COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AANGETEKEND alsmede per gewone post

AAN GVB Exploitatie B.V.
T.a.v. de directie
Postbus 2131
1000 CC AMSTERDAM

DATUM 25 november 2011
ONS KENMERK z2011-00637
CONTACTPERSOON

UW BRIEF VAN 20 juli en 13 september 2011
UW KENMERK 42486/SEN/743311 en
42486/HVR/sen/753858

ONDERWERP Beslissing op bezwaar

Geachte directie,

Het College bescherming persoonsgegevens (*CBP*) heeft tijdens het collegeoverleg van 22 november 2011 een beslissing genomen naar aanleiding van het bezwaarschrift van GVB Exploitatie B.V. (*GVB*) van 20 juli 2011, aangevuld bij brief van 13 september 2011. Hieronder volgen de beslissing en de motivering.

1. Het verloop van de bezwaarschriftprocedure

Onderzoek
Uit dit onderzoek is onder meer naar voren gekomen dat GVB persoonsgegevens langer bewaart dan noodzakelijk is en daarmee in strijd handelt met artikel 6 jo 10 Wet bescherming persoonsgegevens (*Wbp*).

Rapport definitieve bevindingen
Naar aanleiding van voornoemde onderzoeken heeft het CBP op 2 december 2010 het rapport definitieve bevindingen betreffende GVB vastgesteld.

Dwangsombesluit
Het CBP heeft GVB bij brief van 9 februari 2011 in kennis gesteld van zijn voornemen om handhavend op te treden. GVB heeft haar zienswijze op dit voornemen geuit tijdens de hoorzitting van 15 maart 2011. Bij besluit van 9 juni 2011 heeft het CBP GVB een last onder dwangsom opgelegd, hierna 'het bestreden besluit', waarin GVB verplicht wordt een aantal in het bestreden besluit beschreven bewaartermijnen te implementeren.

Bezwaar GVB
GVB heeft bij brief van 20 juli 2011 pro forma bezwaar gemaakt tegen het bestreden besluit. Op 25 juli 2011 heeft het CBP een termijn gesteld voor het indienen van de gronden van het bezwaar. Bij brief van 27 juli 2011 heeft GVB het CBP verzocht in te stemmen met rechtstreeks beroep. Desgevraagd heeft het CBP per e-mail van 22 augustus 2011 laten weten dat het op dit verzoek zal beslissen nadat de gronden van het bezwaar zijn ingediend. De gronden van het bezwaar zijn ingediend bij brief van 13 september 2011. Bij

brief van 27 september 2011 heeft het CBP medegedeeld dat het niet instemt met rechtstreeks beroep.

Het CBP heeft GVB bij brief van 3 oktober 2011 uitgenodigd voor een hoorzitting op 25 oktober 2011. GVB heeft op 4 oktober 2011 laten weten af te zien van het recht te worden gehoord. Bij brief van 21 oktober 2011 heeft het CBP de beslissing op bezwaar verdaagd voor ten hoogste zes weken.

2. De inzet van het bezwaar

GVB heeft – kort weergegeven – de volgende gronden aan haar bezwaar ten grondslag gelegd:

2.1 Primair: geen persoonsgegevens, Wbp niet van toepassing

GVB stelt zich op het standpunt dat transactiegegevens met de studenten OV-chipkaart geen persoonsgegevens zijn in de zin van de Wbp en de Wbp daarom niet van toepassing is. GVB heeft in dit verband aangevoerd dat de identificerende gegevens van de studenten bij TLS bevinden en GVB geen toegang heeft tot die gegevens en dus niet tot identificatie in staat is.

2.2 Subsidiair: strijd met het vertrouwensbeginsel

GVB heeft subsidiair aangevoerd dat, voor zover de transactiegegevens met de studenten OV-chipkaart toch zouden kwalificeren als persoonsgegevens, het vertrouwensbeginsel aan handhaving door het CBP in de weg staat. GVB wijst er in dat verband op dat het CBP naar haar oordeel in het bestreden besluit een ruimer begrip 'persoonsgegevens' hanteert dan ten tijde van het onderzoek in 2007 naar de verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij GVB.

2.3 Overige argumenten

2.3.1 Verantwoordelijke

Aangezien naar het oordeel van GVB de transactiegegevens met betrekking tot de studenten OV-chipkaart geen persoonsgegevens zijn, is de Wbp niet van toepassing op de gegevensverwerking en kwalificeert GVB ook niet als 'verantwoordelijke' in de zin van de Wbp.

2.3.2 Kosten

GVB verzoekt het CBP de kosten die zij redelijkerwijs in verband met de behandeling van het bezwaar maakt, te vergoeden op basis van artikel 7:15 Algemene wet bestuursrecht (*Awb*).

3. Beoordeling van het bezwaar

Het CBP stelt vast dat het bezwaar tijdig is ingediend en voorts voldoet aan de eisen van artikel 6:5 Awb, zodat het ontvankelijk is. Ingevolge artikel 7:11, eerste lid, Awb vindt op grondslag van het bezwaar een heroverweging plaats van het bestreden besluit. Bij deze heroverweging staat de vraag centraal of het CBP terecht en op goede gronden bij besluit van 9 juni 2011 heeft besloten GVB een last onder dwangsom op te leggen.

Het CBP beoordeelt de gronden van bezwaar als volgt.

3.1 Persoonsgegevens

Het CBP heeft in het bestreden besluit vastgesteld dat de volgende gegevens in combinatie met elkaar moeten worden beschouwd als persoonsgegevens:

- Chip-ID;
- Device-ID (apparaatnummer waarop de transactie plaatsvond en op basis waarvan door het systeem het afgelegde traject wordt bepaald);
- Soort abonnement;
- Soort transactie (check-in/check-uit);
- Datum en tijdstip transactie;
- Het saldo voor en na de transactie alsmede de transactiewaarde,

hierna gezamenlijk: 'transactiegegevens'.

Artikel 1, aanhef en onder a, Wbp luidt als volgt:

In de wet en de daarop berustende bepalingen wordt verstaan onder persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon

Dit artikel vormt een implementatie van artikel 2, aanhef en onder a, van de Richtlijn bescherming persoonsgegevens 95/46/EG dat als volgt luidt:

In de zin van deze richtlijn wordt verstaan onder 'persoonsgegevens', iedere informatie betreffende een geïdentificeerde of identificeerbare persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit (in de Engelse versie: 'identity') (onderstreping toegevoegd).

Overweging 26 van Richtlijn 95/46/EG luidt als volgt:

Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet

worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is; dat gedragscodes in de zin van artikel 27 een nuttig instrument kunnen zijn om een indicatie te geven omtrent de middelen waarmee de gegevens anoniem kunnen worden gemaakt en kunnen worden bewaard in een vorm die identificatie van de betrokkene niet langer mogelijk maakt.

GVB heeft zich op het standpunt gesteld dat de transactiegegevens niet kunnen worden aangemerkt als persoonsgegevens zoals bedoeld in artikel 1, sub a, Wbp. Hiertoe voert GVB aan dat de houders van de studenten OV-chipkaart niet kunnen worden geïdentificeerd door GVB, aangezien alleen de Dienst Uitvoering Onderwijs (*DUO*) en TLS beschikken over identificerende gegevens van de student en die gegevens worden afgeschermd voor GVB. GVB heeft derhalve geen toegang tot de NAW-gegevens van de student, waardoor GVB niet in staat is de transactiegegevens te herleiden tot een persoon.

Het CBP overweegt ten aanzien van dit standpunt als volgt. Een gegeven is te beschouwen als persoonsgegeven als het informatie verschaft over een geïdentificeerde of identificeerbare persoon. Deze persoon kan direct identificeerbaar zijn, bijvoorbeeld aan de hand van zijn naam, adres of geboortedatum. Maar ook een indirect identificeerbaar gegeven kan een persoonsgegeven zijn, bijvoorbeeld indien een persoon aan de hand van een identificatienummer kan worden geïdentificeerd.

3.1.1 Identificatie zonder achterhalen van de naam

Identificatie kan ook plaats vinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In dit verband wijst het CBP op de volgende passage uit Advies 4/2007 van de Artikel 29-werkgroep:

Hier moet worden opgemerkt dat hoewel identificatie door middel van naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook dat van de gebruiker daarvan. De persoonlijkheid van de betrokkene kan op deze wijze worden achterhaald, zodat bepaalde besluiten aan hem of haar kunnen worden toegeschreven. Zonder zelfs maar naar de naam en het adres van de persoon te vragen, kan de betrokkene worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde beslissingen aan hem of haar worden toegeschreven, omdat het voor het contactpunt voor de persoon (de computer) niet langer noodzakelijk is zijn of haar identiteit in enge zin bekend te maken. Met andere woorden, de identificatie van een persoon vereist niet langer het

vermogen zijn of haar naam te achterhalen. De definitie van ' persoonsgegeven' weerspiegelt ook dit feit.[1] (onderstreping toegevoegd)

In gevallen waarin het op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen één bepaalde persoon te onderscheiden, kan die persoon wellicht toch "identificeerbaar" zijn doordat aan de hand van die informatie in combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) de betrokkene van andere personen kan worden onderscheiden. [2]

Van belang is dus of de betrokkene van andere personen kan worden onderscheiden, met andere woorden: of de betrokkene 'individualiseerbaar' is. Wanneer een betrokkene individualiseerbaar is, kunnen er aan de hand van de gegevens beslissingen worden genomen die de betrokkene direct raken. Juist dit aspect wordt in de Memorie van Toelichting bij de Wbp van belang geacht:

Als gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt.[3]

Het verwerken van gegevens over een geïndividualiseerd persoon kan vergaande privacy-implicaties hebben, ook als het niet mogelijk is om een naam te verbinden aan de gegevens. Het is daarom van belang dat ook bij dergelijke gegevens de waarborgen van de Wbp gelden en dat betrokkenen in staat worden gesteld om inzicht te hebben in en zeggenschap te hebben over de beslissingen die aan de hand van die gegevens over hen worden genomen.

Juist de individualiseerbaarheid brengt immers mee dat er op basis van de gegevens beslissingen over een persoon kunnen worden genomen die hem raken in het maatschappelijk verkeer. Dat kan vergaande consequenties hebben voor een persoon. Zo kan een IP-adres toegang tot een bepaalde website geweigerd worden, zonder dat men weet wie er precies achter het IP-adres zit. Mede daarom is door zowel de Artikel 29-werkgroep als het CBP bepaald dat een IP-adres altijd als persoonsgegeven moet worden behandeld.[4]

Wanneer gegevens gekoppeld worden aan een uniek nummer, is doorgaans sprake van een geïndividualiseerd persoon. De hiervoor geciteerde definitie van persoonsgegevens in de Richtlijn noemt het gebruik van een identificatienummer dan ook als belangrijk element voor de vraag of sprake is van identificeerbaarheid. Ook hier is niet het achterhalen van de naam van de betrokkene van belang, maar de vraag naar de mogelijke gevolgen voor de behandeling van een onderscheiden betrokkene. Juist het gebruik van een identificatienummer kan immers tot gevolg hebben dat de gegevens bepalend zijn voor de wijze waarop de betrokkene in het maatschappelijk verkeer wordt beoordeeld of behandeld. In de Wbp (artikel 31 en 24) en de Memorie van Toelichting is dan ook speciale aandacht voor identificatienummers.

---

[1] Advies 4/2007, p. 14 en 15.
[2] Advies 4/2007, p. 14.
[3] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46.
[4] Unieke nummers toegekend aan een computer om via internet te communiceren. Zie advies 4/2007 van de Artikel 29-werkgroep en de richtsnoeren publicatie van persoonsgegevens op internet van het CBP.

Uit een oogpunt van bescherming van de persoonlijke levenssfeer werd het noodzakelijk geacht om aan het gebruik van dergelijke nummers beperkingen te stellen. Vast staat immers dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen.[5]

De OV-chipkaart is door middel van het unieke Chip-ID verbonden aan de persoon van de student. De transactiegegevens die GVB verwerkt als met de OV-chipkaart wordt gereisd, geven gedetailleerde informatie over het reisgedrag van de kaarthouder. Zo is af te leiden wanneer, waar en hoe vaak de student aan wie de kaart is uitgegeven reist. Deze gegevens bieden inzage in het leefpatroon van de student en ze kunnen worden gebruikt op een wijze die van invloed is op de bejegening van de kaarthouder in het maatschappelijk verkeer.[6] Het CBP wijst in dit verband tevens naar de in de Memorie van Toelichting bij de Wbp geciteerde uitspraken van de Registratiekamer waarin telefoonnummers en kentekens van auto's als persoonsgegevens worden aangemerkt.[7] Verder worden ook IP-adressen[8] en geolocatiegegevens op smartphones[9] als persoonsgegevens beschouwd. In deze gevallen gaat het eveneens om gegevens zonder direct identificerende elementen, welke gegevens informatie verschaffen over (het gedrag van) een persoon en die via een uniek nummer in verband kunnen worden gebracht met die persoon. Deze gegevens kunnen van invloed zijn op de wijze waarop de betrokkene in het maatschappelijk verkeer wordt bejegend en zijn aldus als persoonsgegevens aan te merken.

3.1.2 Daadwerkelijke identificatie door GVB

Daar komt nog bij dat GVB wel degelijk in staat moet worden geacht om de naam van de betrokkene te achterhalen en dat dat ook mede het doel is van de verwerking van de gegevens. GVB is op twee manieren in staat om de transactiegegevens te koppelen aan de persoon van de kaarthouder: (i) via het bestand met NAW-gegevens bij TLS en (ii) op het moment dat de student zelf contact met GVB opneemt. Het CBP zal hierna op beide mogelijkheden ingaan.

(i) Identificatie via TLS
TLS is opgericht door de vijf grootste OV-bedrijven en fungeert als een 'back-office' voor de OV-bedrijven. De aandelen zijn in het bezit van NS, RET, HTM en GVB. Het CBP heeft in het bestreden besluit vastgesteld dat TLS in staat is om met behulp van de Chip-ID de transactiegegevens te koppelen aan de persoon van de kaarthouder. Het feit dat de identificerende gegevens in het bezit zijn van TLS en niet van GVB, leidt - anders dan GVB in

[5] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 126.
[6] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46.
[7] *Kamerstukken II* 1997/98, 25 892, nr 3, p. 47.
[8] Unieke nummers toegekend aan een computer om via internet te communiceren. Advies 4/2007 van de Artikel 29-werkgroep en de richtsnoeren publicatie van persoonsgegevens op internet van het CBP. Ook in Rb Utrecht, 12 juni 2005, LJN:AT9073 en Hof Amsterdam 13 juni 2006:AY 3854 wordt aangenomen dat IP-adressen persoonsgegevens zijn.
[9] Opinion 13/2011 of the Article 29 Working Party on geolocation services on smart mobile devices.

bezwaar heeft aangevoerd - niet tot de conclusie dat er voor GVB geen sprake meer zou zijn van persoonsgegevens. Voor de vaststelling of een persoon identificeerbaar is moet blijkens bovengenoemde overweging 26 uit Richtlijn 95/46/EG immers worden gekeken naar *alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren.'*(onderstreping toegevoegd)

Ook als niet door de verantwoordelijke zelf, maar wel door derden (bijvoorbeeld door een ontvanger van de gegevens) identificatie kan plaatsvinden, is sprake van persoonsgegevens. Daar ging ook de Artikel 29-werkgroep van uit in haar opinie over de reikwijdte van het begrip 'persoonsgegevens':

In gevallen waarin het op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen één bepaalde persoon te onderscheiden, kan die persoon wellicht toch 'identificeerbaar' zijn doordat aan de hand van die informatie in combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) de betrokkene van andere personen kan worden onderscheiden. [10]

En specifiek met betrekking tot IP-adressen:

Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.[11]

Alleen indien de gegevens voor de verantwoordelijke niet met redelijkerwijs in te zetten middelen te identificeren zijn, is er geen sprake van persoonsgegevens. Hierbij moet blijkens de Memorie van Toelichting bij de Wbp rekening worden gehouden met de voortschrijdende informatietechnologie.[12] Gelet op de toegenomen mogelijkheden tot identificatie geldt in de meeste gevallen dat ook indien de identificerende gegevens in handen zijn van een derde het privacy-risico waartegen de Wbp beoogt bescherming te bieden nog steeds bestaat en er daarom van uit moet worden gegaan dat er ook voor de verantwoordelijke sprake is van persoonsgegevens.

Er kan uitsluitend niet meer worden gesproken van persoonsgegevens indien doeltreffende maatregelen zijn getroffen waardoor daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.[13] GVB beroept zich op een verklaring van PricewaterhouseCoopers (*PWC*) waarin PWC heeft verklaard dat GVB *via de bestaande technische koppelingen* geen toegang heeft tot of de beschikking over de NAW-gegevens van de kaarthouders

[10] Advies 4/2007, p. 14 en 15.
[11] Art. 29 WG, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008.
[12] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.
[13] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.

die zich bij TLS bevinden. In deze verklaring wordt niet ingegaan op andere wijzen waarop GVB toegang zou kunnen verkrijgen tot de NAW-gegevens van de studenten. Verder is niet gebleken dat er maatregelen zijn genomen om te waarborgen dat TLS geen identificerende gegevens over individuele kaarthouders aan GVB kan verstrekken.

In dit verband is relevant, zoals hierboven overwogen, dat TLS mede door GVB is opgericht, GVB mede-aandeelhouder is in TLS en er een nauwe samenwerking bestaat tussen TLS en GVB onder meer bij de afwikkeling van de vervoersovereenkomst. TLS kan derhalve niet worden beschouwd als een onafhankelijke derde partij. Tegen die achtergrond is de enkele verklaring van TLS tijdens de hoorzitting dat TLS geen medewerking aan GVB verleent om identificatie tot stand te brengen onvoldoende om in de praktijk te waarborgen dat identificatie niet kan plaatsvinden.

(ii) Identificatie bij contact met de betrokkene
Daarnaast geldt dat GVB ook in staat is om de transactiegegevens te koppelen aan de individuele student indien de betreffende student zelf contact opneemt met GVB met een vraag, klacht of een verzoek om restitutie.[14] Om het verzoek van de student te kunnen afhandelen zoekt GVB de transactiegegevens bij de betreffende persoon en vindt derhalve identificatie plaats. Het doel van de verwerking van de transactiegegevens is dus mede om in die gevallen de transactiegegevens aan de bijbehorende personen te kunnen koppelen. Het CBP wijst in dit verband op de volgende passage uit de opinie van de Artikel 29-werkgroep:

Nationale gegevensbeschermingsautoriteiten hebben te maken gehad met gevallen waarin enerzijds door de voor de verwerking verantwoordelijke werd aangevoerd dat slechts verspreide stukjes informatie werden verwerkt, zonder verwijzing naar een naam of een ander direct identificatiemiddel, en dat de gegevens niet als persoonsgegevens moesten worden beschouwd en daarom niet onder de regels voor gegevensbescherming vielen. Anderzijds heeft de verwerking van die informatie slechts nut als die het mogelijk maakt specifieke personen te identificeren en op een bepaalde wijze te behandelen. In dergelijke gevallen waarin het doel van de verwerking impliceert dat personen worden geïdentificeerd, kan worden verondersteld dat de voor de verwerking verantwoordelijke over 'redelijkerwijs in te zetten middelen' beschikt om de betrokkenen te identificeren.[15]

De opinie verwijst in dit verband naar het voorbeeld van videobewaking:

In die context wordt door de voor de verwerking verantwoordelijke vaak aangevoerd dat identificatie slechts zal plaatsvinden voor een gering percentage van het verzamelde materiaal en dat er dus vóór de identificatie in die paar gevallen plaatsvindt geen sprake is van verwerking van persoonsgegevens. Het doel van de videobewaking is echter de identificatie van de personen die op de videobeelden te zien zijn, in alle gevallen dat de voor de verwerking verantwoordelijke dat nodig acht. Het hele proces moet dan ook worden beschouwd als de verwerking van gegevens over identificeerbare personen. [16]

[14] Pleitnota GVB 15 maart 2011, p. 5. Zie ook de brief d.d. 21 april 2010 van GVB aan het CBP, p. 2 en de Gedragscode verwerking persoonsgegevens OV-chipkaart door OV-bedrijven, p. 14.
[15] Advies 4/2007 van de Artikel 29-werkgroep over het begrip persoonsgegeven, p. 16.
[16] Idem, p. 17.

Naast het feit dat identificatie mogelijk is met behulp van de middelen die in handen zijn van TLS, geldt derhalve dat GVB eveneens in staat is de kaarthouder te identificeren op het moment dat deze zelf contact opneemt met GVB.

Conclusie
Gelet op bovenstaande overwegingen is het CBP na heroverweging van het bestreden besluit van oordeel dat het terecht en op goede gronden heeft besloten dat transactiegegevens persoonsgegevens zijn in de zin van de Wbp.

3.2 Vertrouwensbeginsel

Anders dan GVB heeft aangevoerd, hanteert het CBP in het bestreden besluit geen ruimer begrip van 'persoonsgegevens' dan het deed ten tijde van het onderzoek naar de verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij GVB in 2007. Het CBP heeft in 2007 - onder meer - onderzoek gedaan naar de doeleinden en grondslagen van de verwerking van persoonsgegevens als bedoeld in artikel 7 en 8 Wbp met betrekking tot de aanvraag van een OV-chipkaart en het gebruik van de OV-chipkaart.

Een persoonsgebonden OV-chipkaart kon bij GVB worden aangevraagd middels een aanvraagformulier waarop de aanvrager onder meer zijn naam, adres, woonplaats, geboortedatum, geslacht, telefoonnummer en e-mailadres diende in te vullen. Ten tijde van de aanvraag van een OV-chipkaart verwerkte GVB alleen deze direct identificeerbare persoonsgegevens. De verwerking van transactiegegevens vond pas plaats op het moment dat de aanvrager de OV-chipkaart in gebruik had genomen.

Ten aanzien van het stadium van de *aanvraag* van een OV-chipkaart heeft het CBP in 2007 geconcludeerd dat GVB geen rechtmatige grondslag had voor het verwerken van persoonsgegevens voor een persoonsgebonden OV-chipkaart zonder product van GVB.[17] Aangezien GVB in dit stadium nog geen transactiegegevens verwerkte, had deze conclusie van het CBP alleen betrekking op de direct identificeerbare persoonsgegevens die op het aanvraagformulier werden ingevuld. Dat GVB en RET deze gegevens hebben verwijderd betekent echter *niet* dat het CBP de transactiegegevens die GVB in een later stadium verwerkt, niet als persoonsgegevens heeft aangemerkt.

Ook in het overige deel van het onderzoeksrapport van 2007, waarin het gaat om het gebruik van de OV-chipkaart, hanteerde het CBP geen enger begrip 'persoonsgegevens'. Het CBP heeft in dat gedeelte immers - onder meer - getoetst of de verwerking van *reisgegevens*[18] voldeed aan diverse bepalingen van de Wbp. Toetsing aan de Wbp is

[17] Behoudens de verwerking van bepaalde persoonsgegevens voor een éénmalige machtiging tot afschrijving van de aanschafkosten van de OV-chipkaart.
[18] Onder reisgegevens moet worden verstaan: transactiegegevens – check in/check-out – met locatie (dat wil zeggen gegevens over de datum en tijdstip van de reis en het afgelegde traject. Onderzoeksrapport Verwerking

vanzelfsprekend alleen mogelijk is als de betreffende gegevens worden aangemerkt als persoonsgegevens in de zin van de Wbp. Bovendien heeft het CBP expliciet geoordeeld dat het kaartnummer een identificeerbaar gegeven is en dat dit nummer, ingeval van een persoonsgebonden kaart, herleidbaar is tot natuurlijke personen:

Nadat marktanalyses hebben plaatsgevonden op basis van gegevens die ontdaan zijn van alle identificeerbare gegevens (dus ook het kaartnummer), kunnen (zonodig) doelgroepen worden benaderd.[19]

Dat chipkaartnummer is, overigens uitsluitend wanneer er sprake is van een persoonsgebonden kaart, herleidbaar tot natuurlijke personen.[20]

Tegen dezelfde achtergrond dienen de door GVB in haar aanvullend bezwaarschrift genoemde brieven aan RET van 18 december 2008 en aan de Staatssecretaris van Verkeer en Waterstaat van 6 november 2008 te worden gelezen. Zo blijkt uit de bijlage van de brief aan RET dat het CBP aan RET heeft gevraagd of zij alle persoonsgegevens heeft vernietigd die zijn vastgelegd *bij aanschaf* van een persoonsgebonden OV-chipkaart zonder product van RET.[21] Zoals hierboven is opgemerkt, worden bij de aanschaf van een OV-chipkaart alleen direct identificeerbare persoonsgegevens verwerkt en geen transactiegegevens.

Volgens GVB is een 'enge' definitie van het begrip 'persoonsgegevens' jarenlang de bestendige lijn van het CBP geweest. GVB wijst in dit verband naar de uitspraak betreffende de Chipknip.[22] Afgezien van het feit dat deze enkele uitspraak geen jarenlange bestendige lijn van het CBP omtrent de definitie van het begrip 'persoonsgegeven' met zich meebrengt, zoals door GVB aangevoerd, wordt in die uitspraak niet uitgegaan van een engere definitie van het begrip 'persoonsgegeven'. Uit de uitspraak blijkt dat de chip op de Chipknip de volgende gegevens bevatte: het kaartnummer, het saldo, de laatste tien uitgegeven bedragen, het referentienummer van de ondernemer/winkelier, de datum, het volgnummer van de transactie en de beveiligingssleutel. De ondernemer kon echter niet het kaartnummer inzien, maar slechts het saldo en de laatste tien transacties. Deze laatstgenoemde gegevens werden *op zichzelf* niet aangemerkt als herleidbare persoonsgegevens. Daarbij heeft het CBP uitdrukkelijk opgemerkt dat ervan wordt uitgegaan dat de gegevens in de betaalautomaat bij de winkelier niet voor de ondernemer toegankelijk zijn en ook niet vatbaar zijn voor andere bewerkingen door de ondernemer. De uitspraak van de Registratiekamer betreffende de Chipknip is dus niet vergelijkbaar met de onderhavige aangelegenheid, aangezien voor de ondernemer geen tot een persoon herleidbaar nummer zichtbaar was, terwijl GVB wel over een dergelijk nummer beschikt.

---

van persoonsgegevens ten behoeve van de OV-chipkaart bij het GVB te Amsterdam, december 2007, z2007-00096, p. 13.

[19] Idem, p. 16.

[20] Idem, p. 17.

[21] Bijlage bij de brief van 18 december 2008 (Z2008-01411), p. 1.

[22] Registratiekamer 21 februari 1996, 95.V.243.

Derhalve kan niet worden geconcludeerd dat het CBP in de uitspraak betreffende de Chipknip een engere definitie van het begrip 'persoonsgegevens' hanteerde dan in het bestreden besluit het geval is.

Voorts overweegt het CBP dat het vertrouwensbeginsel volgens vaste jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State een concrete en ondubbelzinnige toezegging van het bestuursorgaan vereist.[23] Daarvan is in de onderhavige aangelegenheid geen sprake. Het CBP heeft GVB immers schriftelijk noch mondeling medegedeeld dat GVB geen persoonsgegevens verwerkt ten aanzien van de studenten OV-chipkaart ingeval GVB de NAW-gegevens zou verwijderen, en evenmin dat het CBP niet handhavend zou optreden tegen geconstateerde overtredingen in dit kader. Ten overvloede overweegt het CBP dat volgens vaste jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State aan het vertrouwensbeginsel slecht beperkte betekenis toekomt in gevallen waarin belangen van derden een rol spelen.[24] Ten aanzien van de studenten OV-chipkaart geldt dat de belangen van de vele studenten die gebruik maken van een dergelijke kaart in het geding zijn. Dit blijkt temeer uit het feit dat een aantal studenten het CBP heeft verzocht om handhavend op te treden en er veel media aandacht is voor de werking van de (studenten) OV-chipkaart.

Conclusie
Gelet op bovenstaande overwegingen is het CBP na heroverweging van het bestreden besluit van oordeel dat het terecht en op goede gronden het beroep van GVB op het vertrouwensbeginsel heeft afgewezen.

3.3 Overige argumenten

3.3.1 Verantwoordelijke

Aangezien zoals hiervoor overwogen het CBP terecht heeft vastgesteld dat transactiegegevens betreffende de studenten OV-chipkaart persoonsgegevens zijn in de zin van de Wbp, moet de stelling van GVB dat zij niet kwalificeert als 'verantwoordelijke' omdat de Wbp niet van toepassing is worden verworpen

3.3.2 Kosten

In het aanvullend bezwaarschrift heeft GVB verzocht om een vergoeding van de kosten in bezwaar. Ten aanzien van dit verzoek merkt het CBP op dat ingevolge artikel 7:15, tweede lid, Awb geldt dat de kosten die de belanghebbende in verband met de behandeling van het bezwaar redelijkerwijs heeft moeten maken, door het bestuursorgaan uitsluitend

[23] Bijvoorbeeld ABRS 22 juni 2011, LJN: BQ8834; ABRS 24 november 2010, LJN: BO4851; ABRS 15 juli 2009, LJN: BJ3382; ABRS 26 november 2008, LJN: BG5360.
[24] Bijvoorbeeld ABRS 23 maart 2011, LJN: BP8751; ABRS 8 september 2010, LJN: BN6146; ABRS 15 juli 2009, LJN: BJ3382; ABRS 25 juni 2003, LJN: AH8649.

worden vergoed voor zover het bestreden besluit wordt herroepen wegens een aan het bestuursorgaan te wijten onrechtmatigheid. Gelet op het feit dat het CBP niet tot de conclusie komt dat het bestreden besluit moet worden herroepen wegens een aan het CBP te wijten onrechtmatigheid, komt dit verzoek niet voor honorering in aanmerking. Het CBP wijst dit verzoek dan ook af.

4. Conclusie

Het CBP verklaart het bezwaar ongegrond en handhaaft het bestreden besluit met dien verstande dat de motivering met de in het onderhavige besluit opgenomen overwegingen wordt aangevuld.

Het CBP wijst het verzoek om vergoeding van kosten af.

5. Rechtsmiddel

GVB kan tegen dit besluit beroep instellen bij de rechtbank Amsterdam, Sector bestuursrecht, door het indienen van een beroepschrift. De termijn waarbinnen het beroepschrift kan worden ingediend, bedraagt zes weken na de dag waarop dit besluit is verzonden.

Hoogachtend,
Het College bescherming persoonsgegevens,

Mr. J. Kohnstamm
Voorzitter