

Open data and beyond

Exploring existing open data projects to prepare a successful open data strategy

Deelrapport privacy

Deelrapport privacy

Dit onderzoek is uitgevoerd in opdracht van: NGI/ Alliander

Auteurs: *Mr. Stefan Kulk & Dr.ir. Bastiaan van Loenen*

Betrokken in de, cq. lid van de Next Generations
programmaraad:
Drs. Pallas Agterberg
Dr.ir. Harry van Breen MBE
Dr. Judith Schueler
Prof.dr.ir. Margot Weijnen (vz.)

Betrokken bij het tot stand komen van de in-
houd van dit rapport:
Ing. Jan Bruinenberg
Drs. Leen van Doorn
Ir. Paul Juffermans
Ing. Tanju Özel
Dr. Ir. Marisca Zweistra
Mr. Jessica van Kraaij
Mr. Loek Mijtjens

Januari 2012

Onderzoeksinstituut OTB
Technische Universiteit Delft
Jaffalaan 9, 2628 BX Delft
Tel. (015) 278 30 05
Fax (015) 278 44 22
E-mail mailbox@otb.tudelft.nl
<http://www.otb.tudelft.nl>



Dit werk is gelicenseerd onder een Creative Commons Naamsvermelding-NietCommercieel 3.0 Nederland. Bezoek <http://creativecommons.org/licenses/by-nc/3.0/nl/> om een kopie te zien van de licentie of stuur een brief naar Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Inhoudsopgave

Inhoudsopgave.....	1
1 Open data en privacy.....	2
1.1 Open data.....	2
1.2 Privacy.....	3
2 Privacyregelgeving toegepast op open data	4
2.1 College Bescherming Persoonsgegevens en Artikel 29 Werkgroep	4
2.2 Persoonsgegevens.....	5
2.2.1 Direct en indirect identificerende gegevens	5
2.2.2 Contextafhankelijkheid.....	5
2.2.3 Anonieme en geaggregeerde gegevens	6
2.3 Verwerken van persoonsgegevens.....	7
2.3.1 Verwerken	7
2.3.2 Uitzonderingen	8
2.4 Voorwaarden voor het verwerken van persoonsgegevens	9
2.4.1 Verwerkingsgrond	9
2.4.2 Welbepaalde uitdrukkelijke doeleinden en doelbinding	12
2.4.3 Niet onverenigbaar gebruik	12
2.4.4 Minimaal en toereikend verwerken	13
2.4.5 Nauwkeurige gegevens.....	14
2.4.6 Beveiliging	14
2.4.7 Informeren van betrokkene.....	14
2.4.8 Melding aan CBP	15
2.4.9 Voorafgaand onderzoek door CBP.....	16
2.5 Rechten van de betrokkene.....	17
2.5.1 Recht op inzage en informatie.....	17
2.5.2 Recht op verbetering, aanvulling, verwijdering en afscherming	17
2.5.3 Recht van verzet	18
2.6 Bijzondere persoonsgegevens	18
2.6.1 Verbod op verwerken bijzondere persoonsgegevens.....	18
2.6.2 Uitzonderingen	19
2.7 Grensoverschrijdend gegevensverkeer	20
3 Conclusie	21
3.1 Persoonsgegevens.....	21
3.2 Open data-aanbieders mogen geen persoonsgegevens aanbieden.....	21
3.3 Wel geaggregeerde of geanonimiseerde persoonsgegevens	21
4 Rechtspraak.....	23
4.1 Nederland	23
4.2 Documenten CBP	23
4.3 Documenten Artikel 29 Werkgroep	23
4.4 Literatuur.....	23
4.5 Kamerstukken	25
5 Bijlage Stroomschema Persoonsgegevens.....	26

1 Open data en privacy

Bij de selectie van datasets waarvan Alliander overweegt om ze als open data aan te bieden werd privacy vaak genoemd als aandachtspunt. Dat is terecht want aandacht voor privacy is noodzakelijk bij het aanbieden van open data. Privacy is een van de mogelijke argumenten om voor bepaalde gegevens geen open data beleid toe te passen¹.

Dit rapport is een uitwerking van privacybescherming zoals die wordt ingevuld door de Wet bescherming persoonsgegevens en zal uiteenzetten wat deze regelgeving betekent voor open data-aanbieders.

1.1 Open data

In het vervolg van dit rapport zullen we onder open data verstaan:

Juridische eisen aan open data

- Data moeten licentievrij zijn: een ieder moet de data zonder enige voorwaarde kunnen gebruiken voor willekeurige doeleinden.²

Financiële eisen aan open data

- Data is beschikbaar tegen maximaal de marginale verstrekingskosten, bij voorkeur gratis.

Technische eisen aan open data

- Data moeten brondata zijn; de ruwe data die bijvoorbeeld noodzakelijk zijn voor de uitvoering van een wettelijke taak.
- Data formaten moeten open zijn;
- Data moeten kunnen worden verwerkt door een machine;
- Data moet worden voorzien van afdoende metadata (mede omwille van de vindbaarheid).

Organisatorische eisen aan open data

- Data moeten toegankelijk zijn: data moet worden gepubliceerd, bij voorkeur in een algemeen toegankelijk forum, bijvoorbeeld een centraal portaal als data.overheid.nl.
- Data moeten regelmatig worden gecontroleerd of ze aan de open overheidsdata principes voldoen
- Een open data helpdesk moet worden ingericht om gebruikers optimaal van dienst te kunnen zijn.

Een aanvullende eis voor Alliander is de lange-termijn-beschikbaarheid van open data (financiering dus geborgd).

¹ Andere argumenten liggen veelal in het vertrouwelijke karakter van de data (denk aan gegevens die vertrouwelijk zijn medegedeeld, of gegevens die vertrouwelijk zijn omdat de nationale veiligheid bij beschikbaarstelling in het geding kan komen).

² De Nederlandse Rijksoverheid heeft de voorkeur voor een Creative Commons Publiek Domein Verklaring of een Creative Commons ZERO verklaring. Een mogelijke maar geen voorkeurslicentie, vanuit het perspectief van de hergebruiker, kan naamsvermelding zijn. Deze optie heeft in Australië de voorkeur.

1.2 Privacy

Het recht op privacy is een veelomvattend recht dat wordt beschermd in internationale verdragen,³ Europese regelgeving⁴ en onze grondwet.⁵ Één aspect van het recht op privacy is in het bijzonder van belang bij de implementatie van een open data-beleid, namelijk privacy als het recht van het individu om controle uit te oefenen op de informatie die over hem bekend is. Dit recht wordt ook wel het recht op informationele privacy genoemd. Westin legde het fundament voor ons moderne begrip van informationele privacy en definieerde het als *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."*⁶ Het Handvest van de grondrechten van de Europese Unie geeft eenieder het recht op bescherming van de hem betreffende persoonsgegevens.⁷ De Europese Privacyrichtlijn is een uitwerking van dat recht en bepaalt dat persoonsgegevens eerlijk, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag moeten worden verwerkt.⁸ Deze richtlijn is in Nederland geïmplementeerd door de Wet bescherming persoonsgegevens (Wbp). Als open data-aanbieders persoonsgegevens verwerken zullen ze zich aan deze wetgeving moeten houden.

Naast aandacht voor het wettelijke kader is het van belang om aandacht te schenken aan privacy in meer maatschappelijke zin. Onderzoek heeft aangetoond dat Nederlandse burgers zich in toenemende mate bewust worden van de risico's en gevaren die het gebruik van persoonlijke informatie meebrengen.⁹ Dit beeld wordt bevestigd door een studie in opdracht van de Wetenschappelijke Raad voor Regeringsbeleid naar het Burger Service Nummer.¹⁰

O'Hara schrijft over overheidsinformatiebeleid en transparantie het volgende ten aanzien van privacy:

*"Privacy is extremely important to transparency. The political legitimacy of a transparency programme will depend crucially on its ability to retain public confidence. Privacy protection should therefore be embedded in any transparency programme, rather than bolted on as an afterthought."*¹¹

Zijn stelling is dat aandacht voor privacy een voorwaarde is voor politieke legitimiteit van en vertrouwen in overheidstransparantieprogramma's. Hetzelfde geldt voor open data-initiatieven. Het niet waarborgen van privacy zal negatief uitstralen op de open data-aanbieder. Bij de implementatie van een open data-beleid is aandacht voor de bescherming van privacy daarom onontbeerlijk.

³ Bijvoorbeeld artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBRP) en artikel 8 van het Europees verdrag voor de rechten van de mens (EVRM).

⁴ Bijvoorbeeld door Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L281/31).

⁵ Artikel 10 van de Grondwet.

⁶ Westin 1967, p. 7.

⁷ Artikel 8 lid 1 van het Handvest van de grondrechten van de Europese Unie.

⁸ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L281/31).

⁹ Koffijberg et al. 2009. Zie ook Verhue 2007.

¹⁰ Attema & De Nood 2010.

¹¹ O'Hara 2011, p. 6.

2 Privacyregelgeving toegepast op open data

De Wbp geeft regels over de verwerking van persoonsgegevens. Het College Bescherming Persoonsgegevens houdt toezicht op de naleving van de Wbp. Daarover meer in 2.1.

De begrippen *persoonsgegevens* en *verwerken van persoonsgegevens* zijn van belang voor het bepalen van de reikwijdte van de Wbp. Deze begrippen zijn uitgewerkt in 2.2 en 2.3.

Als er sprake is van persoonsgegevens betekent dat nog niet dat die gegevens niet verwerkt mogen worden. De Wbp geeft regels over de verwerking van persoonsgegevens en verbiedt slechts in een aantal bijzondere gevallen de verwerking van gegevens. Het uitgangspunt van de Wbp is dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.¹² De voorwaarden die de Wbp stelt aan het verwerken van persoonsgegevens zijn uitgewerkt in 2.4.

Betrokkenen kunnen zich op grond van de Wbp beroepen op een aantal rechten. Het gaat dan om het recht op inzage en informatie, het recht op verbetering, aanvulling, verwijdering en afscherming van gegevens en het recht op verzet. Deze rechten worden behandeld in 2.5.

Het verwerken van *bijzondere persoonsgegevens* is in beginsel verboden. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens die betrekking hebben op iemands ras, geloofsovertuiging, of seksuele leven. Dit verbod en de uitzonderingen daarop komen aan bod in 2.6.

De Wbp verbiedt in beginsel ook de doorgifte van persoonsgegevens naar de niet EU-landen. Wat dat betekent voor open data-aanbieders wordt uitgewerkt in 2.7.

2.1 College Bescherming Persoonsgegevens en Artikel 29 Werkgroep

Het College Bescherming Persoonsgegevens (CBP) ziet toe op de verwerking van persoonsgegevens waarop de Wbp betrekking heeft.¹³ Die taak moet het CBP onafhankelijk vervullen.¹⁴

Het CBP kan uit eigen beweging of op verzoek van een belanghebbende een onderzoek instellen naar de wijze waarop de verwerking van persoonsgegevens wordt vormgegeven.¹⁵ Ook heeft het CBP de bevoegdheid om een last onder bestuursdwang op te leggen als een partij de verplichtingen in de Wbp niet naleeft.¹⁶ In een aantal gevallen kan het CBP ook een boete opleggen van ten hoogste 4.500 euro.¹⁷

Het CBP neemt deel in de Artikel 29 Werkgroep.¹⁸ Deze werkgroep is het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders.¹⁹ De werkgroep publiceert met enige regelmaat werkdocumenten en opinies over de toepassing van de Europese Privacyrichtlijn waaraan door het CBP veel waarde wordt gehecht. Er zal daarom in dit rapport op enkele plaatsen naar documenten van de Artikel 29 Werkgroep worden verwezen.

¹² Artikel 6 Wbp.

¹³ Artikel 51 lid 1 Wbp.

¹⁴ Artikel 52 lid 2 Wbp.

¹⁵ Artikel 60 lid 1 Wbp.

¹⁶ Artikel 65 Wbp. Zo werd Google in 2011 een last onder dwangsom opgelegd na op onrechtmatige wijze MAC-adressen en netwerknamen te hebben verzameld. De dwangsom liep op tot maximaal 750.000 euro. CBP 23 maart 2011, z2010-0146.

¹⁷ Artikel 66 Wbp.

¹⁸ Zie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

¹⁹ Artikel 29 Privacy richtlijn.

2.2 Persoonsgegevens

2.2.1 Direct en indirect identificerende gegevens

De Wbp heeft betrekking op de verwerking van *persoonsgegevens*. De persoon op wie de persoonsgegevens betrekking hebben wordt de *betrokkene* genoemd.²⁰ Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.²¹ Het gaat daarbij om levende natuurlijke personen.²² Ook gegevens die betrekking hebben op eenmanszaken en maatschappen kunnen een persoonsgegeven zijn omdat ze direct op een natuurlijk persoon betrokken kunnen worden.²³

Een naam is een persoonsgegeven omdat een persoon daarmee direct wordt geïdentificeerd. Als er door de open data-aanbieder direct identificerende gegevens worden aangeboden, zoals namen en adressen, dan is er sprake van persoonsgegevens en zal men zich in het open data- project moeten houden aan de regels die de Wbp stelt.

Ook gegevens die een persoon indirect identificeren kunnen een persoonsgegeven zijn. Dergelijke gegevens kunnen zijn ontstaan van een naam, maar door combinatie met andere gegevens toch met een bepaalde persoon in verband worden gebracht. Voorbeelden zijn telefoonnummers en combinaties van postcodes met huisnummers.²⁴ Van belang is of de identiteit van een persoon er redelijkerwijs, zonder onevenredige inspanning, mee kan worden vastgesteld. Het is niet doorslaggevend of de persoon daadwerkelijk door de gegevens is geïdentificeerd.²⁵

Ook de mate waarin de gegevens door koppeling met andere gegevens identificeerbaar zijn, is van belang. De opmerkingen van de wetgever bij de invoering van de Basisregistraties Adressen en Gebouwen (BAG) zijn daarvan een illustratie. In de memorie van toelichting bij de Wet BAG valt te lezen dat de gegevens in de basisregistraties adressen en gebouwen in beginsel geen persoonsgegevens zijn in de zin van de Wbp omdat ze niet zijn te herleiden tot identificeerbare personen. Wel kan de identiteit van een persoon te herleiden zijn door koppeling met andere gegevens en daarmee moet de verstrekker van BAG-gegevens rekening houden. Als de verstrekker van BAG-gegevens ervan uit mag gaan dat de afnemer de gegevens in combinatie met andere gegevens kan herleiden tot een natuurlijke persoon, dan moeten de gegevens als persoonsgegevens worden aangemerkt.²⁶ Voor open data-aanbieders betekent dat dat niet alleen de aangeboden data betrokken moet worden in de vraag of de gegevens identificierend zijn, maar ook andere beschikbare gegevens.²⁷

2.2.2 Contextafhankelijkheid

In de Memorie van Toelichting bij de Wbp valt te lezen dat als gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, deze gegevens moeten worden aangemerkt als persoonsgegevens.²⁸ Niet alleen objectieve informatie, maar ook subjectieve informatie zoals meningen en oordelen kunnen daarom een persoonsgegeven zijn.²⁹ Te denken valt aan de kredietwaardigheid of betrouwbaarheid van een persoon.

Volgens de Artikel 29 Werkgroep is er sprake van persoonsgegevens als de gegevens "verwijzen naar de identiteit, de kenmerken of het gedrag van een persoon of indien dergelijke informatie wordt gebruikt om de wijze waarop die persoon wordt behandeld of beoordeeld te bepalen of te beïnvloeden."³⁰ Daarmee is dus ook de context waarin de gegevens worden gebruikt of vastgelegd van belang.

²⁰ Artikel 1 sub f Wbp.

²¹ Artikel 1 sub a Wbp.

²² *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 47 en 50. Zie ook: Vزر. Rb. Amsterdam 11 december 2003, *LJN* AN9893.

²³ Rb. Zwolle-Lelystad 21 februari 2006, *LJN* AV3139. Zie ook Klingenbergr 2011. Vergelijk echter Vزر. Rb. Zwolle 22 maart 2004, *LJN* AO6018 waarin de voorzieningenrechter tegenovergesteld oordeelde.

²⁴ Registratiekamer 1996.

²⁵ College Bescherming Persoonsgegevens 2007, p. 10.

²⁶ *Kamerstukken II* 2006/07, 30 968, nr. 3, p. 17.

²⁷ Gegevens die beschikbaar zijn via <http://energielabelapp.nl> waar op adresniveau kan worden gezocht naar het energielabel van een gebouw of woning zijn dus ook persoonsgegevens.

²⁸ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 46.

²⁹ Artikel 29 Werkgroep, Advies 4/2007 over het begrip persoonsgegeven, WP 136, p. 6.

³⁰ Artikel 29 Werkgroep, Working document on data protection issues related to RFID technology, WP 105, p. 8.

Het is van belang om op te merken dat gegevens die uitsluitend voorwerpen aanduiden ook persoonsgegevens kunnen zijn. Zo kan de waarde van een woning betrekking hebben op een persoon omdat de woning behoort tot het vermogen van de eigenaar. Informatie over de waarde van de woning kan bijvoorbeeld worden gebruikt om belastingverplichtingen van de eigenaar vast te stellen en is daarmee een persoonsgegeven geworden. Als dergelijke gegevens daarentegen worden geaggregeerd en gebruikt ter illustratie van de hoogte van de huizenprijzen in een bepaald gebied dan is er niet langer sprake van persoonsgegevens.³¹

Alliander overweegt haar energiemetgegevens als open data aan te bieden. Ten aanzien van door slimme meters verwerkte gegevens heeft de Artikel 29 Werkgroep vastgesteld dat degelijke gegevens doorgaans persoonsgegevens zijn. De Artikel 29 Werkgroep komt tot die conclusie omdat:

- door slimme meters verkregen gegevens in de meeste gevallen gekoppeld zijn aan unieke identificatiegegevens, zoals het identificatienummer van een meter. In geval van particuliere afnemers van energieleveranciers zijn deze identificatiegegevens onlosmakelijk gekoppeld aan de natuurlijke persoon die verantwoordelijk is voor de rekening;
- de informatie die door een slimme meter wordt verzameld gekoppeld is aan het energieprofiel van de consument in het kader van diens energieverbruik en deze informatie wordt gebruikt om beslissingen te nemen die rechtstreeks van invloed zijn op de persoon; en
- de invoering van slimme meters een vermindering van het energiegebruik beoogt. Dit doel kan alleen worden bereikt indien het energieverbruik van individuele consumenten ook wordt beperkt. Volgens energieleveranciers en netten is de verwezenlijking van dit doel in hoge mate afhankelijk van de verzameling van grote hoeveelheden informatie over het gedrag van deze consumenten.³²

Niet geaggregeerde of geanonimiseerde meetgegevens moeten daarom als persoonsgegeven worden aangemerkt. In sommige gevallen kan aannemelijk worden gemaakt dat de meetgegevens als bijzondere persoonsgegevens moeten worden aangemerkt. Te denken valt aan afwijkend energieverbruik in bepaalde perioden van het jaar (ramadan/ suikerfeest).

2.2.3 Anonieme en geaggregeerde gegevens

In een open data-project kunnen geanonimiseerde of geaggregeerde gegevens worden aangeboden. Door anonimisering en aggregatie van persoonsgegevens kunnen deze gegevens ontdaan worden van identificerende kenmerken. Er is dan in beginsel geen sprake meer van persoonsgegevens in de zin van de Wbp.

Of dergelijke gegevens daadwerkelijk geen persoonsgegevens zijn is sterk afhankelijk van de stand van de techniek. Als blijkt dat geanonimiseerde gegevens naderhand toch identificeerbaar zijn dan worden de gegevens persoonsgegevens. In de Memorie van Toelichting bij de Wbp valt daarover het volgende te lezen:

“Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding. [...] Onder omstandigheden zullen de gegevens tevens nader moeten worden bewerkt om identificatie tegen te gaan. Aggregatie kan bijvoorbeeld het onderscheidend vermogen van gegevens doen verminderen. Zolang identificatie van gegevens met behulp van andere bestanden een reële mogelijkheid is, is het wetsvoorstel [de Wbp] van toepassing en moeten de daarin opgenomen spelregels worden nageleefd.”³³

Het is niet bij voorbaat duidelijk op welk detailniveau er geen sprake meer van persoonsgegevens is. De Task Force Smart Grids Expert Group stelt bijvoorbeeld:

“Concerning aggregation of personal data, there is no clear saying on how many persons one needs to aggregate on to protect individual data. This is also very context- and data dependent. Some research indicates that the minimum number of users is around 7 to 8, but in many circumstances it will be more. In case a meter is ‘adjacent’ to a household (i.e. majority of sit-

³¹ Voorbeeld ontleent aan: Artikel 29 Werkgroep, Advies 4/2007 over het begrip persoonsgegeven, WP 136, p. 10.

³² Artikel 29 Werkgroep, Advies 12/2011 over slimme meters, WP 183, p. 5.

³³ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 49.

uations) we cannot say that we have any kind of data aggregation. There are simply too few inhabitants in such a household.”³⁴

Het product energieinbeeld³⁵ gaat uit van anonimiteit bij minimaal 6 waarnemingen bij kleinverbruikers per 6 ppc. Dataland, een overheids bv die als intermediair, via queries op de brondata, toegang geeft tot verschillende geografische gerelateerde bestanden van gemeenten geeft per 6 ppc postcode gebied de gemiddelde woz-waarde op basis van minimaal 5 woningen met dezelfde bouwbestemming. De definitie van de “anonieme” gemiddelde woz-waarde is niet gebaseerd op een afspraak met de toezichthouder, de Waarderingskamer. Deze regel is vanuit de praktijk gedefinieerd. Andere technische oplossingsrichtingen zijn om de beschikbare gegevens limitatief ter beschikking te stellen. Bijvoorbeeld door slechts het gemiddelde verbruik per 6 ppc per jaar te verstrekken in plaats de 15 minuten gemiddelden per 6 ppc (wat mogelijk is bij slimme meters) en queries op de brondata niet toe te staan. De in februari 2012 vrijgegeven data van het CBS beschikt ook over gegevens op 6 ppc niveau. Het NRC Handelsblad heeft deze gegevens geïnterpoleerd zodat er ‘een mooi vloeiend beeld ontstaat’.³⁶ Men maakt gebruik van gewogen gemiddelden per getoonde pixel. Hoe dichterbij de pixel hoe zwaarder het gewicht. Bij minder dan 5 waarden in een straal van 100 meter wordt er niet getoond.³⁷

Bij welk aggregatieniveau er sprake is van afdoende geanonimiseerde gegevens is echter ongewis.³⁸ In 1998 antwoordde de minister bij de behandeling van de Wet bescherming persoonsgegevens³⁹:

“Wat betreft postcodes wijzen wij op een advies van de Registratiekamer waarbij het gebruik van postcodes, zonder nadere aanduiding van een pand duidend op een individueel huishouden, niet als een verwerking van persoonsgegevens wordt aangemerkt.”

In 2000 specificerde de minister zijn eerder gegeven antwoord⁴⁰:

“Indien op grond van postcodesegmentatie of anderszins, bijvoorbeeld op grond van statistisch onderzoek, uit een bepaald gegeven dat aan iemands naam is toegevoegd, bepaalde gevolgtrekkingen worden gemaakt, gaat het om een persoonsgegeven. Het gegeven leidt er immers toe dat iemand in het maatschappelijk verkeer de kans loopt anders te worden bejegend dan wanneer dit gegeven niet over hem bekend was.”

Als geanonimiseerde of aggregierte gegevens in aangeboden open data toch identificeerbaar blijken, moeten de gegevens als persoonsgegevens worden opgevat en is de Wbp van toepassing. Een voorbeeld uit de praktijk toont aan dat dat niet slechts een theoretisch probleem is. Zo lukte het Britse studenten om namen, adressen en salarissen van ambtenaren bloot te leggen door openbare data te combineren met gegevens uit het open data portaal van de Britse overheid.^{41 42} Door technologische ontwikkelingen en de toename van beschikbare data zal het in de toekomst eenvoudiger zijn om geanonimiseerde of geaggregeerde data te identificeren.⁴³ Dat zorgt ervoor dat gegevens die aanvankelijk geen persoonsgegevens zijn, dat in de toekomst wel kunnen worden en dat is iets waar open data-aanbieders rekening mee zullen moeten houden.

2.3 Verwerken van persoonsgegevens

2.3.1 Verwerken

De Wbp is van toepassing op het zowel geheel of gedeeltelijk geautomatiseerd *verwerken* van persoonsgegevens. Ook niet-geautomatiseerde verwerking van persoonsgegevens valt onder de Wbp als de gegevens worden opgenomen in een bestand: een gestructureerd geheel van persoonsgegevens

³⁴ The Task Force Smart Grids Expert Group 2 2011.

³⁵ <http://www.energieinbeeld.nl>

³⁶ Poort, A., Statistiek saai? CBS-cijfers komen tot leven op de kaart, NRC Handelsblad 14 februari 2012, pp. 12-13.

³⁷ Door de honderd meter straal slim te kiezen is het zeer waarschijnlijk mogelijk om individuele waarden uit het bestand te extraheren.

³⁸ Zie ook sectie “Privacy-inbreuk” van het deelrapport Aansprakelijkheid voor open data van dit project.

³⁹ Kamerstukken 1998-1999, 25892, nr. 6, p. 27

⁴⁰ Eerste Kamer, vergaderjaar 1999-2000, 25 892, nummer 92c, p. 13

⁴¹ A. C. Simpson, ‘On privacy and public data: a study of data.gov. uk’, *Journal of Privacy and Confidentiality*, 2011-1, p. 51.

⁴² Zie ook The Task Force Smart Grids Expert Group 2 2011, hoofdstuk 2.2.2.1. Data anonymisation and data aggregation.

⁴³ Narayanan & Shmatikov 2008; Ohm 2010.

dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.⁴⁴ De natuurlijke persoon of rechtspersoon die het doel van en de middelen voor de verwerking vaststellen wordt de *verantwoordelijke* genoemd.⁴⁵

Onder verwerking van persoonsgegevens verstaat de Wbp "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens."⁴⁶ Daaronder verstaat de Wbp in ieder geval het volgende:

"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."⁴⁷

Gegevensverwerking omvat dus het gehele proces dat een gegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietiging.⁴⁸

Als er in een open data-project persoonsgegevens worden aangeboden dan zal er, gelet op de veelomvattende definitie van verwerken, sprake zijn van verwerking van persoonsgegevens waarop de Wbp van toepassing is.

Als persoonsgegevens worden geanonimiseerd of geaggregeerd om te voorkomen dat er persoonsgegevens worden verwerkt, rijst de vraag of het ontdoen van identificerende kenmerken van persoonsgegevens op zichzelf ook als verwerking heeft te gelden. Het gevolg zou zijn dat de het anonimiseren of aggregeren als zodanig aan de vereisten die de Wbp stelt, moet voldoen.

Het antwoord op deze vraag lijkt bevestigend beantwoord te moeten worden. Het anonimiseren of aggregeren van persoonsgegevens is niet expliciet als verwerking in de Wbp genoemd maar valt wel onder het algemene en ruime verwerkingsbegrip van de Wbp ("elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens"). Volgens Berkvens & Prins volgt uit het feit dat het wissen of vernietigen van persoonsgegevens verwerkingen van persoonsgegevens zijn, dat het anonimiseren van persoonsgegevens ook als verwerking van persoonsgegevens moet worden aangemerkt.⁴⁹ Korff is eenzelfde mening aangedaan:

*"The term processing here is clearly defined very widely to include not just "technical" processing but also the collection, recording, consultation, and destruction of personal data. Importantly, it also includes the processes of pseudonymisation and anonymisation of data: as a result, controllers are not just free to pseudonymise or (supposedly) anonymise any data they hold, and then escape the law; rather, in doing so, they must comply with the relevant legal requirements for lawful processing. They may thus, for instance, need to inform the data subject, or indeed obtain their consent for this processing."*⁵⁰

Het gevolg is dat open data-aanbieders die geen persoonsgegevens aanbieden, zich toch moeten houden aan de Wbp als de aangeboden gegevens geanonimiseerde of geaggregeerde persoonsgegevens zijn. De eisen die de Wbp stelt aan het verwerken van persoonsgegevens gelden dan wel slechts ten aanzien van de anonimisering of aggregatie van de gegevens.

2.3.2 Uitzonderingen

De Wbp kent een aantal uitzonderingsgevallen waarin het verwerken van persoonsgegevens is uitgezonderd van de werking van de Wbp. Zo is de wet niet van toepassing op verwerking ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden.⁵¹ Het bijhouden van een adres-

⁴⁴ Artikel 1 sub c en artikel 2 Wbp.

⁴⁵ Artikel 1 sub d Wbp.

⁴⁶ Artikel 1 sub b Wbp.

⁴⁷ Artikel 1 sub b Wbp.

⁴⁸ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 52.

⁴⁹ Berkvens & Prins 2007, p. 30.

⁵⁰ Korff 2010, p. 58.

⁵¹ Artikel 2 lid 2 sub a Wbp.

senlijst voor persoonlijk gebruik is bijvoorbeeld niet aan de regels van de Wbp onderhevig.⁵² Andere uitzonderingsgronden zijn er voor de verwerking ten behoeve van de inlichtingen- en veiligheidsdiensten, de uitvoering van de politietaken en de Wet justitiële en strafvorderlijke gegevens.⁵³ Uitzonderingen zijn er ook voor de verwerking van persoonsgegevens ten behoeve van de uitvoering van de kieswet en de verwerking van persoonsgegevens die is geregeld door de Wet gemeentelijke basisadministratie persoonsgegevens.⁵⁴

De Wbp is gedeeltelijk niet van toepassing op de verwerking van persoonsgegevens met uitsluitend journalistieke, artistieke of literaire doeleinden.⁵⁵ Ook is het toegestaan om meer gevoelige persoonsgegevens ("bijzondere persoonsgegevens") te verwerken voor zover dit voor het journalistieke, artistieke of literaire doeleinde noodzakelijk is.⁵⁶

Geen van de genoemde uitzonderingsgronden kan op open data van toepassing zijn omdat er geen sprake is van een journalistieke, artistieke of literaire doeleinden. Het doeleinde zal immers de algemene verstrekking van allerlei gegevens aan anderen zijn. Een open data-aanbieder zal zich daarom, voor zover hij persoonsgegevens verwerkt, moeten houden aan de regels in de Wbp.

2.4 Voorwaarden voor het verwerken van persoonsgegevens

Als er persoonsgegevens worden verwerkt dan mag dat slechts onder de voorwaarden die de Wbp daaraan stelt. Deze eisen worden in dit hoofdstuk uitgewerkt en toegepast op open data.

2.4.1 Verwerkingsgrond

Persoonsgegevens mogen alleen worden verwerkt op basis van in de artikel 8 Wbp opgesomde verwerkingsgronden:

"Persoonsgegevens mogen slechts worden verwerkt indien:

- a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
- b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiek-rechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
- f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."

Er hoeft niet aan alle voorwaarden te worden voldaan - één van de verwerkingsgronden is voldoende voor de gegevensverwerking.

Op het eerste gezicht lijken een drietal verwerkingsgronden zich te lenen voor open data: een overeenkomst die verwerking noodzakelijk maakt, de behartiging van het belang van de open data-aanbieder of een derde (sub f), of toestemming van de betrokkene (sub a). De overige verwerkings-

⁵² Zie overweging 12 van de Privacyrichtlijn.

⁵³ Artikel 2 lid 2 sub b, c en e Wbp.

⁵⁴ Artikel 2 lid 2 sub d en f Wbp.

⁵⁵ Artikel 3 lid 1 Wbp.

⁵⁶ Artikel 3 lid 2 Wbp.

gronden: uitvoering van een overeenkomst (sub b), wettelijke verplichting (sub c)⁵⁷, vrijwaring van een vitaal belang van de betrokkene (d) en de goede vervulling van een publiekrechtelijke taak (e), zullen niet snel van toepassing zijn op open data van Alliander.⁵⁸

Toestemming (sub a)

Als de personen op wie de persoonsgegevens betrekking hebben hun toestemming verlenen voor gebruik van hun persoonsgegevens in een open data-project dan is dat een geldige grond voor gegevensverwerking. De toestemming van de persoon op wie de persoonsgegevens betrekking hebben, moet ondubbelzinnig zijn. Toestemming wordt in de Wbp verder uitgewerkt als "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt."⁵⁹

Volgens de Artikel 29 Werkgroep kan toestemming niet passief of stilzwijgend plaatsvinden. Toestemming vereist een actie waarmee de betrokkene duidelijk maakt dat hij instemt met de gegevensverwerking.⁶⁰ De toestemming moet vrij gegeven zijn. Het moet gaan om een echte keuze, zonder risico van misleiding, intimidatie of andere significant negatieve consequenties.⁶¹ Zo mag het niet verlenen van toestemming niet leiden tot een substantiële prijsverhoging voor weigeraars.⁶²

De toestemming moet ook specifiek zijn. Een 'blanco cheque' kan dus niet worden gegeven. De toestemming moet betrekking hebben op een heldere en precieze omvang van de gegevensverwerking.⁶³ Daarnaast moet de betrokkene op de hoogte zijn van de gevolgen die toestemming voor de gegevensverwerking met zich meebrengt. De verantwoordelijke dient daartoe de betrokkene in te lichten over onder andere het type gegevens dat zal worden verwerkt, het doel van de verwerking, de mogelijke andere ontvangers van de gegevens en de rechten die de betrokkene heeft.⁶⁴ Een open data-aanbieder zal betrokkenen daarom moeten voorlichten over welke gegevens er gebruikt zullen worden in het open data-initiatief en wat de open data-aanbieder voor ogen heeft met de gegevens: het ongeclausuleerd aanbieden van de gegevens aan anderen.

Als een persoon toestemming geeft tot verwerking van zijn persoonsgegevens, blijven de vereisten van de Wbp, zoals de zorgvuldigheidsdeis, uiteraard gelden. Toestemming ontslaat de open data-aanbieder niet van de plichten die de Wbp aan hem oplegt.

Noodzakelijk voor uitvoeren overeenkomst (sub b)

Een andere grond voor de verwerking van persoonsgegevens is de verwerking ten behoeve van de uitvoering van een overeenkomst. Voorwaarde is dat de betrokkene op wie de informatie betrekking heeft zelf partij is bij de overeenkomst. Het klassieke voorbeeld van verwerking op basis van deze grondslag is het verwerken van naam, adres en woonplaats-gegevens door een bedrijf om zijn klanten te factureren.

Voor een geslaagd beroep op deze verwerkingsgrond moet het voor de uitvoering van de overeenkomst noodzakelijk zijn dat de gegevens worden verwerkt. Sommige gegevens die als open data worden aangeboden zijn door de open data-aanbieder oorspronkelijk verzameld met het oog op de uitvoering van een overeenkomst. Te denken valt aan meetgegevens die worden verzameld om klanten op basis van hun elektriciteitsgebruik te factureren. Zonder verwerking van deze gegevens is de overeenkomst tot levering van elektriciteit moeilijk uitvoerbaar.

De open data-aanbieder zal zich echter niet snel op een dergelijke overeenkomst kunnen beroepen. Voor het delen van meetgegevens door een energieleverancier zou dat betekenen dat het voor de

⁵⁷ Deze grond zal op basis van de Wet op het CBS, van toepassing zijn op het CBS voor de verwerking van energieverbruiksgegevens.

⁵⁸ Ervan uitgaande dat de open data-aanbieder geen overheidsorgaan is.

⁵⁹ Artikel 1 sub i Wbp.

⁶⁰ Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, WP 187, p. 12.

⁶¹ Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, WP 187, p. 12.

⁶² Voorbeeld afgeleid uit: Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, WP 187, p. 15.

⁶³ Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, p. 17.

⁶⁴ Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, p. 19.

overeenkomst tot levering van elektriciteit noodzakelijk is dat de verzamelde meetgegevens als open data worden aangeboden. Daarvan kan geen sprake zijn. Een open data aanbieder zal zich daarom niet snel op deze verwerkingsgrond kunnen beroepen.

Belang van verantwoordelijke of derde (sub f)

Ook het belang van de verantwoordelijke of dat van een derde kan een geldige grond voor de verwerking van persoonsgegevens zijn. Het belang van de betrokkene en zijn fundamentele rechten en vrijheden, in het bijzonder zijn recht op bescherming van de persoonlijke levenssfeer moeten zich dan niet tegen de verwerking verzetten. In de kern gaat het om een belangenafweging tussen het belang van de verantwoordelijke of een derde, en het belang van de betrokkene.

Een voorbeeld waarin het belang van de betrokkene minder zwaar woog is het geval van geheim cameratoezicht in nachtbussen als er een concrete aanwijzing bestaat dat chauffeurs van deze bussen onrechtmatige of strafbare handelingen verrichten.⁶⁵ Een voorbeeld van het tegenovergestelde is de publicatie van een foto in een winkelatalage met het bijschrift dat het om een winkeldief gaat. Het CBP vond dat er dit geval geen sprake was van een maatschappelijk aanvaardbaar doel en daardoor ook geen gerechtvaardigd doel voor de winkelier. Publicatie van de foto was dus niet toegestaan.⁶⁶

Blijkens de Memorie van Toelichting bij de Wbp kan een gerechtvaardigd belang van de verantwoordelijke ook bestaan als de verwerking noodzakelijk is om reguliere bedrijfsactiviteiten kunnen verrichten. Zo dient een schadeverzekeraar ten behoeve van een schadeclaim naast de gegevens van zijn cliënt ook gegevens van de tegenpartij en eventuele getuigen te kunnen verwerken.⁶⁷ Ook als de verwerking van persoonsgegevens niet direct onderdeel uitmaakt van de kernactiviteiten van de verantwoordelijke, maar daarmee nauw verweven is, dan kan gegevensverwerking gerechtvaardigd zijn. Een voorbeeld is een bedrijf dat klantgegevens wil gebruiken voor een mailing over een nieuw product.⁶⁸

Een open data-aanbieder kan zich op deze verwerkingsgrond beroepen als het belang van het open data project zwaarder weegt dan het recht op privacy van personen op wie de aangeboden gegevens betrekking hebben.

Open data-aanbieders en hun open data-projecten kunnen veelsoortige belangen dienen. Te denken valt aan belangen als de goede PR van de open data-aanbieder of het bijdragen aan het verbeteren van de levenskwaliteit van mensen met diabetes.⁶⁹ Het belang dat de open data-aanbieder dient, de noodzakelijkheid van de gegevensverwerking voor behartiging van dat belang en de mate waarin het recht op privacy van betrokkenen worden geraakt, moeten meegenomen worden in de belangenafweging. Zo zal het verbeteren van de levenskwaliteit van mensen met diabetes wat betreft het belang voor de samenleving sneller een gerechtvaardigd belang opleveren dan de goede sier van de open data-aanbieder. Tegelijkertijd zal het gaan om bijzondere persoonsgegevens betreffende iemands gezondheid waardoor de belangenafweging eerder in het voordeel van de betrokkene zal uitvallen.

Het gebruik van persoonsgegevens in een open data-project moet in verband staan met het primaire doel van de verzameling. Als dat niet het geval is dan moet er een nieuwe grondslag gevonden worden. In een open data-project zal dat laatste snel vereist zijn omdat een verband tussen het initiële doel van de verwerking van persoonsgegevens en het algemene doel van het aanbieden van open data moeilijk met elkaar in verband zijn te brengen. Zo vond het College Bescherming Persoonsgegevens ten aanzien van gegevensuitwisseling tussen Nuon en de GGD voor zogenaamde bemoeizorg dat er tussen de tenuitvoerlegging van de overeenkomst van Nuon met zijn klanten, en het voorkomen gezondheidsproblemen bij die klanten te weinig verwantschap bestond.⁷⁰ Er was dus sprake van onverenigbaar gebruik. Als open data-aanbieders persoonsgegevens verwerken zullen zij daarom vaak een nieuwe grondslag voor de verwerking van persoonsgegevens moeten vinden.

Ten aanzien van door slimme meters verzamelde gegevens heeft de Artikel 29 Werkgroep het volgende opgemerkt:

⁶⁵ CRvB 10 juli 2008, *LJN* BD8026.

⁶⁶ CBP 3 mei 2006, z2005-0846.

⁶⁷ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 86.

⁶⁸ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 87.

⁶⁹ Zie voor het laatste: www.datadesigndiabetes.com.

⁷⁰ College Bescherming Persoonsgegevens 2005.

“Het lijkt buiten kijf te staan dat de gerechtvaardigde belangen van de voor de verwerking verantwoordelijke en de samenleving als geheel worden gediend door een almaar doelmatiger energielevering en energiegebruik en dat dit kan worden bewerkstelligd via de door slimme meters verzamelde persoonsgegevens. Maar dat dit specifieke gebruik van persoonsgegevens gerechtvaardigd lijkt (en, voor veel mensen, wenselijk), wil nog niet zeggen dat het ook kan dienen ter rechtvaardiging van elk onderdeel van de verwerking. Met andere woorden: de noodzaak om het energieverbruik te verminderen kan een zinnige doelstelling van het overheidsbeleid zijn, die echter niet in alle gevallen prevaleert boven de rechten en belangen van betrokkenen.”⁷¹

Of er sprake is van een gerechtvaardigd belang hangt onder meer af van ingebouwde mechanismen die de privacy van betrokkenen beschermt:

“Het moge duidelijk zijn dat praktische maatregelen als privacybevorderende technologieën en privacyeffectbeoordelingen – om de veiligheid en privacy van de door slimme meters verwerkte gegevens te verbeteren – ervoor zorgen dat een voor de verwerking verantwoordelijke eerder een beroep kan doen op deze voorwaarde.”⁷²

Het delen van meetgegevens als open data zou kunnen bijdragen aan de bewustwording van het energieverbruik van mensen en kan helpen het energieverbruik te doen dalen. Of dat voldoende is voor Alliander om zich op deze verwerkingsgrond te beroepen is niet zeker. De bewustwording van energieverbruik als verwerkingsgrond om meetgegevens te anonimiseren voor en aggregeren zal daarentegen verdedigbaar zijn omdat het gaat om een minimale vorm van gegevensverwerking die de belangen van betrokkenen niet zal schaden.

2.4.2 Welbepaalde uitdrukkelijke doeleinden en doelbinding

De Wbp vereist dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.⁷³ Het doeleinde dat de open data-aanbieder nastreeft met de verwerking van persoonsgegevens moet dus *voldoende bepaald* zijn. Daarnaast moet het *doel vooraf* en *precies* worden omschreven (zie ook sectie 2.4.8 over de meldingsplicht). Bovendien moeten de gegevens voor een *gerechtvaardigd doeleinde* zijn verzameld (zie sectie 2.4.1 over verwerkingsgronden).

De eis dat gegevensverwerking plaats moet vinden voor een welbepaald doeleinde zal voor open data-aanbieders problemen opleveren. De Wbp bepaalt dat er geen gegevens verwerkt mogen worden zonder een precies doel. Volgens de Memorie van Toelichting bij de Wbp houdt welbepaald in dat de doelomschrijving duidelijk moet zijn en niet zo vaag of ruim dat zij bijvoorbeeld tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden bij beantwoording van de vraag of de gegevens nodig zijn voor dat doel of niet.⁷⁴

De eis van welbepaaldheid lijkt daarmee in strijd met de essentie van de open data filosofie waarin gegevens juist onvoorwaardelijk ter gebruik worden aangeboden aan een zo breed mogelijk publiek dat allerlei andere doeleinden met het gebruik van die gegevens nastreeft. Dit doeleinde is misschien wel uitdrukkelijk, maar niet specifiek en levert daarmee wrijving op met de eis van welbepaaldheid.

2.4.3 Niet onverenigbaar gebruik

Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.⁷⁵ In de praktijk komt het geregeld voor dat een doelomschrijving uit meerdere onderdelen bestaat.⁷⁶ De doelen moeten dan onderling verenigbaar zijn om strijdigheid met de Wbp te voorkomen.

De Wbp geeft een niet-limitatieve lijst met factoren waarmee beoordeeld kan worden of de verwerking verenigbaar is met doelen waarvoor de gegevens zijn verkregen:

⁷¹ Artikel 29 Werkgroep, Advies 12/2011 over slimme meters, WP 183. p. 9.

⁷² Artikel 29 Werkgroep, Advies 12/2011 over slimme meters, WP 183. p. 10.

⁷³ Artikel 7 Wbp.

⁷⁴ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 79.

⁷⁵ Artikel 9 lid 1 Wbp.

⁷⁶ Hooghiemstra & Nouwt 2011, p. 44.

- 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.⁷⁷

Een voorbeeld van niet verenigbare doelen was de gegevensuitwisseling tussen Nuon en de GGD voor zogenaamde bemoeizorg. Nuon wilde gegevens uitwisselen met GGD Amsterdam om mensen met ernstige psychische of psychosociale problemen en die dringend hulp behoeven te signaleren. Het convenant werd ter beoordeling aan het CBP voorgelegd. Het CBP stelde dat het oorspronkelijke doel waarvoor Nuon de persoonsgegevens verzamelde de tenuitvoerlegging van overeenkomsten ter levering van elektriciteit, gas en warmte was. Het CBP oordeelde dat er tussen de tenuitvoerlegging van de overeenkomst van Nuon met zijn klanten en het voorkomen gezondheidsproblemen bij die klanten te weinig verwantschap tussen de doelen bestond.⁷⁸ Er was dus sprake van onverenigbaar gebruik.

In een open data-project zal het initiële doel van de verwerking van persoonsgegevens en het algemene doel van het aanbieden van open data moeilijk met elkaar in verband te brengen zijn. Als open data-aanbieders persoonsgegevens verwerken zullen zij daarom vaak een nieuwe grondslag voor de verwerking van persoonsgegevens in het open data project moeten vinden.

Als de verdere verwerking van gegevens historische, statistische of wetenschappelijke doeleinden heeft dan wordt een dergelijke verwerking niet als onverenigbaar beschouwd.⁷⁹ Voorwaarde is wel dat er de nodige voorzieningen worden getroffen om ervoor te zorgen dat verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

Open data-aanbieders zullen zich niet op deze uitzondering kunnen beroepen. De uitzonderingsbepaling vereist dat er voorzieningen worden getroffen om ervoor te zorgen dat verdere verwerking uitsluitend geschiedt ten behoeve van historische, statistische of wetenschappelijke doeleinden. Een kenmerk van open data is dat de gegevens juist onvoorwaardelijk worden aangeboden, zonder beperkingen die bijvoorbeeld uitsluitend het gebruik voor statistische doeleinden opleggen.

2.4.4 Minimaal en toereikend verwerken

Persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.⁸⁰ Een uitzondering op deze regel is het bewaren van persoonsgegevens voor historische of statistische doeleinden.⁸¹

Bovendien mogen persoonsgegevens slechts worden verwerkt voor zover zij, met het oog op de doeleinden waarvoor zij zijn verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.⁸² Het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, is dus bepalend voor de hoeveelheid en de soort gegevens die verwerkt mogen worden.⁸³ Deze eis ziet toe op zowel het 'te veel' als het 'te weinig' verwerken van persoonsgegevens. De verwerking moet, gelet op de doeleinden van de verwerking niet bovenmatig zijn. Tegelijkertijd moeten de te verwerken gegevens ter zake dienen en toereikend zijn.

Zo achtte het CBP de verstrekking van informatie door een burgemeester aan de woningstichting waarbij het complete politiedossier werd meegestuurd bovenmatig.⁸⁴ Een voorbeeld van het 'te weinig' verwerken is het registreren dat een betrokkene niet heeft betaald voor een bepaald product zonder daarbij te vermelden dat dit niet betalen te wijten is aan het feit dat die betrokkene niet tevreden is met dit product en om die reden de betaling heeft opgeschort.⁸⁵

⁷⁷ Artikel 9 lid 2 Wbp.

⁷⁸ CBP 12 september 2005, z2005-0598.

⁷⁹ Artikel 9 lid 3 Wbp.

⁸⁰ Artikel 10 lid 1 Wbp.

⁸¹ Artikel 10 lid 2 Wbp.

⁸² Artikel 11 lid 1 Wbp.

⁸³ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 96.

⁸⁴ CBP 3 juni 2005, z2004-1185.

⁸⁵ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 96.

De open data-filosofie levert wrijving op met de vereisten van minimaal en toereikend verwerken. Deze vereisten proberen de verwerking van persoonsgegevens tot een minimum te beperken. Wat in een concreet geval als minimum geldt, hangt af van het doel dat de verwerker voor ogen heeft. De open data-filosofie beoogt een onbeperkt aanbod en gebruik van (persoons)gegevens. Als het onbeperkt aanbieden van gegevens het doel is van het open data-project dan levert dat strikt genomen geen strijdigheid het vereiste van minimaal verwerken. Het doel is immers een zo breed mogelijk aanbod van gegevens en daarmee ligt het minimum van de gegevensverwerking heel hoog. Echter, een dergelijke redenering is in strijd met de geest van de eis van minimaal verwerken. Deze redenering maakt het bovendien mogelijk om via een achterdeur (een veelomvattend doeleinde van de verwerking), de eis van minimaal verwerken te omzeilen.

2.4.5 Nauwkeurige gegevens

Daarnaast moet de verwerker van persoonsgegevens er zorg voor dragen dat de persoonsgegevens juist en nauwkeurig zijn.⁸⁶ Er wordt door de Wbp geen absolute verplichting opgelegd, een garantie voor de juistheid van gegevens wordt niet van de verantwoordelijke vereist. De verantwoordelijke moet wel de nodige maatregelen treffen die in redelijkheid van hem kunnen worden gevergd om ervoor te zorgen dat de gegevens juist en nauwkeurig zijn.⁸⁷

Voor open data-aanbieders geldt dus dat zij hun best moeten doen om ervoor te zorgen dat de verwerkte persoonsgegevens juist en nauwkeurig zijn. De verplichting om nauwkeurige gegevens aan te bieden hangt samen met het recht van correctie dat een betrokkene heeft (sectie 2.5.2). De open data-aanbieder kan er daarom voor kiezen om naast het opnemen van contactgegevens op de open data-website, een voorziening aan te bieden waarmee fouten in de gegevens kunnen worden gesignaleerd en verbeterd door gebruikers van de website.

2.4.6 Beveiliging

De verantwoordelijke moet zijn best doen om verlies of enige vorm van onrechtmatige verwerking van gegevens te voorkomen.⁸⁸ De Wbp verplicht verwerkers daarom om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.⁸⁹ Voor de vraag hoever die beveiliging moet strekken zijn van belang:

- de stand van de techniek;
- de kosten van de tenuitvoerlegging;
- en de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengt.

Een open data-aanbieder kan bijvoorbeeld waarschuwingen op de open data-website opnemen om ervoor te zorgen dat gegevens niet op een onrechtmatige manier worden hergebruikt.

2.4.7 Informeren van betrokkene

Uit het beginsel van behoorlijke gegevensverwerking volgt de verplichting voor verantwoordelijken om betrokkenen op de hoogte te brengen van de verwerking.⁹⁰ Betrokkenen worden zo in staat gesteld om de verwerking te volgen en eventueel onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.

Als de betrokkene reeds op de hoogte is van de identiteit van de verwerker en het doel van de verwerking dan hoeft deze informatie niet verstrekt te worden. Betrokkenen waarvan persoonlijke gegevens zijn opgenomen in een open dataverzameling, zullen daar doorgaans niet van op de hoogte zijn. De open data-aanbieder dient daarom betrokkenen te informeren over het open data-beleid.

Er wordt door de Wbp onderscheid gemaakt tussen informatie die is verkregen bij de betrokkene⁹¹ en informatie die op andere wijze is verzameld.⁹² Een voorbeeld van bij de betrokkene verkregen infor-

⁸⁶ Artikel 11 lid 2 Wbp.

⁸⁷ *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 97.

⁸⁸ *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 98.

⁸⁹ Artikel 13 Wbp.

⁹⁰ *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 149.

⁹¹ Artikel 33 Wbp.

⁹² Artikel 34 Wbp.

matie is de informatie die een betrokkene op een invulformulier invult. Een voorbeeld van informatie die op andere wijze is verzameld is de informatie die de verwerker zelf verzameld door observatie van de betrokkene, bijvoorbeeld door cameratoezicht.

Het moment waarop de verwerker informatie moet verstrekken over zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd verschilt afhankelijk van de wijze waarop de gegevens zijn verzameld.

Voor bij de betrokkene zelf verzamelde informatie geldt dat de informatie verstrekt moet worden vóór het moment van verkrijging van de informatie.⁹³ Als het bijvoorbeeld gaat om door de betrokkene opgegeven klantgegevens die ook in een open data-project worden gebruikt dan kan de open data-aanbieder de klant op de hoogte stellen door een boodschap op het (digitale) aanmeldformulier te plaatsen.⁹⁴

Als gegevens op andere wijze zijn verzameld moet de informatie verstrekt worden op het moment van vastlegging van de persoonsgegevens, of als de gegevens voor derden zijn bestemd, uiterlijk op het moment van de eerste verstrekking aan deze derden.⁹⁵ Een open data aanbieder zal de informatie moeten bieden voor de gegevens aan derden beschikbaar worden gesteld: voor het moment dat de gegevens als open data worden aangeboden. Dat kan bijvoorbeeld door een algemene brief of e-mail te sturen aan de betrokkenen of door een mededeling op te nemen in het eigen magazine of een nieuwsbrief die aan alle klanten wordt gestuurd. Als dat echter onmogelijk blijkt of een onevenredige inspanning kost, is de verantwoordelijke niet langer verplicht de informatie over de verwerking te geven.⁹⁶

Een uitzondering op de informatieplicht die geldt voor niet bij de betrokkene verzamelde informatie is er voor de verwerking van gegevens door instellingen of diensten voor wetenschappelijk onderzoek of statistiek. Dan moeten wel de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt.⁹⁷ Een open data-aanbieder zal echter niet aan deze voorwaarde kunnen voldoen en kan zich daarom niet op deze uitzonderingsgrond beroepen.

In sommige gevallen is de informatie over de identiteit en de verwerkingsdoeleinden van de verwerker onvoldoende om de betrokkene inzicht te geven in de gegevensverwerking. De Wbp verplicht dan tot de verstrekking van nadere informatie.⁹⁸

2.4.8 Melding aan CBP

Geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens dienen gemeld te worden bij het CBP of de functionaris voor de gegevensbescherming alvorens er tot verwerking van persoonsgegevens wordt overgegaan.⁹⁹ Het CBP wordt zo in staat gesteld de verwerking van persoonsgegevens te controleren. Een open data-aanbieder zal, als hij persoonsgegevens verwerkt, dat geheel of gedeeltelijke geautomatiseerd doen. De open data-aanbieder hoeft echter niet elke verwerkingshandeling afzonderlijk te melden.¹⁰⁰ Hij kan het geheel van samenhangende verwerkingshandelingen melden om aan de meldingsplicht te voldoen.

Worden de regels omtrent het doen van een melding aan het CBP niet nageleefd, dan kan het CBP daarvoor een bestuurlijke boete opleggen aan de open data-aanbieder.¹⁰¹ Ook wordt het overtreden van deze regels in de Wbp als een strafbaar feit aangemerkt waarvoor een geldboete van de tweede categorie (3.350 euro) kan worden opgelegd.¹⁰² Als de regels opzettelijk worden overtreden dan kan er zelfs een gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie (6.700 euro) worden opgelegd.¹⁰³

⁹³ Artikel 33 lid 1 Wbp.

⁹⁴ Voorbeeld ontleend aan *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 152.

⁹⁵ Artikel 34 lid 1 Wbp.

⁹⁶ Artikel 34 lid 4 Wbp.

⁹⁷ Artikel 44 lid 1 Wbp.

⁹⁸ Artikelen 33 lid 3 en 34 lid 3 Wbp.

⁹⁹ Artikel 27 lid 1 Wbp.

¹⁰⁰ *Kamerstukken II 1997-1998*, 25 892, nr. 3, p. 133.

¹⁰¹ Artikel 66 Wbp.

¹⁰² Artikel 75 lid 1 Wbp.

¹⁰³ Artikel 75 lid 2 Wbp.

Zowel het CBP als de functionaris voor de gegevensbescherming houden een register bij van aangemelde gegevensverwerkingen.¹⁰⁴ Deze registers kunnen door een ieder kosteloos worden geraadpleegd.¹⁰⁵

Een melding bevat een opgave van:¹⁰⁶

- de naam en het adres van de verantwoordelijke (zodat contact opgenomen kan worden met de verwerker);
- het doel of de doeleinden van de verwerking;
- een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben;
- de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;
- de voorgenomen doorgiften van gegevens naar landen buiten de Europese Unie (zie sectie 2.7); en
- een algemene beschrijving om een voorlopig oordeel te kunnen geven over de gepastheid van de voorgenomen beveiligingsmaatregelen.

Bovendien moet de melding het doel of de doeleinden waarvoor de gegevens of de categorieën van gegevens zijn of worden verzameld beschrijven.¹⁰⁷

De Wbp voorziet in een vrijstelling van de meldingsplicht voor gevallen waarin het onwaarschijnlijk is dat de verwerking van persoonsgegevens een inbreuk op de fundamentele rechten en vrijheden van de betrokkene zal vormen.¹⁰⁸ Het Vrijstellingsbesluit Wbp bevat tal van doeleinden en categorieën van verwerkte gegevens waarvan melding onder bepaalde voorwaarden niet verplicht is. Het Vrijstellingsbesluit Wbp bevat echter geen vrijstellingen die van toepassing kunnen zijn op open data-aanbieders.

2.4.9 Voorafgaand onderzoek door CBP

In een aantal bijzondere gevallen stelt het CBP een voorafgaand onderzoek in naar de gegevensverwerking.¹⁰⁹ Het gaat dan om gevallen waarin:

- de verwerker een nummer ter identificatie van personen voor een ander doeleinde wordt gebruikt dan waarvoor het nummer specifiek bestemd is teneinde gegevens in verband te kunnen brengen met gegevens die worden verwerkt door een andere verantwoordelijke, tenzij het gebruik van het nummer wettelijk verplicht is;
- de verwerker voornemens is om gegevens vast te leggen op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen; of
- anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus de verwerker voornemens is strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken ten behoeve van derden.

Gedurende het onderzoek is de verwerker verplicht om de voorgenomen verwerking van persoonsgegevens op te schorten totdat het CBP zijn onderzoek heeft afgerond dan wel heeft besloten geen nader onderzoek in te stellen.¹¹⁰ Het voorafgaande onderzoek leidt tot een niet-bindende verklaring omtrent de rechtmatigheid van de verwerker. Deze verklaring ontslaat de verwerker niet van de plicht een eigen afweging te maken.¹¹¹

Van bovenstaande gevallen zal als het open data gaat echter niet snel sprake zijn.

¹⁰⁴ Artikel 30 Wbp.

¹⁰⁵ Het register van het CBP is raadpleegbaar op: http://www.cbweb.nl/Pages/ind_reg_meldreg.aspx.

¹⁰⁶ Artikel 28 lid 1 Wbp.

¹⁰⁷ Artikel 28 lid 2 Wbp.

¹⁰⁸ Artikel 29 lid 1 Wbp.

¹⁰⁹ Artikel 31 lid 1 Wbp.

¹¹⁰ Artikel 32 lid 2 Wbp.

¹¹¹ Hooghiemstra en Nouwt 2011, p. 123.

2.5 Rechten van de betrokkene

De Wbp voorziet behalve verplichtingen voor de verantwoordelijke en daarmee een open data-aanbieder ook in rechten voor de betrokkene (i.e. degene wiens persoonsgegevens het betreft). Deze rechten worden hieronder uiteengezet en toegepast op open data.

2.5.1 Recht op inzage en informatie

De betrokkene heeft het recht om 'vrijelijk en met redelijke tussenpozen' een verzoek om hem mede te delen of hem betreffende persoonsgegevens worden verwerkt, in te dienen bij de open data-aanbieder.¹¹² Inzage kan men dus alleen vragen in de eigen persoonsgegevens. In persoonsgegevens van anderen kan geen inzage worden gegeven.

Vrijelijk houdt in dat de betrokkene geen belang hoeft te stellen bij een informatieverzoek. De Hoge Raad verwoorde het als volgt: "de betrokkene kan bij het vragen van deze informatie volstaan met een verwijzing naar art. 35 Wbp en behoeft geen nadere redenen op te geven."¹¹³ Aan een verzoek om inzage stelt de Wbp geen vormvereisten. Het verzoek kan dus mondeling, schriftelijk, per fax en e-mail bij de open data-aanbieder worden ingediend.

Met redelijke tussenpozen impliceert dat de betrokkene de open data-aanbieder niet meer dan gemiddeld en noodzakelijk mag benaderen met informatieverzoeken. Als de betrokkene zich niet aan deze regel houdt dan kan de open data-aanbieder het verzoek afwijzen op grond van artikel 43 onder e Wbp. Dit artikel bevat een afwijzingsgrond ter bescherming van de betrokkene en rechten en vrijheden van anderen dan de betrokkene. Tegen een dergelijke beslissing kan een betrokkene op zijn beurt bezwaar instellen als de open data-aanbieder een bestuursorgaan is.¹¹⁴ In de overige gevallen kan de betrokkene een verzoekschrift indienen bij de rechtbank en zo zijn recht op inzage en informatie afdwingen.¹¹⁵

De open data-aanbieder moet binnen vier weken aan de betrokkene mededelen of hem betreffende persoonsgegevens worden verwerkt. De mededeling moet het volgende bevatten:

- en volledig overzicht van de verwerkte gegevens in een begrijpelijke vorm;
- een omschrijving van het doel of de doeleinden van de verwerking;
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën van ontvangers van de gegevens; en
- de beschikbare informatie over de herkomst van de gegevens.¹¹⁶

Als bovenstaande informatie betrekking heeft op een derde en de open data-aanbieder reden heeft om aan te nemen dat die derde bedenkingen zal hebben tegen het verstrekken van deze informatie, dan dient de open data-aanbieder deze derde in de gelegenheid te stellen om zijn zienswijze naar voren te brengen.¹¹⁷ Deze regel lijdt uitzondering als dit onmogelijk blijkt of een onevenredige inspanning van de verantwoordelijke kost.¹¹⁸

Instellingen of diensten voor wetenschappelijk onderzoek of statistiek mogen een inzageverzoek weigeren. Voorwaarde is wel dat de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden worden gebruikt.¹¹⁹ Een open data-aanbieder zal echter niet aan deze voorwaarde kunnen voldoen en kan zich daarom niet op deze uitzonderingsgrond beroepen.

2.5.2 Recht op verbetering, aanvulling, verwijdering en afscherming

Een betrokkene die inzage heeft gekregen in de hem betreffende persoonsgegevens kan als deze gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met de wet zijn, de verantwoordelijke open data-

¹¹² Artikel 35 lid 1 Wbp.

¹¹³ HR 29 juni 2007, *LJN* AZ4664 (Dexia).

¹¹⁴ Artikel 45 Wbp.

¹¹⁵ Artikel 46 Wbp.

¹¹⁶ Artikel 35 lid 2 Wbp.

¹¹⁷ Artikel 35 lid 3 Wbp.

¹¹⁸ Artikel 35 lid 3 Wbp.

¹¹⁹ Artikel 44 lid 1 Wbp.

aanbieder verzoeken om deze gegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen.¹²⁰

De open data-aanbieder dient binnen vier weken na ontvangst van het verzoek aan de betrokkene berichten of dan wel in hoeverre hij aan het verzoek voldoet. Weigert de open data-aanbieder het verzoek dan dient hij deze weigering met redenen te omkleden.¹²¹ Tegen weigering staat een bezwaarschriftprocedure¹²² dan wel verzoekschriftprocedure bij de rechtbank open.¹²³ Als de open data-aanbieder beslist tot verbetering, aanvulling, verwijdering of afscherming, dan moet hij dat zo spoedig mogelijk doen.¹²⁴

Omdat de open data-aanbieder de gegevens ook aan derden verstrekt, moet hij deze derden in beginsel in kennis stellen van de verbetering, aanvulling, verwijdering of afscherming. De open data-aanbieder hoeft dat niet te doen als blijkt dat dit onmogelijk is of een onevenredige inspanning kost.¹²⁵ Een open data-aanbieder kan zich waarschijnlijk op deze uitzonderingsgrond beroepen omdat de derden die gebruik maken van de gegevens niet bekend zullen zijn bij de open data-aanbieder. Dat is anders als de open data-aanbieder voor gebruik van de data registratie door de gebruikers vereist omdat de open data-aanbieder dan wel in staat is om contact te leggen met de open data-gebruikers.

2.5.3 Recht van verzet

Indien de gegevensverwerking plaatst vindt op grond van een van de hierna volgende verwerkingsgronden dan heeft de betrokkene het recht om verzet aan te tekenen:

- Artikel 8 onder e Wbp. De gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt; of
- Artikel 8 onder f Wbp: De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt.

Als een open data-aanbieder de verwerking van persoonsgegevens baseert op het eigen belang dat hij heeft of het belang van anderen dan hebben betrokkenen het recht op verzet aan te tekenen. Een betrokkene moet zich dan voor een succesvol verzet kunnen beroepen op zijn bijzondere omstandigheden.¹²⁶ De open data-aanbieder beoordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Als de open data-aanbieder het verzet gerechtvaardigd acht dan dient hij de verwerking van persoonsgegevens terstond te beëindigen.¹²⁷

Als het verzet door de open data-aanbieder wordt afgewezen kan de betrokkene met een bezwaarschriftprocedure¹²⁸ of verzoekschriftprocedure bij de rechtbank zijn gelijk proberen te halen.¹²⁹

2.6 Bijzondere persoonsgegevens

2.6.1 Verbod op verwerken bijzondere persoonsgegevens

In beginsel verbiedt de Wbp de verwerking van bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn:

- Persoonsgegevens betreffende iemands godsdienst of levensovertuiging;
- Persoonsgegevens betreffende iemands ras;
- Persoonsgegevens betreffende iemands politieke gezindheid;
- Persoonsgegevens betreffende iemands gezondheid;

¹²⁰ Artikel 36 lid 1 Wbp.

¹²¹ Artikel 36 lid 2 Wbp.

¹²² Artikel 45 Wbp.

¹²³ Artikel 46 Wbp.

¹²⁴ Artikel 36 lid 3 Wbp.

¹²⁵ Artikel 38 lid 1 Wbp.

¹²⁶ Artikel 40 lid 1 Wbp.

¹²⁷ Artikel 40 lid 2 Wbp.

¹²⁸ Artikel 45 Wbp.

¹²⁹ Artikel 46 Wbp.

- Persoonsgegevens betreffende iemands seksuele leven;
- 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.¹³⁰

2.6.2 Uitzonderingen

De Wbp voorziet in uitzonderingsgronden waarin het verwerken van bijzondere persoonsgegevens toch is toegestaan. Het is van belang om op te merken dat deze uitzonderingsgronden de verwerking niet zonder meer legitimeren, maar slechts het verbod opheffen. De voorwaarden beschreven in sectie 2.4 en het algemene principe dat gegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt blijven ook na opheffing van het verbod van toepassing.¹³¹ De Wbp biedt zowel een algemene uitzonderingsgrond als een aantal concrete uitzonderingsgronden. Het verbod om bijzondere persoonsgegevens te verwerken is niet van toepassing als:

- dit geschiedt met uitdrukkelijke toestemming van de betrokkene;
- de gegevens door de betrokkene duidelijk openbaar zijn gemaakt;
- dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;
- dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting of;
- dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend. Het CBP kan bij de verlening van ontheffing beperkingen en voorschriften opleggen.¹³²

Ook als er bijzondere persoonsgegevens worden verwerkt ten behoeve van wetenschappelijk onderzoek of statistiek kan een verantwoordelijke zich op een uitzonderingsgrond beroepen.¹³³ Het onderzoek of de statistiek moet dan wel aan de volgende vereisten voldoen:

- Het onderzoek dient een algemeen belang;
- De verwerking is noodzakelijk voor het betreffende onderzoek of de betreffende statistiek;
- Het vragen van uitdrukkelijke toestemming is onmogelijk of kost een onevenredige inspanning kost; en
- Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Hoewel bepaalde open data waarschijnlijk voor statistische of wetenschappelijke doeleinden gebruikt zal worden, kan een open data-aanbieder zich waarschijnlijk niet op deze uitzonderingsgrond beroepen. Het hergebruik van de open data is immers niet aan voorwaarden gebonden en zal niet uitsluitend voor statistische of wetenschappelijke doelen plaatsvinden.

Behalve deze algemene uitzonderingsgronden, biedt de Wbp meer concrete aan specifieke voorwaarden gebonden uitzonderingsgronden. Deze uitzonderingsgronden hebben onder andere betrekking op:

- Het verwerken van persoonsgegevens betreffende iemands godsdienst of levensovertuiging door kerkgenootschappen;¹³⁴
- Het verwerken van persoonsgegevens betreffende iemands etniciteit ter uitvoering van een voorkeursbeleid;¹³⁵
- Het verwerken van persoonsgegevens betreffende iemands politieke gezindheid door politieke instellingen.¹³⁶
- Het verwerken van persoonsgegevens betreffende iemands gezondheid door hulpverleners.¹³⁷

Geen van de specifieke uitzonderingsgronden in het Vrijstellingsbesluit Wbp is van toepassing op open data-aanbieders.

¹³⁰ Artikel 16 Wbp.

¹³¹ *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 101.

¹³² Artikel 23 lid 1 Wbp.

¹³³ Artikel 23 lid 2 Wbp.

¹³⁴ Artikel 17 lid 1 onder a Wbp.

¹³⁵ Artikel 18 onder b Wbp.

¹³⁶ Artikel 19 lid 1 onder a Wbp.

¹³⁷ Artikel 21 lid 1 onder a Wbp.

2.7 Grensoverschrijdend gegevensverkeer

Het doorgeven van persoonsgegevens naar landen buiten de Europese Unie is in beginsel verboden. Persoonsgegevens mogen wel naar een land buiten de Europese Unie worden doorgegeven indien in dat land een passend beschermingsniveau biedt.¹³⁸ De Wbp biedt aanknopingspunten om te beoordelen of er sprake is van een 'passend beschermingsniveau'. Er moet gelet worden op de omstandigheden van het geval, in het bijzonder op:

- de aard van de gegevens;
- het doeleinde of de doeleinden;
- de duur van de voorgenomen verwerking of verwerkingen;
- het land van herkomst en het land van eindbestemming;
- de algemene en sectorale rechtsregels die in het betrokken derde land gelden; en
- de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.¹³⁹

Als een land geen passend beschermingsniveau biedt is het onder een van de volgende voorwaarden toch toegestaan om persoonsgegevens naar dat land door te geven:

- de betrokkene uitdrukkelijk zijn ondubbelzinnige toestemming voor de doorgifte heeft gegeven;
- de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- de doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst;
- de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht;
- de doorgifte noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of
- de doorgifte geschiedt vanuit een register dat bij wettelijk voorschrift is ingesteld en dat door een ieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, voor zover in het betrokken geval is voldaan aan de wettelijke voorwaarden voor raadpleging.

Ook kan de Minister van Justitie na advisering door het CBP een vergunning verlenen voor het doorgeven van bepaalde gegevens aan landen die geen passend beschermingsniveau bieden.¹⁴⁰

Het Europees Hof van Justitie heeft uitgemaakt dat het plaatsen van persoonsgegevens op een internetpagina die voor een ieder toegankelijk is – en dus ook voor personen in derde-landen - geen doorgifte is in de zin van de Wbp.¹⁴¹ Ook het CBP is van oordeel dat er in dergelijke gevallen geen sprake is van verboden doorgifte naar niet-EU landen.¹⁴²

Open data wordt op websites aangeboden die voor iedereen toegankelijk zijn. Hoewel de aangeboden gegevens ook toegankelijk zijn voor personen buiten de EU, is er gelet op de uitspraak van het Europees Hof van Justitie en de richtsnoeren van het CBP geen sprake van doorgifte naar niet-EU landen. Het aanbieden van open data die persoonsgegevens bevatten, is daarom niet verboden wegens doorgifte naar niet-EU landen.

¹³⁸ Artikel 76 lid 1 Wbp.

¹³⁹ Artikel 76 lid 2 Wbp.

¹⁴⁰ Artikel 77 lid 2.

¹⁴¹ HvJEG 6 november 2003, *PbEG* 2004, C-7.

¹⁴² College Bescherming Persoonsgegevens 2007, p. 49.

3 Conclusie

3.1 Persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) heeft betrekking op de verwerking van *persoonsgegevens*. Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Als er door de open data-aanbieder direct identificerende gegevens worden aangeboden, zoals namen en adressen, dan is er sprake van persoonsgegevens en zal men zich in het open data-project moeten houden aan de regels die de Wbp stelt.

Ook gegevens die een persoon indirect identificeren kunnen een persoonsgegeven zijn. Dergelijke gegevens kunnen zijn ontdaan van een naam, maar door combinatie met andere gegevens toch met een bepaalde persoon in verband worden gebracht. Voorbeelden zijn telefoonnummers en combinaties van postcodes met huisnummers. Van belang is of de identiteit van een persoon er redelijkerwijs, zonder onevenredige inspanning, mee kan worden vastgesteld. Het is niet doorslaggevend of de persoon daadwerkelijk door de gegevens is geïdentificeerd. Ook is het van belang of gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Als dit het geval is, zullen deze gegevens moeten worden aangemerkt als persoonsgegevens. Niet geaggregeerde of geanonimiseerde energieverbruikgegevens moeten als persoonsgegeven worden aangemerkt. Op de verwerking van deze gegevens is de Wbp van toepassing.

3.2 Open data-aanbieders mogen geen persoonsgegevens aanbieden

Als Alliander persoonsgegevens aanbiedt dan moet zij daarvoor een rechtmatige verwerkingsgrond hebben. Persoonsgegevens kunnen mogelijk als open data worden aangeboden op grond van het belang dat Alliander of een derde heeft. Het belang van betrokkenen en hun fundamentele rechten en vrijheden mogen zich dan niet tegen het aanbieden als open data verzetten. Of Alliander zich op deze verwerkingsgrond kan beroepen is afhankelijk van haar belangen of die van derden zich verhouden tot de belangen van betrokkenen. Als Alliander zich niet op deze verwerkingsgrond kan beroepen dan zal er voor het aanbieden van de persoonsgegevens toestemming van betrokkenen gevraagd moeten worden.

Toestemming van betrokkenen is echter ook niet zaligmakend. Alliander zal ook na toestemming van betrokkenen moeten voldoen aan de voorwaarden die de Wbp aan de verwerking van persoonsgegevens stelt. Alliander zal niet aan alle vereisten kunnen voldoen.

In de eerste plaats levert het idee van open data wrijving op met de eis van minimaal en toereikend verwerken. In Wbp is de regel neergelegd dat persoonsgegevens niet verder worden verwerkt dan noodzakelijk is voor het gestelde doel. Deze regel strekt tot minimalisering van de verwerking van persoonsgegevens. Open data-aanbieders hebben daarentegen een onbeperkt aanbod en gebruik van (persoons)gegevens voor ogen en dat levert strijd op met de eis van minimaal verwerken.

In de tweede plaats verhoudt de open data-filosofie zich niet met de eis van een welbepaald doeleinde. Open data wordt onvoorwaardelijk aan iedereen aangeboden. Deze doelstelling is onvoldoende welbepaald om een toetsingskader voor de rechtmatigheid van de verwerking te kunnen vormen. Alliander zal daarom niet aan deze eis kunnen voldoen.

Wij raden het aanbieden van persoonsgegevens als open data om bovenstaande redenen af.

3.3 Wel geaggregeerde of geanonimiseerde persoonsgegevens

Alliander kan persoonsgegevens wel in geaggregeerde of geanonimiseerde vorm aanbieden. Geanonimiseerde of geaggregeerde gegevens zijn in de regel geen persoonsgegevens. De Wbp is niet van toepassing op het aanbieden van dergelijke data.

Het is belangrijk om te constateren het aggregeren of anonimiseren van persoonsgegevens geen garantie is voor onherleidbaarheid van de persoonsgegevens. Aangeboden open data kunnen door com-

binatie met andere gegevens toch persoonsgegevens zijn. Het is van belang daarmee rekening te houden bij het anonimiseren en aggregeren van gegevens.

De Wbp is wel van toepassing op het proces van anonimiseren en aggregeren als zodanig. Voor het ontdoen van identificerende kenmerken is dus een geldige verwerkingsgrond nodig en moet er aan het bepaalde in de Wbp voldaan worden.

Als Alliander overweegt bepaalde persoonsgegevens te aggregeren en deze als open data aan te bieden, dan loont het om uit te zoeken of deze gegevens ook langs een andere weg dan door aggregatie van persoonsgegevens kunnen worden verkregen. Zo kan in plaats van het aggregeren van individuele meetgegevens gekozen worden voor een meetgegeven dat door Alliander op meetstation- of wijk-niveau wordt verzameld. Er worden dan geen persoonsgegevens verwerkt en Alliander hoeft zich dan ook niet aan het in de Wbp gestelde te houden.

Indien het niet mogelijk is om bepaalde (meet)gegevens langs een andere weg te verkrijgen, zal er in het geval van meetgegevens sprake zijn van persoonsgegevens en is de Wbp van toepassing.

4 Rechtspraak

4.1 Nederland

CRvB 10 juli 2008, *LJN* BD8026.
 HR 29 juni 2007, *LJN* AZ4664 (Dexia).
 Rb. Zwolle-Lelystad 21 februari 2006, *LJN* AV3139.
 Vزر. Rb. Zwolle 22 maart 2004, *LJN* AO6018.
 HvJEG 6 november 2003, *PbEG* 2004, C-7.

4.2 Documenten CBP

CBP 23 maart 2011, z2010-0146.
 CBP 3 mei 2006, z2005-0846.
 CBP 12 september 2005, z2005-0598.
 CBP 3 juni 2005, z2004-1185.

4.3 Documenten Artikel 29 Werkgroep

Opinion 15/2011 on the definition of consent, WP 187.
 Advies 12/2011 over slimme meters, WP 183.
 Advies 4/2007 over het begrip persoonsgegevens, WP 136.
 Working document on data protection issues related to RFID technology, WP 105.

4.4 Literatuur

Attema & De Nood 2010

J. Attema & D. de Nood, *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit*, WRR-webpublicatie nr. 47.

Berkvens & Prins 2007

J. Berkvens & C. Prins, *Privacyregulering in Theorie en Praktijk*, Deventer: Kluwer 2007.

College Bescherming Persoonsgegevens 2005

College Bescherming Persoonsgegevens, *Convenant gegevensuitwisseling Nuon/GGD*, z2005-059.

College Bescherming Persoonsgegevens 2007

College Bescherming Persoonsgegevens, *Richtsnoeren publicatie van persoonsgegevens op internet*, december 2007.

Hooghiemstra & Nouwt 2011

T.F. Hooghiemstra & S. Nouwt, *Sdu Commentaar Wet bescherming persoonsgegevens*. Den Haag: Sdu Uitgevers 2011.

Koffijberg et al. 2009

J. Koffijberg, S. Dekkers, G. van Homburg & B. van den Berg, *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan Beleidsonderzoek 2009.

Korff 2010

D. Korff, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, study commissioned by the European Commission.

Murray-Rust 2008

P. Murray-Rust, 'Open data in science', *Serials Review* 1, p. 52-64.

Narayanan & Shmatikov 2008

A. Narayanan & V. Shmatikov, 'Robust de-anonymization of large sparse datasets', IEEE Symposium on Security and Privacy, 2008, p. 111-125.

O'Hara 2011

K. O'Hara, *Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office*.

Klingenberg 2011

A.E. Klingenberg, Bestuursrecht, e-mail en internet. Bestuursrechtelijke aspecten voor elektronische overheidscommunicatie, Dissertatie:
<http://dissertations.ub.rug.nl/faculties/jur/2011/a.m.klingenberg/>

Registratiekamer 1996

Registratiekamer. Credit Scoring Database, juni 1996

Simpson 2011

A.C. Simpson, 'On privacy and public data: a study of data.gov.uk', *Journal of Privacy and Confidentiality* 2011-1, p. 4.

The Task Force Smart Grids Expert Group 2 2011

The Task Force Smart Grids Expert Group 2, Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection (draft 3 June 2011).

Verhue 2007

D. Verhue, *Nationaal vrijheidsonderzoek – opiniedeel*, Amsterdam: Veldkamp/Comité 4 en 5 mei 2007.

Westin 1967

A. Westin, *Privacy and freedom*, New York: Atheneum 1967.

4.5 Kamerstukken

Kamerbrief Hergebruik en Open Data: naar betere vindbaarheid en herbruikbaarheid van overheidsinformatie, *Kamerstukken II* 2010/11, 32 802, nr. 2.

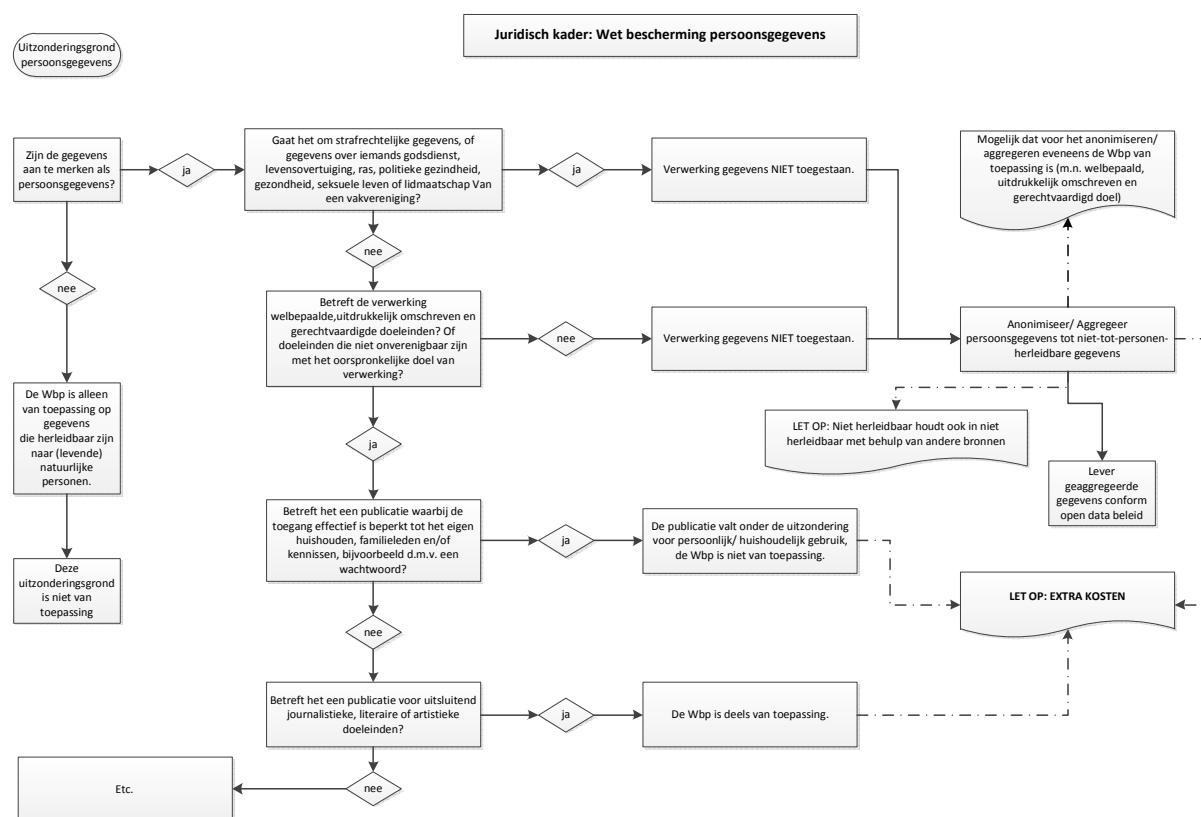
Memorie van Toelichting bij De Wet BAG, *Kamerstukken II* 2006/07, 30 968, nr. 3

Memorie van Toelichting bij de Wet bescherming persoonsgegevens, *Kamerstukken II* 1997-98, 25 892, nr. 3 (MvT).

Kamerstukken 25892 nr. 6, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) Nr. 6 NOTA NAAR AANLEIDING VAN HET VERSLAG, Ontvangen 2 december 1998.

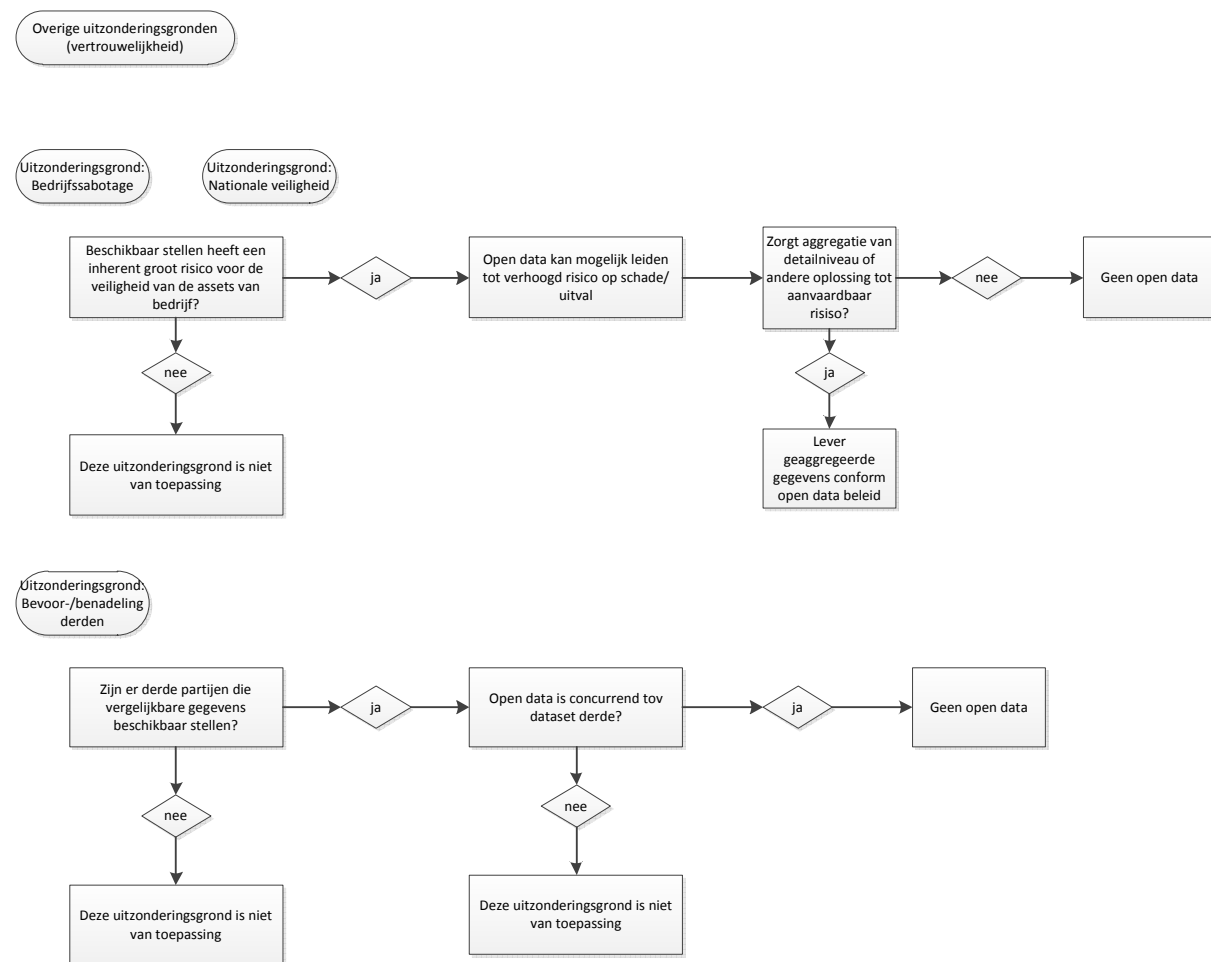
Eerste Kamer, vergaderjaar 1999–2000, 25 892, nr. 92c, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) MEMORIE VAN ANTWOORD, Ontvangen 19 mei 2000.

5 Bijlage Stroomschema Persoonsgegevens



143

¹⁴³ Op basis van: http://www.cbppweb.nl/downloads_rs/rs_conc_actieve_openbaarmaking.pdf



Onderzoeksinstituut OTB

Delft University of Technology

Jaffalaan 9, 2628 BX Delft, The Netherlands

Postbus 5030, 2600 GA Delft, The Netherlands

Telefoon +31 (0)15 278 30 05

Fax +31 (0)15 278 44 22

E-mail mailbox@otb.tudelft.nl

www.otb.tudelft.nl