Sociaal en Cultureel Planbureau

**Inlichtingen bij**
Ineke Stoop
i.stoop@scp.nl
T

**Datum**
10 April 2015

**Kenmerk**
/

**C.c.**

*j:\project\bescherming persoonsgegevens\handboek wet bescherming persoonsgegevens scp pc en ineke 25 juni 2015.docx*

# Handboek Wet bescherming persoonsgegevens SCP: Onderzoeksdata

Inhoudsopgave

**Samenvatting**

Het SCP gebruikt voor onderzoeksdoeleinden regelmatig persoonsgegevens. Dat zijn gegevens over geïdentificeerde of identificeerbare personen. Volgens de Wet bescherming persoonsgegevens is dat toegestaan, maar er moet dan wel aan een aantal voorwaarden worden voldaan.

De **beheerder** (de directeur van het SCP) is ervoor verantwoordelijk dat bij nieuwe dataverzamelingen de juiste stappen worden gevolgd. Dat houdt onder andere in dat deelnemers aan onderzoek de juiste informatie krijgen over het doel van het onderzoek en het gebruik van hun gegevens. Ook moet worden getoetst of een gegevensbestand daadwerkelijk persoonsgegevens bevat. In het dat geval moet het bestand in zo'n vroeg mogelijk stadium worden gemeld bij de **Functionaris Gegevensverwerking** (FG) van VWS. De beheerder is ook verantwoordelijk voor de jaarlijkse rapportage over persoonsgegevens, en het afhandelen van verzoeken to inzage en correctie.

De **contactpersoon** (hoofd OMM bij het SCP) is door de beheerder belast met de uitvoering van de Wbp. In de praktijk worden veel van de activiteiten op het terrein van de Wbp uitgevoerd door de **methodologen**. Zij ondersteunen de onderzoekers (ofwel de **verwerkers**) bij het verkrijgen van *informed consent* van deelnemers aan onderzoek, bij het nemen van de gepaste veiligheidsmaatregelen en bij meldingen aan de FG.

De **SCP-onderzoekers** dienen zich bewust te zijn van de noodzaak zorgvuldig om te gaan met persoonsgegevens. Dat betekent dat ze geen persoonsgegevens op onbeveiligde informatiedragers laten staan, maar deze op beveiligde schijfruimte laten plaatsen, dat ze deelnemers aan onderzoek informeren over het doel van het onderzoek en het beoogde gebruik van de gegevens. Het betekent vooral dat ze de ondersteuning van de methodologen inroepen die hen kunnen helpen bij het beschermen van persoonsgegevens.

In deze nota worden de achtergronden van de Wbp geschetst, en wordt uiteengezet welke stappen bij het SCP genomen moeten worden bij het gebruik van onderzoeksdata.

## 1. Introductie

De Wet bescherming Persoonsgegevens (Wbp)[1] reguleert het gebruik van persoonsgegevens. Dat zijn gegevens over geïdentificeerde of identificeerbare personen. Voor onderzoeksdoeleinden[2] verwerkt het SCP veel gegevens over natuurlijke personen. Meestal zijn die niet identificeerbaar, en daarmee zijn het geen persoonsgegevens. Het SCP mag persoonsgegevens verwerken, mits dat voor wetenschappelijk onderzoek gebeurt. Bij het gebruik van persoonsgegevens voor onderzoek moet het SCP echter aan een grote hoeveelheid regels en richtlijnen voldoen. Deze staan in dit handboek beschreven.

Dit handboek beschrijft dus hoe binnen het Sociaal en Cultureel Planbureau moet worden omgegaan met gegevens over geïdentificeerde of identificeerbare personen. De regels in dit handboek zijn gebaseerd op deel B[3] het Handboek Wet bescherming persoonsgegevens (Wbp) van VWS, dat de uitvoering binnen VWS van de WbP beschrijft, en op de *Gedragscode voor onderzoek en statistiek*[4]**,** goedgekeurd door het College bescherming persoonsgegevens (Cbp)[5].

## 2. Wat zijn persoonsgegevens

Een persoonsgegeven is volgens de Wbp elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Een gegeven is dus een persoonsgegeven als het informatie bevat over een natuurlijke persoon en die persoon identificeerbaar is. Bijlage 1 toetst wat tot persoonsgegevens gerekend moet worden.

Natuurlijke personen van wie gegevens worden verwerkt zijn bijvoorbeeld identificeerbaar als hun naw-gegevens (naam, adres, woonplaats) bekend zijn. In principe zijn alle gegevens die over identificeerbare personen worden verwerkt persoonsgegevens, denk aan:

- naam, adres, postcode, woonplaats, telefoon- en faxnummer(s), e-mailadres(sen);
- leeftijd, opleiding, werkervaring;
- schulden, vorderingen, kenmerken/kentekens van eigendommen, videobeelden.

[1] https://cbpweb.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens Hier vindt u ook de link naar de actuele wettekst.
[2] Dit handboek heeft uitsluitend betrekking op persoonsgegevens die gebruikt worden voor onderzoek. Het SCP bewerkt ook persoonsgegevens voor administratieve doeleinden. Deze vallen buiten het bereik van dit handboek.
[3] Van dit handboek is sinds 2010 een conceptversie beschikbaar. http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/ciskernprocessen/cisjuridischportaal/cisvws_juridisch/cisrechtsgebieden_2/cisbeschermingvanpersoonsgegevens
[4] www.moaweb.nl/Richtlijnen/gedragscode-voor-onderzoek-en-statistiek www.cbpweb.nl/downloads_gedragscodes/gedragscode-onderzoek-statistiek.pdf
[5] Het is van belang te vermelden dat de Gedragscode Onderzoek en Statistiek wordt herzien in 2015. Bovendien werkt de Europese Commissie sinds enige tijd aan nieuwe regelgeving op het terrein van “Data Protection” (http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm). De verwachting is dat deze nieuwe regelgeving binnen afzienbare tijd wordt geïntroduceerd.

Er zijn ook persoonsgegevens die worden opgevat als 'bijzondere persoonsgegevens'[6]. Hier wordt onder andere verstaan gegevens over ras, gezondheid en strafrechtelijke gegevens. De Wbp bevat een aantal zeer specifieke regels ten aanzien van de verwerking van 'bijzondere' persoonsgegevens. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij daarvoor een ontheffingsgrond in de wet staat (zoals bij het gebruik voor onderzoek en statistiek)[7]. Zie voor een uitgebreid overzicht van bijzondere persoonsgegevens bijlage 1. Het SCP mag dus ook bijzondere persoonsgegevens gebruiken, maar dan zijn de regels nog strikter.

In het algemeen zijn *uitkomsten* van statistisch onderzoek niet terug te voeren tot identificeerbare personen en dus geen persoonsgegevens. Ze vallen derhalve buiten de reikwijdte van de Wbp (zie ook bijlage 1). Gegevens over een rechtspersoon (een bv of een vereniging bijvoorbeeld) zijn in het algemeen ook geen persoonsgegevens.

## 3. Bescherming van persoonsgegevens in onderzoek en statistiek

Voor onderzoek en statistiek is het toegestaan de burger bepaalde persoonsgegevens te vragen[8]. Hierbij bestaan uitzonderingen op de algemene regels. Bij persoonsgegevens in het algemeen geldt bijvoorbeeld dat ze worden verwijderd als ze niet meer nodig zijn. Voor onderzoek en statistiek[9] wordt anderzijds de regel gehanteerd dat ruwe data minimaal vijf jaar worden bewaard met het oog op controleerbaarheid en repliceerbaarheid. Het SCP bewaart daarom ruwe data minimaal tien jaar (zie ook hoofdstuk 9).

De burger heeft echter het recht op privacy. De Wbp legt vast hoe rechtmatig met persoonsgegevens moet worden omgegaan[10]. Zo is vastgelegd dat:

- Persoonsgegevens alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier mogen worden verwerkt.
- Persoonsgegevens alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
- De gegevensverwerking op een passende manier moeten worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

[6] Zie artikel 16 Wbp
[7] Zie artikel 23 lid 2 Wbp voor de voorwaarden
[8] Zie artikel 8 van de Wbp
[9] www.vsnu.nl/files/documenten/Domeinen/Onderzoek/Code_wetenschapsbeoefening_2004_(2014).pdf
[10] https://cbpweb.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

Het feit dat burgers aan het SCP persoonsgegevens verstrekken, betekent dus dat zij van het SCP mogen verwachten dat die de persoonsgegevens goed beheert en daar op zorgvuldige wijze mee omgaat. Het SCP handelt conform de Gedragscode voor Onderzoek en Statistiek en hanteert de Tien Gouden Regels uit de Gedragscode, weergegeven in Tekstblok 1.

***Tekstblok 1. Tien Gouden Regels voor Onderzoek & Statistiek en Gegevensbescherming:***
*Handel in overeenstemming met de tekst en de geest van de Gedragscode voor Onderzoek en Statistiek en leef de volgende bepalingen te allen tijde na.*

1. Informeer de respondent over het doel van het onderzoek.
2. Bejegen de respondent die aan het onderzoek deelneemt met respect, ook wanneer hij niet wenst deel te nemen, een weigering is een weigering.
3. Verzamel niet meer gegevens dan noodzakelijk voor de uitvoering van het onderzoek.
4. Extra zorgvuldigheid is geboden bij het verzamelen en verwerken van bijzondere gegevens. Dit zijn persoonsgegevens omtrent iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke Persoonsgegevens en Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
5. Verwerk gegevens in identificeerbare vorm niet langer dan noodzakelijk voor de uitvoering van het onderzoek, anonimiseer zo snel mogelijk.
6. Rapporteer nooit over individuele respondenten met identificeerbare gegevens tenzij de respondent daarvoor ondubbelzinnige toestemming heeft gegeven.
7. Neem technische en organisatorische maatregelen ter beveiliging van de verzamelde gegevens tegen onrechtmatig gebruik.
8. Zorg voor een tijdige melding van de verwerking bij het College bescherming persoonsgegevens door de opdrachtgever, als persoonsgegevens verkregen uit het onderzoek langer dan zes maanden na verkrijging worden bewaard.
9. Houd alle persoonsgegevens die worden verzameld en bewerkt geheim en verstrek persoonsgegevens alleen aan geautoriseerde functionarissen.
10. Wijs bij irritatie van de respondent, bij onaangekondigd onderzoek per spraaktelefoon, op de mogelijkheid om zijn persoonsgegevens tegen dergelijke vorm van onderzoek te blokkeren via www.onderzoekfilter.nl.

## 4. Wie doet wat bij de bescherming persoonsgegevens bij het SCP

Bij de uitvoering van de Wbp spelen diverse personen en organisaties een rol. Hier volgt een overzicht, toegespitst op het SCP (zie figuur 1).


**Figuur 1 Rollen Wbp en invulling door het SCP**

*De betrokkene*
Degene op wie de persoonsgegevens betrekking hebben, is de 'betrokkene'.
***De respondent, persoon in registratie, geïnterviewde of informant is de betrokkene.***

*De verantwoordelijke*
Het bestuursorgaan dat het doel en de middelen vaststelt voor de verwerking van persoonsgegevens is de 'verantwoordelijke'. Binnen de rijksoverheid is de minister de verantwoordelijke voor de verwerkingen van persoonsgegevens door zijn departement.
***De minister van VWS is de verantwoordelijke voor de verwerkingen van persoonsgegevens door het SCP.***

*De beheerder*
De minister kan zijn verplichtingen en taken op grond van de Wbp mandateren aan een beheerder. De beheerder is de directeur of het hoofd van een organisatieonderdeel aan wie krachtens de geldende organisatie- en mandaatregeling de taken en bevoegdheden van de minister zijn gemandateerd. De beheerder is dus hiërarchisch ondergeschikt aan de minister. De beheerder zal namens de minister vaak het beheer hebben over die verwerkingen van persoonsgegevens waarvoor hij als directeur of hoofd van een organisatieonderdeel de verantwoordelijkheid draagt. De beheerder is namens de minister verantwoordelijk voor de uitvoering van de Wbp. Formeel, dat wil zeggen op grond van de Wbp, blijft de minister de verantwoordelijke. Als het College bescherming persoonsgegevens vragen heeft over een verwerking van persoonsgegevens van het SCP zal het CBP deze richten aan de minister.
***Bij het SCP is de Directeur de beheerder van de verwerkingen van persoonsgegevens van het SCP.***

*De contactpersoon*[11]
De beheerder belast vaak één of meer specifieke medewerkers met de uitvoering van de Wbp. Dit is meestal de zogenaamde contactpersoon. Deze contactpersoon zal het grootste deel van de activiteiten op grond van de Wbp voor zijn rekening nemen. Gedacht kan worden aan het melden, de periodieke controle en het ervoor zorgen dat aan de doorlopende verplichtingen kan worden voldaan. De contactpersoon voert in opdracht van de beheerder de Wbp uit.
***Bij het SCP is hoofd OMM contactpersoon op het terrein van onderzoeksdata.***

*De verwerker*
De verwerker van persoonsgegevens is degene die gegevens bij zijn werkzaamheden moet inzien, dan wel invoeren of muteren. De verwerker verkrijgt daartoe meestal expliciet de bevoegdheid.
***Bij het SCP zijn onderzoekers (inclusief de methodologen, ICT-ers en incidenteel medewerkers BV) de verwerkers.***

*De bewerker*
De bewerker verwerkt de persoonsgegevens ten behoeve van het SCP, maar is geen SCP medewerker (oftewel niet hiërarchisch ondergeschikt aan de minister). Er is niet altijd sprake van een bewerker. Als het SCP gebruik maakt van een bewerker, moet daaraan een bewerkersovereenkomst ten grondslag liggen.[12]
***Bij het SCP zijn o.a. marktonderzoekbureaus, externe interviewers, moderatoren van focusgroepen en degenen die interviews transcriberen de bewerkers.***

[11] In artikel 1 definieert de Wbp de begrippen betrokkene, verantwoordelijke, bewerker, derde, ontvanger en FG. De begrippen beheerder, contactpersoon en verwerker zijn rollen die het SCP heeft gedefinieerd. Deze rollen zijn de uitwerking van de dagelijkse praktijk binnen het SCP en de praktische invulling van het Wbp-begrip "verantwoordelijke".
[12] Zie artikel 14 Wbp voor de begrippen bewerker en bewerkersovereenkomst.

*De ontvanger*
Degene aan wie persoonsgegevens worden verstrekt is een ontvanger. Onder verstrekken valt ook het bekend maken of ter beschikking stellen van persoonsgegevens aan een ander persoon. Een derde, maar ook de betrokkene, de verantwoordelijke, de beheerder, de bewerker, de contactpersoon en de gebruiker kunnen 'ontvangers' van persoonsgegevens zijn.
***Bij SCP-onderzoek worden alle gegevens idealiter ontvangen door een van de methodologen.***

*De derde*
Het kenmerk van een derde is, dat dit juist niet de betrokkene, niet de verantwoordelijke, niet de bewerker, noch enig persoon onder het rechtstreeks gezag van de verantwoordelijke of de bewerker is. Hoewel de minister geen gezag heeft over de derde kan deze echter wel gerechtigd zijn persoonsgegevens te verwerken. Gedacht kan worden aan bijvoorbeeld een medewerker van een ander overheidsorgaan, die gegevens voor zijn taakuitoefening of op grond van een wettelijk voorschrift nodig heeft.
***Het SCP levert geen onderzoeksgegevens/persoonsgegevens aan derden. Gegevens die via DANS beschikbaar worden gesteld zijn ontdaan van identificerende informatie, en vallen daarmee niet onder de Wbp.***

*Het College bescherming persoonsgegevens (Cbp)*
Het Cbp houdt onafhankelijk toezicht op het verwerken van persoonsgegevens overeenkomstig de geldende wet- en regelgeving. Het Cbp kan onderzoek instellen, bestuursdwang toepassen, bestuurlijke boeten opleggen en misstanden in de publiciteit brengen.

*Functionaris voor de Gegevensbescherming (FG)*
Binnen de Rijksoverheid is voor ieder ministerie een FG aangesteld[13]. De FG is belast met het houden van toezicht op de verwerkingen van persoonsgegevens door het ministerie. In een overeenkomst tussen de minister en de FG zijn de taken en bevoegdheden vastgelegd. De FG heeft op grond van deze overeenkomst toegang tot alle gegevensverwerkingen binnen het ministerie. De FG kan zelf audits uitvoeren of audits door een interne of externe accountantsdienst laten uitvoeren. De FG werkt onafhankelijk van de minister en het Cbp. Naast het houden van toezicht, houdt de FG het register met onder andere de meldingen bij, adviseert hij de minister en de medewerkers van het ministerie gevraagd of ongevraagd over de wijze waarop met persoonsgegevens moet worden omgegaan, onderhoudt hij contact met het Cbp en stelt hij een jaarverslag op.
***De FG van het ministerie van VWS is ook bevoegd ten aanzien van het SCP.***

*De Accountantsdienst*
Een Accountantsdienst (AD) kan (achteraf) de naleving van de Wbp controleren, al dan niet op verzoek van de FG.

[13] De functie van de FG is omschreven in artikel 62 van de Wbp.

## 5. Het verwerken van persoonsgegevens bij onderzoek

### 5.1 Wanneer is er sprake van persoonsgegevens?

Bij de Wbp gaat het niet om het verwerken van 'zomaar' gegevens, maar om het verwerken van persoonsgegevens:

*Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*

Om te bepalen of een gegeven een persoonsgegeven is, moet worden vastgesteld of het gegeven informatie bevat over een natuurlijke persoon. Volgens het VWS handboek zijn persoonsgegevens o.a. naam, adres, woonplaats (zogenaamde NAW-gegevens), telefoonnummer, kenteken van auto, bankrekeningnummer, burgerservicenummer en gegevens in het personeelsdossier.
Een persoon is identificeerbaar indien zijn identiteit redelijkerwijze, zonder onevenredige inspanning, kan worden vastgesteld. Twee factoren spelen hierbij een rol: de aard van de gegevens en de mogelijkheden van de verantwoordelijke – de minister – om de identificatie tot stand te brengen.

Bij onderzoeksgegevens wordt de combinatie van kenmerken als middel ter identificatie meegenomen. Leeftijd, geslacht, beroep, en huishoudenssamenstelling zijn op zich niet identificerend, en ook in combinatie niet. Bij zeldzame beroepen (Commissaris van de Koning) is identificatie wel mogelijk. Regionale gegevens maken identificatie een stuk makkelijker omdat binnen één regio een combinatie van persoonskenmerken minder vaak voorkomt.

Het SCP verwerkt verschillende soorten gegevensbestanden voor onderzoek (zie hieronder). Deze bestanden kunnen soms persoonsgegevens bevatten. Als dat zo is, geldt het gehele bestand als gegevensverwerking in de zin van de Wbp.
Bij onderzoek van het SCP worden daardoor bestanden met de volgende gegevens wel als verwerkingen van persoonsgegevens beschouwd:

- Surveybestanden met gegevens over personen waarvan de naam en het adres (of andere identificerende gegevens zoals BSN) bij het SCP bekend zijn en mogelijk koppelbaar zijn.
- Administratieve bestanden met naam, adres en andere identificerende gegevens van contactpersonen, sleutelfiguren, informanten, etc.
- Bestanden waarin de vier-cijferige postcode van het woonadres is opgenomen (in combinatie met andere kenmerken (leeftijd, huishoudenssamenstelling, beroep, etc.) kan identificatie niet worden uitgesloten).
- Transcripten, audio-opnamen of video-opnamen van interviews of focusgroepgesprekken. Het herkennen van personen is in deze gevallen niet uit te sluiten. Ook kunnen bij video-opnamen bijzondere persoonskenmerken worden onthuld (ras).

## 5.2 Verwerken van persoonsgegevens

Het verwerken van persoonsgegevens staat centraal in de Wbp. Het verwerken van persoonsgegevens omvat elke handeling of elk geheel van handelingen vanaf het verzamelen tot aan het vernietigen van de gegevens.

Definitie: Verwerking van persoonsgegevens
*Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*

Een verwerking van persoonsgegevens kan bijvoorbeeld bestaan uit het verzamelen van gegevens in een survey en vervolgens het opslaan van deze gegevens. Het bestand kan door een onderzoeker worden geraadpleegd en bewerkt. Het resultaat van de bewerking wordt in de tabel vastgelegd. Deze verschillende verwerkingen kunnen als een geheel van handelingen worden aangemerkt, dus als één 'verwerking van persoonsgegevens'.`

## 5.3 Behoorlijk en zorgvuldig verwerken van persoonsgegevens

De Wbp schrijft voor dat persoonsgegevens altijd 'behoorlijk en zorgvuldig' verwerkt moeten worden[14]. Deze begrippen staan centraal in de Wbp en zijn leidend bij de uitvoering en interpretatie van de Wbp. Alle artikelen uit de Wbp geven invulling aan de voorwaarden 'behoorlijk en zorgvuldig'
Zo bepaalt de Wbp onder andere dat de burger geïnformeerd moet worden over welke persoonsgegevens door de minister over hem worden verwerkt (transparantie) en voor welk doel zijn persoonsgegevens worden verwerkt (doelbinding).

*Transparantie* houdt in dat verwerkingen van persoonsgegevens bij het SCP moeten worden gemeld bij de Functionaris voor de Gegevensbescherming *(*FG). Burgers kunnen inzien welke persoonsgegevens bij de FG zijn gemeld.

*Doelbinding* houdt in dat persoonsgegevens moeten worden verzameld voor een *welbepaald*, *uitdrukkelijk omschreven* en *gerechtvaardigd* doel[15]. Die doeleinden moeten reeds zijn vastgesteld vóórdat de persoonsgegevens worden verzameld. Dit mag dus niet pas gebeuren in de loop van het verzamelproces. Dit betekent dat het SCP voorafgaand aan een dataverzameling moet vastleggen voor welk doel de gegevens verwerkt worden. Hierbij gelden de volgende eisen:

[14] Zie artikel 6 van de Wbp.
[15] Zie artikel 7 van de Wbp.

- *Welbepaald*: de doelomschrijving moet duidelijk zijn, niet zo vaag of ruim dat bij bijvoorbeeld het verzamelen geen kader kan worden geboden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet.
- *Uitdrukkelijk omschreven*: het doel of de doelen moet(en) zijn omschreven in de melding.
- *Gerechtvaardigd*: het doel moet gebaseerd zijn op één van de (gerechtvaardigde) verwerkingsgrondslagen uit de Wbp[16].

*Bij SCP-onderzoek is de (gerechtvaardigde) doelbinding wetenschappelijk onderzoek ten behoeve van het werkprogramma. Vervolgens zal ook specifiek (i.e., welbepaald en uitdrukkelijk omschreven) moeten worden aangegeven op welk deelterrein de data zullen worden gebruikt. Een te brede omschrijving voldoet niet aan de wet; een te gedetailleerde omschrijving zal de gebruiksmogelijkheden van verzamelde data ernstig beperken (en leiden tot zeer hoge kosten of zeer beperkt onderzoek).*
***Bij de melding van een gegevensverwerking aan de FG formuleren de methodologen, in overleg met de projectleider van het onderzoek, de omschrijving van de doeleinden van de verwerking.***

De Wbp behandelt ook het verder verwerken van reeds verzamelde gegevens, bijvoorbeeld het opslaan, het bewerken, het inzien of het verstrekken van de persoonsgegevens[17]. Eenmaal verzamelde persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Of sprake is van verenigbaarheid tussen de doeleinden van het verzamelen en het verdere verwerken, hangt af van een aantal omstandigheden:
- de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens;
- de gevolgen van de beoogde verwerking voor de betrokkene;
- de wijze waarop de gegevens zijn verkregen en
- de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

***De persoonsgegevens bij het SCP worden altijd en uitsluitend gebruikt voor onderzoeksdoeleinden van het SCP. De doeleinden van hergebruik zullen daarmee vrijwel altijd overeen komen met de doeleinden van gebruik. In dat geval is hergebruik dus toegestaan.***

### 5.4 Wanneer mag het SCP persoonsgegevens verwerken

Dit handboek heeft betrekking op het gebruik door het SCP van persoonsgegevens ten behoeve van wetenschap en statistiek. Dat is een gerechtvaardigde grondslag[18] voor gebruik.

[16] Zie artikel 8 van de Wbp.
[17] Zie artikel 9 van de Wbp.
[18] Artikel 8 van de Wbp omschrijft limitatief de gevallen waarin persoonsgegevens mogen worden verwerkt. Dit betekent dat op andere gronden dan in dit artikel opgesomd, persoonsgegevens niet mogen worden verwerkt. Belangrijk is dat elke handeling met persoonsgegevens op één of meer van

Het is hier wel van belang dat de betrokkene aanvaardt dat de hem of haar betreffende persoonsgegevens worden verwerkt, ofwel dat er sprake is van *informed consent*. Een van de verwerkingsgronden van de Wbp is *ondubbelzinnige* toestemming[19]. Dit houdt in dat elke twijfel moet zijn uitgesloten over de vraag òf de betrokkene zijn toestemming heeft gegeven en voor welke specifieke verwerking deze is gegeven. Er bestaan verschillende vormen van toestemming. Zo mag de toestemming stilzwijgend of impliciet worden gegeven. Deze vorm is vrij gangbaar bij SCP onderzoek. Zo worden bijvoorbeeld bij SCP-onderzoek potentiële deelnemers aan een survey op de hoogte gesteld van het doel van het onderzoek, wie de gegevens gebruikt, etc., d.m.v. een aanschrijfbrief. Een ander voorbeeld van *stilzwijgende* of *impliciete* toestemming bij SCP-onderzoek betreft interviews onder sleutelpersonen (bijv. ambtenaren). Hier wordt een beschrijving van het onderzoek vaak vooraf (per post of email) opgestuurd. Ook dit is een *informed consent* procedure (met een impliciete toestemming).

Een andere vorm van toestemming betreft *uitdrukkelijke* toestemming[20]. Een stilzwijgende of impliciete toestemming is onvoldoende wanneer de verantwoordelijke bijzondere persoonsgegevens in de zin van artikel 16 Wbp wil gaan verwerken. De betrokkene moet in woord, schrift of gedrag (bijvoorbeeld een muisklik) uitdrukking hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking. Bij SCP-onderzoek geldt deze vorm van uitdrukkelijke toestemming met name bij focusgroepen en interviews onder burgers. In deze gevallen vereist het SCP uitdrukkelijke toestemming. Dit betekent dat deelnemers vooraf schriftelijk toestemming geven, of dat de introductie en de toestemming van de geïnterviewde worden opgenomen.

Uitdrukkelijke toestemming is ook noodzakelijk in de zeldzame gevallen dat een betrokkene herkenbaar in een publicatie wordt opgevoerd (zoals in de paragraaf De elite over de elite, in het Sociaal en Cultureel Rapport 2014). Ook hier is van belang dat betrokkenen vooraf goed geïnformeerd worden hoe over hun reacties wordt gepubliceerd.

### 5.5 Privacytoets en Toetsmodel PIA Rijksdienst

Het recht op privacy is een grondrecht (zie bijvoorbeeld artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden, EVRM). Een burger van een lidstaat kan rechtstreeks, dus los van de Wbp, een beroep doen op artikel 8 EVRM als hij meent dat de overheid zich ongerechtvaardigd inmengt in zijn privésfeer. Dit heeft tot gevolg dat bij voorgenomen verwerkingen die inbreuk zullen maken op de privacy altijd moet worden gecontroleerd of bij het verwerken van persoonsgegevens de belangen van de minister zwaarder wegen dan de belangen van een burger.

---

de gronden in artikel 8 van de Wbp moet kunnen worden gebaseerd. Dus het verzamelen, maar ook het vervolgens sorteren, archiveren, verwijderen etc. moet op één van de gronden in artikel 8 van de Wbp kunnen worden gebaseerd.

[19] Zie art. 8 van de Wbp.

[20] Zie art. 23 van de Wbp.

De beginselen van evenredigheid en proportionaliteit die gebaseerd zijn op de grondrechten van artikel 8 EVRM nemen ook in de Wbp een centrale positie in. Op veel plaatsen in de Wbp[21] wordt de verwerking van gegevens bovendien gebonden aan het noodzakelijkheidscriterium.
Met name in de publieke sector (een 'sterke' overheid tegenover de 'zwakke' burger) moeten de belangen zorgvuldig worden afgewogen. Er moet daarom worden vastgesteld (voor alle onderdelen van de verwerking van persoonsgegevens) dat:

- De inbreuk op de belangen van de bij de verwerking betrokkene niet onevenredig is in verhouding tot het met de verwerking te dienen doel (de zogenaamde eis van *proportionaliteit*);
- het doel waarvoor de persoonsgegevens worden verwerkt niet in redelijkheid op een andere voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kan worden verwerkelijkt (de zogenaamde eis van *subsidiariteit*).

Door ministeries en andere organen vallend onder de Rijksdienst wordt sinds 1 september 2013 standaard een "privacy impact assessment" (PIA) toegepast bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bij de bouw van ICT-systemen of bij de aanleg van databestanden. Deze privacytoets dient om privacyrisico's op gestructureerde en heldere wijze in kaart te brengen.[22]

Het doel waarvoor persoonsgegevens worden verzameld en het doel waarvoor deze gegevens vervolgens verder worden verwerkt, en de toets aan de grondrechten en de begindelen van proportionaliteit en subsidiariteit staan centraal in de PIA. Het belang van een goede doelomschrijving (welke gegevens, over wie, voor welk doel) wordt hiermee nogmaals onderstreept.

*Een privacytoets bij SCP-onderzoek betekent dat men voor de start van een project moet nagaan welk doel een project dient, of er nieuwe gegevens verzameld moeten worden, welke vragen in een survey moeten worden gesteld, etc. Veelal worden deze overwegingen al vastgelegd in het projectvoorstel. Niet in alle gevallen zal de gehele vragenlijst van het PIA-toetsmodel Rijksdienst moeten worden doorlopen. Het Toetsmodel acht een "PIA-light" bijvoorbeeld toereikend wanneer "bij gebruik van een bestaand databestand (…) voor aanvullende of nieuwe doelen".*[23]

### 5.6 De kwaliteit van de persoonsgegevens

De eis van behoorlijke en zorgvuldige verwerking van persoonsgegevens gaat ook in op de kwaliteit van de persoonsgegevens. Zo moeten de persoonsgegevens juist en nauwkeurig zijn. De kwaliteit heeft echter ook betrekking op de verwerking van de persoonsgegevens, met name met betrekking tot de doelbinding (zie 5.3). Zo

[21] Zie bijvoorbeeld art. 8 van de Wbp
[22] Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst. www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html
[23] Toetsmodel PIA Rijksdienst, p. 3

mogen de persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij zijn verzameld of vervolgens worden verwerkt. Voorts moeten de persoonsgegevens gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
Bij wetenschappelijk onderzoek spelen ook eisen aan de repliceerbaarheid en controleerbaarheid van onderzoek een rol, vandaar de eis om ruwe data minimaal vijf jaar te bewaren (zie hoofdstuk 3). Het streven naar juistheid en nauwkeurigheid van gegevens sluit hiermee aan op de kwaliteitseisen aan surveyonderzoek.

### 5.7 Inzage- en correctieverzoeken

In de Wbp is het verstrekken van persoonsgegevens geregeld[24]. Hierbij kan men denken aan het verstrekken aan derden. Het SCP levert geen persoonsgegevens aan derden, behalve als via *informed consent* is geregeld dat dezen ook toegang hebben tot de data.

De Wbp geeft burgers ook de mogelijkheid hun gegevens in te zien en te laten corrigeren. Voor statistisch en wetenschappelijk onderzoek geldt echter in artikel 44 van de Wbp een uitzondering opgenomen. Deze uitzondering betekent dat individuen geen recht hebben op inzage in of wijzigingen van hun, door het SCP opgeslagen, persoonlijke gegevens die voor onderzoek gebruikt worden. In de praktijk is inzage ook niet mogelijk: in databestanden zijn individuele personen onherkenbaar door het ontbreken van naam en adres. In andere gevallen is inzage wel mogelijk, bijvoorbeeld in het geval van het transcript van een interview. De gedragscode Onderzoek en statistiek beveelt aan de wet niet te streng te interpreteren. Zo is het bijvoorbeeld wel mogelijk geïnterviewden het transcript van hun eigen interview in te laten zien. Bij goed onderzoek hoort ook dat verslagen van interviews of citaten die opgenomen worden in publicaties aan betrokkenen worden voorgelegd. Dit moet vooraf weer geregeld worden in een *informed consent* afspraak. Het laten zien van opnamen van focusgroepgesprekken is bijvoorbeeld niet mogelijk, omdat daar ook anderen in herkenbaar zijn.

Het kan ook voorkomen dat een geïnterviewde na afloop verzoekt de gegevens te verwijderen. Ook aan dit verzoek zou men gehoor moeten geven. Wel is het belangrijk dat men verifieert dat het verzoek daadwerkelijk van de betrokkene komt.

[24] Volgens Wbp hebben betrokkenen het recht om te weten welke gegevens de overheid verwerkt, met welk doel dit gebeurt en vanuit welke bronnen deze gegevens komen. In het algemeen kunnen betrokkenen dit zien in het meldingsregister.

## 6. De taken van de beheerder in de praktijk

Bij het SCP is de Directeur beheerder, en hoofd OMM contactpersoon. Beheerstaken worden in de praktijk vervuld door de methodologen. Namens de minister moet de beheerder diverse taken uitvoeren. Deze taken kunnen in twee groepen worden verdeeld. Ten eerste zijn er taken die bij iedere nieuwe verwerking van persoonsgegevens moeten worden uitgevoerd (zie hoofdstuk 7). Het gaat dan bijvoorbeeld om het invullen en opsturen van het meldingsformulier of het op de hoogte stellen van de betrokkene.

Nieuwe verwerkingen van persoonsgegevens worden gesignaleerd bij de intake van nieuwe projecten in het accountmanagement, uitgevoerd door de methodologen. Als er sprake is van nieuwe dataverzamelingen, of van hergebruik van bestaande, of de aanschaf van externe bestanden, zullen zij – in overleg met de projectleider – de melding aan de FG voorbereiden. Zij ondersteunen de projectleider ook bij het verkrijgen van *informed consent*, en bij het uitvoeren van de privacy-toets.

Methodologen leveren ook ondersteuning bij het afsluiten van een bewerkersovereenkomst, bij een veilige uitwisseling van gegevens, en bij een veilige opslag van gegevens.

Ten tweede zijn er doorlopende taken (zie hoofdstuk 8). Het zijn niet eenmalige of periodiek terugkerende acties maar het zijn doorlopende taken waaraan op ieder willekeurig moment moet kunnen worden voldaan. Hierbij kan gedacht worden aan een verzoek om inzage. Niet iedere dag wordt zo'n verzoek ingediend, maar iedere dag moet wel op zo'n verzoek kunnen worden gereageerd. Ook aan het beëindigen van een verwerking zijn taken voor de beheerder verbonden.

Om te kunnen voldoen aan de doorlopende taken zorgen de methodologen voor een jaarlijks overzicht van de gegevensverwerkingen en controleren zij de compleetheid.

Bovendien controleren de methodologen ook of gegevensverwerkingen verwijderd kunnen of moeten worden. In het geval van de wetenschappelijke gegevens bij het SCP zal dit vooral het geval kunnen zijn bij ruwe data (inclusief video-opnamen) en bij adressenbestanden van contactpersonen en deelnemers aan onderzoek. Bij het verwijderen van gegevensverwerkingen wordt hiervan melding gedaan bij de FG.

## 7. Nieuwe verwerkingen

Wanneer in de Wbp wordt gesproken over een nieuwe verwerking, betreft dat niet alleen een nieuwe dataverzameling in opdracht van het SCP, maar ook het aanschaffen van een alreeds verzameld (extern) bestand met het doel daarop verwerkingen uit te voeren. Onder nieuwe verwerkingen vallen dus een survey dat door een marktonderzoekbureau wordt uitgevoerd, een bestand dat van DANS of Eurostat wordt verkregen, interviews die door SCP-ers worden gehouden, focusgroepgesprekken die door het SCP worden georganiseerd of een administratief bestand dat ten behoeve van SCP-onderzoek is aangeschaft/verkregen. Opgelet, ook de koppeling tussen een nieuwe dataverzameling met bestaande gegevens moet worden opgevat als een nieuwe verwerking.

De te nemen acties bij een nieuwe dataverzameling, bestaande gegevens en een koppeling van nieuwe en bestaande gegevens wijken iets van elkaar af. Van alle vormen staat hieronder een overzicht van de te nemen acties. Overigens ondersteunen de methodologen SCP-onderzoekers bij het volgen van de Wpb-regels vanaf de intake bij het accountmanagement.

### 7.1 Acties bij nieuwe verwerkingen

*Bij een nieuwe verwerking geïnitieerd door het SCP (de gegevens zijn verkregen in een survey, interview, focusgroep e.d. van de betrokkene zelf):*

- Schakel de methodologen in en volg onderstaande stappen.
- Ga na of de verwerking onder de Wbp valt. Zie het toetsingsschema in bijlage 1.
- Zo ja:
  - Bepaal de risicoklasse (zie 7.2)
  - Vul met behulp van een methodoloog het meldingsformulier FG in,
  - Als er sprake is van een externe bewerker (marktonderzoeksbureau, externe interviewers, bureau dat transcripten maakt), sluit dan een bewerkersovereenkomst[25],
  - Zorg dat de deelnemer van het onderzoek op de hoogte is van het doel en het gebruik van de gegevens, d.w.z. zorg voor *informed consent* (zie bijlage 2 en 3),
  - Zorg bij transcriptie dat namen van personen niet in het transcript zijn opgenomen (pseudonymisatie).
  - Neem gepaste beveiligingsmaatregelen (zie 9)

*Bij aanschaf van een bestaande verwerking (de gegevens worden verkregen van een andere organisatie (DANS, Eurostat, een departement, het CBS)):*

- Schakel de methodologen in en volg onderstaande stappen.
- Ga na of de verwerking onder de Wbp valt. Zie het toetsingsschema in bijlage 1.
- Zo ja:
  - Bepaal de risicoklasse (zie 7.2)

[25] https://www.pianoo.nl/document/9596/model-bewerkersovereenkomst-arvodi

- Vul met behulp van een methodoloog het meldingsformulier FG in,
- Ga na of de deelnemer van het onderzoek op de hoogte is gesteld van het doel en het gebruik van de gegevens, d.w.z. is er sprake van *informed consent.*
- Als de betrokkene niet voldoende op de hoogte gesteld is, is dat bij bestanden voor onderzoek en statistiek meestal niet achteraf mogelijk (al is het maar omdat naam en adres ontbreken). Het kost nu onevenredige inspanning de betrokkene alsnog op de hoogte te stellen. Leg de herkomst van de gegevens vast op het meldingsformulier.
- Neem gepaste beveiligingsmaatregelen (zie 9).

*Bij koppeling van nieuwe gegevens en bestaande gegevens:*

- Ga na of de verwerking onder de Wbp valt. Zie het toetsingsschema in bijlage 1.
- Zo ja:
  - Bepaal de risicoklasse (zie 7.2)
  - Ga na of de deelnemer van het onderzoek op de hoogte is gesteld van mogelijke koppeling.
  - Als de betrokkene niet voldoende op de hoogte gesteld is, is dat bij bestanden voor onderzoek en statistiek meestal niet achteraf mogelijk (al is het maar omdat naam en adres ontbreken). Ga na of koppeling in overeenstemming is met het doel van het onderzoek, en leg de herkomst van de gegevens vast op het meldingsformulier. Wees terughoudend en raadpleeg de contactpersoon Bescherming persoonsgegevens onderzoeksdata.
  - Neem gepaste beveiligingsmaatregelen (zie 9).

*Bewerkers*

Wanneer de beheerder persoonsgegevens laat verwerken door een bewerker, moet de beheerder er zorg voor dragen dat deze bewerker voldoende technische en organisatorische beveiligingsmaatregelen biedt[26].

Bewerkersovereenkomsten kunnen betrekking hebben op het verzamelen van surveydata, het organiseren van focusgroepgesprekken, het houden van interviews, het transcriberen van focusgroepgesprekken en interviews, en andersoortige bewerkingen.
De beheerder ziet toe op de naleving van deze bewerkersovereenkomsten.

### 7.2 Risicoklassen

Welke mate van beveiliging van persoonsgegevens noodzakelijk is, wordt vooral bepaald door de aanwezige risico's op onzorgvuldig of onbevoegd gebruik van persoonsgegevens. De omvang van deze risico's kan worden ingeschat aan de hand van de kans dat dergelijk onbevoegd gebruik zich voordoet en van de schade die dat zou opleveren. In de Wbp wordt een beschermingsniveau dat rekening houdt met deze risico's, de aard van de te beschermen gegevens, de stand van de techniek en

[26] https://www.pianoo.nl/document/9596/model-bewerkersovereenkomst-arvodi

de kosten van tenuitvoerlegging een ‘passend’ beveiligingsniveau genoemd. De beheerder heeft de plicht om technische en organisatorische maatregelen te nemen die een dergelijk niveau waarborgen (Wbp art. 13). Deze maatregelen moeten er mede op gericht zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Het Cbp heeft in 2001 in haar Achtergrondstudies en Verkenningen nummer 23 een handvat aangereikt waarmee de verantwoordelijke de persoonsgegevens op effectieve wijze kan beveiligen. Het biedt een hulpmiddel bij de invulling van het begrip ‘passende technische en organisatorische maatregelen’. De technische aspecten zijn mogelijk verouderd. Wel is van belang dat in dit rapport verwerkingen met behulp van een risicoanalyse in een bepaalde risicoklasse worden ingedeeld. Het rapport benoemt de volgende risicoklassen:

Risicoklasse 0
Het gaat hier om openbare persoonsgegevens. De in deze klasse opgenomen persoonsgegevens vormen bij normaal gebruik geen risico voor de betrokken. Hieronder vallen bijvoorbeeld telefoonboeken, brochures, publieke internet sites etc.

Risicoklasse I
De risico’s voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Het gaat dan meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld arbeidsrelaties, klantrelaties en lidmaatschappen. De beheerder draagt zorg voor de naleving van het beveiligingsbeleid dat voor de directie of het organisatieonderdeel is vastgesteld. Iedere medewerker moet het geldende en vastgestelde beveiligingsbeleid naleven.

Risicoklasse II
De verwerkingen die in deze risicoklasse vallen zijn dusdanig van belang dat bij verlies of onrechtmatig/onzorgvuldig gebruik er extra negatieve gevolgen ontstaan voor de betrokkene. De te nemen (informatie)beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basisniveau van risicoklasse I. In deze risicoklasse passen onder andere de verwerkingen van bijzondere persoonsgegevens (zie bijlage 1 punt c).

Risicoklasse III
Het risico voor de betrokkene is dusdanig hoog dat het gerechtvaardigd is de hoogste eisen te stellen aan de maatregelen die genomen moeten worden om deze persoonsgegevens te beveiligen. Verwerkingen in deze klasse hebben o.a. betrekking op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad als dit onzorgvuldig of onbevoegd gebeurt.

De risicoklassen en bijbehorende beveiligingsstappen bij het SCP staan beschreven in tabel 1.[27]

Tabel 1. Risicoklassen en beveiligingsstappen SCP-onderzoeksbestanden

| Risico-klasse | Omschrijving | Actie |
|---|---|---|
| 0 | • Bestanden ontvangen van nationaal of internationaal data-archief (ESS, ISSP)<br>• Bestanden met als laagst regionaal niveau gemeente, geen bijzondere persoonsgegevens: | Geen actie |
| 1 | • Bestanden met gegevens op lager regionaal niveau dan gemeente (4-cijferige postcode), geen herkenbare informatie (Culturele Veranderingen) | • Melden bij FG<br>• Toegankelijk voor SCP-medewerkers |
| 2 | • Bestanden met groter identificatierisico of kwetsbare groep (Minderhedenonderzoeken)<br>• Panels met identificerende informatie (OSA-panel)<br>• Kwalitatieve data (transcripten, audio, video) | • Melden bij FG<br>• Bestand beschikbaar voor project-medewerkers<br>• Bestanden in beveiligde map<br>• NAW-info loskoppelen (alleen toegankelijk beheerder), vernietigen als niet meer noodzakelijk<br>• Bij kwalitatieve gegevens ATLAS-TI bestanden consolideren; bij hergebruik terugzetten naar de oorspronkelijke plek.<br>• Ruwe data zonodig vernietigen na 5 jaar (melden bij FG) |
| 3 | Nvt | Nvt |

Surveys onder de algemene bevolking lijken bij het SCP onder risicoklasse II te vallen, door het voorkomen van bijzondere persoonsgegevens. Echter, wanneer namen en adressen ontbreken, en in die gevallen slechts sprake is van 4-cijferige postcode worden, worden deze bestanden wegens beperkte identificerende mogelijkheden onder risicoklasse I geschaard. Interviews en focusgroepgesprekken over algemene onderwerpen worden ook tot categorie I gerekend. De surveys onder bijzondere groepen (etnische minderheden), interviews waarin bijzondere persoonsgegevens centraal staan (zie bijlage 1 punt c), worden dan weer wel tot risicoklasse II gerekend.

[27] Ook bij databestanden die geen persoonsgegevens bevatten kunnen extra beveiligingsmaatregelen noodzakelijk zijn. Een voorbeeld zijn anonieme Eurostat-bestanden die slechts door een beperkt aantal SCP-ers mogen worden gebruikt.

## 8. Doorlopende taken

*Wat moeten SCP-onderzoekers weten*
SCP-onderzoekers moeten zich ervan bewust zijn dat zorgvuldig met persoonsgegevens omgegaan moet worden. De methodologen kunnen helpen de juiste stappen te nemen.

Hoewel het (vooralsnog) niet de bedoeling is dat iedere verwerker (SCP-onderzoeker) de regels uit de Wbp volledig kent, is het wel noodzakelijk dat de SCP-medewerkers zich in ieder geval van de navolgende punten bij het uitvoeren van zijn of haar werkzaamheden bewust is:

- Dat deel van het beveiligingsbeleid uitvoeren, waarvoor hij of zij zorg kan dragen, bijvoorbeeld een password niet 'uitlenen', 'eigen' dossiers opbergen, geen vertrouwelijke gegevens op het bureau laten liggen etc. (zie 9).
- Gegevens alleen uitwisselen via beveiligde media (zie 9).
- Ruwe data zo snel mogelijk verwijderen na opslag op een veilige plaats van de oorspronkelijke informatiedrager (USB-stick, laptop (bij interview)).
- Het raadplegen van de contactpersoon in geval van twijfel of een bepaalde verwerking is toegestaan of niet.
- Raadplegen van de contactpersoon in geval van een verzoek om persoonsgegevens te verstrekken (zie hieronder).

*Wat moet de contactpersoon doen*

- Volgen van veranderingen in wetgeving op het terrein van Bescherming Persoonsgegevens en naar mogelijke gevolgen voor het SCP.
- Jaarlijks inventariseren (via sectorhoofden) of er onderzoeksdata zijn die nog niet gemeld zijn en wel gemeld hadden moeten worden.
- Jaarlijks controleren welke dataverwerkingen gemeld zijn, en of hier aanpassingen nodig zijn (hernieuwd gebruik, verwijderen).
- De bestanden die via Remote Access bij het CBS worden gebruikt in een apart overzicht melden aan de Functionaris Gegevensverwerking.
- Afhandelen inzage- en correctieverzoeken (zie 4).
- Overleggen met medewerkers verantwoordelijk voor beveiliging over de juiste beveiligingsniveaus.

*Wat moeten de methodologen doen*

- Bij de intake als accountmanager nagaan welke data verzameld, aangekocht en/of hergebruikt gaan worden (zie 7).
- Na afloop van projecten: ga na of er gegevensverwerkingen verwijderd moeten worden, of onderdelen verwijderd kunnen worden (ruwe data, zoals databestanden; namen en adressen voor mogelijke herbenadering). Bij verwijdering: pas meldingsformulier aan.

## 9. Beveiligingsbeleid SCP

Het beschermen van persoonsgegevens en het beveiligen van informatie hangen nauw met elkaar samen. Niet alleen in de praktijk blijken deze onderwerpen onlosmakelijk met elkaar verbonden te zijn, ook in de samenhang tussen de diverse regelgeving komt dit tot uitdrukking.

Persoonsgegevens moeten op grond van de Wbp worden beveiligd. Hierbij moet worden voldaan aan een 'passend beveiligingsniveau' (Wbp art. 12, 13, 14). Daarnaast kent de overheid de Baseline Informatiebeveiliging Rijksdienst (BIR)[28]. De Wbp staat als formele wet echter hoger in de rangorde dan de BIR. Bij de uitvoering van de BIR vormen daardoor alle regels uit de Wbp (dus niet alleen die informatiebeveiliging betreffen) een externe randvoorwaarde.

Het beveiligingsbeleid van het SCP bestaat uit de volgende onderdelen:
- Fysieke beveiliging toegang ministerie, inclusief organisatorische controle
- Firewalls en virus
- Logische toegangscontrole m.b.v. wachtwoord
- Plaatsen bestanden risicoklasse twee op afgeschermde schijf (alleen toegang voor geautoriseerde onderzoekers)
- Gegevensuitwisseling via surfdrive
- Verwijdering ruwe data van oorspronkelijke informatiedragers.

*Schriftelijke vastlegging beveiligingsbeleid*
Bij de melding van een verwerking van persoonsgegevens wordt een algemene beschrijving gegeven van het beveiligingsbeleid. Daarnaast zijn alle beveiligingsmaatregelen van het SCP schriftelijk vastgelegd.

*Controle beveiliging*
De beheerder moet periodiek de kwaliteit van de verwerkingen van persoonsgegevens beoordelen. De frequentie van deze beoordelingen hangt af van de aard van de persoonsgegevens (bijzondere persoonsgegevens ingevolge de Wbp of maatschappelijk gevoelig), de hoeveelheid gegevens die zijn opgenomen en het gebruik dat van die gegevens wordt gemaakt (o.a. frequentie raadplegen, gebruikte techniek). Bij de jaarlijkse controle op de uitvoering en naleving van de Wbp wordt dit aspect meegenomen.

*Controle beveiliging bij bewerkers*
De controle op de beveiliging strekt zich ook uit tot de bewerkers die in opdracht van het SCP persoonsgegevens verwerken. Het SCP is verantwoordelijk voor de controle en handhaving van het beveiligingsniveau dat in de bewerkersovereenkomst is afgesproken. [29]

28
http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/vws_2/kernprocessen_13/een_veilig_vws/bestanden_1735/informatiebeveiliging/BIR_TNK_10_definitief.pdf
29 Artikel 14 Wbp

**Bijlage 1: Overzicht en toetsschema's**

Het volledig overzicht en de toetsschema's staan in het concept-Handboek Wet bescherming persoonsgegevens (Wbp) van VWS uit 2010.
http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/kernprocessen_1/rjp/juridisch_forum_vws/rechtsgebieden_3/bestanden_5184/microsoft-word---100410-handboek-wbp---vws---deel-b-0-7_tcm17-195181pdf.pdf
Hieronder staat een vereenvoudigd schema, van toepassing op onderzoeksdata bij het SCP.

*A. Worden onderzoeksgegevens verwerkt?*

*Persoonsgegevens worden verwerkt als een bestand gegevens bevat over één of meer levende personen, de identiteit van personen kan worden vastgesteld en de gegevens worden verzameld, ingezien of geanalyseerd.*

Om te bepalen of er sprake is van een verwerking van persoonsgegevens moet eerst worden bekeken of een gegeven een persoonsgegeven is. Om te spreken van een persoonsgegeven moet een gegeven informatie bevatten over één of meerdere levende
natuurlijke personen (zie eerste vraag hieronder) en moet de persoon identificeerbaar
zijn (zie tweede vraag). Als er geen sprake is van persoonsgegevens valt een bestand niet onder de Wbp.

*A1. Bevat een gegeven informatie over één of meerdere levende natuurlijke personen?*

Om te bepalen of een gegeven een persoonsgegeven is, moet worden vastgesteld of het gegeven informatie bevat over een natuurlijke persoon. Gegevens worden als persoonsgegevens aangemerkt als de gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt behandeld of beoordeeld. De context waarin een gegeven wordt gebruikt, speelt een rol.
Voorbeelden van persoonsgegevens zijn:

- naam, adres, woonplaat (zogenaamde NAW-gegevens)
- geboortedatum, leeftijd
- nationaliteit of ras
- telefoonnummer, kenteken van auto, bankrekeningnummer, burgerservicenummer, personeelsnummer
- gegevens over godsdienst of levensovertuiging, lidmaatschap politieke partij,
- gegevens over beroep, inkomen, vermogen
- gegevens over ziekte
- gegevens over (strafrechtelijk) gedrag
- gegevens in subsidies of ontheffingen
- gegevens in het personeelsdossier van een bepaalde persoon, bijvoorbeeld
- verslag van functioneringsgesprek.

*A2. Kan de identiteit van een persoon worden vastgesteld?*
Een gegeven is een persoonsgegeven indien de persoon is geïdentificeerd of indien een persoon kan worden geïdentificeerd. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijze, zonder onevenredige inspanning, kan worden vastgesteld. Twee factoren spelen een rol: de aard van de gegevens en de mogelijkheden van de verantwoordelijke om de identificatie tot stand te brengen. De vaststelling of een persoonsgegeven herleidbaar is, is niet eenvoudig. Onder omstandigheden kunnen bijvoorbeeld ook gegevens over kleine bedrijven of eenmanszaken als persoonsgegevens worden aangemerkt. In Deel A wordt hierop nader ingegaan.

*A3. Worden deze persoonsgegevens verwerkt?*
Per definitie worden alle onderzoeksbestanden bij het SCP verwerkt.

*B. Is de Wbp van toepassing?*
*Als aan voorwaarde A voldaan is, vallen SCP onderzoeksbestanden onder de Wbp. Ze worden geautomatiseerd verwerkt en ze vallen niet onder uitzonderingsregels*

*C. Worden bijzondere persoonsgegevens verwerkt?*
*Bevat de verwerking persoonsgegevens over: godsdienst of levensovertuiging, ras, politieke gezindheid, lidmaatschap vakvereniging, gezondheid, seksuele leven, overtredingen, strafrechtelijke veroordelingen of veiligheidsmaatregelen, wettelijk voorgeschreven persoonsnummer*

De Wbp bevat een aantal zeer specifieke regels ten aanzien van de verwerking van 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn onder andere gegevens over ras, gezondheid en strafrechtelijke gegevens. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij daarvoor een ontheffingsgrond in de wet staat.

*Belang context bij verwerken van bijzondere persoonsgegevens*
Welke gegevens precies onder de verschillende categorieën van bijzondere persoonsgegevens vallen, staat niet in de Wbp. Bij persoonsgegeven betreffende iemands ras kan bijvoorbeeld gedacht worden aan iemands huidskleur. Maar ook bijvoorbeeld de geboorteplaats of het geboorteland van een persoon kunnen als bijzonder gegeven worden beschouwd. Het verband waarin en het doel waarvoor gegevens worden gebruikt kunnen dus bepalend zijn of er sprake is van een bijzonder persoonsgegeven. Het gaat erom of uit de gegevens rechtstreeks een gevoelig kenmerk kan worden afgeleid. Wordt in een bepaalde lijst bijvoorbeeld het geboorteland of de etnische afkomst opgenomen om een voorkeursbeleid ten aanzien van minderheden te voeren, dan zijn deze gegevens ook als bijzondere persoonsgegevens te beschouwen.
Een ander voorbeeld is een ledenlijst, die op zich geen gevoelig karakter hoeft te hebben. Als de ledenlijst echter door een kerkgenootschap wordt aangelegd, is daaruit af te leiden welke godsdienst wordt aangehangen door de leden op de lijst. Daardoor verkrijgen de namen en adressen een gevoelig karakter en gaat het om de verwerking van bijzondere persoonsgegevens.

Hieronder volgt een korte toelichting per categorie van bijzondere persoonsgegevens.

*Gegevens betreffende iemands godsdienst of levensovertuiging*
Het gaat hierbij om het verwerken van persoonsgegevens over iemands godsdienst of levensovertuiging, dus of iemand katholiek of hindoestaan is, etc.

*Gegevens betreffende iemands ras*
Het begrip ras wordt ruim geïnterpreteerd. Het kan gaan om iemands huidskleur, afkomst en nationale of etnische herkomst. Ras is al snel herkenbaar bij video-opnamen.

*Gegevens betreffende iemands politieke gezindheid*
Hierbij gaat het om de verwerking van persoonsgegevens waaruit de politieke voorkeuren of 'kleur' blijkt.

*Gegevens betreffende iemands lidmaatschap van een vakbond*
Het gaat hierbij zowel om de vaststelling dat, als om de mate waarin iemand actief is in een vakbond.

*Gegevens betreffende iemands gezondheid*
Het begrip gezondheid moet ruim worden opgevat. Het gaat om gegevens over iemands gesteldheid (ziek of niet) en alle gegevens die de lichamelijke of geestelijke gezondheid van een persoon betreffen. Ook erfelijkheidsgegevens en in sommige gevallen gegevens betreffende iemands seksuele leven worden tot gegevens betreffende iemands gezondheid gerekend. Psychologische gegevens zullen vaak de lichamelijke of geestelijke gezondheid raken, maar dit hoeft niet per definitie zo te zijn.

*Gegevens betreffende iemands seksuele leven*
Gedacht kan worden aan gegevens betreffende iemands seksuele geaardheid.

*Gegevens betreffende overtredingen, strafrechtelijke veroordelingen en veiligheidsmaatregelen*
In de Wbp wordt letterlijk gesproken over de verwerking van: 'strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag'. Strafrechtelijke gegevens hebben zowel betrekking op veroordelingen voor overtredingen en misdrijven als op min of meer gegronde verdenkingen.
Het kan bij deze bijzondere gegevens over hinderlijk gedrag tevens gaan om gegevens betreffende iemands seksuele leven, bijvoorbeeld in het geval er afspraken worden gemaakt met een persoon omtrent zijn gedrag ter bestrijding van seksuele intimidatie op de werkvloer.

*Wettelijke voorgeschreven persoonsnummers*

Het gaat om een nummer dat ter identificatie van een persoon bij wet is voorgeschreven. Een voorbeeld is het burgerservicenummer (BSN) (Wet algemene bepalingen burgerservicenummer), het sociaal-fiscaalnummer (Algemene wet inzake Rijksbelastingen) of het administratienummer (Wet gemeentelijke basisadministratie persoonsgegevens). Het moet gaan om een nationaal identificatienummer of een ander identificatiemiddel van algemene aard.

*D. Is het toegestaan bijzondere persoonsgegevens te verwerken?*
*Voor wetenschappelijk onderzoek is het toegestaan bijzondere persoonsgegevens te verwerken. Dit moet wel worden vermeld in het meldingsformulier. Deze gegevens vereisen ook een zorgvuldige omgang (zie hoofdstuk 7).*

*E. Is dit een (deels) geautomatiseerde verwerking?*
*Ja, geldt voor alle onderzoeksdata SCP*

*F. Voldoet de verwerking aan de voorwaarden uit het vrijstellingsbesluit?*
Nee, niet van toepassing voor onderzoeksbestanden SCP

*G. Is dit een verwerking met een bijzonder risico?*
*In principe niet van toepassing voor onderzoeksdata van het SCP.*

Bij het koppelen van bestanden (zeker met behulp van een persoonsnummer) kan een verwerking ontstaan die een bijzonder risico inhoudt voor de persoonlijke rechten en vrijheden van de betrokkene. In zo'n geval is een voorafgaand onderzoek door het CBP noodzakelijk (artikel 31 Wbp).

**Bijlage 2: Informed consent Voorbeeld aanschrijfbrief survey-onderzoek**

> Retouradres I&O Research, Postbus 563, 7500 AN Enschede
<Adresnaam, Verdana 9>
<Adres>
<Postcode> <Plaats>

Datum 8 maart 2014
Onderwerp Onderzoek 'Verschil in Nederland'
<<Briefhoofd, verdana 9>>,

Nederland verandert voortdurend, en daardoor kan het verschil tussen bevolkingsgroepen groter of kleiner worden. Om hier een beter beeld van te krijgen doet het Sociaal en Cultureel Planbureau (SCP) regelmatig onderzoek. Dit keer stellen we de vraag hoe de Nederlandse maatschappij er in 2014 uit ziet. Waarin verschillen bijvoorbeeld jongeren en ouderen, gezonde en ongezonde mensen, en mensen met een hoge en een lage opleiding? Dat zijn de belangrijkste thema's in dit nieuwe onderzoek.

Natuurlijk kunnen we niet alle inwoners van Nederland ondervragen. Daarom trekt het Centraal Bureau voor de Statistiek (CBS) een willekeurige steekproef uit het bevolkingsregister. De volgende naam is daarbij te voorschijn gekomen: **<< Naam >>.**

Graag nodig ik u daarom uit om mee te doen aan dit onderzoek. Door de gegevens die we verzamelen kan het beleid beter aansluiten op de wensen van de Nederlandse bevolking. Het SCP rapporteert de uitkomsten van het onderzoek aan de Tweede Kamer en aan de Ministerraad. Uw deelname is heel belangrijk: u vertegenwoordigt zo veel andere inwoners van Nederland.

Ik stel het zeer op prijs als u de vragenlijst op het internet in wilt vullen. Dat kunt u doen vanaf elke plaats waar u toegang heeft tot internet. Het gaat als volgt: tik het adres **www.startvragenlijst.nl/verschil** in de adresbalk boven in uw scherm (intikken in Google of een andere zoekmachine werkt niet). Vul daarna het volgende unieke wachtwoord in: **<wachtwoord>.**

Bij al onze onderzoeken is uw privacy volledig gewaarborgd. De gegevens worden vertrouwelijk behandeld en alleen voor onderzoeksdoeleinden gebruikt. Op de achterzijde van deze brief leest u daar meer over.

Hoe meer mensen meedoen, hoe beter we straks een beeld krijgen van verschillen in de Nederlandse samenleving! Als dank verloten wij daarom onder de deelnemers drie HEMA-cadeaubonnen ter waarde van €100 en een iPad mini.

Wilt u meer informatie over het onderzoek of heeft u vragen? Neem dan contact op met I&O Research, dat de enquête uitvoert voor het SCP. U kunt daarvoor bellen naar het gratis telefoonnummer 0800-4050602. Dit nummer is van maandag tot en met vrijdag bereikbaar, tussen 09.00 en 17.00 uur. Ook kunt u een e-mail met uw vragen of opmerkingen sturen naar: helpdesk@ioresearch.nl

U doet ons een groot plezier als u één van de komende dagen de vragenlijst invult.

Ik dank u alvast hartelijk voor uw medewerking.

Met vriendelijke groet,

Prof. Dr. Kim Putters,
Directeur Sociaal en Cultureel Planbureau

*NB. Op de achterzijde van de brief staat het volgende*

*In dit onderzoek werkt het SCP samen met het Centraal Bureau voor de Statistiek (CBS). Het CBS levert de adresgegevens voor het onderzoek. Het CBS krijgt veel bestanden van andere instellingen. In dit onderzoek zullen de antwoorden die u geeft, automatisch worden gecombineerd met gegevens over de huishoudenssamenstelling, de woonsituatie en de inkomenssituatie die het CBS al heeft. Door het combineren van deze informatie krijgt u minder vragen voorgelegd en kunnen statistieken zo efficiënt mogelijk worden samengesteld.*

**Bijlage 3. Informed consent (in kwalitatief onderzoek)**

*Informed consent*, ofwel geïnformeerde toestemming, wijst op de procedure dat respondenten voorafgaand aan hun medewerking aan onderzoek worden geïnformeerd over het onderzoek en de wijze waarop met gegevens wordt omgegaan. Bij survey-onderzoek betekent dat dat de respondent duidelijk wordt gemaakt dat deelname vrijwillig is, dat duidelijk is waarvoor het onderzoek uitgevoerd wordt, en door wie en waarvoor de data worden gebruikt. Dat gebeurt in het algemeen in de aanschrijfbrief. *Informed consent* is dan passief.

Bij kwalitatief onderzoek kan *informed consent* passief worden gegeven door een informatieformulier te verstrekken of voor te lezen (vergelijkbaar met survey onderzoek) of actief door ondertekening van het formulier of mondelinge toestemming opgenomen via een recorder. Ook kan bij benadering van respondenten via e-mail de informatie in de betreffende e-mail worden verstrekt. Afhankelijk van het type onderzoek en respondent kan men kiezen voor passief of actief *informed consent*.

In kwalitatief onderzoek door het SCP is niet duidelijk in hoeverre er altijd sprake is van *informed consent*. Bij interviews met professionals lijkt dit nog minder gangbaar. Ook bij hen verdient het principe van *informed consent* aandacht, omdat professionals soms meer risico lopen op herleidbaarheid.
Wanneer voorafgaande informering de uitvoering van het onderzoek onmogelijk maakt, dan kan informatieverstrekking achteraf plaatsvinden (zie toelichting bij de Gedragscode[30]).

*Voorstel*:
In kwalitatief onderzoek standaard het principe van *informed consent* hanteren, bij alle type respondenten waaronder individuele ervaringsdeskundigen, deelnemers aan focusgroepen en professionals. Er wordt minimaal een informatieformulier verstrekt (passief) of informatie wordt per e-mail vooraf verstrekt. Waar mogelijk en wenselijk wordt het informatieformulier ondertekend of wordt mondeling ingestemd (actief).

Bij de voorbereiding van een onderzoek (de intake of later) wordt bepaald en voor welke vorm van informed consent wordt gekozen. Hier wordt ook vermeld wanneer er van deze standaard wordt
afgewezen, bijv. bij experimenten.

De sectie Methodologie ontwikkelt in overleg met kwalitatieve onderzoekers een *informed consent formulier/tekst* dat kan worden aangepast aan de omstandigheden (eventueel in overleg met onderzoeksbureaus).
De volgende informatie dient in ieder geval in het informatieformulier/tekst te worden opgenomen:

[30] www.cbpweb.nl/downloads_gedragscodes/gedragscode-onderzoek-statistiek.pdf

- doel van de onderzoek, de onderzoeksorganisatie, opdrachtgever, wijze van rapportage, gebruik van video- of audio-apparatuur, en waar meer informatie over het onderzoek beschikbaar is (Gedragscode, artikel 5.4, 5.5 en 5.6).
- na welke termijn identificerende persoonsgegevens worden vernietigd (in principe na 5 jaar).
- reikwijdte voor gebruik van de data (voor doelen buiten de reikwijdte mogen de gegevens niet gebruikt worden).
- In hoeverre sprake is van anonimisering, mogelijke herleidbaarheid, vertrouwelijkheid van gegevens, veilige opslag van gegevens. Vertrouwelijkheid kan altijd worden gegarandeerd, maar dat geldt niet altijd voor anonimisering en herleidbaarheid.