwerkersovereenkomst staan bepalingen

en afspraken opgenomen dat het onderzoeksbureau voldoet aan de AVG en handelt conform de instructies van de gemeente als opdrachtgever. In gesprekken en op basis van documentatie moet in ieder geval duidelijk worden:

- a. Wat het onderzoeksdoel is en welke gegevens hiervoor noodzakelijk zijn;
- b. Of het onderzoeksbureau voldoet aan de Baseline informatiebeveiliging overheid (BIO) of ISO:27001 dan wel vergelijkbare normen op het gebied van informatiebeveiliging;
- c. Op welke wijze voldoet zij aan deze informatiebeveiligingsnormen en toont zij dit aan;
- d. Hoe worden de gegevens beveiligd bij het benaderen, de uitvraag of afname van de enquête of het interview, het verzamelen, de verdere analyse en delen van de resultaten/rapportage;
- e. Welke applicaties/software/systemen worden voor het uitvoeren van de opdracht gebruikt;
- f. Waar worden de gegevens opgeslagen (uitgangspunt binnen de EU/EER); en
- g. Wie hebben binnen het onderzoeksbureau of de opdrachtnemer toegang tot de gegevens; en
- h. Worden de onderzoeksresultaten vernietigd, geanonimiseerd of terug gegeven aan de opdrachtgever.

Belangrijk: de gemeente blijft (onder de AVG) eindverantwoordelijk voor de wijze waarop het onderzoeksbureau omgaat met de persoonsgegevens die worden gebruikt! Het daadwerkelijk controleren of een onderzoeksbureau is lastig in de fase van contractering en vraagt ook om medewerking. Tijdens het onderzoek of achteraf kan op basis van de juiste bepalingen in de verwerkersovereenkomst op te nemen de gemeente wel het onderzoeksbureau controleren op de correcte naleving. Betrek hierbij de CISO (in verband met informatiebeveiliging) als de Privacy Officer en/of Functionaris Gegevensbescherming. Zij kunnen de risico's vooraf vaak beter inschatten.

Verwerkersovereenkomsten

In een verwerkersovereenkomst maken de opdrachtgever van het onderzoek (*verwerkingsverantwoordelijke*) en de opdrachtnemer (*verwerker*) afspraken over hoe zij omgaan met het verwerken van persoonsgegevens bij het uitvoeren van de opdracht. Voor de gemeenten betekent dit dat een verwerkersovereenkomst moet worden gesloten indien:

- de gemeente gebruik maakt van een extern onderzoeksbureau; of
- de gemeente zelf door andere partijen wordt ingeschakeld om een onderzoek (in opdracht) uit te voeren.

Als er sprake is van een onderzoek waarbij alleen geanonimiseerde gegevens door de gemeente worden aangeleverd en door het *externe* onderzoeksbureau verwerkt, is er geen verwerkersovereenkomst nodig. Let op: als er sprake is van het verwerken van gepseudonimiseerde persoonsgegevens door het onderzoeksbureau moet er wel een verwerkersovereenkomst worden gesloten.

Het is verstandig eerst de onderdelen uit Hoofdstuk 1 verder te bepalen. Immers kan op die manier inzichtelijk worden gemaakt voor welk doel het onderzoek wordt uitgevoerd en welke persoonsgegevens als onderzoeksdata benodigd zijn. Deze informatie moet namelijk ook expliciet in de verwerkersovereenkomst worden beschreven, namelijk het doel van de verwerking, welke persoonsgegevens, en hoe lang de gegevens worden bewaard. Hanteer voor de verwerkersovereenkomst de 'Standaard VNG verwerkersovereenkomst' zoals verplicht gesteld voor alle gemeenten. Tenzij hier intern binnen de gemeente andere afspraken over zijn gemaakt.

Leg de Startnotitie en verwerkersovereenkomst vervolgens voor aan de Privacy Officer en/of Functionaris Gegevensbescherming ter beoordeling en accordering. De verwerkersovereenkomst moet overigens door de hiertoe bevoegde intern verantwoordelijke worden ondertekend.

Het onderzoeksdoel en de grondslag

Voordat een onderzoek kan aanvangen moet verantwoord worden wat het onderzoeksdoel is/de onderzoeksdoelen zijn. Daarnaast moet je onderbouwen op basis waarvan (welke grondslag) de daarvoor vereiste persoonsgegevens verwerkt mogen worden. Dit leg je vast in de Startnotitie.

Het formuleren van het onderzoeksdoel en de grondslag volgt uit twee belangrijke AVG-eisen:

1. Er moet een legitiem doel zijn (*doelbinding*); en
2. Een rechtmatige grondslag (*rechtmatigheid*).

Het onderzoeksdoel

Het onderzoeksdoel moet goed afgebakend worden en zo concreet en specifiek mogelijk worden beschreven. Dit houdt in dat het doel geformuleerd moet worden in termen van het te verwerven/presenteren inzicht en de achterliggende ratio: welke inzichten wil je verkrijgen met het onderzoek en waarom wil je deze inzichten verkrijgen?

Kortom, bepaal en beschrijf zo concreet en specifiek mogelijk:

- a. Wat wil je onderzoeken?
- b. Waarom wil je dit onderzoeken?
- c. Welke inzichten verwacht je met het onderzoek te verkrijgen? en
- d. Waarvoor wil je de onderzoeksresultaten gebruiken?

De grondslag

Wanneer het onderzoeksdoel is geformuleerd moet er bepaald worden op basis waarvan je dat doel wilt bereiken. Dit wordt de grondslag genoemd. Als je voor het onderzoeksdoel ook onderzoeksdata nodig hebt die bestaat uit persoonsgegevens, zijn er vijf grondslagen die het verwerken van persoonsgegevens in het kader van statistisch onderzoek kunnen rechtvaardigen:

1. Onderzoek in het kader van een wettelijke verplichting:

Als een onderzoek moet worden uitgevoerd, omdat dit in een wet is voorgeschreven, voer je het onderzoek uit omdat een wet (of lagere regeling) dit verplicht. Denk hierbij aan het cliëntervaringsonderzoek dat op grond van de Jeugdwet of Wet maatschappelijke ondersteuning 2015 (Wmo2015) moet worden uitgevoerd:

Artikel 2.5.1 lid 1 Wmo2015:

Het college onderzoekt hoe de cliënten de kwaliteit van de maatschappelijke ondersteuning ervaren en publiceert jaarlijks voor 1 juli de uitkomsten hiervan.

Hier staat dus letterlijk in de wet de verplichting voor de gemeente om jaarlijks een cliëntervaringsonderzoek uit te voeren. In de Uitvoeringsregeling Wmo2015 staat vervolgens waar dit onderzoek in ieder geval aan dient te voldoen:

- 2 Voor het onderzoek, bedoeld in het eerste lid, wordt gebruik gemaakt van een vragenlijst die ten minste ingaat op hoe personen als bedoeld in het eerste lid indien toepasbaar:
 - a. de toegankelijkheid van voorzieningen ervaren;
 - b. de kwaliteit van de ondersteuning ervaren; of
 - c. de ondersteuning vinden bijdragen aan de zelfredzaamheid en participatie.
- 3 Het onderzoek, bedoeld in het eerste lid, kan door middel van een representatieve steekproef worden uitgevoerd.

2. Onderzoek in het kader van een publieke taak van algemeen belang

Deze grondslag moet je gebruiken indien het doel van het onderzoek voortvloeit en samenhangt met een publieke taak die, bijvoorbeeld, een gemeente uitoefent voor het algemeen belang of openbaar gezag. Het gaat hierbij wel om publieke taken van de gemeente die ergens in een wet zijn vastgelegd. Denk hierbij aan het analyseren van gegevens die nodig zijn om het beleid met betrekking tot een publieke taak of de kwaliteit hiervan te evalueren en te verbeteren.

Hoe bepaal je of er sprake is van een algemeen belang? In tegenstelling tot een onderzoek vanwege een wettelijke verplichting waar de verplichting in de specifieke wet staat, volgt het verrichten van een kwantitatief of kwalitatief onderzoek bij 'algemeen belang' niet uit de wet. Het onderzoeksdoel kan dus heel breed zijn! Belangrijk is dat het onderzoek wordt uitgevoerd voor doeleinden die samenhangen met de taken die door de gemeente worden uitgevoerd. Het is aan de interne (of externe) opdrachtgever om aan te geven waarom het onderzoek en onderzoeksdoel gelet op de publieke taak van de opdrachtgever moet worden uitgevoerd. Feitelijk kun je als vuistregel hanteren dat elke vorm van statistisch onderzoek waarbij het onderzoeksdoel direct of indirect samenhangt met de aan de gemeente opgedragen taken, plaatsvindt op basis van deze grondslag.

Voorbeelden zijn het in kaart brengen en rapporteren van hoog geaggregeerde gegevens (niet herleidbaar tot individuen) met betrekking tot:

Evaluatie heffingsmaatstaf rioolbelasting

Het evalueren van het beleid met betrekking tot de heffing van de gemeentelijke rioolbelasting en heffingsmaatstaf. Het kan zijn dat op dit moment bij een gemeente de WOZ-waarde wordt gebruikt als de heffingsmaatstaf voor het heffen van rioolbelasting. Mogelijk zou het heffen op basis van waterverbruik andere inzichten kunnen opleveren, waardoor dit – bijvoorbeeld – meer rendement oplevert voor de gemeentelijke begroting. De Gemeentewet geeft de gemeente de bevoegdheid om gemeentelijke belastingen te heffen. Om te kunnen verantwoorden welke heffingsmaatstaf zij/de gemeente hierbij hanteert kan dit – voor zover wettelijk toegestaan – andere vormen onderzoeken. Als de gemeente hierbij persoonsgegevens als onderzoeksdata gebruikt, moet zij zich baseren op de grondslag 'algemeen belang'.

Kwalitatief woononderzoek

Een gemeente wil weten of de beschikbare woningvoorraad in de gemeente nog aansluit op de woningbehoefte van haar inwoners. Dit om de woonvisie en het woonbeleid van de gemeente aan voor de komende 10 jaar op te stellen. Hierbij wordt gekozen voor:

1. Een onderzoek naar de omvang en samenstelling van de bestaande woningvoorraad:
Bij dit onderzoek gebruikt de gemeente enkel de voor haar beschikbare gegevens uit haar basisregistraties. De resultaten gebruikt zij om haar publieke taken en daarmee samenhangend beleid uit te voeren. De onderzoeksresultaten worden gebruikt voor de woonvisie en het woonbeleid; en
2. Een woonbehoefteonderzoek onder inwoners:
Bij een enquête onder inwoners kan het verwerken van die eventuele persoonsgegevens niet worden gebaseerd op 'algemeen belang'. In dat geval moet de gemeente zich baseren op 'toestemming'.

Aanpassen handhavingsbeleid vuurwerkoverlast

De gemeente wenst inzichten te verkrijgen in de effectiviteit van haar handhavingsbeleid openbare orde, specifiek gelet op vuurwerkoverlast. De gemeente wil inzicht in hoe zij de aanpak van vuurwerkoverlast nog effectiever kan voorkomen en handhaven. Uit de Gemeentewet volgt dat de gemeente, specifiek de burgemeester, de taak heeft de openbare orde en veiligheid binnen de gemeente te handhaven. Hierbij wordt onderzoek gedaan naar het aantal geconstateerde meldingen van vuurwerkoverlast over de afgelopen jaren, de schade, het aantal meldingen, en welke hot-spots er binnen de gemeente bestaan waar de kans op vuurwerkoverlast groot is. Dit onderzoek is ondersteunend aan het gemeentelijk beleid en hangt zodoende samen met een publieke taak.

3. Onderzoek op basis van een overeenkomst

Deze grondslag moet je gebruiken voor onderzoeken die plaatsvinden doordat (een groep) burgers, medewerkers of belanghebbenden structureel en periodiek deelnemen aan panel-onderzoeken. Hierbij gaan respondenten akkoord om deel te nemen aan een panel-onderzoek, waarbij zij akkoord gaan om op regelmatige basis uitgenodigd te worden voor deelname aan een panel-onderzoek. Zij moeten wel de mogelijkheid hebben om niet deel te nemen aan een onderzoek. Ook moeten zij zich af kunnen melden voor deelname aan het panel-onderzoek (denk aan een opt-out (link)).

4. Onderzoek op basis van gerechtvaardigd belang

Het kan ook zijn dat je een onderzoek uit gaat voeren voor de bedrijfsvoering van de gemeente. Bijvoorbeeld een onderzoek naar het Arbeidsomstandighedenbeleid binnen de gemeente. Dit betreft geen publieke taak van de gemeente, maar hierbij treedt de gemeente op net als ieder andere (commerciële) werkgever. In die gevallen zul je voor statistisch onderzoek dat niet samenhangt met een wettelijke verplichting of publieke taak je moeten baseren op 'gerechtvaardigd belang'. Daarbij moet je verantwoorden waarom je als 'werkgever' een belang hebt een statistisch onderzoek uit te voeren. In dat geval moet je wel een belangenafweging maken en verantwoorden. Het belang van de gemeente moet dan zwaarder wegen dan het belang van de individuele medewerker. Met name moet je deze belangenafweging goed kunnen uitleggen als je persoonsgegevens gaat verwerken. Als je een medewerkersenquête over bijvoorbeeld tevredenheid wilt uitvoeren, kun je medewerkers niet verplichten aan het statistisch onderzoek mee te doen. Ook zal er geen 'gerechtvaardigd belang' zijn dat zwaarder weegt voor de gemeente. Daarom moet je in dergelijke gevallen gebruik maken van 'toestemming'. Zie hieronder.

5. Onderzoek op basis van voorafgaande toestemming:

Als er geen sprake is van één van de bovengenoemde grondslagen, dan zou je alsnog op basis van voorafgaande toestemming van de respondent een onderzoek kunnen verrichten. Hier zal met name sprake van zijn bij enquêtes, interviews en focusgroepen. Het is wel van belang dat de respondent vooraf duidelijk wordt geïnformeerd over waarvoor men toestemming geeft (doel onderzoek), welke gegevens (bij voorkeur geanonimiseerd) worden verwerkt, of bijvoorbeeld de naam van de geïnterviewde wordt gepubliceerd, wanneer de persoonsgegevens worden vernietigd, en dat men de mogelijkheid heeft om de toestemming in te trekken. Deze informatie kan je in een privacyverklaring opnemen die bij het toestemmingsformulier wordt verstrekt.

Let op: feitelijk kun je bij het uitzetten en uitvoeren van een onderzoek te maken hebben met twee vormen van toestemming. Dit wordt onderscheiden in:

- a. Het benaderen van respondenten: in de gevallen dat het je niet op basis van een wettelijke verplichting, een taak van algemeen belang, overeenkomst of gerechtvaardigd belang respondenten wilt benaderen voor een deelname – bijvoorbeeld middels enquête – aan het

onderzoek, dan zul je als je respondenten wilt uitnodigen eerst voor het uitnodigen en benaderen om toestemming moeten vragen. Zie hiervoor verder de toelichting bij 'Het benaderen van respondenten'.

- b. Het verkrijgen van de respons van de respondenten: het is noodzakelijk dat de respondent toestemming geeft het verkrijgen, verzamelen en (verder) verwerken van de respons.

Daarnaast is het van groot belang om de toestemming vast te leggen! Dit om discussies te voorkomen over de vraag of toestemming is gegeven. Hanteer hierbij een veld waarbij men het veld aan moet vinken en daarbij verklaart toestemming te geven voor het onderzoek. Houd er ook rekening mee dat de toestemming voor niet-geanonimiseerde persoonsgegevens kan worden ingetrokken. Dit betekent dat de persoonsgegevens niet meer mogen worden gebruikt voor het onderzoek, tenzij hierdoor het bereiken van het doel van het onderzoek onmogelijk is. Zorg er in dat geval voor dat de onderzoeksdata volledig geanonimiseerd worden. Overigens geniet het sterk de voorkeur om altijd met geanonimiseerde gegevens te werken, dan wel met gepseudonimiseerde gegevens op hoog geaggregeerd niveau, zodat deze niet herleidbaar kunnen zijn tot een individu. In de rapportage van het onderzoek is dat immers ook niet nodig.

Let wel: het intrekken van toestemming voor reeds gerapporteerde of gepubliceerde onderzoeksrapporten of interviews geldt enkel voor het verdere gebruik van die resultaten en interviews. De eerder gerapporteerde en gepubliceerde interviews hoeven, tenzij er sprake is van feitelijke onjuistheden, niet te worden verwijderd.

Wanneer je bijzondere persoonsgegevens (zie de *paragraaf* Data onder de AVG) wilt verwerken op grond van toestemming, is de 'gewone' toestemming van een respondent onvoldoende. In dat geval moet je namelijk 'uitdrukkelijke' toestemming verkrijgen. De beste manier om uitdrukkelijke toestemming te verkrijgen is door de respondent een schriftelijke verklaring op te laten stellen, inclusief handtekening of in ieder geval expliciet akkoord middels een *leeg* selectievakje waarin de toestemming wordt gevraagd. Dit kan bijvoorbeeld via een online formulier, e-mail of een brief ondertekend door de respondent.

Let op:

1. Respondenten die jonger zijn dan 12 jaar hebben toestemming nodig van de wettelijke vertegenwoordiger, tenzij het kind middelbaar onderwijs volgt.
2. Respondenten die via internet deelnemen en jonger zijn dan 16 jaar hebben toestemming nodig van de wettelijk vertegenwoordiger. Verricht redelijke inspanningen om dergelijke toestemming te controleren. Stuur een brief naar het adres van de ouder/wettelijk vertegenwoordiger met de link voor het geven van toestemming tot deelname aan een onderzoek via internet. Of vraag om het e-mailadres van de ouder, stuur daar een bevestigingslink heen, en laat hen pas deelnemen zodra de bevestiging is ontvangen. Laat niet deelnemen bij twijfel. De toestemming van de ouder moet ook net zo eenvoudig weer kunnen worden ingetrokken.

Is geen van de vijf bovengenoemde grondslagen van toepassing of kun je dit niet verantwoorden en onderbouwen? Dan mag het onderzoek niet plaatsvinden!

Verdere verwerkingen

In sommige gevallen kom je er na het formuleren van een doel en grondslag achter dat je de verwerkte persoonsgegevens ook nog voor een ander doel wilt gebruiken. Dit wordt een verdere verwerking genoemd. Onder de AVG zijn verdere verwerkingen niet zonder meer toegestaan: elk nieuw doel vereist ook weer een nieuwe grondslag. Daartoe bestaat echter wel een uitzondering in

het geval persoonsgegevens verder worden verwerkt met het oog op archivering in het algemeen belang of voor wetenschappelijk, historisch of statistisch onderzoek.

De voor het onderzoek noodzakelijke data

Zodra je hebt bepaald wat het doel van het onderzoek gaat zijn, kun je bepalen welke persoonsgegevens noodzakelijk zijn om te verwerken om dat doel te bereiken. Voordat daar verder op in wordt gegaan, worden de belangrijkste regels en overwegingen uit de AVG met betrekking tot data besproken.

Data onder de AVG

De AVG is van toepassing op de verwerking van één specifieke soort data: persoonsgegevens. We spreken van persoonsgegevens wanneer het gaat om data die betrekking hebben op een geïdentificeerd of identificeerbare persoon. Geanonimiseerde gegevens zijn dus geen persoonsgegevens; deze hebben namelijk niet betrekking op een geïdentificeerd of identificeerbare persoon!

Binnen de kaders van de AVG wordt gewerkt met verschillende typen persoonsgegevens: 'gewone', 'bijzondere' en 'gevoelige' persoonsgegevens. Wanneer je bijzondere of gevoelige persoonsgegevens verwerkt moet je meer beschermingsmaatregelen treffen, waarover meer in de *paragraaf* 'Maatregelen om data en analyses te beveiligen'.

Gewone persoonsgegevens

Gewone persoonsgegevens zijn de meest voorkomende persoonsgegevens, het gaat dan bijvoorbeeld om NAW-gegevens, leeftijd, en geslacht. Deze gegevens mogen verwerkt worden als daar een legitiem doel en rechtmatige grondslag voor is. Dit ligt anders bij bijzondere persoonsgegevens.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met het oog op unieke identificatie, gezondheid of seksuele leven. Dit type data geniet extra bescherming onder de AVG omdat er een bijzonder hoog privacy risico aan kleeft voor respondenten. Het zijn namelijk gegevens op basis waarvan iemand gediscrimineerd of uitgesloten zou kunnen worden. Het verwerken van bijzondere persoonsgegevens is in beginsel dan ook verboden, deze gegevens mogen alleen worden verwerkt in de volgende gevallen:

1. Er is uitdrukkelijke toestemming (zie *paragraaf* De grondslag) verkregen van de respondent; of
2. Het statistisch-onderzoek
 - a. dient een algemeen belang; **en**
 - b. de verwerking is voor statistisch-onderzoek noodzakelijk; **en**
 - c. het vragen van uitdrukkelijke toestemming blijkt onmogelijk of kost een onevenredige inspanning; **en**
 - d. er zijn technische en organisatorische maatregelen genomen en beschreven ter bescherming van de privacy.

Of:

3. Bijzondere persoonsgegevens worden anoniem geleverd. Er is in het geval van anonieme gegevens geen sprake van persoonsgegevens. In dat geval is er ook geen DPIA verplicht.

Gevoelige persoonsgegevens

Tot slot is er nog data die niet als bijzondere persoonsgegevens erkend worden, maar waaraan wel een relatief hoog privacy risico kleeft; dit noemen we gevoelige persoonsgegevens. Het gaat dan om wettelijke identificatienummers, zoals het BSN, A-nummers of paspoortnummers, gegevens over iemands strafrechtelijke verleden en ook financiële gegevens.

Let op! Identificatienummers die voortvloeien uit de wet (BSN, A-nummer, paspoortnummer en vergelijkbare nummers) mogen alleen worden verwerkt voor de uitvoering van de wet. De Nederlandse UAVG (artikel 44) schrijft voor dat een nationaal identificatienummer, zoals het BSN of A-nummer, slechts gebruikt mag worden ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald. Alleen wanneer er een wettelijke grondslag is om bijvoorbeeld het BSN-nummer te verwerken voor onderzoek, zoals in de Wet algemene bepalingen burgerservicenummer (Wabb), Wet gemeentelijke basisadministratie (artikel 109), het Besluit gemeentelijke basis administratie (artikel 67), de Wet op het Centraal bureau en de Centrale commissie voor de statistiek (artikelen 33 tot en met 36), is het gebruik van het BSN toegestaan. Voor statistisch onderzoek kun je het BSN buiten de genoemde gevallen dus niet gebruiken, omdat de UAVG dan wel overige nationale wet- en regelgeving hiervoor geen ruimte biedt!

In de praktijk bestaat er de werkwijze dat het BSN of hiermee vergelijkbaar identificeerbaar nummer (als een A-nummer) wordt gebruikt voor het koppelen van informatie, het verrijken met informatie over personen uit andere databases (of basisregistraties), of het gebruik van het BSN als 'identificatie' voor vervolgonderzoek. Dergelijk gebruik is dus niet toegestaan als hiervoor geen wettelijke mogelijkheid is. Zie hoofdstuk 3 voor meer informatie over alternatieven.

Dataminimalisatie

Zodra je hebt bepaald wat het doel van je onderzoek gaat zijn, is het zaak te bepalen welke (persoons)gegevens je nodig hebt om dat doel te bereiken. Hierbij komt een belangrijke eis uit de AVG kijken: *dataminimalisatie*. Deze eis stelt dat er niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is om het omschreven doel te bereiken. Het uitgangspunt is dan ook dat er gewerkt wordt met geanonimiseerde gegevens, in dat geval spreken we namelijk niet van persoonsgegevens en is de AVG niet van toepassing. Zie voor de wijze waarop je voorafgaand en tijdens het selecteren en verzamelen van de gegevens, en/of tijdens de analyse van de onderzoeksdata, én bij het presenteren van de onderzoeksresultaten om moet gaan met anonimiseren en pseudonimiseren Hoofdstuk 3 'Anonimiseren, pseudonimiseren en aggregeren'.

Mocht het vanwege het doel van het onderzoek niet mogelijk zijn om te anonimiseren dan dien je uit te gaan van alleen die data die noodzakelijk is om het doel van het onderzoek te bereiken. Ga in dat geval eerst uit van pseudonimiseren van de gegevens op een passend niveau. Mocht dat ook niet mogelijk zijn, dan zal je moeten verantwoorden waarom je bepaalde niet geanonimiseerd of gepseudonimiseerde onderzoeksgegevens (ruwe data) moet gebruiken. Dit alles leg je vast in de Startnotitie.

De data die je nodig hebt om het onderzoek uit te voeren kan uit verschillende bronnen afkomstig zijn. Deze worden hieronder besproken. Ook wordt ingegaan op het koppelen van verschillende databronnen en de (privacy)risico's die daaraan kleven.

Data reeds aanwezig binnen de gemeente

De gemeente beschikt over veel persoonsgegevens binnen uiteenlopende beleidsterreinen. Het is de gemeente toegestaan om statistisch onderzoek uit te voeren op basis van data (en persoonsgegevens) waar de gemeente reeds over beschikt. Het is wel van groot belang dat de data,

die voor bijvoorbeeld een aanvraag omgevingsvergunning is verstrekt, binnen statistische onderzoeken op ditzelfde beleidsterrein wordt gebruikt. De inwoner of persoon die de persoonsgegevens voor de aanvraag heeft verstrekt zal er rekening mee (moeten) houden dat die data ook voor beleid en inzichten op het gebied van ruimtelijke ordening kan worden gebruikt. Het gebruiken van die persoonsgegevens voor onderzoeken op het gebied van bijvoorbeeld de Jeugdwet is echter niet een beleidsterrein waar men rekening mee hoeft te houden.

Kortom, statistisch onderzoek met inzichten over doelgroepen en populaties is toegestaan zolang dit valt binnen het beleidsterrein of de publieke taak waarvoor de informatie in eerste instantie is verzameld. Informatie verkregen binnen een bepaald beleidsterrein of voor een bepaalde publieke taak mag dus niet zomaar door een andere afdeling gebruikt worden voor een statistisch onderzoek. Er moet dan éérst een beoordeling plaatsvinden of dit wel rechtmatig kan. Raadpleeg in dat geval de Privacy Officer en/of Functionaris Gegevensbescherming. Daarbij moet rekening gehouden worden met diverse factoren:

- Het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld (het doel en kader van verstrekking);
- De aard van de persoonsgegevens (bijvoorbeeld bijzondere, financiële of strafrechtelijke gegevens);
- Of de benodigde informatie geanonimiseerd of passend gepseudonimiseerd kan worden;
- Of degene wiens persoonsgegevens het betreft redelijkerwijs kon verwachten dat de voor het oorspronkelijke doel verstrekte persoonsgegevens ook voor het gewenste onderzoek worden gebruikt. Naarmate het doel en of het beleidsterrein verder uit elkaar liggen, zal men dit minder snel kunnen verwachten;

Het gebruik van basisregistraties

Gemeenten hebben ten behoeve van de uitvoering van hun publieke taken ook de beschikking over basisregistraties als de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Kadaster (BRK). Daarnaast voeren gemeenten ook het beheer over de Gemeentelijke Basisadministratie (GBA/BRP) en hebben ze toegang tot de GBA-V, de landelijke voorziening. Het is zodoende afhankelijk van de publieke taak of taken waarvoor het statistisch onderzoek wordt uitgevoerd of voor die publieke taak/taken gebruik mag worden gemaakt van de basisregistraties. Is het gebruik van de persoonsgegevens uit die basisregistratie(s) voor de publieke taak toegestaan, dan zal men gelet op het vereiste van 'verenigbaarheid met het oorspronkelijke doeleinde van de verwerking' en 'noodzakelijkheid' moeten beoordelen of en welke informatie uit de basisregistratie in het statistisch onderzoek mag worden meegenomen. Voor het gebruik van persoonsgegevens uit de basisregistraties geldt:

1. De publieke taak waarvoor het statistisch onderzoek wordt uitgevoerd, rechtvaardigt het gebruik van de persoonsgegevens uit de desbetreffende basisregistratie;
2. Voor het statistische onderzoeksdoeleinde is het noodzakelijk persoonsgegevens uit de desbetreffende basisregistratie te gebruiken.

Indien het gebruik van de persoonsgegevens voor de publieke taak dan wel het onderzoeksdoeleinde niet redelijkerwijs kan worden verondersteld, mag die data niet worden gebruikt. Een mogelijkheid kan dan zijn om bij respondenten informatie te verkrijgen middels toestemming. Zie hiervoor de *paragraaf*: 'Het verkrijgen van onderzoeksdata bij respondenten'.

Data uit externe bronnen

Het gevaar in het gebruik van externe bronnen zit in de kans dat de externe bronnen informatie bevatten die herleidbaar zijn. Behalve publieke bronnen, moet voor de herleidbaarheid ook naar niet-publieke bronnen gekeken worden, ook als die niet-publieke bronnen alleen door een derde partij benaderd kunnen worden. Ook indien het databestand gepseudonimiseerd is door de externe partij en niet herleidbaar is gemaakt, kan dit voor de gemeente – omdat zij de beschikking heeft over andere data en basisregistraties – mogelijk weer wel herleidbaar zijn tot een individu. De risico's zitten daarbij met name op het gebied van het kunnen koppelen van verschillende databronnen.

Het koppelen van verschillende databronnen

Doordat de gemeente beschikt over een grote verscheidenheid en hoeveelheid aan persoonsgegevens, kan het bij het verrichten van een onderzoek met verschillende databronnen zijn dat hierdoor de kans op herleidbaarheid tot een individu wordt vergroot. Zodoende is het van groot belang altijd vooraf te beoordelen:

1. Of het, gelet op het onderzoeksdoel en de 'grondslag', gerechtvaardigd is dat data uit verschillende databronnen wordt gekoppeld. Licht dit ook toe in de Startnotitie.
2. Het koppelen van data uit verschillende interne en/of externe bronnen geldt namelijk ook als een verwerking, en daar is dus ook een grondslag voor vereist!
3. Welke data benodigd is voor het onderzoeksdoel én ook te beoordelen welke data uit de verschillende bronnen mogelijk gecombineerd herleidbaar kunnen zijn. Met name wanneer onderzoeksresultaten vervolgens intern of extern worden gedeeld omdat de onderzoeksresultaten dan met eigen data gekoppeld kunnen worden waardoor de pseudonimisering ongedaan wordt gemaakt;
4. Of in de privacyverklaring van de gemeente of op een aparte pagina van de gemeente over '(statistisch) onderzoek' duidelijk wordt vermeld dat bij bepaalde nader te noemen onderzoeken data uit verschillende bronnen gekoppeld wordt;
5. In het geval van respondenten, of ook zij hierover geïnformeerd worden in de privacyverklaring of de uitleg bij de enquête. Zorg dat zij hier voorafgaand aan de deelname aan het onderzoek van op de hoogte kunnen zijn.

Zie in Hoofdstuk 3: 'Anonimiseren, pseudonimiseren en aggregeren' over hoe je rekening kunt houden met de wijze waarop de onderzoeksdata uit diverse databronnen kan worden gekoppeld door middel van anonimiseren en pseudonimiseren.

Maatregelen om data en analyses te beveiligen

Als er persoonsgegevens voor het onderzoek worden ontvangen, zal je passende beveiligingsmaatregelen moeten nemen om deze gegevens te beschermen. Ook dit is een eis die volgt uit de AVG. Hoe gevoeliger de gegevens hoe zwaarder de maatregelen moeten zijn. Wanneer je gewone persoonsgegevens verwerkt, hoef je in de regel minder vergaande maatregelen te treffen dan wanneer je bijzondere persoonsgegevens verwerkt (zie ook de *paragraaf* Data onder de AVG). Worden er gevoelige gegevens, zoals informatie over financiën, minderjarigen, of maatschappelijke ondersteuning gevraagd, wees dan kritisch welke informatie nodig is (denk aan de *paragraaf* Data onder de AVG!) en neem passende maatregelen om die gegevens goed te beveiligen. Denk hierbij aan maatregelen als het enkel verlenen van toegang tot de gegevens voor personen die het onderzoek uitvoeren, het gebruikmaken van afgeschermd schijven of applicaties met beperkte autorisaties, en het vernietigen (of op andere wijze onherleidbaar maken) van de onderzoeksgegevens zodra deze niet meer nodig zijn, zoals in ieder geval wanneer de analyse heeft plaatsgevonden. Ook het anonimiseren, pseudonimiseren of aggregeren van persoonsgegevens zijn maatregelen die toegepast kunnen worden om data en analyses te beveiligen en/of onherleidbaar te maken.

Beschrijf in je Startnotitie met betrekking tot de maatregelen dus de volgende onderdelen:

1. De systemen waarmee het onderzoek wordt uitgevoerd. Besteed daarbij ook aandacht aan technieken en applicaties, zoals PowerBI, waarmee je geaggregeerde gegevens weer terug kan herleiden tot een individu;
2. De wijze waarop de onderzoeksgegevens (ruwe data) worden verkregen;
3. Of er gebruik wordt gemaakt van versleutelingstechnieken, en zo ja welke en op welke wijze wordt dit toegepast;
4. Waar de verkregen onderzoeksgegevens (ruwe data) worden opgeslagen;
5. Wie toegang heeft tot de onderzoeksgegevens (ruwe data);
6. Wanneer de onderzoeksgegevens (ruwe data) worden vernietigd en op welke wijze is geborgd dat de vernietiging ook daadwerkelijk plaatsvindt.

Data Protection Impact Assessment

Als onderdeel van de planvormingsfase van een onderzoek zal het in bepaalde gevallen noodzakelijk zijn om de privacy risico's van het onderzoek gestructureerd in kaart te brengen. Dit gebeurt in een Data Protection Impact Assessment, afgekort DPIA (Nederlands: 'Gegevensbeschermingseffectbeoordeling', GEB). Het uitvoeren van een DPIA valt onder de verantwoordelijkheid van de *verwerkingsverantwoordelijke* (zie ook de *paragraaf* 'Het opdrachtgeverschap'). De uitkomst van een DPIA kan zijn dat er bepaalde risico's kleven aan het onderzoek die onvoldoende worden gemitigeerd door de al getroffen technische en organisatorische maatregelen (*restrisico's*). Het is dan zaak om aanvullende maatregelen te treffen om die restrisico's alsnog te mitigeren.

De AVG noemt een aantal situaties waarin een DPIA verplicht uitgevoerd moet worden. Deze verplichting geldt in ieder geval wanneer in een onderzoek:

- Systematisch en uitgebreid persoonlijke aspecten worden geëvalueerd op basis van geautomatiseerde verwerkingen, zoals bij profiling; of
- Op grote schaal bijzondere persoonsgegevens worden verwerkt; of
- Op grote schaal en systematisch mensen gevolgd worden in een publiek toegankelijk gebied (bijvoorbeeld met (flexibel) cameratoezicht).

De AVG geeft niet expliciet aan wat er verstaan wordt onder 'op grote schaal'. Dit is bewust opengelaten om te voorkomen dat bepaalde situaties op voorhand uitgesloten worden. Wel geeft de werkgroep van Europese privacy toezichthouders, de European data Protection Board (hierna 'EDPB'), hier een aantal handvatten voor. Om te bepalen of er sprake is van een 'grote schaal', moet rekening gehouden worden met:

- Het aantal respondenten (bijvoorbeeld de hoeveelheid mensen die in een publiek toegankelijk gebied worden gevolgd);
- De hoeveelheid en typen persoonsgegevens die worden verwerkt. Hoe meer (verschillende soorten) persoonsgegevens verwerkt worden, des te eerder er sprake zal zijn van een 'grote schaal';
- De duur van de gegevensverwerking (hoeveel maanden, weken, jaren worden de gegevens verwerkt);
- De geografische reikwijdte van de verwerking.

Indien gevoelige of bijzondere persoonsgegevens worden verwerkt, bestanden (datasets) worden gekoppeld, als er sprake is van monitoring (volgen) of een samenwerkingsverband waarbij gevoelige of bijzondere persoonsgegevens worden verwerkt, dan moet je vooraf en tijdig af te stemmen met de Privacy Officer/Functionaris Gegevensbescherming of een DPIA mogelijk verplicht is.

In Bijlage 2: DPIA Checklist van dit Handboek is een checklist opgenomen waarmee een eerste inschatting gemaakt kan worden van de noodzakelijkheid van een DPIA. Volgt uit de checklist dat er een DPIA uitgevoerd moet worden, of bestaan er twijfels? Benader dan altijd de Privacy Officer/Functionaris Gegevensbescherming en vraag om advies.

Het informeren van respondenten en de rechten van respondenten

De laatste belangrijke AVG-eis die in dit hoofdstuk wordt besproken is de eis dat een verwerkingsverantwoordelijke de respondent vooraf informeert over de verwerking(en) van zijn of haar persoonsgegevens. Respondenten hebben namelijk het recht om precies te weten wat er met hun persoonsgegevens gaat gebeuren (*transparantie*). Om precies te zijn moeten respondenten over het volgende geïnformeerd worden:

- De identiteit en de contactgegevens van de verwerkingsverantwoordelijke;
- De contactgegevens van de FG;
- Het onderzoeksdoel en de grondslag van de verwerking;
- De (categorieën van) ontvangers van de persoonsgegevens;
- Of de persoonsgegevens worden doorgegeven naar een land buiten de EU of een internationale organisatie en op basis waarvan dat gebeurt;
- De bewaartermijn van de gegevens;
- Hun rechten, waarover meer hieronder;
- De mogelijkheid om de gegeven toestemming voor een bepaalde verwerking in te trekken.
- De mogelijkheid om een klacht in te dienen bij de nationale toezichthouder (de AP);
- Of en waarom de respondent verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt;
- Of gebruik wordt gemaakt van geautomatiseerde besluitvorming, inclusief profiling, en hoe die besluiten worden genomen;
- Waar de persoonsgegevens vandaan komen (c.q. van de gemeente of een externe bron), en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

Een veel geziene methode om dergelijke informatie te verstrekken is in een privacyverklaring. Deze moet voorafgaand aan de verzameling van persoonsgegevens verstrekt worden. Beschrijf in je Startnotitie op welke wijze je invulling hebt gegeven aan de informatieverplichting. Zie Bijlage 3: 'Template privacyverklaring voor respondenten' voor een voorbeeld van een privacyverklaring. Dit template kan gebruikt worden om een privacyverklaring voor een specifiek onderzoek op te stellen. Je kunt kiezen voor het meesturen van de privacyverklaring (bijvoorbeeld in print) of je kunt bij de uitnodiging of voordat men digitaal de respons gaat geven, verwijzen naar een aparte webpagina met de privacyverklaring. Belangrijk is dat men voorafgaand kennis moet kunnen nemen van de privacyverklaring!

Naast het dienen van transparantie is er een andere belangrijke reden waarom respondenten deze informatie nodig hebben: zodat zij hun AVG-rechten kunnen uitoefenen. De AVG verleent aan respondenten een bepaalde set rechten die zij kunnen uitoefenen jegens de verwerkingsverantwoordelijke. Het gaat om de volgende rechten:

- Recht van inzage: Respondenten hebben het recht om te weten of, en zo ja welke, hen betreffende persoonsgegevens worden verwerkt, voor welke doelen dat gebeurt, hoe lang de gegevens bewaard worden, uit welke bron de gegevens afkomstig zijn en of er geautomatiseerde besluitvorming wordt toegepast.
- Recht op rectificatie: Als een respondent erachter komt dat hem betreffende persoonsgegevens onjuist zijn, bijvoorbeeld door middel van een inzageverzoek, kan dit recht gebruikt worden om die gegevens te laten rectificeren.

- Recht op gegevenswissing (right to be forgotten): Wanneer gegevens niet meer noodzakelijk zijn voor het doel waarvoor zij zijn verzameld, de respondent zijn toestemming heeft ingetrokken, bezwaar is gemaakt tegen de verwerking, de persoonsgegevens onrechtmatig zijn verwerkt of er een wettelijke verplichting is, kan een respondent met een beroep op dit recht zijn persoonsgegevens laten wissen.
- Recht op beperking van de verwerking: Een respondent kan eisen dat de verwerking van hem betreffende persoonsgegevens tijdelijk wordt gestaakt wanneer de juistheid van de gegevens wordt betwist (gedurende de tijd dat de verwerkingsverantwoordelijke de juistheid controleert), wanneer de verwerking onrechtmatig is, de gegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld of de respondent bezwaar heeft ingediend tegen de verwerking.
- Recht op overdraagbaarheid (dataportabiliteit): Indien een verwerking berust op toestemming, op basis van een overeenkomst wordt uitgevoerd of via geautomatiseerde procedés wordt verricht, heeft een respondent het recht om hem betreffende gegevens in een overdraagbaar format overgedragen te krijgen.
- Recht van bezwaar: Indien een verwerking plaatsvindt in het kader van een taak van algemeen belang, kan een respondent bezwaar maken tegen de verwerking van hem betreffende persoonsgegevens vanwege met zijn situatie verband houdende redenen.
- Recht om niet aan geautomatiseerde besluitvorming onderworpen te worden: Respondenten hebben het recht om te ageren tegen een verwerking waarbij gebruik wordt gemaakt van geautomatiseerde besluitvorming.
- Recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP): Indien een respondent van mening is dat een verwerking niet conform de AVG geschiedt, kan gebruik gemaakt worden van het recht een klacht in te dienen bij de AP.

Wanneer er een verzoek van een respondent tot uitoefening van zijn/haar rechten binnenkomt moet er zo snel mogelijk, in ieder geval een maand na ontvangst, gevolg aan worden gegeven. Als het een complex verzoek betreft kan dit verlengd worden tot twee maanden, maar de respondent moet daar dan wel binnen een maand na ontvangst over geïnformeerd worden. Vraag om advies van de Privacy Officer/Functionaris Gegevensbescherming wanneer je een verzoek van een respondent ontvangt.

Let op: ten aanzien van de AVG-rechten bestaat er bij het uitvoeren van statistisch onderzoek wel een mogelijkheid om op grond van de AVG en de Nederlandse Uitvoeringswet AVG (UAVG) de volgende rechten te beperken, namelijk: het recht op inzage, het recht op correctie en recht op beperking van de verwerking.³ Dit betekent echter wel dat de persoonsgegevens uitsluitend voor statistische onderzoeksdoeleinden mogen worden gebruikt én men passende maatregelen heeft getroffen om de onderzoeksdata te beveiligen en – bij voorkeur – te anonimiseren dan wel te pseudonimiseren.

Beschrijf in je Startnotitie op welke wijze je respondenten in staat stelt gebruik te maken van hun AVG-rechten en hoe je daaraan gehoor zult geven.

³ Art. 44 UAVG

Hoofdstuk 2: Het uitvoeren van het onderzoek

Als de onderzoeksdoeleinden, benodigde (persoons)gegevens, en de beveiliging van de onderzoeksdata zijn bepaald en de Startnotitie is geaccordeerd, kun je gaan starten met het uitvoeren van het onderzoek. Het kan zijn dat je reeds beschikt over de benodigde onderzoeksdata. Maar het kan ook zijn dat je nog data moet verkrijgen bij respondenten (bijvoorbeeld middels enquêtes) of een bestand dat je legitiem mag gebruiken moet verkrijgen bij een derde partij. Hieronder worden de aandachtspunten beschreven wanneer je nog onderzoeksdata moet verkrijgen en in het algemeen wat te doen met de onderzoeksdata zodra je de analyse hebt verricht.

Het verkrijgen van onderzoeksdata bij respondenten

Als je geen gebruik maakt van bestaande gegevens, maar je deze informatie nog moet verkrijgen van de respondenten, dan moet je rekening houden met de volgende zaken:

Het benaderen van respondenten

Bij zowel steekproeven als andere onderzoeksvormen in de vorm van enquêtes waarbij gegevens van respondenten worden gebruikt om hen voor deelname uit te nodigen, is het van groot belang dat je de adresgegevens van de respondenten strikt scheidt van de ontvangen onderzoeksgegevens. Dit om ervoor te zorgen dat de onderzoeksgegevens niet herleidbaar zijn tot individuen die op basis van de geselecteerde respondenten en adressen zijn aangeschreven of uitgenodigd. Een alternatief is uitnodigingen aan respondenten niet persoonlijk te adresseren, maar te richten aan het woonadres. Dat ziet er dan zo uit: "Aan de bewoners van ..."

Onderzoek bij respondenten op basis van panel-onderzoek

Respondenten van een panel-onderzoek kunnen altijd worden benaderd – op voorwaarde dat zij hebben aangegeven dat zij deel willen nemen aan het panel-onderzoek. Zorg er bij iedere uitnodiging aan de respondenten van het panel-onderzoek voor dat er telkens een mogelijkheid is om zich af te melden (opt-out).

Onderzoek op basis van een algemeen belang of wettelijke verplichting

Voor onderzoeken die betrekking hebben op de publieke taken van de gemeente in het kader van algemeen belang, zoals bijvoorbeeld de doelmatigheid van een beleid, geldt dat je voor het benaderen van respondenten een aselechte steekproef kunt laten trekken uit de BRP. Ten aanzien van onderzoeken op grond van een wettelijke verplichting, zoals cliëntervaringsonderzoeken, kun je gebruik maken van de gegevens van actuele cliënten. Toestemming vragen voor het benaderen is in beide gevallen niet verplicht en niet nodig.

Adreslijsten

Zorg ervoor dat adreslijsten van de benaderde respondenten (enquête, interview en panel-onderzoek) altijd separaat worden gehouden van de onderzoeksgegevens. Dit is namelijk een maatregel waardoor de kans op 'herleidbaarheid' van de respondenten wordt verminderd. In een vragenlijst is het bijvoorbeeld niet nodig om naar de naam en achternaam, en het specifieke postcode 6 adres inclusief huisnummer te vragen. Doe je dat wel, zorg er dan voor dat die onderzoeksdata wordt verwijderd uit het databestand zodra de analyse heeft plaatsgevonden. De voorkeur gaat uit naar het opslaan op een andere schijf met strikte scheiding, zodat ook degene die de onderzoeken uitvoeren/analyseren geen toegang hebben tot de adreslijsten.

Een ander voordeel van adreslijsten strikt scheiden van de respons op enquêtes en interviews is dat de benaderde respondenten ook makkelijker hun persoonsgegevens kunnen laten verwijderen zonder dat dit impact heeft op de onderzoeksdata.

Indien de gemeente werkt met een extern onderzoeksbureau dat in opdracht van de gemeente een onderzoek uitvoert, dwing dan dezelfde maatregelen af. Dit kan je in de verwerkersovereenkomst regelen (zie de *paragraaf* 'Verwerkersovereenkomsten').

Het ontvangen en verwerken van de resultaten van de respondenten

Voor alle informatie en respons die je als gemeente wenst te ontvangen van de respondenten zal je voor het meewerken en gebruiken van de onderzoeksdata altijd toestemming moeten vragen. Let op: als je een onderzoek uitvoert met data waar je reeds intern over beschikt, bijvoorbeeld over het aantal voorzieningen die in een jaar zijn verstrekt, is toestemming voor het gebruiken van die data in principe niet vereist. De toestemming geldt dus enkel als je de benodigde onderzoeksdata nog middels enquête of interview moet verkrijgen van de respondent.

Toestemming voor enquêtes kan op verschillende wijzen worden gevraagd. De wijze waarop is mede afhankelijk van de vraag of er persoonsgegevens worden verkregen/gevraagd. Als het een anonieme enquête betreft en enkel anonieme onderzoeksdata wordt gevraagd, dan kan naast het vooraf informeren worden volstaan met een korte verklaring dat men door verzending van de enquête 'toestemming' geeft. Of voordat men de enquête start of gaat inzenden dan wel per brief verstuurt kan een apart *leeg* selectievakje worden gevraagd dat men door middel van het aanvinken toestemming geeft voor het verwerken van de onderzoeksdata ten behoeve van het onderzoeksdoel. Wordt bijvoorbeeld voor het onderzoek ook om een naam, e-mailadres en telefoonnummer gevraagd, dan wel bijzondere persoonsgegevens dan zal de toestemming daarvoor expliciet moeten worden gevraagd. Als ook de mogelijkheid wordt geboden om voor vervolgonderzoeken te worden benaderd, dan zal daar apart toestemming voor moeten worden gevraagd. Belangrijk is dat:

- De respondent voorafgaand aan het invullen van de enquête wordt geïnformeerd over het doel van de enquête, waarvoor de resultaten worden gebruikt, hoe lang de onderzoeksdata wordt gebruikt, of de enquête en onderzoeksdata anoniem zijn, en hoe men gebruik kan maken van de AVG-rechten, eventueel met verwijzing naar de privacyverklaring;
- Indien persoonsgegevens worden gevraagd dan wel dit in open tekstvelden mogelijk is, hiervoor expliciet toestemming wordt verkregen. Let hierbij op dat indien digitaal antwoorden tijdelijk worden opgeslagen, dit ook al een verwerking is waarvoor toestemming vereist is. Vraag in dat geval reeds voor de start van de enquête om toestemming/akkoord voor het gebruik van de onderzoeksdata. Dit kan middels een duidelijke tekst waarin de toestemming wordt gevraagd voor het verwerken van de (bijzondere) persoonsgegevens ten behoeve van het onderzoeksdoel door een *leeg* selectievakje aan te vinken;
- De toestemming (of het akkoord) voor het deelnemen aan de enquête wordt vastgelegd!
- Het beheer van de individueel verleende toestemming en de daaraan gekoppelde onderzoeksdata mogelijk is voor het geval de toestemming wordt ingetrokken.

Naast de hierboven geschetste aandachtspunten bij het uitvoeren van kwantitatief onderzoek wordt door de VSO-leden ook kwalitatief onderzoek uitgevoerd in de vorm van interviews of gebruik gemaakt van focusgroepen. Voor deze vormen van onderzoek kunnen dezelfde kaders worden gehanteerd als hierboven beschreven. Hierbij is het wel verstandig vooraf duidelijke schriftelijke afspraken te maken met de geïnterviewde en de focusgroepen. Bij een interview zal het voor de hand liggen dat tevens de naam van de geïnterviewde of andere persoonsgegevens worden verwerkt. Leg ook de medewerking aan het interview of de focusgroep schriftelijk vast en vraag – bij voorkeur – tegelijkertijd om toestemming voor het gebruik van het interview en de informatie inclusief persoonsgegevens die zijn verstrekt dan wel de respons. Zie voor een voorbeeld Bijlage 4: 'Template toestemmingsformulier interview'.

Het verkrijgen van onderzoeksdata buiten respondenten

Als de onderzoeksdata niet (alleen) wordt verkregen bij respondenten, maar (ook) wordt verkregen van interne afdelingen of andere externe bronnen is het van belang rekening te houden met de volgende zaken:

Interne afdelingen

Indien de onderzoeksdata van een interne afdeling of afdelingen wordt verkregen, is het verstandig om als onderzoeker zelf te bepalen welke onderzoeksdata nodig is om het doel van het statistisch onderzoek te behalen. Kortom, welke inzichten zijn gewenst en welke data heb ik daar als onderzoeker gelet op de opdracht voor nodig! Hiermee zorg je als onderzoeker:

- dat je alleen die data ontvangt die gelet op het onderzoeksdoel gerechtvaardigd en noodzakelijk is; en
- dat je niet te veel data ontvangt die je niet nodig hebt voor het onderzoeksdoel.

Belangrijk: de onderzoeker respectievelijk de onderzoeksafdeling is niet de opdrachtgever. Het opdrachtgeverschap is altijd de afdeling of het college indien het onderzoek afdelingoverstijgend is.

Externe bestanden

Het kan zijn dat je andere externe bestanden gebruikt die afkomstig zijn van openbare of niet-openbare bronnen. Zorg er in dat geval voor dat je eerst bepaalt dat je die onderzoeksdata *moet* en *mag* gebruiken voor het onderzoeksdoel. Het is de verantwoordelijkheid van de verstrekker van de onderzoeksdata, bijvoorbeeld een woningcorporatie, om te bepalen of zij de onderzoeksdata verstrekken.

Maak duidelijke afspraken over het verstrekken en het gebruik van het bestand. Zorg er voor dat als de externe partij eist dat ze de onderzoeksresultaten willen ontvangen deze worden geanonimiseerd of op een dusdanig hoog niveau worden geaggregeerd dat herleidbaarheid – juist voor die externe partij – nooit mogelijk is. Immers, men zou met onderzoeksresultaten op onvoldoende geaggregeerd niveau een koppeling kunnen maken met een eigen databestand of andere data waardoor herleidbaarheid weer mogelijk is.

Het ontvangen, bewaren en vernietigen van onderzoeksdata

Versleutelen

Het is verstandig om onderzoeksgegevens die nodig zijn van interne afdelingen, dan wel derden, versleuteld aan te laten leveren (of vice versa). Daarbij geniet het sterk de voorkeur om onderzoeksgegevens die tot een persoon herleidbaar zijn, te anonimiseren of middels een sleutel te pseudonimiseren. In dat laatste geval is het verstandig de sleutel na aanlevering door de desbetreffende afdeling of partij te laten vernietigen. Op die wijze zijn de onderzoeksgegevens niet meer herleidbaar.

Bewaren en vernietigen van onderzoeksdata

Vanuit de AVG is het van groot belang dat als de onderzoeksdata niet meer nodig zijn voor het onderzoeksdoel, deze onderzoeksdata wordt vernietigd of op een andere wijze onherleidbaar wordt gemaakt (denk aan anonimiseren). In de regel betekent dit dat als de analyse op de onderzoeksdata heeft plaatsgevonden de onderzoeksdata wordt gewist, verwijderd, onleesbaar gemaakt of geanonimiseerd. Indien de onderzoeksdata op correcte wijze wordt geanonimiseerd, kun je de geanonimiseerde onderzoeksdata blijven gebruiken.

Uitgangspunt is dat als de analyse van een onderzoek uiterlijk 6 maanden na de start van het onderzoek is afgerond, dan kan worden overgegaan tot de vernietiging van de onderzoeksdata. Mocht de analyse al eerder gereed zijn, dan zal je dus eerder tot vernietiging over moeten gaan. Als dit technisch niet mogelijk of lastig is, zal je moeten verantwoorden (uitleggen) waarom de onderzoeksdata langer wordt bewaard. Motiveer in dat geval eerst goed waarom het gelegitimeerd is dat je de onderzoeksdata langer bewaard. Mogelijk zou je ook reeds een deel van de onderzoeksdata kunnen anonimiseren of pseudonimiseren waardoor je enkel nog moet motiveren waarom de resterende onderzoeksdata langer wordt bewaard. Stem je nadere motivatie nog wel af met de Privacy Officer of vraag advies aan de Functionaris Gegevensbescherming.

Met de onderzoeksresultaten en rapportage(s) wil je uitspraken doen over doelgroepen en populaties. Dit betekent dat het niet nodig is dat deze onderzoeksresultaten en -rapportages herleidbaar zijn tot individuen. Indien deze hieraan voldoen, kun je de onderzoeksresultaten en rapportages gewoon bewaren.

Let wel, mochten de resultaten en rapportages op een gegeven moment wel herleidbaar worden tot individuen, bijvoorbeeld vanwege technische innovatieve ontwikkelingen of de beschikking over nieuwe data, dan dienen de resultaten en rapportages 'opnieuw' te worden geanonimiseerd. Daarbij moet je denken aan applicaties als PowerBI die het mogelijk maken om met slimme oplossingen, als Artificial Intelligence, de onderzoeksresultaten terug te brengen naar een lager aggregatieniveau. Hierdoor zou het mogelijk kunnen zijn om toch personen direct of indirect te herleiden.

Hoofdstuk 3: Het presenteren van de onderzoeksresultaten

Zodra de analyse van de onderzoeksdata heeft plaatsgevonden en de onderzoeksresultaten beschikbaar zijn, is het van groot belang dat de onderzoeksresultaten niet meer herleidbaar (kunnen) zijn tot individuen. Waarom dit niet is toegestaan en hoe je de onderzoeksresultaten wel binnen de kaders van de AVG kunt presenteren, lees je in dit hoofdstuk.

Wijze van rapporteren

Het is van groot belang dat het doel van statistisch onderzoek altijd voorop blijft staan: het doen van uitspraken over doelgroepen of populaties. Dit betekent dat het resultaat van het statistisch onderzoek – de presentatie van de onderzoeksresultaten – altijd moet worden gepresenteerd als zijnde uitspraken over doelgroepen of populaties, en niet over (individuele) personen!

Kortom, de onderzoeksresultaten en de presentatie hiervan mogen nooit uit persoonsgegevens bestaan, alleen uit geaggregeerde gegevens. Verder is het niet toegestaan om de onderzoeksresultaten en de persoonsgegevens te gebruiken als ondersteunend materiaal voor maatregelen of beslissingen die een bepaald individu betreffen of (kunnen) treffen.

Onderzoeksresultaten kunnen in papieren of op digitale wijze worden gepresenteerd. Als men gebruik maakt van software om de analyse te maken en te presenteren, is het van groot belang dat het na de analyse niet mogelijk is om met de software-applicatie de geaggregeerde (en gepresenteerde) resultaten technisch terug te herleiden tot de individuen van wie de persoonsgegevens zijn gebruikt in het onderzoek.

De onderzoeksresultaten moeten altijd op een dusdanig geaggregeerd niveau worden weergegeven, dat de resultaten niet direct of indirect herleidbaar zijn of kunnen zijn. Hoe dit moet worden toegepast, is te lezen in de volgende paragraaf.

Er is één uitzondering op het niet geanonimiseerd of geaggregeerd weergeven van de onderzoeksresultaten, namelijk: als de respondent uitdrukkelijk toestemming heeft gegeven voor het op individueel niveau presenteren van de onderzoeksresultaten! Hierbij gelden wel een paar voorwaarden:

- a. Het moet ten behoeve van het onderzoek noodzakelijk zijn om de onderzoeksresultaten op individueel niveau te presenteren én dit moet ook rechtmatig zijn; én
- b. De respondent moet expliciet vooraf toestemming hebben gegeven voor het op individueel niveau presenteren van de onderzoeksresultaten. Hier moet dus ook met voldoende duidelijke en begrijpelijke informatie specifiek toestemming voor zijn gevraagd én verleend. Denk hierbij met name aan interviews waarbij het wenselijk is dat de naam van de respondent/geïnterviewde ook gepubliceerd wordt; én
- c. Voorafgaand aan de start van het onderzoek moet voldoende informatie zijn verstrekt over de benodigde persoonsgegevens, de categorieën van ontvangers, zoals de opdrachtgever, aan wie identificerende gegevens worden verstrekt en voor welke doeleinden dit gebeurt; én
- d. De informatie moet schriftelijk (of elektronisch) gecommuniceerd worden. Ook moet de informatie eenvoudig geraadpleegd kunnen worden. Dit kan in de begeleidende brief bij het onderzoek waarbij je voor meer informatie verwijst naar de pagina van de gemeente of het onderzoeksbureau met meer informatie over het onderzoek; én
- e. Er moet worden voorzien in een mogelijkheid om de data van de respondenten te vernietigen. Als respondenten namelijk besluiten dat hun gegevens niet gebruikt mogen

worden (intrekking van toestemming), dan mag de data niet worden gebruikt voor de rapportage en dient deze te worden vernietigd.

Anonimiseren, pseudonimiseren en aggregeren

Tijdens een onderzoek is het belangrijk om zo min mogelijk persoonsgegevens te verwerken. Wat de minimale hoeveelheid persoonsgegevens is voor een onderzoek zal van geval tot geval anders kunnen zijn. Maar het kan betekenen dat direct na het verzamelen persoonsgegevens worden gepseudonimiseerd zodat degenen met toegang tot de onderzoeksgegevens bijvoorbeeld minder makkelijk gegevens van bekenden kunnen opzoeken. Resultaten van een onderzoek kunnen vaak gepresenteerd worden als geaggregeerde statistieken die niet meer te herleiden zijn tot individuele personen zodat de resultaten makkelijker gedeeld kunnen worden.

Geaggregeerde persoonsgegevens

Geaggregeerde data lijken vaak geen persoonsgegevens te bevatten. Toch zitten er allerlei risico's aan statistische data die toch kunnen zorgen dat er persoonsgegevens lekken wanneer de statistische data gedeeld wordt. Het CBS heeft een uitgebreid handboek statistische beveiliging⁴ om deze risico's te voorkomen. Vanwege de complexiteit is het aan te raden om geaggregeerde gegevens te toetsen aan de vier vuistregels die het CBS omschrijft in de *Guidelines For Output Checking*⁵ om een indicatie te krijgen of het waarschijnlijk is dat er persoonsgegevens kunnen lekken uit geaggregeerde data.

De vier vuistregels, in het kort:

1. *10 eenheden*: elke cel in een tabel moet informatie van minimaal 10 eenheden (bijvoorbeeld: personen) bevatten.

Een voorbeeld is de onderstaande tabel met volkomen fictieve inkomens-statistieken. Omdat er maar één burgemeester in Utrecht is, bevat deze tabel herleidbare inkomens-gegevens over de Burgemeester van Utrecht. In een grotere tabel kunnen dergelijke uitschieters minder opvallen.

Woonplaats	Beroep	Gemiddeld inkomen
Amsterdam	Bakkerijmedewerker	1.400 euro
Utrecht	Burgemeester	10.000 euro
Den Haag	Advocaat	8.500 euro

2. *10 vrijheidsgraden*: het aantal vrijheidsgraden is gelijk aan het aantal observaties min het aantal parameters min het aantal restricties van het model en moet groter zijn dan tien. Een voorbeeld hiervan is een groep van vier personen waarvan het gemiddelde inkomen, minimale inkomen, maximale inkomen en de standaarddeviatie bekend is. Dat zijn vier observaties met vier parameters of restricties waardoor er nul vrijheidsgraden zijn en de individuele inkomens van de vier personen te achterhalen is.
3. *Groep onthulling*: een enkele waarde mag niet voor meer dan 90% uit de bijdrage van een enkel individu bestaan. Bijvoorbeeld: het gemiddelde inkomen van een groep mensen met één extreem hoog inkomen geeft teveel informatie over het inkomen van die ene persoon.
4. *Dominantie (van een specifiek resultaat)*: een enkele bijdrage mag niet meer dan 50% van het totaal bevatten. Bijvoorbeeld: in de onderstaande (fictieve) tabel, waarin meer dan 50% van

⁴ CBS Statistische beveiliging: <https://www.cbs.nl/nl-nl/onze-diensten/methoden/statistische-methoden/output/output/statistische-beveiliging>

⁵ Guidelines for the checking of output based on microdata research: https://research.cbs.nl/casc/ESSnet/GuidelinesForOutputChecking_Dec2009.pdf

de inwoners van Simpelveld Rooms-Katholiek zijn. Let op: dit ziet niet enkel op bijzondere persoonsgegevens die worden weergegeven, maar geldt voor alle categorieën (persoons)gegevens. Betreft een specifieke bijdrage/waarde meer dan 50% van het totaal, dan bestaat er een zogenaamd onthullingsrisico waardoor het eenvoudiger wordt om terug te rekenen of terug te herleiden.

Gemeente	Rooms-Katholiek	Nederlands Hervormd	Gereformeerd
Simpelveld	90,6%	0,2%	0,0%
Stein	73,3%	0,7%	0,1%

Wanneer aan deze vier vuistregels is voldaan geeft dat een indicatie dat de meest opvallende fouten waardoor geaggregeerde gegevens toch iets over herleidbare individuen kunnen onthullen waarschijnlijk niet gemaakt zijn. Als de data de vier vuistregels heeft doorstaan kan een statisticus de gegevens beoordelen op restrisico's aan de hand van de twee hierboven genoemde handleidingen.

Pseudonimisatie door middel van hashing

Een veelgebruikte techniek om persoonsgegevens te pseudonimiseren is hashing. Hashing is een (cryptografische) techniek waarmee gegevens onomkeerbaar kunnen worden 'versleuteld'⁶. Het idee van deze toepassing van hashing is dat een duidelijke 'identificer' zoals een BSN in een dataset wordt vervangen door de hash van dat BSN. Twee keer dezelfde BSN geeft dezelfde hash, maar de hashes zijn niet terug te rekenen.

Dat ziet er bijvoorbeeld als volgt uit wanneer (fictieve) BSN's worden vervangen met de MD5-hash van elk BSN. MD5 is een veelgebruikt hash-algoritme.

BSN	Woonplaats	Beroep	Inkomen
209497397	Amsterdam	Bakkerijmedewerker	1.400 euro
562992212	Utrecht	Burgemeester	10.000 euro
597206028	Den Haag	Advocaat	8.500 euro

MD5(BSN)	Woonplaats	Beroep	Inkomen
ea314cd6968992d71d544765b684ff64	Amsterdam	Bakkerijmedewerker	1.400 euro
5d69d251ofd638dae3f2b2730fc5e12a	Utrecht	Burgemeester	10.000 euro
125f897838ee943404776f11922bd50e	Den Haag	Advocaat	8.500 euro

De aanname dat cryptografische hashes niet "terug te rekenen" zijn leidt vaak tot de aanname dat de gehashte gegevens niet te herleiden zijn. In dit voorbeeld is het bijvoorbeeld mogelijk alle mogelijke

⁶ Versleuteling is strikt genomen niet correct, maar voor deze uitleg een redelijke abstractie. Een meer correcte uitleg is te vinden op Wikipedia: https://en.wikipedia.org/wiki/Cryptographic_hash_function

BSNs met een moderne computer in een fractie van een seconde te hashen. Daarmee kan van elke hash dus alsnog het oorspronkelijke BSN worden achterhaald. Deze vorm van hashing wordt dan ook niet aangeraden in situaties waar meer veilige alternatieven beschikbaar zijn.

Hashing kan ook worden toegepast op een manier die het risico van "terugrekenen" reduceert door een geheime sleutel toe te voegen. Daar zijn verschillende methoden voor, maar een veilige methode is bcrypt. Het gebruik van standaardmethoden van hashing voorkomt dat er fouten gemaakt worden in de implementatie. Het verschil met voorgaande hashing methode is dat elk onderzoek of elke verzameling data die aan elkaar gekoppeld moet kunnen worden een eigen sleutel toegewezen krijgt.

Zolang er geen andere methoden zijn waarop de gegevens herleid kunnen worden kan alleen degene met toegang tot de sleutel nieuwe data pseudonimiseren en koppelen aan andere data die is gepseudonimiseerd. Wanneer de sleutel wordt vernietigd kan herleiding via de gegenereerde pseudonieme identifiers vrijwel geheel worden uitgesloten.

Onderstaand een implementatie-voorbeeld (in de Python-programmeertaal) om een enkele BSN te pseudonimiseren die door data-analysten als voorbeeld gebruikt kan worden.

```
>>> import base64
>>> import bcrypt
>>> sleutel = bcrypt.gensalt()
>>> sleutel
b'$2b$12$SyNjSIsAq0/AZ/wW6a8yJ.'
```

De gegenereerde sleutel moet veilig bewaard blijven zodat de data-analisten geen toegang hebben tot de sleutel. Bovenstaande sleutel moet dus ook niet hergebruikt worden en dient slechts als voorbeeld.

```
>>> bsn = b"209497397"
>>> base64.b64encode(bcrypt.kdf(bsn, sleutel, desired_key_bytes=32, rounds=100))
b'4aj1KjplTu1dvhi1RWNZbtBUugWkhcOHLX0EtNbmug0='
```

De laatste regel bevat het gegenereerde pseudoniem voor het fictieve bsn 209497397.

Deze constructie kan op verschillende manieren worden toegepast. De organisatie die persoonsgegevens aanlevert kan gevraagd worden om de pseudonimisering toe te passen en de gebruikte sleutel niet te verstrekken. Maar de sleutel kan ook intern gescheiden worden door duidelijke afspraken te maken over wie de sleutel mag benaderen en wie niet. Daarbij moeten dan deze maatregelen technisch en organisatorisch worden afgedwongen.

Een alternatieve oplossing voor het pseudonimiseren van gegevens is door de identificerende gegevens te vervangen door willekeurige gegevens. Bijvoorbeeld door een koppeltabel op te stellen die apart bewaard wordt en vernietigd wordt zodra herleiding niet meer noodzakelijk is.

Toestemming

Als het voor het onderzoeksdoel wenselijk is dat persoonsgegevens, als naam en andere bijzondere kenmerken, wel worden opgenomen in het onderzoeksrapport, dan zal altijd voorafgaand

toestemming moeten worden gevraagd en verleend. Denk hierbij met name aan kwalitatief onderzoek waarbij het wenselijk kan zijn dat de namen van de geïnterviewden worden opgenomen in het onderzoeksrapport.

Externe bronnen

Externe bronnen kunnen op onvoorspelbare manieren zorgen dat gegevens herleidbaar zijn wanneer er geen statistische garanties zijn om herleidbaarheid te voorkomen. In het bovenstaande voorbeeld is bijvoorbeeld de combinatie van 'Burgemeester' en 'Utrecht' uniek en makkelijk met behulp van openbare bronnen te herleiden. In minder opvallende voorbeelden is het soms mogelijk om met behulp van bijvoorbeeld sociale media-accounts personen te herleiden aan de hand van een combinatie van eigenschappen. Behalve publieke bronnen, moet voor de herleidbaarheid ook naar niet-publieke bronnen gekeken worden, ook als die niet-publieke bronnen alleen door een derde partij benaderd kunnen worden. De herleidbaarheid van IP-adressen is daar een voorbeeld van.⁷ Omdat de politie toegang tot IP-adressen kan vorderen én bij de internetprovider gegevens kan vorderen waarmee de IP-adressen herleid kunnen worden tot de specifieke abonnee, zijn IP-adressen (vaak) persoonsgegevens.

⁷ HvJ EU, 19 oktober 2016, C-582/14, Patrick Breyer tegen Bundesrepublik Deutschland: <http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=NL>

Hoofdstuk 4: Het delen van onderzoeksdata, resultaten en rapportages

In dit hoofdstuk wordt beschreven met welke aandachtspunten de gemeente of de onderzoekers rekening moeten houden als zij de onderzoeksdata, -resultaten of -rapportages intern of met derden willen delen.

Onderzoeksdata

Het is van groot belang dat de onderzoeksdata die is gebruikt ten behoeve van het statistische onderzoek niet wordt gedeeld met interne afdelingen dan wel externe partijen.

De enige twee uitzondering hierop zijn:

- a. Als de gemeente wettelijk verplicht is onderzoeksdata te delen, maar ook dan mag alleen de data verstrekt worden die men verplicht is te verstrekken; of
- b. Indien de gemeente besluit om de onderzoeksdata verder of opnieuw te laten onderzoeken door een extern onderzoeksbureau voor het oorspronkelijke statistische onderzoeksdoel. Immers, ieder statistisch onderzoek vergt dat alle in Hoofdstuk 1: 'Het plan voor het uitvoeren van een statistisch onderzoek' beschreven onderdelen opnieuw worden beoordeeld. De dataset met onderzoeksdata zoals deze voor het oorspronkelijke statistische onderzoek is verzameld, bewerkt en samengesteld is immers voor dat onderzoeksdoeleinde bepaald. Een nieuw soort onderzoek of een vervolgonderzoek vraagt altijd om een nieuwe beoordeling.

Als onderzoeksdata is verzameld ten behoeve van trendanalyses, is het van groot belang dit in de initiële Startnotitie goed te beschrijven en te verantwoorden. Als het legitiem is om de onderzoeksdata te bewaren ten behoeve van trendanalyses, neem in dat geval na de eerste analyse maatregelen om de onderzoeksdata goed te beveiligen en passend te versleutelen. Zo zorg je ervoor dat die onderzoeksdata niet kan worden herbruikt voor andere (onderzoeks)doeleinden.

In de gevallen dat derden verzoeken om het leveren van onderzoeksdata ten behoeve van het verrichten van statistisch onderzoek informeer dan altijd de Privacy Officer en/of Functionaris Gegevensbescherming. Als door hen positief wordt geadviseerd en door de gemeente wordt besloten onderzoeksdata te verstrekken, dan moet dat altijd in geanonimiseerde vorm gebeuren.

Onderzoeksresultaten en -rapportages

Onderzoeksresultaten en rapportages kunnen intern worden gedeeld of met andere partijen respectievelijk derden indien zij daarom verzoeken. Verstrek alleen onderzoeksresultaten en -rapportages die echt geanonimiseerd zijn of op dusdanig hoog geaggregeerd niveau zijn weergegeven, en waarvoor geen vertrouwelijkheid geldt. Immers, belangrijk is dat de onderzoeksresultaten of de -rapportage niet herleidbaar zijn. Dit geldt zowel voor interne afdelingen als externe partijen. Voorkomen moet worden dat zij met behulp van software en/of andere voor hen beschikbare data de onderzoeksresultaten alsnog kunnen herleiden tot individuen, bijvoorbeeld door de onderzoeksresultaten te koppelen aan andere externe of interne bronnen.

Slot

Met dit Handboek AVG is getracht de leden van VSO handvatten te bieden zodat rekening wordt gehouden met de AVG bij het uitvoeren van kwalitatief en kwantitatief onderzoek. Het Handboek AVG is naast een naslagwerk tevens te gebruiken om als gemeentelijke organisatie uit te kunnen leggen en aan te kunnen tonen op welke wijze de organisatie bij het uitvoeren van statistisch onderzoek voldoet aan de AVG. Zorg bij ieder onderzoek ervoor dat duidelijk wordt verantwoord en vastgelegd op welke wijze wordt voldaan, zodat deze verslaglegging tevens bijdraagt aan het aantoonbaar (willen) voldoen aan de AVG.

Bijlage 1: Startnotitie

Deze Startnotitie kan worden gebruikt voor de voorafgaande beoordeling of het voorgenomen kwalitatieve of kwantitatieve onderzoek voldoet aan de eisen die gesteld worden onder de AVG en aanverwante wet- en regelgeving.

Instructies: beschrijf zo duidelijk en concreet mogelijk de antwoorden/onderdelen, waarbij duidelijk wordt onderbouwd. Dit is van belang om ervoor te zorgen dat de degene die het voorgenomen onderzoek op de AVG moet toetsen: 1. een goede beoordeling kan doen op de rechtmatigheid; en 2. eventuele informatie kan gebruiken voor bijvoorbeeld het opnemen van de verwerking in het verwerkingsregister dan wel een aanpassing hiervan. Leg voorafgaand aan de start van het kwalitatieve of kwantitatieve onderzoek deze Startnotitie voor aan de Privacy Officer/Functionaris Gegevensbescherming.

A. Algemeen

Projectnummer onderzoek:	
Naam/titel onderzoek:	

Naam opdrachtgever:	<i>B&W, Afdeling, Team</i>
Naam verantwoordelijke:	<i>Intern (eind)verantwoordelijke voor de taak waarmee het onderzoek samenhangt</i>
Contactgegevens verantwoordelijke:	<i>E-mailadres en telefoonnummer</i>
Naam opdrachtnemer (ook extern):	<i>Afdeling/Team onderzoek & statistiek, extern onderzoeksbureau.</i> <i><u>Let op bij een extern onderzoeksbureau: beoordeel of een verwerkersovereenkomst moet worden gesloten (zie verder onderdeel D van de startnotitie)</u></i>
Namen onderzoeker(s):	
Contactgegevens onderzoeker(s):	

Gewenste startdatum onderzoek:	
Gewenste datum afronding analyse:	
Gewenste datum oplevering rapportage:	

B. Beschrijving onderzoeksdoel en benodigde persoonsgegevens

Onderzoeksdoel:	<i>Beschrijf hier het doel van het onderzoek</i>
Toelichting onderzoeksdoel:	<i>Beschrijf hier meer toelichting op het onderzoeksdoel, namelijk:</i> <ul style="list-style-type: none"> - <i>Achtergrond van het onderzoeksdoel;</i> - <i>Nut en noodzaak van het onderzoeksdoel;</i> - <i>Eventuele eerder uitgevoerde onderzoeken.</i>
Onderzoeksmethoden:	<i>Beschrijf hier welke onderzoeksvorm (specificeer kwalitatief/kwantitatief en welke vorm) én leg uit waarom</i>
Grondslag:	<i>Vink de grondslag aan en licht toe op basis waarvan het onderzoek wordt uitgevoerd:</i>

	<input type="checkbox"/> Toestemming	<i>Toelichting waarom toestemming</i>
	<input type="checkbox"/> Overeenkomst	<i>Toelichting waarom op basis van overeenkomst</i>
	<input type="checkbox"/> Wettelijke verplichting	<i>Toelichting op grond van welke wet, noem wetsartikel</i>
	<input type="checkbox"/> Publieke taak/algemeen belang	<i>Toelichting op basis van welke publieke taak én noem de wettelijke bepaling van die publieke taak en samenhang met het onderzoek</i>
	<input type="checkbox"/> Gerechtvaardigd belang	<i>Toelichting waarom gerechtvaardigd belang en licht toe waarom het belang van het onderzoek zwaarder weegt</i>
Toelichting bij toestemming:	<i>[Indien van toepassing:] Beschrijf op welke wijze de toestemming wordt gevraagd en hoe de toestemming voor deelname aan het onderzoek wordt geregistreerd en beheerd. Leg ook uit hoe wordt gehandeld bij het intrekken van toestemming. <u>Voeg screenshots/voorbeelden bij van de wijze waarop de toestemming gevraagd wordt.</u></i>	

Onderzoeksdata:	<i>Beschrijf hier alle voor het onderzoek <u>benodigde</u> onderzoeksdata</i>	<i>Licht per data toe waarom deze voor het onderzoeksdoel vereist is</i>
Gebruik van anonieme of gepseudonimiseerde data:	<i>Beschrijf of er gebruik wordt gemaakt van anonieme onderzoeksdata of dat de data wordt gepseudonimiseerd. Neem hier ook in mee wanneer de data wordt geanonimiseerd/gepseudonimiseerd en op welke wijze.</i>	
Herkomst van de onderzoeksdata:	<i>Beschrijf hier uit welke bronnen de onderzoeksdata wordt verkregen:</i> <ul style="list-style-type: none"> - <i>Interne databases;</i> - <i>Externe databases;</i> - <i>Respondenten.</i> 	
Selectie en uitnodiging voor onderzoek (bij enquêtes/interviews/focusgroepen):	<i>[Indien van toepassing:] Beschrijf:</i> <ul style="list-style-type: none"> - <i>hoe de (potentiële) respondenten worden geselecteerd voor deelname aan een enquête (bijvoorbeeld middels a-selectie steekproef);</i> 	

	<ul style="list-style-type: none"> - op welke wijze de (potentiële) respondenten worden uitgenodigd; - op welke wijze (potentiële) respondenten een herinnering krijgen voor de uitnodiging om deel te nemen; én - hoe wordt voorkomen dat respondenten die al hebben gereageerd op wel/geen deelname niet de herinnering ontvangen; - op welke wijze de uitnodiging wordt gescheiden van de ontvangen enquêteresultaten (onderzoeksdata).
Informatievoorziening/communicatie:	Beschrijf op welke wijze men wordt geïnformeerd over het onderzoek. Bijvoorbeeld middels een privacyverklaring, een passage bij de uitnodiging, of op welke andere wijze.
Rechten van betrokkenen:	Hoe worden de betrokkenen/respondenten geïnformeerd over hun AVG-rechten, en welke rechten hebben de betrokkenen/respondenten? Zijn er eventueel beperkingen op het recht op inzage of correctie?

C. Methoden en technieken (beveiliging & verwerking onderzoeksdata)

Gebruikte applicatie(s):	<p>Beschrijf in ieder geval:</p> <ul style="list-style-type: none"> • De naam/namen van de applicatie(s) die worden gebruikt; • De applicatie(s) zijn goedgekeurd door ICT of Informatisering & Automatisering (I&A); • Op welke wijze de applicatie(s) voldoen aan de BIO-normen; • Indien de applicatie(s) afwijken van de BIO-normen, beschrijf op welke wijze en welke beveiligingsmaatregelen dan zijn geïmplementeerd.
Wijze van verkrijging/verzameling onderzoeksdata:	<p>Beschrijf in ieder geval:</p> <ul style="list-style-type: none"> • Op welke wijze wordt de onderzoeksdata aangeleverd; en • Op welke wijze wordt de onderzoeksdata beveiligd bij de aanlevering? • Wordt er gebruik gemaakt van een Data Lake of een vergelijkbare toepassing en op welke wijze is de beveiliging geborgd?
Versleutelingstechnieken:	<ul style="list-style-type: none"> • Wordt er gebruik gemaakt van versleutelingstechnieken, welke en op welke wijze wordt dit toegepast; • Als er geen versleutelingstechnieken worden gebruikt, leg uit waarom de onderzoeksdata niet wordt versleuteld.
Opslag(locatie):	<p>Beschrijf in ieder geval:</p> <ul style="list-style-type: none"> • Waar (database/applicatie/netwerkschijf) wordt de onderzoeksdata opgeslagen; • Welke beveiligingsmaatregelen zijn getroffen voor de opslaglocatie

Toegang tot onderzoeksdata	<p>Beschrijf in ieder geval:</p> <ul style="list-style-type: none"> • Wie heeft/hebben toegang tot de onderzoeksdata en licht toe waarom: <ul style="list-style-type: none"> ○ Functie(s): ○ Aantallen: • Welke beveiligingsmaatregelen zijn getroffen om onbevoegde toegang tot de onderzoeksdata te voorkomen.
Bewaar- en vernietigingstermijn:	<p>Hoe lang wordt de onderzoeksdata bewaard of wanneer wordt de onderzoeksdata vernietigd: _____ periode</p> <p>Motiveer waarom de onderzoeksdata voor ____ termijn (maanden/jaren) wordt bewaard.</p> <p>Als er sprake is van anonimisering, leg dan uit op welke wijze dit plaatsvindt.</p>
	Op welke wijze is geborgd dat de vernietiging (of anonimisering) ook daadwerkelijk tijdig en correct plaatsvindt?

D. Externe partijen

Extern onderzoeksbureau:	<p>Wordt er gebruik gemaakt van een extern onderzoeksbureau? Zo ja:</p> <ul style="list-style-type: none"> • Naam: _____ • Moet een verwerkersovereenkomst met deze partij worden gesloten? <ul style="list-style-type: none"> <input type="checkbox"/> Ja, want: <input type="checkbox"/> Nee, want: • Voeg de (concept) verwerkersovereenkomst bij deze startnotitie
Delen van onderzoeksdata:	<p>Wordt de onderzoeksdata gedeeld met derden? Licht toe indien van toepassing, o.a. naam partij, doeleinde, grondslag en welke onderzoeksdata</p>

E. Rapportage onderzoeksresultaten

Presentatie/rapportage:	Beschrijf op welke wijze de onderzoeksresultaten worden gepresenteerd
Aggregatieniveau:	Beschrijf op welke aggregatieniveau(s) de onderzoeksresultaten worden gepresenteerd of gerapporteerd.
Waarborgen géén herleidbaarheid:	Beschrijf hoe geborgd wordt dat op basis van de te presenteren of rapporteren onderzoeksresultaten het niet mogelijk is de resultaten te herleiden tot individuen.
Delen/publicatie onderzoeksresultaten:	Worden de onderzoeksresultaten intern of extern gedeeld of op de gemeentelijke website gepubliceerd? Zo ja, beschrijf met wie en op welke wijze.

Startnotitie ingevuld door:

.....

Datum: / /

Goedkeuring Privacy Officer:

.....

Datum: / /

Optioneel:

Advies Functionaris Gegevensbescherming:.....

Bijlage 2: DPIA Checklist

Instructies: Door de volgende checklist te doorlopen kan een eerste beoordeling van de noodzaak van het uitvoeren van een Data Protection Impact Assessment gemaakt worden. Vink aan wat van toepassing is. Leg de checklist na het invullen voor aan de Privacy Officer/Functionaris Gegevensbescherming..

Geef een korte omschrijving van het onderzoek en de verwerkingen van persoonsgegevens die daarbij plaatsvinden:

1. Wordt bij het onderzoek één van de volgende verwerkingen uitgevoerd?
 - Een systematische en uitgebreide beoordeling van persoonlijk aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking waaronder profiling en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treft (denk hierbij aan situaties waarin de computer beslist o.b.v. een aantal kenmerken of iemand wel of niet in aanmerking komt voor een levensverzekering)
 - Grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (denk hierbij aan gezondheidsgegevens of bijvoorbeeld het bijhouden van zwarte lijsten)
 - Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten (denk hierbij aan cameratoezicht)

Als één van de vakjes hierboven is aangekruist, is er een grote kans dat er een DPIA uitgevoerd moet worden. Stem af met de Privacy Officer/Functionaris Gegevensbescherming.

De hierboven beschreven situaties zullen niet snel voorkomen omdat het moet gaan om "grootschalige" of "stelselmatige" verwerkingen. Dat neemt niet weg dat een aantal veel voorkomende verwerkingsactiviteiten wel een hoog risico voor de betrokkene tot gevolg kan hebben. Daarom heeft de Autoriteit Persoonsgegevens een lijst opgesteld met verwerkingsactiviteiten waarop een DPIA uitgevoerd moet worden. Nu zal bij statistisch onderzoek ook niet snel sprake zijn van één van de onderstaande verwerkingen. Om wel de hele toets te doorlopen waarvoor een DPIA verplicht is gesteld, adviseren we de onderstaande vragen A. en B. inclusief lijst met verplichte DPIA-verwerkingen wel mee te nemen in de beoordeling:

- A. Wordt bij het onderzoek één van de volgende verwerkingen uitgevoerd?
 - Heimelijk onderzoek: Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen. Denk hierbij aan (verborgen) cameratoezicht, het gebruik van warmtecamera's of locatietracking zonder dat de betrokkenen daarvan op de hoogte zijn gesteld.
 - Zwarte lijsten: Verwerkingen waarbij persoonsgegevens betreffende 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 deze gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers.

- Fraudebestrijding: Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.
- 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.
- 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.
- Genetische persoonsgegevens: Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.
- 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.
- 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.
- Cameratoezicht: Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.
- 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.
- 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 ten behoeve van diefstal- en fraudebestrijding.
- 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.
- 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.

- 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.
- 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.
- Monitoring 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.
- Biometrische gegevens: Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens (bijv. irisscans of vingerafdrukken) met als doel een natuurlijk persoon te identificeren.

Als één van de vakjes hierboven is aangekruist, is er een grote kans dat er een DPIA uitgevoerd moet worden. Stem af met de Privacy Officer/Functionaris Gegevensbescherming.

Naast de bovenstaande lijst van de Autoriteit Persoonsgegevens hebben de Europese privacytoezichthouders (European Data Protection Board) ook een aantal criteria bepaald aan de hand waarvan beoordeeld kan worden of een DPIA noodzakelijk is. Als aan 2 of meer van de 9 criteria wordt voldaan, dan moet er een DPIA uitgevoerd worden, stem af met de Privacy Officer/Functionaris Gegevensbescherming.

B. Worden één of meer van de volgende verwerkingen uitgevoerd met het statistische onderzoek?

- 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.
- 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. Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.
- Stelselmatige en grootschalige monitoring: Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht.
- 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.
- 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.

- Gekoppelde databases: Het gaat hierbij om 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.
- Gegevens over kwetsbare personen: Denk hierbij aan werknemers, kinderen, gehandicapte personen of patiënten.
- Gebruik van nieuwe technologieën: Denk hierbij aan slimme apparaten/Internet of Things toepassingen.
- 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.

Checklist ingevuld door:

.....

Datum: / /

Goedkeuring Privacy Officer:

.....

Datum: / /

Bijlage 3: Template privacyverklaring voor respondenten

*Instructies: de onderstaande template kan worden gebruikt om bij een onderzoek in de vorm van een enquête, interview, focusgroep of panelonderzoek de respondent of geïnterviewde te informeren over de wijze waarop met persoonsgegevens wordt omgegaan en wat de rechten zijn. De template bevat diverse keuzes die de organisatie kan maken. De open velden en keuzes zijn **geel gearceerd**. De template kan onverkort als aparte link voor aanvang van de enquête worden opgenomen of separaat als bijlage worden bijgevoegd. Delen van deze template kunnen ook worden gebruikt bij het informeren over het voorafgaand doel van de enquête en op welke wijze met (persoons)gegevens wordt omgegaan. Zorg in dat geval altijd nog voor een verwijzing naar de volledige privacyverklaring.*

Privacyverklaring gemeente _____ [naam gemeente] ten behoeve van onderzoek en respondenten

In deze privacyverklaring kunt u lezen hoe de gemeente _____ [naam gemeente] omgaat met de gegevens die u bij deelname aan het onderzoek _____ [naam onderzoek] aan ons verstrekt. Bij het uitvoeren van het onderzoek respecteren wij uw privacy en handelen wij binnen de wettelijke kaders van de Algemene Verordening Gegevensbescherming (AVG). Meer informatie over hoe de gemeente _____ [naam gemeente] verder omgaat met uw persoonsgegevens kunt u lezen in: _____ [voeg link toe naar 'algemene' privacyverklaring gemeente].

Het doel van het onderzoek:

Het onderzoek _____ [naam onderzoek] heeft als doel: _____ [omschrijving onderzoeksdoel]. Het onderzoek wordt uitgevoerd ten behoeve van _____ [naam opdrachtgever (bijv afdeling of college van B&W)], de gemeente _____ [naam gemeente] is hiervoor verwerkingsverantwoordelijke onder de AVG. Wij verwerken de door u gegeven antwoorden als onderzoeksdata op basis van uw toestemming of doordat u een enquête heeft ingevuld en met ons heeft gedeeld (geïnformeerde toestemming). Deelname aan het onderzoek is vrijwillig. U beslist zelf of u wel of niet deelneemt. Als u besluit deel te nemen, dan verwerken wij uw gegevens alleen voor het onderzoeksdoel en statistisch onderzoek. Wij gebruiken uw gegevens nooit voor handhaving, controles of andere individuele besluiten.

De (persoons)gegevens die wij van u verwerken:

Uitnodiging voor deelname:

Voor de deelname aan het onderzoek heeft u een uitnodiging ontvangen. Deze uitnodiging is aan u verzonden, omdat u _____ (bijv. bent geselecteerd op basis van een a-selectie steekproef uit de Basisregistratie Personen / bent geselecteerd in verband met cliëntervaringsonderzoek vanwege voorzieningen die u ontvangt op grond van de Jeugdwet of Wmo2015 / heeft aangegeven deel te nemen aan een interview of panelonderzoek of focusgroep). Wij hebben hiervoor uw naam en _____ (e-mailadres/adres) gebruikt.

Welke (persoons)gegevens verwerken wij voor dit onderzoek:

Keuze ten aanzien van het wel/niet verwerken persoonsgegevens ten behoeve van het onderzoek:

- **Indien alleen anonieme onderzoeksdata wordt verwerkt:**

Voor dit onderzoek verzamelen wij als gemeente _____ [naam gemeente] door middel van deze enquête enkel anonieme data. Deelname aan dit onderzoek is geheel anoniem en niet herleidbaar tot u.

De adreslijst voor de uitnodiging voor de deelname aan het onderzoek houden wij strikt gescheiden van de door u verstrekte antwoorden. Hierdoor is het niet mogelijk de door u gegeven antwoorden naar u te herleiden.

- **Indien persoonsgegevens worden verwerkt:**

Voor dit onderzoek verzamelen wij als gemeente _____ [naam gemeente] middels een _____ [keuze: *enquête/interview/focusgroep/panelonderzoek*] met uw toestemming de volgende gegevens: **[Opsomming welke persoonsgegevens worden verwerkt die rechtstreeks van de betrokkene wordt verkregen]**

- _____
- _____
- Etc.

[Indien van toepassing voor het onderzoek:

(Persoons)gegevens die niet van u afkomstig zijn:

Bij dit onderzoek gebruiken wij naast de door u verstrekte antwoorden en informatie ook nog informatie en onderzoeksdata uit andere bronnen. Dit betreft _____ [*interne basisregistraties/onzoeksdata van externe partijen als CBS/openbare bronnen*]. Hierbij gebruiken wij de volgende (persoons)gegevens:

[Opsomming welke persoonsgegevens worden verwerkt die uit andere bronnen wordt verkregen]

- _____
- _____
- Etc.

Noodzaak voor het gebruik van persoonsgegevens:

De persoonsgegevens zijn noodzakelijk voor het onderzoek omdat: _____ [*uitleg gelet op onderzoeksdoel*].

Toestemming intrekken:

Op grond van de AVG heeft u het recht om de eerder gegeven toestemming weer in te trekken. Als u uw toestemming wilt intrekken, dan hanteren wij als gemeente _____ [naam gemeente] hierbij de volgende uitgangspunten:

- indien met het onderzoek alleen geanonimiseerde gegevens (onderzoeksdata) zijn of worden verwerkt, kunt u de toestemming niet intrekken. De reden is dat de door u gegeven antwoorden niet meer naar u herleidbaar zijn en wij zodoende ook niet kunnen achterhalen wie de antwoorden heeft gegeven;
- indien de toestemming voorafgaand aan het onderzoek wordt ingetrokken, dan worden uw antwoorden niet meegenomen in het onderzoek én worden uw gegevens verwijderd;
- indien de toestemming tijdens het uitvoeren van het onderzoek wordt ingetrokken, dan worden alle gegevens van u verwijderd. De uitzondering hierop is indien de intrekking van de toestemming het bereiken van het doel van het onderzoek onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dat geval wordt de onderzoeksdata volledig geanonimiseerd, waardoor deze niet meer herleidbaar is naar u;
- indien u uw toestemming intrekt nadat het onderzoek is afgerond, gepubliceerd of gerapporteerd dan worden de door u gegeven antwoorden en gegevens niet verwijderd. Voor zover dat nog niet heeft plaatsgevonden, worden uw gegevens voor zover mogelijk geanonimiseerd. In het geval van toekomstige vervolgonderzoeken of bij hergebruik van de onderzoeksdata worden uw gegevens niet meegenomen.

Als u de eerder gegeven toestemming voor het onderzoek wilt intrekken, dan kunt u een e-mail sturen naar _____ [*@gemeente.nl*] onder vermelding van *intrekken toestemming* voor _____ [naam onderzoek].

Bescherming van gegevens:

Om uw gegevens te beschermen treffen wij zowel fysieke als technische maatregelen. Zo zorgt de gemeente _____ [naam gemeente] ervoor dat er geen onbevoegde toegang tot de gegevens mogelijk is. Alle gegevens die worden verzameld en verwerkt in bijvoorbeeld computersystemen zijn goed beveiligd. Ook zorgen wij ervoor dat geen gegevens gepubliceerd worden die herleidbaar zijn tot personen. Als wij als gemeente bij een onderzoek samenwerken met een onderzoeksbureau dan zorgen wij ervoor dat wij afspraken hebben gemaakt over hoe dit bureau met de gegevens omgaat. Zo mag dit onderzoeksbureau de gegevens alleen gebruiken voor dit onderzoek, niet delen met derden, en als de opdracht is afgelopen worden alle gegevens vernietigd. Tevens zien wij erop toe dat het onderzoeksbureau zich aan de afspraken houdt.

Delen van gegevens:

Keuze maken afhankelijk van soort onderzoek:

Niet delen:

De door u gegeven antwoorden op de vragen worden niet met andere organisaties gedeeld. De resultaten, rapportages en publicaties van het onderzoek kunnen wel worden gedeeld, maar zijn niet herleidbaar tot individuele personen. Hier wordt vooraf streng op toegezien.

Wel delen:

De gegevens kunnen gedeeld worden met andere onderzoekers, maar alleen zo dat de gegevens niet herleidbaar zijn. Wij delen bij dit onderzoek de gegevens (onderzoeksdata) met de volgende organisaties, omdat _____ [uitleg reden van delen onderzoeksdata]. De volgende organisaties ontvangen uw niet tot u herleidbare gegevens:

[Opsomming]

Met deze organisaties hebben wij afspraken gemaakt over hoe zij omgaan met de gegevens zodat uw privacy gewaarborgd wordt.

Opslag en bewaren van gegevens:

Uw gegevens worden niet langer bewaard dan noodzakelijk is voor het onderzoek. Hiervoor hanteren wij als gemeente _____ [naam gemeente] een termijn van _____ [maanden/jaar]. Als deze termijn is afgelopen zorgen wij ervoor dat uw gegevens worden _____ [vernietigd of geanonimiseerd].

De gegevens die wij van u verwerken, worden opgeslagen in goed beveiligde computersystemen binnen de EU [of evt. in Nederland indien van toepassing en ander land binnen de EU bijv. gelet op back-ups].

Uw AVG-rechten:

Onder de AVG heeft u verschillende rechten. Zo heeft u onder meer het recht op inzage, het recht op correctie van uw gegevens of het recht op verwijdering van uw gegevens. Meer informatie over wat deze rechten inhouden en hoe u uw AVG-rechten kunt uitoefenen, kunt u lezen in de privacyverklaring van de gemeente _____ [naam]. Deze privacyverklaring kunt u hier raadplegen: _____ [link naar 'algemene' privacyverklaring]. Hier staat ook hoe u gebruik kunt maken van uw AVG-rechten.

Vragen of klachten over dit onderzoek:

Voor vragen over dit onderzoek kunt u contact opnemen met:

Naam gemeente

Afdeling

Contactgegevens

Heeft u vragen of klachten over de wijze waarop de gemeente _____ [naam gemeente] bij dit onderzoek omgaat met uw persoonsgegevens, dan kunt u contact opnemen met de Functionaris Gegevensbescherming (FG). Dit is de onafhankelijk toezichthouder die toeziet op de naleving van de AVG. De contactgegevens van de FG zijn:

Functionaris Gegevensbescherming _____ [naam gemeente]

Adres

E-mail en/of telefoonnummer

Indien u vindt dat de gemeente _____ [naam gemeente] bij de uitvoering van dit onderzoek de AVG (privacywetgeving) schendt, dan heeft u altijd het recht om naast uw klacht bij de FG kenbaar te maken een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Bijlage 4: Template toestemmingsformulier interview of panelonderzoek

Met dit formulier geef ik [volledige naam respondent] toestemming aan de gemeente [naam gemeente] om gegevens over mij te verwerken in het kader van [naam/aanduiding onderzoek(en)]. Het betreft gegevens en antwoorden die ik zelf ten behoeve van het onderzoek [of de onderzoeken] verstrek.

De manier waarop de gemeente [naam gemeente] omgaat met uw persoonsgegevens kunt u nalezen in de Privacyverklaring respondenten.

[Keuze maken:

Deze Privacyverklaring kunt u verder hier raadplegen: [link website verklaring]

[OF]

Door het vakje hieronder aan te kruisen geeft u aan kennis te hebben genomen van deze Privacyverklaring.

- Ja, ik heb kennis genomen van de Privacyverklaring respondenten

De volgende voorwaarden zijn verder van toepassing:

- Mijn toestemming geldt alleen voor de hierboven beschreven doelen en voorwaarden. Voor nieuwe onderzoeksdoeleinden vraagt de gemeente [naam gemeente] mij opnieuw om toestemming. **Toelichting: indien sprake is van 'vervolgonderzoeken' of 'panelonderzoeken', dan is het advies om dit ook concreet in de bovenstaande beschrijving met doelen op te nemen.**
- De gemeente [naam gemeente] informeert mij over de gegevens die over mij worden uitgewisseld en de gegevens die over mij worden geregistreerd. Dat betekent bijvoorbeeld dat mij wordt uitgelegd om welke specifieke gegevens het gaat en waarom deze gegevens noodzakelijk zijn voor het onderzoek of de vervolgonderzoeken.
- Ik kan ervoor kiezen om geen toestemming te geven of om alleen aan bepaalde onderzoeken deel te nemen of daarvoor toestemming te geven.
- Deelname aan het onderzoek is vrijwillig. Ik bepaal zelf welke informatie ik wel deel en welke informatie ik niet wil delen.
- Ik kan mijn deelname en mijn toestemming voor het gebruiken van mijn gegevens op ieder gewenst moment intrekken. De gemeente [naam gemeente] zal mij informeren over de gevolgen wanneer ik ervoor kies om mijn toestemming in te trekken.
- Als gegevens niet (meer) noodzakelijk zijn voor de hierboven beschreven doelen zal de gemeente [naam gemeente] deze verwijderen of anonimiseren.



PRIVACY
C O M P A N Y

www.privacycompany.eu

info@privacycompany.nl

070 – 820 96 90

Privacy Company
Maanweg 174
2516 AB Den Haag
14e verdieping

Postbus 95315
2509 CH Den Haag

