Ministerie van Volksgezondheid,
Welzijn en Sport

Jaarverslag 2009-2010

Functionaris voor de Gegevensbescherming

Management samenvatting

Algemeen

Organisaties dienen zorgvuldig om te gaan met de persoonsgegevens. In de Wet Bescherming Persoonsgegevens (Wbp) zijn de belangrijkste regels neergelegd voor het vastleggen en gebruiken van persoonsgegevens.

Organisaties dienen inzichtelijk (transparant) te maken welke (persoons)gegevens zij verwerken en voor welk doel. Verder mogen niet meer gegevens worden verwerkt en niet langer bewaard dan strikt noodzakelijk. Bovendien moet een organisatie passende beveiligingsmaatregelen treffen.

Onder de verantwoordelijkheid van de minister van Volksgezondheid, Welzijn en Sport (vws) vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om gegevens van burgers en (andere) organisaties, maar ook om gegevens van de eigen medewerkers. Vanuit de verantwoordelijkheid als overheidsorganisatie en als werkgever moet ook het ministerie zorgvuldig met persoonsgegevens omgaan.

Het College bescherming persoonsgegevens (Cbp) houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen, zoals de Wbp. Organisaties kunnen ook een interne toezichthouder aanstellen: de Functionaris voor de Gegevensbescherming (FG). Begin 2002 heeft de minister van vws een FG aangesteld.

Het lijnmanagement, als beheerder, is verantwoordelijk voor verwerking van persoonsgegevens binnen de eigen directie of dienstonderdeel.
Elke directie heeft een contactpersoon voor de Wbp aangesteld. Zij fungeren als belangrijke schakel en aanspreekpunt voor Wbp vraagstukken binnen de directie. Ook zorgen zij dat nieuwe meldingen bij de FG worden aangemeld en de huidige meldingen periodiek worden geëvalueerd en, waar nodig, bijgesteld.

Werkzaamheden en bevindingen, aanbevelingen

Het Strategisch Beveiligingsberaad van het ministerie van vws heeft in de verslagperiode, op voordracht van de FG, opdracht gegeven om de naleving van de Wbp binnen het ministerie te actualiseren. Aanleiding voor deze opdracht was de constatering van de functionaris voor de gegevensbescherming en de directie WJZ dat er geen actueel overzicht was van de meldingen van verwerkingen van persoonsgegevens als gevolg van organisatorische veranderingen binnen het ministerie van vws.
Het door de Wbp voorgeschreven openbare register van meldingen was na 2007 niet meer bijgewerkt.

Het ministerie van vws heeft zich bij het actualiseren van de “privacy compliance” laten ondersteunen door Duthler Associates.

Na afronding van het project “Actualisering Wbp” is in het eindrapport een aantal aanbevelingen aan de vws organisatie gedaan. Bij elke aanbeveling wordt de huidige stand van zaken[1] weergegeven en daar, waar nodig, aanvullend advies gegeven.

Aanbeveling Eindrapport Duthler: onderhoud de kennis van de Wbp-contactpersonen

De huidige Wbp-contactpersonen vervullen een spilfunctie in de naleving van de Wbp binnen het ministerie van vws. Om de werkzaamheden te kunnen uitvoeren die bij deze verantwoordelijkheid horen, is het noodzakelijk dat de Wbp-contactpersonen in staat worden gesteld hun kennis van de Wbp en de toepassing daarvan binnen het ministerie van vws op peil te houden. Ook het organiseren van periodieke bijeenkomsten kan ertoe bijdragen dat de kennis wordt geborgd.

Stand van zaken

Voor september 2011 zijn een tweetal opfriscursussen gepland voor de Wbp contact-personen.

Aanvullend advies FG

Het is aan te bevelen de Wbp contactpersonen in de gelegenheid te stellen hun kennis en kunde te onderhouden. Door het organiseren van periodieke bijeen-komsten wordt het contact gestructureerd en het belang van contactpersonen benadrukt.

Aanbeveling Eindrapport Duthler: zorg voor aanvullende interne regelgeving resp. borging in de planning- en controlcyclus

Om de naleving van de Wbp goed in de organisatie te verankeren verdient het aanbeve-ling om een Regeling bescherming persoonsgegevens vast te stellen, waarin taken, verantwoordelijkheden en bevoegdheden op het gebied van de Wbp worden neergelegd.

1 juli 2011

Stand van zaken

Medio 2010 is door de sg een Wbp regeling vastgesteld[2]. Een AO (administratieve organisatie) is in voorbereiding.
Met DBV, FEZ en de RAD zijn gesprekken over op welke wijze de Wbp te borgen door dit onderwerp mee te nemen in de jaarplannen van de dg's en directeuren en op te nemen in de planning- en controlcyclus. Dit onderwerp wordt meegenomen in de bredere verantwoordingscyclus die ook geldt voor de informatiebeveiliging en de beveiliging van gerubriceerde informatie.

Aanvullend advies FG

Het is aan te bevelen de Wbp – in een breder verband tezamen met de Informatiebeveiliging en beveiliging van gerubriceerde informatie – onderdeel te maken van de jaarplannen van de dg's en directeuren en op te nemen in de planning- en controlcyclus

Aanbeveling Eindrapport Duthler: inventariseer jaarlijks

Om de naleving van de Wbp te verankeren in de organisatie is het actueel houden van de - verplichte - meldingen van verwerkingen van persoonsgegevens van groot belang. Daartoe moet er jaarlijks een inventarisatie plaatsvinden. Hierdoor wordt voorkomen dat er opnieuw achterstallig onderhoud optreedt.
Om te garanderen dat de Wbp-inventarisatie een vast jaarlijks proces wordt, zou de Wbp-inventarisatie opgenomen kunnen worden in de planning- en controlcyclus.
Als "naleving Wbp" onderdeel is van de risicomanagement paragraaf van het jaarplan van een organisatieonderdeel, krijgt het onderwerp ook aandacht in de management-rapportages.
De FG kan – gewenst – gelijktijdig een signaal afgeven aan het netwerk van Wbp-contact-personen, zodat het onderwerp niet alleen langs de hiërarchische maar ook langs de functionele lijn de nodige aandacht krijgt.

Aanvullend advies FG

Het is aan te bevelen periodieke (jaarlijkse) inventarisaties uit te voeren.

2 Zie: www.rijksoverheid.nl/meldingenregister-ministerie-van-vws

Inhoudsopgave

Voorwoord

De Wet bescherming persoonsgegevens (Wbp) bestaat in september 2011 precies 10 jaar. Formeel bekrachtigd in 2001, kregen organisaties tot (september) 2002 de tijd om de wet te implementeren. vws, en ook andere departementen, hebben toen alle zeilen bijgezet om de implementatie door te zetten. Daartoe zijn alle verwerkingen binnen vws geïnventariseerd en de meldingsplichtige, zoals de wet voorschrijft, in een openbaar register vermeld. In de Wet Bescherming Persoonsgegevens (Wbp) zijn de belangrijkste regels neergelegd voor het vastleggen en gebruiken van persoonsgegevens.

Organisaties dienen inzichtelijk (transparant) aan te geven welke (persoons)gegevens zij verwerken en voor welk doel. Verder mogen niet meer gegevens worden verwerkt en niet langer bewaard dan strikt noodzakelijk. Bovendien moet een organisatie passende beveiligingsmaatregelen treffen.

Onder de verantwoordelijkheid van de minister van Volksgezondheid, Welzijn en Sport (vws) vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om gegevens van burgers en (andere) organisaties, maar ook om gegevens van de eigen medewerkers. Vanuit de verantwoordelijkheid als overheidsorganisatie en als werkgever moet ook het ministerie zorgvuldig met persoonsgegevens omgaan.

Het College bescherming persoonsgegevens (Cbp) houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen, zoals de Wbp. Organisaties kunnen ook een interne toezichthouder aanstellen: de Functionaris voor de Gegevensbescherming (FG). Begin 2002 heeft de minister van vws een FG aangesteld.

De FG dient jaarlijks een verslag uit te brengen aan de “verantwoordelijke” van zijn werkzaamheden en bevindingen en, waar nodig, aanbevelingen te doen.

Dit verslag betreft de periode 2009-2010. In deze periode is begonnen met een inhaalslag om weer te kunnen voldoen aan de Wbp. In mijn functie van FG heb ik in 2009 vastgesteld dat het wettelijk verplichte meldingenregister niet meer actueel was. Op mijn voorstel zijn in 2010 verwerkingen van persoonsgegevens binnen vws wederom geïnventariseerd en, waar nodig, geactualiseerd. Verder heb ik geadviseerd om de Wbp te borgen in de planning- en controlcyclus. In 2010 is een inhaalslag gemaakt en met de organisatorische borging een aanvang gemaakt. In 2011 zal de borging, tezamen met de informatiebeveiliging, definitief gestalte moeten krijgen. Dat proces zal ik nauwlettend volgen.

Den Haag, augustus 2011

F. Hoek
Functionaris voor de Gegevensbescherming

1 Algemeen

Inleiding

De Functionaris voor de Gegevensbescherming (FG) dient jaarlijks een verslag uit te brengen aan de "verantwoordelijke" van zijn werkzaamheden en bevindingen en, waar nodig, aanbevelingen te doen.

Leeswijzer

Hoofdstuk 1 geeft het gebied aan waarin de verschillende actoren zich bewegen. In hoofdstuk 2 wordt de (huidige) stand van zaken uiteengezet. De activiteiten voor de komende periode worden weergegeven in hoofdstuk 3. Hoofdstuk 4 gaat in op de – belangrijkste – adviezen in 2009/2010 van de FG aan de organisatie. Tot slot geeft hoofdstuk 5 inzicht in belangrijke ontwikkelingen in het kader van privacy en de eventuele gevolgen voor VWS.

Verantwoordelijken

In het kader van naleving van de Wbp binnen VWS dient een aantal activiteiten te worden uitgevoerd. Daarbij zijn verschillende actoren betrokken. De daarbij behorende taken en verantwoordelijkheden worden hieronder weergeven.

Minister

De minister stelt het beleid vast inzake de bescherming van persoonsgegevens die onder zijn verantwoordelijkheid vallen. Dit beleid is neergelegd in het beleidsdocument informatiebeveiliging en bescherming persoonsgegevens (IB&BP). Het document wordt periodiek geëvalueerd en, waar nodig, herzien.

Lijnmanagement

Het lijnmanagement, als beheerder, is verantwoordelijk voor verwerking van persoonsgegevens binnen de eigen directie of dienstonderdeel.
Daartoe behoren onder andere de volgende – structurele – activiteiten, die in de praktijk grotendeels door de Wbp contactpersonen worden uitgevoerd:

- Periodiek evalueren en, waar nodig, herzien van de procesbeschrijvingen Wbp
- Opnemen van de Wbp in de reguliere planning- en controlcyclus
- Rapporteren, door tussenkomst van de Directie Bedrijfsvoering (DBV), aan de FG aan de hand van de vragenlijst in het kader van de jaarlijkse update

- Analyseren van tussentijdse verwerkingen
- Toezenden van deze meldingen aan de FG
- Aanwijzen en opleiden van (nieuwe) Wbp-contactpersonen

Directie Bedrijfsvoering (DBV)

De directeur Bedrijfsvoering (DBV) ondersteunt de PSG bij de ontwikkeling en uitvoering van de departementale beveiliging op concern niveau en draagt zorgt voor de vertaalslag van interdepartementale ontwikkelingen naar departementaal beleid. Hier gaat hier met name om de gebieden die binnen het specifieke taakveld van de directeur DBV vallen, zoals informatiebeveiliging, bescherming van persoonsgegevens, documentaire informatiehuishouding, ICT-infrastructuur, gebouwbeveiliging en toegangsbeveiliging. Daarnaast draagt de directeur DBV zorg voor het toezicht op de naleving van het departementale beleid integrale beveiliging voor zover dat onder zijn, hierboven omschreven, taakveld valt. De directeur DBV is de plaatsvervanger van de PSG als voorzitter van het Beveiligingsberaad.

Op het gebied van IB en Wbp vervult DBV de rol van departementale coördinator op tactisch niveau. In het kader van de Wbp is (thans) DBV verantwoordelijk voor:

- het ondersteunen van de directies bij de periodieke evaluatie en herziening van de Wbp procedurebeschrijvingen
- het ondersteunen van de directies bij het borgen van de Wbp in de reguliere planning- en controlcyclus en het aanleveren van (management)informatie
- het aansturen van directies t.b.v. de jaarlijkse actualisering van de verwerkingen / meldingen
- het volgen van beleidsontwikkelingen
- het zorgdragen voor evaluatie en, waar nodig, bijstelling van het Wbp beleid
- het voorzien in opleidingsmogelijkheden
- het verzorgen van de communicatie binnen vws (bewustwording)

Functionaris voor de Gegevensbescherming (FG)

- houdt toezicht op de verwerkingen van persoonsgegevens;
- kan een onderzoek uitvoeren op de naleving van de Wbp, of een verzoek tot onderzoek indienen bij een onafhankelijke deskundige (zie ook onder de AD);
- brengt aan de verantwoordelijke (minister) verslag uit van onregelmatigheden die hij aantreft bij de verwerking van persoonsgegevens;
- houdt een (openbaar) register bij van de meldingsplichtige verwerkingen;
- maakt jaarlijks een verslag van zijn werkzaamheden en bevindingen;
- geeft, waar nodig, aanbevelingen aan de verantwoordelijke, die strekken tot een betere bescherming van de gegevens die worden verwerkt;
- brengt gevraagd en ongevraagd advies uit aan de departementsonderdelen;
- onderhoudt contacten met externe partijen, waaronder het College bescherming persoonsgegevens en het Rijksplatform voor Privacyfunctionarissen (RPPF).

In de Wet zelf is voor de FG een aantal (minimum)taken neergelegd. Zo dient hij toezicht te houden op de naleving van de wet, houdt hij een openbaar register bij en doet verslag aan de verantwoordelijke.
De meeste (overheids)FG's hebben in de praktijk meer taken dan het minimum pakket. Dat geldt ook voor vws. Zo maakt de adviestaak een belangrijk onderdeel uit van de functie (zie hoofdstuk 4).
Verder heeft de FG ook een adviserende rol bij de implementatie (en borging) van de Wbp binnen de vws organisatie.

Op basis van rapportages (vragenlijsten) vanuit de organisatie kan de FG de gemelde verwerkingen (en daarmee het openbaar register) actualiseren. Zodoende wordt inzicht gegeven welke persoonsgegevens en met welk doel vws persoonsgegevens verwerkt (transparantie en zorgvuldigheid).

De FG's van de departementen hebben zich verenigd in het Rijksplatform voor Privacy-Functionarissen (RPPF). Het RPPF overlegt elke 6 weken.
De (plv) FG van vws is secretaris van het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG). Dit genootschap komt 4 x per jaar bij elkaar.

Rijksauditdienst (RAD)

De RAD vervult de rol van onafhankelijke deskundige en kan de FG bij de toezichthoudende taak ondersteunen. Ook het lijnmanagement van vws kan de RAD verzoeken de toereikendheid van het privacy beleid alsmede de implementatie en uitvoering daarvan te beoordelen.
Tot slot kan de RAD, op basis van hun wettelijke taak, ook zelf – ongevraagd – periodieke controles uitvoeren.

Wbp contactpersoon

Elke directie/dienstonderdeel binnen vws heeft een Wbp contactpersoon aangesteld. In het kader van de Wbp vervult deze een rol in het toezicht en controle. De Wbp contactpersoon dient periodiek de kwaliteit van de verwerkingen van persoonsgegevens te beoordelen. De frequentie van beoordelingen hangt af van:

- de aard van de persoonsgegevens (bijzondere gegevens ingevolge Wbp of maatschappelijk gevoelig), of
- de hoeveelheid gegevens die zijn opgenomen, of
- het gebruik dat van de gegevens (o.a. frequentie raadplegen, gebruikte techniek) wordt gemaakt.

De Wbp contactpersonen fungeren als belangrijke schakel en aanspreekpunt voor Wbp zaken binnen de directie.

2 Werkzaamheden en bevindingen

2.1 Project actualisering Wbp

Het Strategisch Beveiligingsberaad van het ministerie van vws heeft, op voordracht van de FG, opdracht gegeven om de naleving van de Wbp binnen het ministerie te actualiseren. Aanleiding voor deze opdracht was de constatering van de Functionaris voor de Gegevensbescherming en de directie WJZ dat er geen actueel overzicht was van de meldingen van verwerkingen van persoonsgegevens als gevolg van organisatorische veranderingen binnen het ministerie van vws.

Het door de Wbp voorgeschreven openbare register van meldingen was na 2007 niet meer bijgewerkt. Dit kan leiden tot klachten van burgers, boetes van het College bescherming persoonsgegevens en imagoschade. Dit was voor het Strategisch Beveiligingsberaad aanleiding om opdracht te geven om de Wbp binnen het ministerie van vws op orde te brengen. Het actualiseren van het register van verwerkingen van persoonsgegevens heeft daarbij de eerste prioriteit gekregen.

Daartoe moest een inhaalslag gemaakt worden om de verwerkingen van persoonsgegevens opnieuw in beeld te brengen. Het ministerie van vws heeft zich bij het actualiseren van de “privacy compliance” laten ondersteunen door Duthler Associates.

2.1.1 Aanpak

In overleg met de (plv.) FG heeft Duthler Associates door middel van workshops en interviews de Wbp-contactpersonen van de directies ondersteund bij het actualiseren van de gegevensverwerkingen in hun organisatieonderdeel, zodat het ministerie van vws weer “privacyproof” is gemaakt. De workshops dienden daarbij om de kennis van de Wbp te actualiseren. De interviews waren erop gericht om samen met de Wbp-contactpersonen vast te stellen welke verwerkingen er binnen hun directie plaatsvinden en Wbp-contactpersonen, waar nodig, te helpen met het invullen van de meldings- en vrijstellingsformulieren.

De Wbp-contactpersonen hebben, na de interviews, de verwerkingen van persoonsgegevens opgesteld en gemeld aan de FG. Ook in deze fase zijn vele vragen van Wbp-contactpersonen beantwoord. Om zaken te vergemakkelijken voor Wbp-contactpersonen zijn formats voor meldingen en vrijstellingen ontwikkeld en ter beschikking gesteld. Op de voorgenomen einddatum van 1 juli 2010 waren nagenoeg alle - verplichte - meldingen geactualiseerd. De resterende meldingen zijn kort daarna gereedgekomen.

2.1.2 Uitgevoerde werkzaamheden en behaalde resultaten

Aan het project “actualisering Wbp” hebben nagenoeg alle directies, instellingen en raden deelgenomen. De Directie Bedrijfsvoering (DBV), het Centraal Informatiepunt

Beroepen Gezondheidszorg (CIBG) en het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) ontbreken in deze opsomming. De naleving van de Wbp was daar grotendeels op orde of er was al zelfstandig begonnen met een actualiseringsslag.

2.1.3 Brief aan directeuren

Bij de start van het project hebben alle directeuren c.q. hoofden van de betrokken organisatieonderdelen een brief ontvangen waarin de achtergronden van het project werden geschetst. De brief bevatte ook een oproep om de Wbp-contactpersoon van het betrokken onderdeel in staat te stellen mee te werken aan de actualiseringsslag.

2.1.4 Brief aan Wbp-contactpersonen

In vervolg op de brief aan de directeuren zijn ook Wbp-contactpersonen op de hoogte gesteld van het project. Zij werden uitgenodigd om deel te nemen aan de Wbp-workshop. In de brief is verzocht om medewerking aan het project te verlenen. Van het begin af aan was immers duidelijk dat voor het slagen van het project de medewerking van de Wbp-contactpersonen onontbeerlijk was.

2.1.5 Workshop Wet bescherming persoonsgegevens

Er zijn op 20 en 28 april 2010 workshops voor de Wbp-contactpersonen verzorgd. Het doel van de workshop was om de Wbp-contactpersonen op de hoogte te stellen van het project Actualisering Wbp bij het ministerie van vws en hun rol daarin. Bovendien diende de workshop om zodanige informatie te geven over Wbp dat de Wbp-contactpersonen in staat zouden zijn om deze kennis toe te passen in het project, met name bij het inventariseren van meldingsplichtige verwerkingen van persoonsgegevens. Bij de opzet van de workshop is rekening gehouden met het uiteenlopende kennisniveau van de Wbp-contactpersonen. Met het oog op recent aangestelde Wbp-contactpersonen begon de workshop met een inleiding over het privacybegrip en de hoofdlijnen van de Wbp.

Vervolgens spitste de workshop zich toe op de rol van contactpersoon in het project. Er zijn voorbeelden gegeven van bijzondere persoonsgegevens. Het Vrijstellingsbesluit is behandeld en Wbp-contactpersonen hebben geoefend met het invullen van een meldingsformulier.

Omdat bij de eerste workshop niet alle Wbp-contactpersonen aanwezig konden zijn is er een tweede workshop gehouden op 28 april 2010. Uiteindelijk hebben nagenoeg alle Wbp-contactpersonen de workshop bijgewoond. Wbp-contactpersonen van organisatieonderdelen die niet in het project betrokken waren, maar wel wilden deelnemen aan de workshop en Wbp-contactpersonen die een collega wilden meenemen zijn daartoe aangemoedigd. In totaal hebben circa 30 personen de workshop gevolgd. Ter voorbereiding op de workshop is aan Wbp-contactpersonen een informatiepakket toegestuurd met uitleg over de rol van de Wbp-contactpersoon en toetsschema's voor de inventarisatie van verwerkingen van persoonsgegevens. Bij de workshop werd een informatiebundel en een hand-out van de presentatie uitgedeeld.

De ervaring uit het project leert dat de workshop heeft gezorgd voor een nuttige kennisbasis bij Wbp-contactpersonen. In de praktijk bleek echter ook dat Wbp-contactpersonen toch nog vragen hadden als men daadwerkelijk aan de slag ging met de inventarisatie. In het kader van het project konden deze vragen beantwoord worden tijdens de interviews. De meest voorkomende vragen zijn door Duthler Associates verzameld en beantwoord in een mailbericht aan alle Wbp-contactpersonen.

2.1.6 Handboek

Er is een "Handboek Wet bescherming persoonsgegevens (Wbp)" voor het ministerie van vws geschreven. Oorspronkelijk was de gedachte dat volstaan kon worden met een eenvoudige bewerking van het model Handboek dat eerder voor het ministerie van VROM was gemaakt. In de praktijk vergde het meer bewerking dan verwacht om het organisatiespecifieke gedeelte van het model Handboek geschikt te maken voor het ministerie van vws.

Het Handboek is gepubliceerd op het intranet van het ministerie van vws onder het tabblad "Kennis" en vervolgens onder "Bescherming van persoonsgegevens"[3]. Ook de meldings- en vrijstellingsformulieren zijn ten behoeve van de Wbp-contactpersonen online beschikbaar gesteld.

2.1.7 Interviews met Wbp-contactpersonen

De interviews met Wbp-contactpersonen hadden tot doel om de Wbp-contactpersonen ondersteuning te bieden bij het inventariseren van verwerkingen en het invullen van de meldings- c.q. vrijstellingsformulieren. De interviews hebben plaatsgevonden in de periode vanaf 11 mei tot en met 22 juni 2010.

Een interview nam gewoonlijk een uur in beslag. In bilaterale gesprekken met de Wbp-contactpersoon is doorgenomen welke verwerkingen van persoonsgegevens bij het betreffende organisatieonderdeel aanwezig waren. Uitgangspunt daarbij was de meest recente lijst met verwerkingen. Deze dateerde van enkele jaren geleden. Vervolgens werd doorgenomen welke veranderingen er sindsdien waren opgetreden in de verwerkingen. Het interview bood Wbp-contactpersonen ook de gelegenheid om vragen te stellen over hoe om te gaan met Wbp-verplichtingen.

3 http://vwsintranet/kenniscentrum/juridisch/bescherming-van-persoonsgegevens

Daaruit bleek onder meer dat er behoefte was aan een gestandaardiseerde werkwijze ten aanzien van veel voorkomende verwerkingen. Hierin werd voorzien door het opstellen van een standaard vrijstellingsformulier voor verwerkingen die bij meerdere organisatieonderdelen voorkomen. Uitgaande van het Vrijstellingsbesluit zijn hiermee de meest voorkomende verwerkingen gedekt. Eveneens is een meldingsformulier voor personeelsadministratie en intern beheer gemaakt. Bovendien is aan de Wbp-contactpersonen een overzicht van mogelijke beveiligingsmaatregelen gestuurd. Deze aanpak heeft Wbp-contactpersonen veel werk uit handen genomen.

In de oorspronkelijke opzet van het project was voorzien dat er twee interviews per directie c.q. onderdeel zouden plaatsvinden. In de praktijk bleek het efficiënter om de ondersteuning na het eerste interview telefonisch of via de email te laten verlopen. De gemiddelde tijdsbesteding aan individuele ondersteuning per Wbp-contactpersoon bedroeg zodoende toch twee uur, zoals oorspronkelijk begroot.

2.1.8 Rapportage

Opdrachtleider P. Coté heeft op 12 april 2010 verslag uitgebracht over de voortgang van het project in het Strategisch Beveiligingsberaad. Op 17 juni 2010 heeft hij een schriftelijke tussenrapportage verzorgd voor het Strategisch Beveiligingsberaad.

2.1.9 Resultaten

Als resultaat van het project "actualisering Wbp" beschikt het ministerie van vws over:

- Actuele Wbp-kennis bij Wbp-contactpersonen;
- Het Handboek Wbp voor het ministerie van vws, online beschikbaar;
- Een actueel Wbp-dossier (verplichte meldingen, vrijgestelde verwerkingen en bewerkersovereenkomsten) bij de directies;
- Een actueel register van - verplichte - verwerkingen ten behoeve van het wettelijke verplichte openbare register. Het register is op internet gepubliceerd. Zie www.rijksoverheid.nl
- Aanbevelingen om de Wbp-procedures te verankeren in de organisatie en regelgeving waardoor het ministerie van vws ook in de toekomst Wbp-compliant zal blijven.

2.1.10 Verantwoording

Het project "Actualisering Wbp bij het ministerie van vws" is mede tot stand gekomen dankzij de inspanningen van de (toenmalige) medewerkers van het Stafbureau Beveiliging VROM/vws en vooral ook dankzij de inspanning van de Wbp-contactpersonen.

2.2 Functionaris voor de Gegevensbescherming

2.2.1 Organisatie

De Functionaris voor de Gegevensbescherming (FG) houdt toezicht op de naleving van de wet. De werkzaamheden in het verslagjaar 2009/10 omvatten onder andere de volgende activiteiten:

- Signaleren noodzaak inhaalslag.
  Al in eerdere jaarverslagen hebben wij aandacht gevraagd voor de tekortkoming van vws op het gebied van de naleving van de Wbp. De directie WJZ deelde ons standpunt. In 2010 heeft het Strategisch Beveiligingsberaad van het ministerie van vws, op onze voordracht, opdracht gegeven om de naleving van de Wbp binnen het ministerie te actualiseren. Het actualiseren van het register van verwerkingen van persoonsgegevens heeft daarbij de eerste prioriteit gekregen.
- Daartoe moest een inhaalslag gemaakt worden om de verwerkingen van persoonsgegevens opnieuw in beeld te brengen. Het ministerie van vws heeft zich bij het actualiseren van de "privacy compliance" laten ondersteunen door Duthler Associates
- Organiseren inhaalslag. De directie DBV, als concern beleidsverantwoordelijke voor de Wbp, is als opdrachtgever opgetreden. Wij hebben DBV geadviseerd in het selectieproces van externe ondersteuning, gezien onze expertise van onafhankelijke deskundigen.
- Actualiseren openbaar register. Volgens de Wbp dienen de meldingsplichtige verwerkingen in een openbaar register te worden opgenomen. Zo hebben betrokkenen inzage in wie welke gegevens over hen verwerkt. Dit register moet periodiek worden geactualiseerd. De Wbp stelt geen vormvereiste aan het register. Gekozen is om, evenals sommige andere departementen, de meldingen via www.rijksoverheid.nl te publiceren.
- Adviseren vws organisatie. In de functie van toezichthouder kan de Functionaris voor de Gegevensbescherming de organisatie gevraagd en ongevraagd adviseren. Ook het afgelopen jaar is gebleken dat vanuit de organisatie behoefte bestaat aan deskundig, onafhankelijk advies inzake de Wbp. Het College bescherming persoonsgegevens (Cbp) richt zich bijna uitslutend op de handhavende en toezichthoudende taak. Uiteraard blijft het lijnmanagement wel verantwoordelijk voor de juiste naleving van de privacy wetgeving.

In hoofdstuk 4 zijn de belangrijkste – schriftelijke – adviezen voor 2009 en 2010 weergegeven.

3 Planning en aanbevelingen

3.1 Algemeen

Na afronding van het project “Actualisering Wbp” is in het eindrapport een aantal aanbevelingen aan de vws organisatie gedaan. Bij elke aanbeveling wordt de huidige stand van zaken[4] weergegeven en daar, waar nodig, aanvullend advies gegeven.

Aanbeveling eindrapport Duthler: onderhoud de kennis van de Wbp-contactpersonen

De huidige Wbp-contactpersonen vervullen een spilfunctie in de naleving van de Wbp binnen het ministerie van vws. Het is de bedoeling dat er in de toekomst ook aanspreekpunten voor de Wbp voor alle dienstonderdelen zijn. Om de werkzaamheden te kunnen uitvoeren die bij deze verantwoordelijkheid horen, is het noodzakelijk dat de Wbp-contactpersonen in staat gesteld worden hun kennis van de Wbp en de toepassing daarvan binnen het ministerie van vws op peil te houden.

Dat vraagt om een training waarin niet alleen wordt uitgelegd wat de achtergronden van de Wbp inhouden, maar waarin ook het invullen van de meldingsformulieren en formulieren voor van melding vrijgestelde verwerking aan de orde zou moeten komen. Hiermee blijft het complete beeld van de naleving van de Wbp binnen het ministerie van vws duidelijk en zijn Wbp-contactpersonen in staat om de meest voorkomende werkzaamheden zelfstandig uit te voeren. Een dergelijke training is niet alleen voor nieuw aan te stellen Wbp-contactpersonen van groot belang. Voor de huidige Wbp-contactpersonen kan de training als opfriscursus dienen op het moment dat de gegevensverwerkingen opnieuw geïnventariseerd moeten worden. Daarnaast is het mogelijk om verdiepingscursussen aan te bieden over specifieke onderwerpen waar organisatieonderdelen mee te maken hebben. Op dit gebied is samenwerking met de directie Wetgeving en Juridische Zaken (wjz) nuttig en wenselijk.

Stand van zaken

Voor september 2011 zijn een tweetal opfriscursussen gepland voor de Wbp-contactpersonen.

Aanvullende advies FG

Het is aan te bevelen de Wbp contactpersonen in de gelegenheid te stellen hun kennis en kunde te onderhouden

4 juli 2011

Aanbeveling eindrapport Duthler: zorg voor aanvullende interne regelgeving resp. borging in de planning- en controlcyclus

Om de naleving van de Wbp goed in de organisatie te verankeren verdient het aanbeveling om een Regeling bescherming persoonsgegevens op te stellen. Deze Regeling past in de onlangs gekozen structuur van het Statuut integrale beveiliging van het ministerie van vws, waarin de taken, verantwoordelijkheden en de bevoegdheden op dit gebied (inclusief de Wbp) op hoofdlijnen zijn vastgelegd. Daarnaast is de Regeling een welkome aanvulling op het bestaande Beleidsdocument Informatiebeveiliging en Bescherming Persoonsgegevens van het ministerie van vws uit juni 2006. Het Statuut heeft tot doel om de bescherming van persoonsgegevens een plaats te geven in het integrale beveiligingsbeleid van het ministerie. Een Regeling biedt de organisatie de mogelijkheid om een nadere invulling te geven aan de open normen van de Wbp. Samen met het in het kader van dit project tot stand gekomen Handboek Wbp beschikt het ministerie van vws met deze documenten over een compleet framework voor de naleving van de verplichtingen uit de Wbp.

Stand van zaken

Medio 2010 is door de sg een Wbp regeling vastgesteld. Een AO (administratieve organisatie) is in voorbereiding.
Met DBV, FEZ en de RAD zijn gesprekken over op welke wijze de Wbp te borgen door dit onderwerp mee te nemen in de jaarplannen van de dg's en directeuren en op te nemen in de planning- en control cyclus. Dit onderwerp wordt meegenomen in de bredere verantwoordingscyclus die ook geldt voor de informatiebeveiliging en de beveiliging van gerubriceerde informatie.

Aanvullend advies FG

Het is aan te bevelen de Wbp – in een breder verband tezamen met de Informatie-beveiliging en beveiliging van gerubriceerde informatie – onderdeel te maken van de jaarplannen van de dg's en directeuren en op te nemen in de planning- en controlcyclus

Aanbeveling eindrapport Duthler: structureer het contact met de Wbp-contactpersonen

Een bijkomend resultaat van het project is dat er intensief contact geweest is met de Wbp-contactpersonen om het overzicht van meldingen tot stand te brengen. Om de naleving van de Wbp ook in de toekomst te laten voortduren en het onderwerp actueel te houden verdient het aanbeveling om het contact met de Wbp-contactpersonen gestructureerd te onderhouden.

Aanbeveling eindrapport Duthler: benadruk het belang van de rol van de Wbp-contactpersonen

Duthler Associates heeft veel medewerking van de Wbp-contactpersonen ondervonden. In het project is gebleken dat nagenoeg alle Wbp-contactpersonen gemotiveerd zijn voor hun taak als contactpersoon. Men ziet zelf het belang van een zorgvuldige omgang met persoonsgegevens. Om de aanwezige goodwill voor de naleving van de Wbp te behouden verdient het aanbeveling om regelmatig het belang van deze taakvervulling uit te spreken, ook door het eigen management. Voor de Wbp-contactpersonen is hun Wbp-taak een bijkomstigheid bij hun hoofdtaak. Sommige Wbp-contactpersonen hebben dit tot uitdrukking gebracht bij de interviews met Duthler Associates door erop te wijzen dat de aanwijzing als Wbp-contactpersoon niet geleid heeft tot een vermindering van de hoofdtaak. Enkelen vinden dat dat wel zou bijdragen aan een goede vervulling van de Wbp-taak.

Stand van zaken

Op 7 oktober 2010 zijn tijdens een bijeenkomst de resultaten van het project "actualiseringsslag" uiteengezet. Daarbij is nogmaals het belang van het werk van de Wbp-contactpersonen uitgesproken, ook door de psg. De bijeenkomst werd afgesloten door de officiële opening door de psg van het digitale, openbare register van meldingen. De meldingen worden voortaan op internet gepubliceerd in het digitale register. Op deze manier kunnen de Wbp-contactpersonen kennis nemen van het collectieve resultaat van hun individuele inspanningen. Aandacht voor de rol van Wbp-contactpersonen kan ook tot uitdrukking gebracht worden door middel van gestructureerd contact en een opleidingsaanbod.

Aanvullend advies FG

Het is aan te bevelen periodieke bijeenkomsten van de Wbp-contactpersonen te organiseren.

Aanbeveling eindrapport Duthler: inventariseer jaarlijks

Om de naleving van de Wbp te verankeren in de organisatie is het actueel houden van de - verplichte - meldingen van verwerkingen van persoonsgegevens van groot belang. Daartoe moet er jaarlijks een inventarisatie plaatsvinden. De Wbp-contactpersonen moeten daarvoor elk jaar op een vast moment een signaal krijgen met het verzoek om na te gaan of de meldingen nog actueel zijn of dat er wijzigingen zijn opgetreden. Door jaarlijks te inventariseren wordt voorkomen dat er opnieuw achterstallig onderhoud optreedt.
Om te garanderen dat de Wbp-inventarisatie een vast jaarlijks verschijnsel wordt zou de Wbp-inventarisatie opgenomen kunnen worden in de planning- en controlcyclus. Als "naleving Wbp" onderdeel is van de risicomanagement paragraaf van het jaarplan van een organisatieonderdeel, krijgt het onderwerp ook aandacht in de managementrapportages.

De FG kan een gelijktijdig signaal afgeven aan het netwerk van Wbp-contactpersonen, zodat het onderwerp niet alleen langs de hiërarchische maar ook langs de functionele lijn de nodige aandacht krijgt.

Aanvullend advies FG
Het is aan te bevelen periodieke (jaarlijkse) inventarisaties uit te voeren.

3.2 Toezicht en advies

De Algemene Rekenkamer (ARK) had eerder aangegeven dat het kerndepartement op het gebied van de informatiebeveiliging niet kan verklaren in control te zijn. Dat gold ook op het gebied van de Wbp. In het kader van de Wbp heeft het ministerie het wettelijke verplichte openbare register geactualiseerd door verwerkingen van persoonsgegevens bij het kerndepartement en baten-lastendiensten opnieuw te inventariseren. Hiermee heeft het ministerie een goede eerste stap gezet binnen het kader van de Wbp. In hoeverre de Wbp voorschriften binnen het ministerie worden nageleefd, heeft de ARK voor 2010 niet kunnen vaststellen. Het inzicht in de naleving ontbreekt, vanwege de volgende zaken, aldus de ARK:

- Het toetsen aan de vereisten die in de Wbp worden gesteld is door het lijnmanagement niet gedaan in 2010 (de eerder toegezegde compliance toets is niet uitgevoerd en er is evenmin een alternatief instrument ingezet om de naleving van Wbp voorschriften na te gaan en inzichtelijk te maken
- De RAD heeft geen privacy audits uitgevoerd

In het kader van de integrale benadering is het interne toezicht daar waar mogelijk verbreed. Het Strategisch Beveiligingsberaad speelt ook bij het toezicht en controle op het gebied van de Wbp een prominente(re) rol.
Met FEZ, DBV en de RAD vinden gesprekken plaats over de wijze waarop het inzicht (in de naleving) kan worden verkregen en/of verbeterd.

4 Adviezen

In de functie van toezichthouder kan de Functionaris voor de Gegevensbescherming de organisatie gevraagd en ongevraagd adviseren. Afgelopen jaren is gebleken dat vanuit de organisatie ook behoefte bestaat aan deskundig, onafhankelijk advies inzake de Wbp. Het laat onverlet dat het lijnmanagement verantwoordelijk blijft voor de juiste naleving van de privacy wetgeving.
Hieronder zijn enkele (in het kader van privacy) belangrijke adviezen voor 2009 en 2010 weergegeven[5].

Sociaal Cultureel Planbureau (SCP)

Het SCP laat met enige regelmaat veldwerkbureaus data verzamelen voor onderzoeksprojecten. Daarbij worden persoonsgegevens gebruikt zoals NAW-gegevens[6], bij het benaderen van potentiële respondenten.
Wij hebben geadviseerd om in de contracten met de bureaus standaard regels op te nemen ten behoeve van de bescherming van persoonsgegevens van betrokkenen. Punten van aandacht daarbij zijn de geheimhouding, bewaartermijnen en het vernietigen van persoonsgegevens (en de wijze waarop).

Elektronisch Patiëntendossier; de minister als (mede) verantwoordelijke?

De regel is dat organisaties (verantwoordelijken volgens de Wet bescherming persoonsgegevens) alle verwerkingen van persoonsgegevens moeten melden bij het Cbp. Wanneer een organisatie een eigen Functionaris voor de Gegevensbescherming (FG) heeft benoemd, kunnen de verwerkingen bij deze persoon worden gemeld.
Rondom het EPD is ook de vraag aan de orde geweest of het Landelijk Schakelpunt (LSP) een bestand respectievelijk verwerking is in de zin van de Wbp en wie daarvoor verantwoordelijk is.
Het landelijk uitwisselen van gegevens gaat via het Landelijk Schakelpunt (LSP). Uitgangspunt is dat het beheer van het medisch dossier bij de zorgverleners blijft. Het Landelijk Schakelpunt (LSP) beheert de zogenoemde landelijke verwijsindex. Deze verwijsindex houdt bij van welke patiënt gegevens, in welk zorginformatiesysteem, bij welke zorgaanbieder, ligt opgeslagen. Volgens deze omschrijving valt de verwerking onder de Wbp.

5 In totaal zijn in de jaren 2009 en 2010 18 formele, schriftelijke adviezen geconcipieerd
6 Naam, adres, woonplaats

In een rapport van (onder andere) Theo Hooghiemstra van Het Expertise Centrum[7] wordt gesteld dat het LSP een bestand is in de zin van de Wbp. Daarmee is een deel van de vraag beantwoord. Over de vraag wie als verantwoordelijke in de zin van de Wbp kan worden beschouwd, lopen de meningen uiteen. Het Cbp beschouwt de minister (met MEVA als beleidsverantwoordelijke) vooralsnog als (mede) "verantwoordelijke" voor verwerkingen die in het LSP plaatsvinden. NICTIZ wordt beschouwd als medeverantwoordelijke. De minister deelt dit standpunt niet. Volgens haar zijn de zorgaanbieders zelf als "verantwoordelijke" aan te wijzen.

In het rapport van Hooghiemstra wordt aangegeven, dat, hoewel de minister van VWS formeel juridisch verantwoordelijke wordt voor het LSP, het juridisch, technisch en organisatorisch – op dit moment – zo is geregeld dat de minister geen feitelijke invloed kan en mag uitoefenen op de data in het LSP. Het rapport doet verder geen uitspraken over de vraag wie nu uiteindelijk als verantwoordelijke in de zin van de Wbp kan worden beschouwd.

Het Cbp is duidelijk van mening dat VWS als (mede)verantwoordelijke kan worden aangewezen en heeft de minister in een brief van 25 mei 2011 formeel hierop gewezen. In onze functie van FG heb ik de minister, via MEVA, deze brief formeel onder de aandacht gebracht.

Uitgifte Rijkspas

Op basis van interdepartementale ontwikkelingen en signalen vanuit de organisatie heb ik het aanvraagproces van de Rijkspas onderzocht. Ik ben daarbij tot de conclusie gekomen dat het proces op sommige punten verbetering behoefde en behoeft.
Het gaat dan met name om het soort persoonsgegevens dat moet worden verstrekt bij de aanvraag, de manier waarop de behandelaar de gegevens heeft opgeslagen en bewaard, de borging van de veiligheid van de opgeslagen gegevens en procedures die worden gevolgd bij verlies of diefstal van de pas. Ten aanzien daarvan heb ik een aantal aanbevelingen gedaan. Zo heb ik geadviseerd om terughoudendheid betrachten bij het gebruik van het BSN in de bedrijfsvoering, om te voorkomen dat wellicht achteraf dure – ICT – aanpassingen noodzakelijk blijken. Verder heb ik aanbevolen uitbreiding van het gebruik van het burgerservicenummer (BSN) vooraf ter besluitvorming aan het Strategisch Beveiligingsberaad voor te leggen. Tot slot heb ik DBV geadviseerd om de procedures aan te passen, zodat conform de Wbp wordt gehandeld. Dat betekent ook dat periodieke controles worden uitgevoerd naar de werking van de genomen maatregelen en vastgestelde procedures.

7 Zeggenschap over het EPD, ethisch en juridisch perspectief, 14 februari 2011.

Verstrekken gegevens aan KLM

Het reisboekingskantoor van VWS (ATP) kreeg vanuit KLM het verzoek om (persoons) gegevens van klanten, zoals e-mailadres en telefoonnummer, aan hen te verstrekken zodat de KLM de passagiers direct zou kunnen informeren bij vluchtwijzigingen en/of vertragingen, ook als de reis via het reisbureau is geboekt.
Indien de gegevens niet beschikbaar worden gesteld dan kan volgens de KLM een verstoring alleen maar aan de reisagent worden doorgegeven (mits die op dat moment bereikbaar is). Dit proces heeft volgens de KLM vaker tot problemen geleid. Daarbij komt dat de vliegmaatschappijen thans, op basis van een EU Richtlijn, aansprakelijk zijn voor vertragingen en daarbij een eventuele schadevergoeding dienen te betalen. Ik heb aangegeven dat het aan de reisagent is het verzoek (om persoonsgegevens te verstrekken) te motiveren en aan de klant voor te leggen.

Verstrekken gegevens t.b.v. grieppandemie

Het RIVM was voornemens – in opdracht van VWS – om een onderzoek uit te voeren naar mensen die de griep hadden gekregen. Deelnemers die de griep hadden gehad dienden daarvoor digitaal 3 vragenlijsten in te vullen. De vragen betroffen bijzondere – medische – gegevens. Om deze gegevens te mogen verwerken volgens de Wbp moesten de deelnemers hun expliciete toestemming geven. Deze toestemmingsverklaring werd de deelnemers eveneens digitaal toegezonden. Formeel, conform de Wbp, zouden deelnemers deze verklaring hebben moeten uitprinten, ondertekenen en verzenden.

Deze omslachtige werkwijze kon hoogdrempelig werken en niet in het belang van het onderzoek.

In samenspraak (RIVM/FG) is daarom besloten om digitale versturing[8] van de toestemming toe te staan. Betrokkenen maken expliciet hun medewerking bekend door hiervoor een toestemmingsvakje aan te kruisen. Bovendien kan worden betoogd dat in casu het gebruik (van de bijzondere persoonsgegevens) is toegestaan, omdat het onderzoek het algemeen belang dient (zie hiervoor artikel 23, lid 2a Wbp).

8 Dus zonder de vereiste handtekening

5 Ontwikkelingen

5.1 Evaluatie Wbp en Privacyrichtlijn

Aan de orde is momenteel, althans waar het de bescherming persoonsgegevens betreft, de evaluatie van de Wet bescherming persoonsgegevens en de herziening van de Europese Privacyrichtlijn (95/46). Na diverse consultatierondes zal de Europese Commissie (EC) uiterlijk eind 2011 met een concreet voorstel komen. Verwacht wordt dat in ieder geval de volgende onderwerpen aan de orde komen: betere bescherming voor de burger/consument, harmonisatie van wetgeving, nadruk op gebruik van techniek (Privacy by Design) en de rol van de Functionaris voor de Gegevensbescherming (FG). In een eerder document pleitte de EC nog voor een verplichte aanstelling van een FG. Deze verplichting zou met name voor het MKB een onevenredige inspanning vergen. Het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) heeft een brochure uitgegeven waarin organisaties, middels een checklist, kunnen bepalen of het aanwijzen van een FG voor hun organisatie van toegevoegde waarde is.

Zeker is dat de open, materiële normen in de Wbp gehandhaafd blijven. Uit onderzoek is gebleken dat organisaties moeite hebben om deze in concrete gevallen in te vullen. Aangezien het College bescherming persoonsgegevens (Cbp) zich vooral richt op toezicht en handhaving, fungeert de FG voor de verantwoordelijke als eerste vraagbaak.
Anno 2011 is het vraagstuk van het gebruik van het BSN in de bedrijfsvoering van de overheid nog niet uitgekristalliseerd. Het ministerie van BZK, als beleidsverantwoordelijke voor de Wbp, en het Cbp staan hier lijnrecht tegenover elkaar. Het Cbp wijst het gebruik van het BSN voor dit soort verwerkingen per definitie af.

5.2 Rapport WRR

Het Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft in haar rapport "iOverheid" aandacht gevraagd voor het veranderende karakter van de overheid onder invloed van digitalisering. In de kern gaat het rapport over de verantwoordelijkheid van de overheid voor de eigen gebruik van ICT. Maar de overheid heeft natuurlijk ook een rol te spelen in de informatiesamenleving. De Raad concludeert dat zich een praktijk heeft ontwikkeld waarin samenhangende informatiestromen het karakter van de overheid domineren.
Deze samenhang creëert nieuwe mogelijkheden, maar tevens nieuwe kwetsbaarheden en afhankelijkheden. In de dagelijkse werkelijkheid van politiek en bestuur wordt – volgens de Raad – niet gewerkt vanuit de samenhangstrategie. Het overgrote deel van de overheidsinitiatieven voor digitalisering en de informatiestromen die daaruit volgen, wordt geïsoleerd bepleit, beoordeeld en ingevoerd. De iOverheid staat niet op de agenda van politiek en beleid. Volgens de Raad is het noodzakelijk op institutioneel niveau aanpassingen te verrichten, zodat een adequate verantwoordelijkheidsstructuur kan worden ontwikkeld.

6 Lijst met afkortingen

Lijst met afkortingen

ARK : Algemene Rekenkamer
BIG : Beroepen in de Individuele Gezondheidszorg
BP : Bescherming Persoonsgegevens
BSN : Burger service nummer
CBG : College ter Beoordeling van Geneesmiddelen
Cbp : College bescherming persoonsgegevens
CIBG : Centraal Informatiepunt Beroepen Gezondheidszorg
DBV : Directie Bedrijfsvoering
dFEZ : directie Financieel-Economische Zaken
EC : Europese Commissie
FG : Functionaris voor de Gegevensbescherming
IB : Informatiebeveiliging
LSP : Landelijk Schakelpunt
dMEVA : directie Macro-Economische Vraagstukken en Arbeidsvoorwaardenbeleid
NGFG : Nederlands Genootschap Functionarissen Gegevensbescherming
NVI : Nederlands Vaccin Instituut
psg : plaatsvervangend secretaris generaal
RIVM : Rijksinstituut voor Volksgezondheid en Milieu
RPPF : Rijks Platform voor Privacy Functionarissen
sg : secretaris generaal
VIR : Voorschrift Informatiebeveiliging Rijksdienst
VIR-bi : Voorschrijft Informatiebeveiliging Rijksdienst – bijzondere informatie
VWS : Ministerie van Volksgezondheid, Welzijn en Sport
Wbp : Wet Bescherming Persoonsgegevens
dwjz : Directie Wetgeving en Juridische Zaken

Dit is een uitgave van
Ministerie van Volksgezondheid,
Welzijn en Sport

Bezoekadres
Parnassusplein 5 | 2511 VX Den Haag

Postadres
Postbus 20350 | 2500 EJ Den Haag

Internet
www.rijksoverheid.nl

Vormgeving
www.lafille.nl

augustus 2011