COLOFON
Januari 2002
Uitgave: College bescherming persoonsgegevens
Grafisch ontwerp: Miriam Monster
Druk: Sdu Grafisch Bedrijf bv

LLEGE BESCHERMING
RSOONSGEGEVENS
liana van Stolberglaan
10
ostbus 93374
509 AJ Den Haag
LEFOON 070 888 85 00
K 070 888 85 01
MAIL info@cbpweb.nl
TERNET www.cbpweb.nl

Mag het een bitje minder zijn?

INHOUD

Over Privacy-Enhancing Technologies

COLLEGE BESCHERMING PERSOONSGEGEVENS

PRIVACY-ENHANCING TECHNOLOGIES BESCHERMEN DE PERSOONLIJKE LEVENSSFEER DOOR HET ELIMINEREN OF VERMINDEREN VAN PERSOONSGEGEVENS OF DOOR HET VOORKOMEN VAN ONNODIGE DAN WEL ONGEWENSTE VERWERKING VAN PERSOONSGEGEVENS, ZONDER VERLIES VAN DE FUNCTIONALITEIT VAN HET INFORMATIESYSTEEM.

INHOUDSOPGAVE

< VORIGE INHOUD VOLGENDE >

INLEIDING

De invoering van wetgeving ter bescherming van persoonsgegevens, conform EG Richtlijn 95/46, heeft gevolgen voor de inrichting van informatiesystemen van alle organisaties. De verantwoordelijke voor het verwerken van persoonsgegevens, dat is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, moet ervoor zorgen dat die wetgeving wordt nageleefd. De verantwoordelijke kan altijd aansprakelijk gesteld worden voor een onrechtmatige verwerking. De bewerker, dat is degene die in opdracht van de verantwoordelijke persoonsgegevens verwerkt, is zelfstandig aansprakelijk voor gebreken binnen zijn organisatie.

Wil men tot een zorgvuldige verwerking van persoonsgegevens komen, dan zal het verwerkingsbeleid een belangrijke plaats in de managementcyclus moeten innemen. Zo worden ook de privacyrechten van burger of consument op de juiste manier ondersteund. Privacybescherming zal doorgaans een aanvullend stelsel van maatregelen en procedures zijn. Bestaande maatregelen en procedures voor beheer, beveiliging en verwerking van persoonsgegevens dienen wellicht te worden heroverwogen en getoetst aan de doelstellingen van de nationale wetgeving.

De minister van Justitie heeft bij de behandeling van de Wet bescherming persoonsgegevens in de Eerste Kamer het standpunt ingenomen dat ook technische middelen ingezet moeten worden (art. 13 WBP). Deze zogenaamde Privacy-Enhancing Technologies (PET) kunnen een belangrijk hulpmiddel zijn om een behoorlijke en zorgvuldige omgang met persoonsgegevens te waarborgen en de werking van de privacybeginselen te realiseren. In de aangenomen motie 31 van het Tweede Kamerlid NicolaÔ wordt de regering opgeroepen in haar eigen informatiesystemen ook PET toe te passen. Er is tevens budget gereserveerd waarmee de overheid een ëlaunching customerí van PET wordt.

PET heeft inmiddels een belangrijke plaats verworven in het praktisch en theoretisch repertoire van privacybeschermende middelen. In deze brochure wordt een toelichting gegeven op de rol die PET bij de bescherming van privacy kan spelen.

1

BASISNIVEAU VAN PRIVACYBESCHERMING

De WBP schrijft, voor het rechtmatig verwerken van persoonsgegevens en het zorgvuldig omgaan met persoonsgegevens, een aantal dwingende normen voor. Deze normen zijn uitgewerkt in de volgende basisvoorwaarden:

1 Melden: voornemen en verwerking

De verwerking van persoonsgegevens moet vooraf worden gemeld bij het College bescherming persoonsgegevens (CBP) of een functionaris voor de gegevensbescherming, tenzij de verwerking daarvan is vrijgesteld. Van bepaalde persoonsgegevens moet ook al het plan (voornemen) deze te verwerken gemeld worden met het oog op een beoordeling door het CBP (voorafgaand onderzoek).

2 Transparantie van de verwerking

De betrokkene, dat is de persoon wiens persoonsgegevens worden verwerkt, moet kunnen overzien door wie en voor welk doel zijn gegevens worden verwerkt.

3 Doelbinding voor de verwerking

Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

4 Rechtmatige grondslag voor de verwerking

De verwerking van persoonsgegevens moet berusten op een in de WBP genoemde grondslag, zoals toestemming, overeenkomst, wettelijke plicht, gerechtvaardigd belang en dergelijke. Voor bijzondere gegevens (onder meer ras, gezondheid, seksuele geaardheid) gelden striktere normen.

5 Kwaliteit van de gegevens

De persoonsgegevens moeten zoveel mogelijk juist, nauwkeurig, toereikend, terzake dienend en niet bovenmatig zijn.

6 Rechten van de betrokkenen

De betrokkenen hebben het recht om kennis te nemen van hun gegevens en die te laten verbeteren of te laten verwijderen. Tevens hebben zij er recht op om bezwaar te maken tegen het verwerken van persoonsgegevens.

7 Beveiliging tegen verlies en onrechtmatige verwerking

Passende maatregelen van technische en organisatorische aard vormen het noodzakelijke sluitstuk van een rechtmatige verwerking van persoonsgegevens.

8 Verwerking van persoonsgegevens door een bewerker

Als de verwerking wordt uitbesteed aan een bewerker, moet worden verzekerd dat deze zich houdt aan de aanwijzingen van de verantwoordelijke.

9 Gegevensverkeer met landen buiten de EU

Het verkeer van persoonsgegevens naar een land buiten de Europese Unie (EU) is in principe alleen toegestaan als dat land een toereikend niveau van bescherming heeft.

2

DE WETTELIJKE BASIS VOOR PET

Artikel 13 van de WBP vormt de grondslag van de inzet van Privacy-Enhancing Technologies. Artikel 13 van WBP luidt: 'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.'

Dit artikel schrijft dus voor dat de verantwoordelijke voor de verwerking van persoonsgegevens passende technische maatregelen neemt om persoonsgegevens te beveiligen tegen verlies en tegen enige vorm van onrechtmatige verwerking. Bovendien geldt dat de maatregelen onnodige verzameling en onnodige verdere verwerking van persoonsgegevens dienen te voorkomen.

Deze maatregelen worden gewogen aan de hand van de volgende criteria:

- stand van de techniek;
- kosten;
- risico's van zowel de verwerking als de aard en omvang van de gegevens.

Daar waar technische maatregelen niet voldoende of niet haalbaar zijn, kunnen organisatorische maatregelen genomen worden of kunnen organisatorische maatregelen de technische ondersteunen in een samenhangend pakket van maatregelen.

De Registratiekamer heeft in een brief van 13 januari 1999 aan de Tweede Kamer erop gewezen, dat: ëde verantwoordelijke dan ook passende maatregelen zal moeten nemen tegen het verzamelen, vastleggen en bewaren van persoonsgegevens in strijd met de voorwaarden die daaraan elders in de WBP worden gesteld. In het bijzonder betekent dit, dat het verzamelen en verwerken van persoonsgegevens zonder toereikende grondslag als bedoeld in artikel 8 WBP zal moeten worden tegengegaan. Artikel 13 WBP zet de verantwoordelijke er toe aan de juridische normen van de WBP te vertalen in de feitelijke inrichting van de verwerking van persoonsgegevens en daarmee ook rekening te houden bij het ontwerp en verdere ontwikkeling van informatiesystemen.í

3

KLASSIEKE BEVEILIGINGSMAATREGELEN NIET VOLDOENDE

Wanneer organisaties wordt gevraagd welke maatregelen zij hebben getroffen om de privacy te beschermen, dan wijzen zij er steevast op dat zij zich hebben ingespannen om de persoonsgegevens te beveiligen. Hoewel het gebruik van beveiligingsmaatregelen om ongeautoriseerde toegang tot persoonsgegevens te voorkomen een belangrijke component van privacybescherming is, is een dergelijke beveiliging op zich niet toereikend. De gegevens van betrokkenen zijn immers vrijwel nooit versleuteld opgeslagen en de bescherming van de privacy is daarmee totaal afhankelijk van het correct functioneren en uitvoeren van de beveiligingsmaatregelen.

Het verdient daarom de voorkeur technische maatregelen te nemen waarmee de privacy van het individu direct bij het verzamelen beschermd wordt. Het gaat dan om technische maatregelen die ervoor zorgen dat er geen enkel gegeven wordt gegenereerd en vastgelegd. Het kunnen echter ook technische maatregelen zijn die ertoe bijdragen dat het gebruik en de opslag van identificerende gegevens tot een minimum worden beperkt of zelfs achterwege blijven.

Gezien het wettelijk voorgeschreven basisniveau van privacybescherming zal duidelijk zijn, dat - wil privacy in technisch opzicht adequaat beschermd worden - er dus meer moet gebeuren dan alleen maar informatiebeveiliging, namelijk het inzetten van PET. Artikel 13 WBP heeft dan ook gevolgen voor de verantwoordelijken voor persoonsgegevens, bewerkers en systeemontwikkelaars.

4

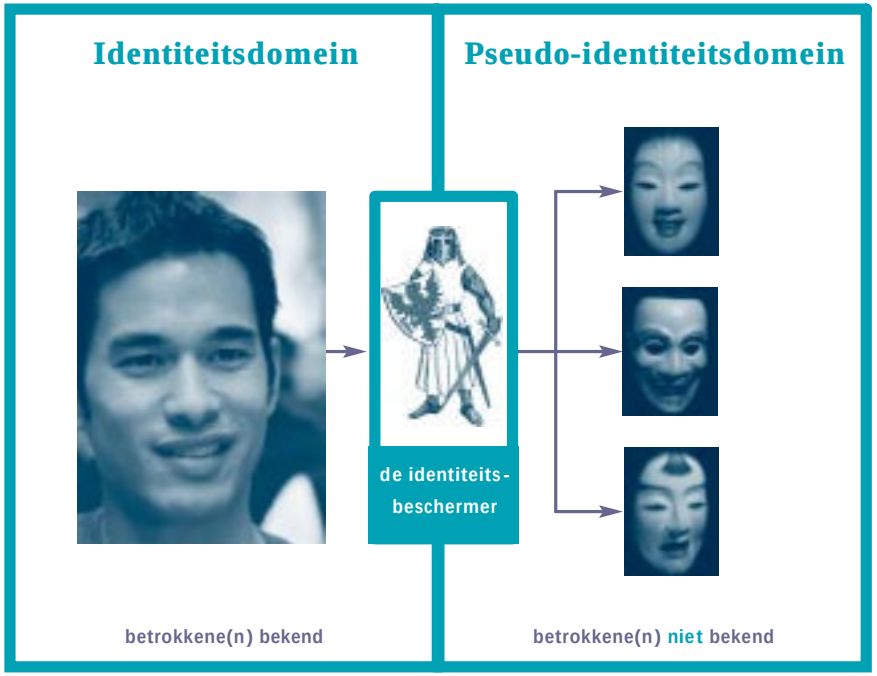
HET PET-RAPPORT

In augustus 1995 verscheen de publicatie: *Privacy-Enhancing Technologies: The Path to Anonymity*, dat in nauwe samenwerking met TNO/FEL in Den Haag en de Information and Privacy Commissioner van de Canadese provincie Ontario in Toronto geschreven was.

In het rapport wordt aangetoond dat het vaak niet nodig is de identiteit van de gebruiker, consument of burger te weten. Er zijn evenwel situaties waar - soms om wettelijke redenen - de identiteit wel bekend moet zijn, bijvoorbeeld bij het betalen voor het gebruik van bepaalde dienstverlening of bij het openen van een bankrekening.

Om technisch te realiseren dat de identiteit van de betrokkene wordt afgeschermd, kan binnen het informatiesysteem gebruik gemaakt worden van een systeemelement dat ëIdentity Protectorí of Identiteitsbeschermer wordt genoemd (zie figuur 1). Deze converteert de identiteit van de betrokkene in ÈÈn of meerdere pseudo-identiteiten.

Figuur 1: **Privacy-enhancing technologies**



Door het plaatsen van de identiteitsbeschermer (zie figuur 1) ontstaan minimaal twee soorten domeinen binnen het informatiesysteem: ÈÈn of meerdere domeinen waar de identiteit van de betrokkene bekend of toegankelijk is (het identiteitsdomein) en ÈÈn of meerdere domeinen waar dit niet het geval is (het pseudo-identiteitsdomein). De identiteitsbeschermer kan overal in het informatiesysteem geplaatst worden.
Het doel van het pseudo-identiteitsdomein is enerzijds ervoor te zorgen dat de betrokkene niet kan worden getraceerd aan de hand van eerder verkregen persoonsgegevens. Anderzijds zorgt het pseudo-identiteitsdomein ervoor dat de persoonsgegevens niet kunnen worden gevonden aan de hand van de verkregen identiteit.

In informatiesystemen kan de identiteitsbeschermer op verschillende manieren gestalte krijgen:

- als aparte functie geÔmplementeerd in het informatiesysteem;
- als apart informatiesysteem dat onder toezicht staat van de

consument (bijvoorbeeld de smartcard bij biometrische identificatie);

- als informatiesysteem dat onder toezicht staat van een door de dienstverlener en de burger/consument vertrouwde onafhankelijke partij (ëTrusted Third Partyí of ëTTPí).

Het gebruik van een identiteits-beschermer maakt het dus mogelijk preventief binnen het informatiesysteem in te grijpen in de identificeerbaarheid van de betrokkene. Een aantal voorbeelden van technieken die hierbij gebruikt kunnen worden, zijn de digitale handtekening, digitale certificaten en MIX nodes.

Een bijna onontkoombare techniek voor het garanderen van betrouwbaarheid in een open elektronische omgeving is het gebruik van geheimschrift (cryptografie). Een techniek die snel aan populariteit wint, is de openbare-sleutelcryptografie. Deze vorm van cryptografie kan op twee manieren gebruikt worden. Is de vercijfersleutel openbaar, dan kan iedereen deze sleutel gebruiken om een vercijferd bericht te maken dat alleen de eigenaar van de bijbehorende privÈsleutel weer kan ontcijferen. Is daarentegen de ontcijfersleutel openbaar, dan kan deze dienen tot authenticatie van de bron van een vercijferd bericht: alleen de eigenaar van de bijbehorende privÈsleutel kan het bericht vercijferd hebben. Deze laatste toepassing staat bekend als het zetten van een digitale handtekening.

Het gebruik van openbare-sleutelcryptografie vereist dat de sleutel op betrouwbare wijze gekoppeld is aan de identiteit of andere attributen van de houder ervan. De infrastructuur die nodig is om dit te faciliteren heet een public-key infrastructure (PKI). Een trusted third party (TTP) staat binnen een PKI in voor de genoemde koppeling. De TTP doet dat door zelf gebruik te maken van een elektronische handtekening. Een digitaal certificaat is een door een TTP uitgegeven en digitaal ondertekend elektronisch document dat het verband legt tussen een openbare sleutel en attributen van de certificaathouder.

Het inzetten van MIX nodes in telecom- en andere netwerken lijkt veelbelovend voor het beschermen van de verkeersgegevens van de zender en de ontvanger. Met een serie van MIX-nodes en een bepaalde toepassing van encryptie en decryptie kunnen onder andere verkeersgegevens zo worden gemodificeerd en gehergroepeerd dat het vrijwel onmogelijk is om vast te stellen of een bericht ëbinnenkomtí of ëuitgaatí. Daarmee kan de analyse van verkeersgegevens worden voorkomen.

Het arsenaal aan PET-middelen binnen netwerken wordt steeds groter, waardoor het niet-identificeerbaar zijn van zowel de gebruiker als de aanbieder, en het niet-waarneembaar zijn van het netwerk, de server, de query enz. gerealiseerd kan worden.

5 PET-STRATEGIEËN

Bij het inzetten van PET om de privacy te beschermen, kan de verantwoordelijke voor verschillende strategieën kiezen:

- hij richt zich op het voorkomen of verminderen van de identificeerbaarheid;
- hij zet in, conform de WBP, op het voorkomen van het onrechtmatig verwerken van persoonsgegevens;
- hij gebruikt andere technologieën die de privacy ondersteunen;
- hij combineert deze strategieën.

Daarnaast zal de verantwoordelijke vaak ook organisatorische maatregelen nemen.

5.1 Voorkomen van identificatie en het criterium van onevenredige inspanning

Voor de eerste strategie is het van belang om te bepalen of er sprake is van een persoonsgegeven en daarbij is ook het element ëidentificeerbaarheidí van belang. Onder persoonsgegevens verstaat de WBP: elk gegeven betreffende een geÔdentificeerde of identificeerbare natuurlijke persoon. Volgens artikel 2 van de EG Richtlijn 95/46 kan een natuurlijk persoon direct of indirect identificeerbaar zijn. Direct identificeerbaar is men aan de hand van de naam, adres en woonplaats (NAW-gegevens), een persoonsnummer, een pseudo-identiteit die in brede kring bekend is, een biometrisch kenmerk (zoals bijvoorbeeld een vingerscan). Indirect identificeerbaar is men aan de hand van andere unieke kenmerken of attributen of een combinatie van beide, waaruit voldoende informatie is af te leiden voor de identificatie. Zo kan met behulp van de cd-foongids uit de postcode en het huisnummer de naam van de bewoner van een huis achterhaald worden.
Met PET kunnen de direct identificerende gegevens binnen een informatiesysteem geanonimiseerd worden. Wanneer deze gegevens ook van indirect identificerende kenmerken zijn ontdaan, zijn er helemaal geen persoonsgegevens meer aanwezig. Dan is de WBP ook niet langer van toepassing omdat er geen persoonsgegevens beschermd hoeven te worden.

Niet-identificeerbaarheid wordt ook aangenomen als de hoeveelheid en de aard van de indirect identificerende gegevens dusdanig is dat alleen door een onevenredige inspanning tot identificatie van het individu kan worden gekomen. Eveneens wordt niet-identificeerbaarheid aangenomen als hiervoor de medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is. Of er sprake is van onevenredige inspanning hangt aan de ene kant af van de aard van de gegevens en de grootte van de populatie. Aan de andere kant hangt dit af van de middelen (tijd en geld) die men bereid is te spenderen om tot identificatie te komen.

5.2 Waarborgen tegen onrechtmatige verwerking van persoonsgegevens

PET kan toegepast worden bij het beveiligen van persoonsgegevens tegen verschillende vormen van onrechtmatig verwerken. Daarmee wordt voorkomen dat persoonsgegevens onnodig verzameld, vastgelegd, bewaard, in- of extern verstrekt of samengebracht en met elkaar in verband gebracht (gekoppeld) worden.

Door het inzetten van PET bij het verwerken van identificerende gegevens, kan de verantwoordelijke ervoor kiezen zijn informatiesysteem met een identiteitsdomein en pseudo-identiteitsdomeinen zo in te richten dat minder of geen persoonsgegevens worden verwerkt (bijvoorbeeld bij het verzamelen of vastleggen van gegevens). Hij kan er ook voor zorgen dat

afhankelijk van de toegekende rechten binnen het informatiesysteem aan verschillende gebruikers al dan niet geanonimiseerde gegevens worden verstrekt of al dan niet toegang wordt verleend. Bijvoorbeeld voor wetenschappelijk onderzoek en statistiek verkrijgt men niet-identificerende gegevens. Daarentegen worden in een ziekenhuis op basis van een functionele autorisatie en de relatie tussen zorgverlener en patiÎnt identificerende gegevens wel verstrekt.

Het is een belangrijk privacybeginsel dat niet meer gegevens mogen worden verzameld en verwerkt dan strikt noodzakelijk is voor het vastgestelde doel. Als uit onderzoek mocht blijken dat met PET minder gegevens gebruikt kunnen worden, en dat daarmee aan dit beginsel voldaan kan worden, dan zal PET ook daadwerkelijk moeten worden ingezet. Bovendien levert PET een bijdrage aan het handhaven van doelbinding, omdat de techniek er tevens voor kan zorgen dat gegevens geblokkeerd worden wanneer ze op een andere manier gebruikt worden dan waarvoor ze verzameld zijn. PET kan ook uitstekend ingezet worden in het kader van de informatiebeveiliging. Dit is conform de toelichting bij artikel 13 van de WBP waarin erop gewezen wordt dat dit artikel zich uitstrekt over alle onderdelen van het proces van gegevensverwerking.

Of in redelijkheid mag worden gevergd dat PET moet worden ingezet, hangt ñ volgens de brief van 13 januari 1999 van de Registratiekamer aan de Tweede Kamer ñ af van de maatstaven die artikel 13 van de WBP aanlegt (zie hoofdstuk 3). Het niet-toepassen van PET zal voor de verantwoordelijke, naarmate PET makkelijker toegepast kan worden, steeds minder goed te verdedigen zijn.

5.3 Voorbeeld van een Ziekenhuis Informatie Systeem met PET

Het PET Ziekenhuis Informatie Systeem, dat inmiddels in tientallen ziekenhuizen gebruikt wordt, is een informatiesysteem waarin verschillende domeinen zijn gecreÎerd waarbinnen personen deels bekend en deels anoniem zijn. Bovendien kunnen alleen geautoriseerde gebruikers gegevens in pseudo-identiteitsdomeinen identificeerbaar maken. In juni 1997 is door een internationale software ontwikkelaar de identiteitsbeschermer in het ziekenhuisinformatiesysteem met succes toegepast.

Het proces om de PET-oplossing te implementeren verliep als volgt. Na een door het College bescherming persoonsgegevens uitgevoerde privacy audit werd de leverancier van het gebruikte ziekenhuis informatiesysteem verzocht de theoretische beschrijving van de Identity Protector in concrete technische maatregelen te vertalen en in het ziekenhuis informatiesystemen (inclusief het elektronisch patiÎntendossier) te implementeren.

De gegevens van de patiÎnten in de database werden gesplitst in drie groepen. De eerste groep omvat de direct tot de patiÎnt herleidbare gegevens als naam, adres, geboortedatum, verzekering enz. (het identiteitsdomein). In de tweede groep werden alle diagnostische en behandelgegevens verzameld (het pseudo-identiteitsdomein).
In beide domeinen worden de patiÎnten geÔdentificeerd door een patiÎntnummer. Deze zijn echter niet aan elkaar gelijk en bovendien versleuteld. Dit betekent dat er op het niveau van de database geen relatie gelegd kan worden tussen de gegevens in de twee domeinen. Het resultaat hiervan is dat een gebruiker die niet langs een geautoriseerde weg toegang heeft weten te krijgen tot deze database, geen samenhangende verzameling van gegevens aantreft.

Bij het ontwerpen van de systematiek van de patiÎntnummers is in het eerste domein gekozen voor een systeem van volgnummers. Het patiÎntnummer in het tweede domein wordt verkregen door encryptie (versleuteling) van dit volgnummer. Het gebruikte encryptieprotocol maakt het mogelijk het oorspronkelijke patiÎntnummer te ontcijferen (decryptie). De encryptie / decryptie vindt plaats binnen de toepassingssoftware. Het protocol maakt gebruik van encryptiesleutels. Deze sleutels worden pas verstrekt, bij voorkeur door een onafhankelijk en vertrouwde derde partij, nadat de identiteit van de gebruiker van de toepassing is vastgesteld.

Voor statistisch en wetenschappelijk onderzoek werd een derde domein aangelegd. In dit domein worden alleen geaggregeerde gegevens verwerkt.

5.4 Andere privacyondersteunende technologieën

Wanneer de hiervoor besproken PET strategieÎn niet ingezet kunnen worden, kan ook gebruik worden gemaakt van andere

technologieÎn die bijdragen tot een betere privacybescherming. Uit de privacybeginselen kunnen immers basisvoorwaarden voor de verwerking van persoonsgegevens worden afgeleid, zoals:

- transparantie;
- kwaliteit;
- rechten van de betrokkenen;
- beveiliging.

Enkele voorbeelden van het inzetten van technologie ter bevordering van privacy:

- Transparantie wordt bevorderd door het gebruik van P3P (een technologie om het privacybeleid van websites te toetsen), maar dit hangt met name af van de default setting. Deze dient zo te zijn dat niet automatisch alle ingevoerde gegevens geopenbaard worden.
- Een statistisch-taalkundige analyse binnen een adressensysteem kan de juistheid van de gegevens optimaliseren en daarmee de kwaliteit van de gegevens verbeteren.
- De rechten van betrokkenen kunnen beter bewaakt worden door feedback en controle. Deze ontwerpbeginselen zorgen ervoor dat informatiesystemen op elk gewenst moment de betrokkene kunnen informeren over wat deze aan persoonsgegevens heeft afgestaan aan het informatiesysteem. Betrokkene kan dan reageren met een verzoek om inzage, aanvulling, wijziging of verwijdering van persoonsgegevens.
- Logging (het vastleggen in een elektronisch ëlogboekí van handelingen binnen het informatiesysteem) is een uitstekend beveiligingsmiddel. Bij het verzamelen en vastleggen kan de herkomst van de gegevens automatisch worden gelogd. Bij opvragen, raadplegen, wijzigen of verstrekken (intern of extern) kan eveneens automatische logging plaatsvinden. Dergelijke vastleggingen dienen dan uitsluitend door de systeembeheerder verwijderd te kunnen worden, waarbij van een dergelijke verwijdering een log wordt gemaakt, waarover de verantwoordelijke zich dan zal moeten verantwoorden.
- Ook de toegang tot de gegevensverwerking moet worden vastgelegd in een elektronisch logboek. Bij het afschermen, raadplegen, wijzigen, uitwissen en vernietigen van gegevens kan automatische toegangscontrole als beveiligingsmiddel worden ingezet.
- Automatisch wissen van gegevens kan eveneens ingezet worden. Bewaartermijnen kunnen softwarematig worden vastgelegd en bij het verstrijken van de bewaartermijn worden de gegevens automatisch gewist.
- Voor wat betreft de verwerking door een bewerker en het gegevensverkeer buiten de EU via internet is het eveneens mogelijk om technische maatregelen te treffen om onrechtmatige handelingen in de zin van de WBP tegen te gaan.

5.5 Gestapelde technologieën

Wanneer slechts aan ÈÈn van de privacybasisnormen die in de WBP zijn vastgelegd, technisch wordt voldaan, dan is die technologie op zichzelf niet voldoende om optimale privacybescherming te realiseren. Bijvoorbeeld: een statistisch-taalkundige analyse binnen een adressensysteem kan de juistheid van de gegevens optimaliseren, maar is op zichzelf niet in staat om privacybescherming te garanderen.
Het gebruik van een aantal op elkaar gestapelde technische maatregelen binnen het informatiesysteem kan wel leiden tot een bevredigende privacyveilige omgeving, bijvoorbeeld door een statistisch-taalkundige analyse te combineren met gespreide opslag, protocollering van herkomst, gebruik en verstrekking van gegevens en logging.

Het inbouwen van PET in systemen is niet alleen een technische opgave, maar ook een normatieve. Voordat ëPET-INSIDEí (de term is ëgeleendí van de reclame: ëINTEL INSIDEí) in informatiesystemen zit, moet duidelijk zijn welke eisen de WBP aan een informatiesysteem stelt. Technologen en juristen zullen normen moeten vertalen in technische systeemeisen.
Omgekeerd, door middel van een PET Scan of privacy audit kan worden getoetst of systeemeisen en toepassingen voldoen aan de WBP. Gebeurt dat niet, dan zal van een effectieve privacybescherming geen sprake zijn.
Als noch Privacy-Enhancing Technologies noch andere technische maatregelen afdoende zijn, dan dienen er organisatorische maatregelen te worden ingezet. Hoewel met de huidige ICT-toepassingen theoretisch in elk informatiesysteem tenminste ÈÈn van de privacybeginselen kan worden verwezenlijkt, is dat soms zo kostbaar in verhouding tot het te beschermen belang dat het invoeren van dergelijke technische maatregelen niet gevergd kan worden. Organisatorische maatregelen garanderen dan de privacy van de gebruiker van het informatiesysteem, van de consument of burger van wie persoonsgegevens worden verwerkt.

6

CONCLUSIE

De ontwikkelingen in de informatie- en communicatietechnologie bieden steeds meer mogelijkheden om gegevens over personen te verzamelen, op te slaan, te bewerken en te verspreiden. De kans op inbreuk op de privacy van de consument en burger neemt hierdoor toe. Diezelfde informatie- en communicatietechnologie biedt echter ook oplossingen om de bescherming van de privacy van de gebruiker, consument en burger vorm te geven.

PET is een uitstekend en veelbelovend hulpmiddel om met name de privacybasisnorm ërechtmatige grondslag voor gegevensverwerkingí te realiseren. Uiteraard blijft aandacht en research noodzakelijk en zal er voortdurend inspanningen moeten worden verricht om PET-toepassingen in informatiesystemen te stimuleren, zoals thans in het door de Europese Unie gesubsidieerde PISA project gebeurt. Dit project ñ PISA staat voor Privacy Incorporated Software Agent ñ richt zich op het ontwikkelen van een privacyveilige omgeving voor gebruikers van internet.

Bovendien zal via privacy audits of specifieke PET Scans moeten worden gecontroleerd of met PET uitgeruste systemen werkelijk voldoen aan de WBP. Certificering in het kader van een privacy audit kan hieraan bijdragen en de noodzakelijke zekerheid bieden aan burgers en consumenten dat hun privacy binnen informatiesystemen afdoende beschermd wordt.

Privacy-Enhancing Technologies (PET)
H. van Rossum, H. Gardeniers, J.J. Borking, A. Cavoukian, J. Brans, N. Muttupulle, N. Magistrale, *Privacy-Enhancing Technologies: The Path to Anonymity*, The Hague 1995.
R. Hes en J.J. Borking, *Privacy-enhancing technologies: the path to anonimity, revised edition*, Achtergrondstudies en verkenningen 11, Registratiekamer Den Haag 2000.
O. Berthold, A. Pfitzman, R. Standke, ëThe disadvantages of the free MIX router and how to overcome themí in: *Proceedings of the Workshop on Design Issues in Anonimity and Unobservability*, Berkely (CA), pag. 27-42.

WBP Algemeen
L.B. Sauwerwein en J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens. Wet bescherming persoonsgegevens*, Ministerie van Justitie Den Haag januari 2001.
Privacy in Bedrijf, AWVN, FME-CWM, VNO-NCW Den Haag 2000.

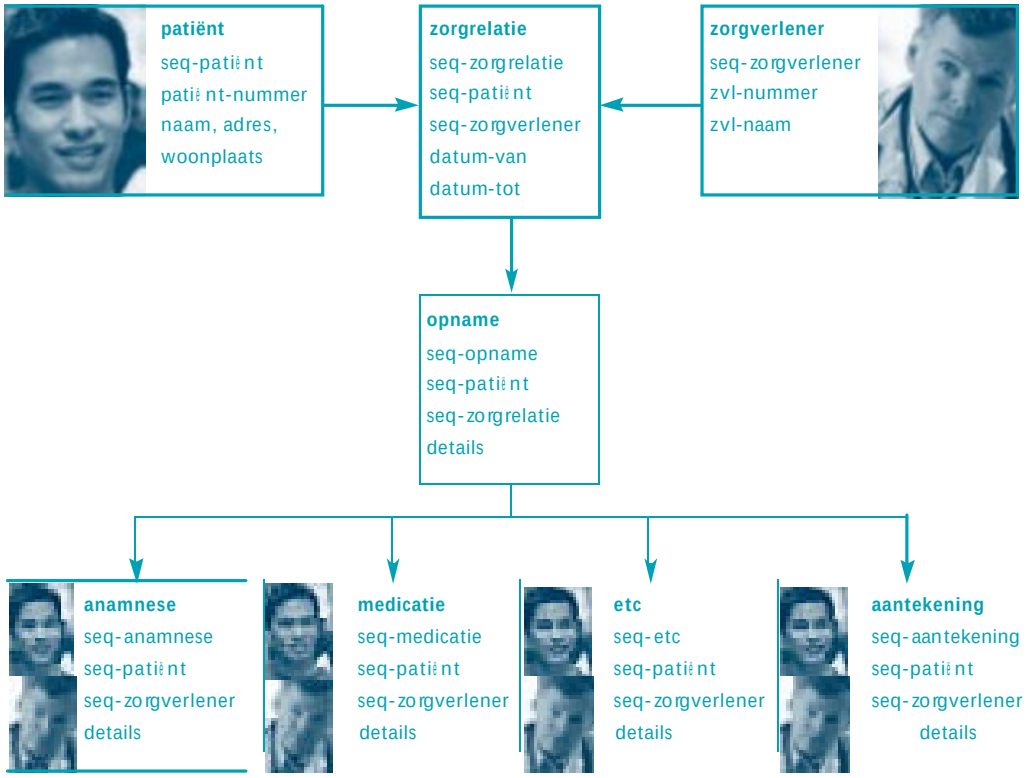
Auditproject
Wet bescherming persoonsgegevens Raamwerk Privacy Audit, Samenwerkingsverband Audit Aanpak Den Haag 2001.
Wet bescherming persoonsgegevens WBP zelfevaluatie, Samenwerkingsverband Audit Aanpak Den Haag 2001.

Beveiliging persoonsgegevens
G.W. van Blarkom en J.J.Borking *Beveiliging van Persoonsgegevens*, Achtergrondstudies en Verkenningen 23, Registratiekamer Den Haag 2001.

Vertrouwde derde partij (Trusted third Parties)
J. Versmissen, *Sleutels van Vertrouwen, TTP-dienstverlening en privacy ñ de juridische randvoorwaarden verkend*, Achtergrondstudies en Verkenningen 22, Registratiekamer Den Haag 2001.

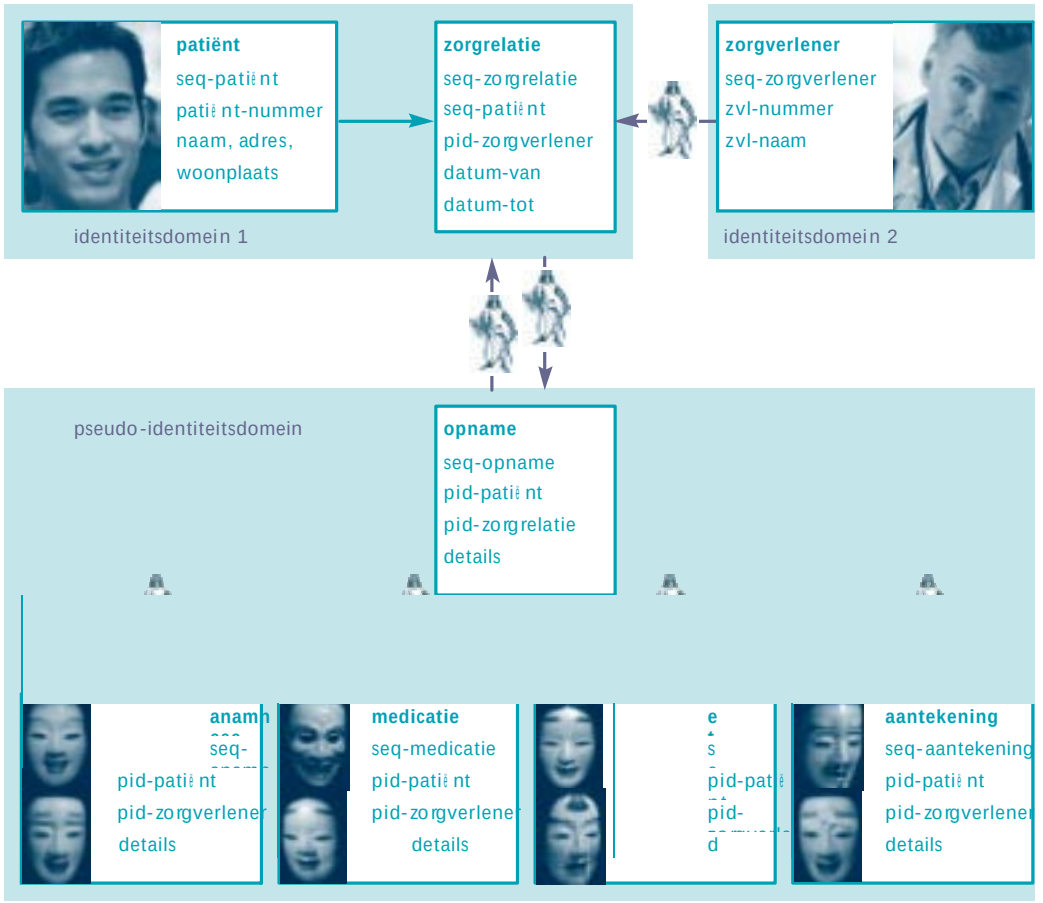
Privacy incorporated software agent (PISA)
J.J. Borking, ëPrivacy Incorporated Software Agent (PISA): A Proposal for Building a Privacy guardian for the Electronic Ageí, in: H. Federath, *Designing Privacy Enhancing Technologies*, Springer Verlag Berlin 2001, pag. 130-140.

Figuur 1: **Basistabellen met relaties**



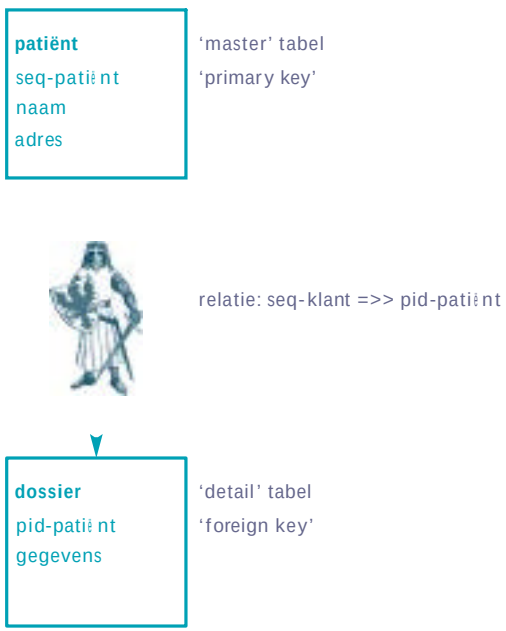
In een database gebaseerd op het standaard relationele model is het zonder meer mogelijk om de naam-adres gegevens van de patiÎnt te relateren aan het medisch dossier. De identifice- rende codes (primary en foreign key: seq-patiÎnt) zijn namelijk gelijk.

Figuur 2: **Indeling in domeinen**



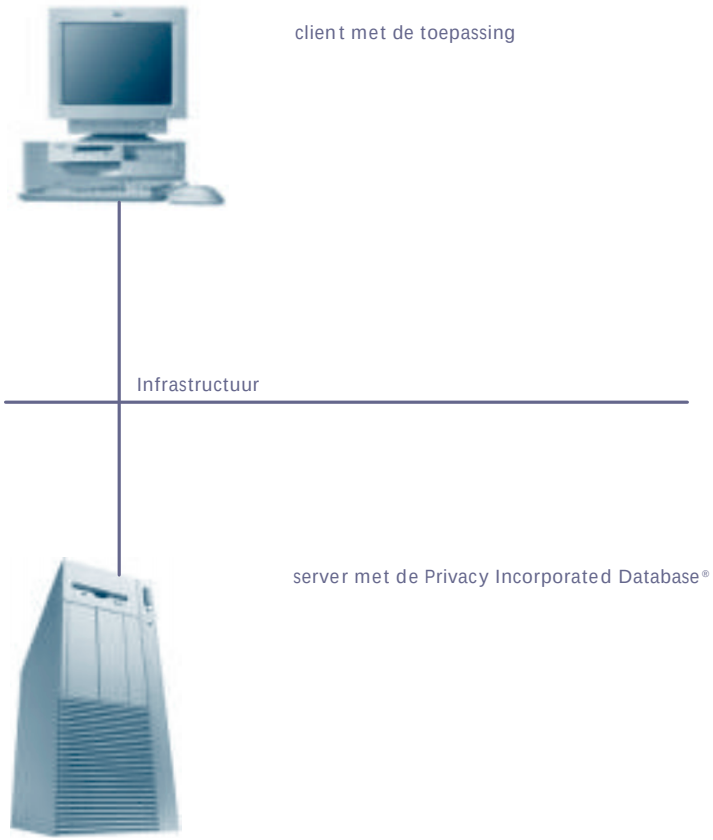
In een database gebaseerd op de Privacy Incorporated Database® zijn de opgeslagen gegevens verdeeld over een aantal domeinen. In het eerste domein worden de naam-adres gegevens van de patiÎnt opgeslagen. In het tweede domein dezelfde gegevens, maar dan van de zorgverlener(s).In het derde domein worden de medische dossiers opgeslagen.De patiÎnt (maar ook de zorgverlener) wordt in de verschillende domeinen verschillend geÔdentificeerd. De primary key van de patiÎnt in identiteitsdomein 1 (seq-patiÎnt) wordt versleuteld in het pseudo-identiteitsdomein (pid-patiÎnt). Een vergelijkbare situatie bestaat tussen identiteitsdomein 2 (seq-zorgverlener) en het pseudo-identiteitsdomein (pid-zorgverlener).

Figuur 3: **Privacy Incorporated Database®**



De versleuteling van de primary key vindt plaats in de client toepassing. De sleutel die hiervoor benodigd is wordt pas ter beschikking gesteld na een positieve authenticatie van de gebruikers. Dat gebeurt bijvoorbeeld op basis van biometrie. Het inschakelen van een ëtrusted third partyí wordt hierbij sterk aanbevolen.

Figuur 4: **Client/Server Architectuur**



Wet bescherming persoonsgegevens

De privacybescherming in Nederland wordt sinds 2001 geregeld in de Wet bescherming persoonsgegevens (WBP). Deze wet, als opvolger van de Wet Persoonsregistraties (WPR), stelt eisen aan de wijze waarop organisaties persoonsgegevens verwerken. Vrijwel elke organisatie in Nederland doet dat en heeft dus te maken met de WBP. De eisen in de WBP zijn veranderd en uitgebreid ten opzichte van de WPR. Dit betekent dat als uw organisatie voldoet aan de wettelijke bepalingen van de WPR dit niet zonder meer betekent dat zij voldoet aan alle WBP-bepalingen. Het College bescherming persoonsgegevens (CBP) is als opvolger van de Registratiekamer belast met het toezicht op de naleving van de WBP.

Doel van de Quickscan

Als u vindt dat personeelsleden, klanten, debiteuren, bezoekers en andere relaties vertrouwen moeten hebben in uw organisatie dan moet uw organisatie dat vertrouwen verdienen en vervolgens waarmaken. Een zorgvuldige verwerking van persoonsgegevens draagt bij aan dit vertrouwen. Het is daarom belangrijk vast te stellen hoe uw organisatie persoonsgegevens verwerkt. Een eerste stap hierbij is het creÎren van voldoende bewustzijn over het belang van de zorgvuldige omgang met persoonsgegevens binnen uw organisatie. Om het proces van bewustwording te stimuleren, is een korte privacyvragenlijst opgesteld. De uitkomsten van deze vragenlijst geven een globale indruk hoe het met de privacybescherming binnen uw organisatie is gesteld. De uitkomsten van de vragenlijst zijn nuttig voor de leiding van de organisatie die verantwoordelijk is voor de naleving van de privacywetgeving, maar ook voor de ondernemingsraad en, indien benoemd, de functionaris voor de gegevensbescherming. Ook in werkoverleg kan aandacht besteed worden aan de uitkomsten van deze vragenlijst.
Let op: De vragenlijst is beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens, zoals die in de WBP zijn geregeld.

Hoe werkt de vragenlijst?

Elke medewerker in een organisatie kan de vragenlijst zelfstandig invullen. De vragenlijst bestaat uit dertien vragen. U kunt de vragen beantwoorden met ëjaí of ëneeí. Door een vraag met ëjaí te beantwoorden, geeft u aan dat uw organisatie aandacht heeft voor het onderwerp van die vraag. Of er in voldoende mate en op de juiste wijze aandacht wordt besteed, kan pas worden gezegd na gericht onderzoek. Indien u ëneeí heeft geantwoord dan vraagt het betreffende onderwerp om nadere aandacht binnen uw organisatie. Mogelijk schiet uw organisatie tekort in het naleven van de wettelijke bepalingen. Op welke wijze de organisatie hier vervolg aan kan geven, vraagt eveneens om meer gericht onderzoek.
Op de website van het CBP (www.cbpweb.nl) vindt u per vraag een toelichting op de antwoordmogelijkheden van deze vragenlijst. Via deze toelichting kunt u zelf de voor uw organisatie beste vervolgstap bepalen.

Vervolgstap

Na het bekend worden van de uitkomsten van de vragenlijst kan de organisatie een gericht onderzoek uitvoeren naar de concrete invulling van de privacyeisen binnen de organisatie. Daarvoor is in eerste instantie een uitgebreide WBP Zelfevaluatie te verkrijgen. Via deze zelfevaluatie kunnen medewerkers van uw organisatie zelfstandig de kwaliteit van de maatregelen ter bescherming van persoonsgegevens beoordelen en nagaan op welke gebieden noodzakelijke maatregelen ontbreken of ontoereikend zijn. Daarmee vergroot u het vertrouwen van relaties in de zorgvuldige omgang met persoonsgegevens binnen uw organisatie.

Meer informatie?

Mocht u meer informatie willen over deze Quickscan of over het omgaan met persoonsgegevens in het algemeen dan kunt u de website van het College bescherming persoonsgegevens (www.cbpweb.nl) raadplegen. Via deze website kunt u ook de *WBP Zelfevaluatie* downloaden. Op de website treft u ook het *Raamwerk Privacy Audit* aan. Op basis van dit raamwerk kan een interne of externe auditor een gedetailleerd onderzoek uitvoeren naar de wijze waarop en de mate waarin uw organisatie omgaat met de bescherming van persoonsgegevens. Ook kunt u tussen 09.00 en 12.30 uur bellen met een adviseur van het CBP via telefoonnummer 070 381 13 00. U kunt ook faxen: 070 381 13 01 of e-mailen: info@cbpweb.nl.

Van wie is de vragenlijst afkomstig?

De vragenlijst is ontwikkeld in een samenwerkingsverband bestaande uit het CBP, diverse koepelorganisaties en verschillende marktpartijen van audit- en adviesorganisaties.

QUICKSCAN VRAGENLIJST

Het is mogelijk dat u geen zicht heeft op de totale organisatie waarin u werkzaam bent. In dat geval kunt u voor onderstaande vragen voor het woord organisatie ook de afdeling lezen waarin u werkzaam bent.

Privacybewustzijn in de organisatie

Voor het realiseren van een goede bescherming van de persoonsgegevens in een organisatie is privacybewustzijn en het proces van privacybewustwording van belang.

1 Is in uw bedrijf voorlichting gegeven over de nieuwe privacywet (WBP)? Ja Nee

2 Heeft de directie of leiding uitgesproken dat de organisatie de privacy van personen moet respecteren? Ja Nee

De directie of leiding van een organisatie kan op verschillende manieren de privacy bij haar medewerkers onder de aandacht brengen. Daarbij kan gedacht worden aan: informatiesessies over privacy, een privacyrichtlijn voor medewerkers, specifieke acties en maatregelen ter bescherming van de privacy.

3 Wordt er op uitvoerend niveau binnen uw organisatie aandacht besteed aan privacybescherming? Ja Nee

Uitvoering wettelijke bepalingen

Onder het verwerken van persoonsgegevens wordt onder meer verstaan het, zowel geautomatiseerd als handmatig, verzamelen, vastleggen, bewerken, bewaren, verstrekken, verwijderen en vernietigen van persoonsgegevens door organisaties.
De wet beperkt het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn, zoals door de organisatie vooraf geformuleerd, en doelstellingen die daarmee verenigbaar zijn.

4 Beperkt uw organisatie het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn en doelstellingen die daarmee verenigbaar zijn? Ja Nee

Het verwerken van persoonsgegevens kan uitsluitend plaatsvinden als daarvoor een rechtmatige grondslag aanwezig is. De WBP geeft aan op welke gronden verwerking toegestaan is.

5 Vindt het verwerken van persoonsgegevens binnen uw organisatie plaats in overeenstemming met de grondslagen van de WBP? Ja Nee

Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt.

6 Zijn er regels vastgesteld voor het verwerken van persoonsgegevens binnen uw organisatie? Ja Nee

De wet stelt strengere eisen aan de verwerking van bijzondere persoonsgegevens. Dit betreft gegevens over: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

7 Zijn er specifieke regels vastgesteld voor het verwerken van bijzondere persoonsgegevens binnen uw organisatie? Ja Nee

Voor een zorgvuldige verwerking moeten de persoonsgegevens die in uw organisatie worden verwerkt, correct zijn.

8 Controleert uw organisatie persoonsgegevens op juistheid en volledigheid? Ja Nee

De WBP legt organisaties die persoonsgegevens verwerken een informatieplicht op. Daardoor weten de personen (betrokkenen) van wie persoonsgegevens worden verwerkt hoe de organisatie met hun persoonsgegevens omgaat.

9 Leeft uw organisatie de informatieplicht naar betrokkenen na? Ja Nee

De WBP kent aan personen (betrokkenen) van wie persoonsgegevens worden verwerkt bepaalde rechten toe. Dit betreft het recht tot inzage, wijziging en verwijdering van persoonsgegevens en het recht op verzet tegen het verwerken van persoonsgegevens.

10 Komt uw organisatie de rechten van betrokkenen na? Ja Nee

Beveiliging

Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt. Dit betekent dat niet iedereen in een organisatie toegang mag hebben tot persoonsgegevens of deze mag bewerken, verstrekken of verwijderen.

11 Heeft uw organisatie bevoegdheden aan medewerkers toegekend zodat uitsluitend geautoriseerde medewerkers toegang hebben tot persoonsgegevens? Ja Nee

De WBP stelt dat een organisatie passende technische en organisatorische maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, met inbegrip van onnodige verwerking.

12 Heeft uw organisatie maatregelen getroffen die verlies en onrechtmatige verwerking van persoonsgegevens tegengaan? Ja Nee

Controle
Controle op de naleving van de maatregelen die de organisatie getroffen heeft, bij de onderwerpen van de vragen 4 tot en met 12, is belangrijk voor een goede bescherming van de persoonsgegevens.

13 Wordt de naleving van de maatregelen voor privacybescherming binnen uw organisatie van tijd tot tijd gecontroleerd? Ja Nee

COLLEGE BESCHERMING PERSOONSGEGEVENS

Het College bescherming persoonsgegevens (CBP) – onder de Wet bescherming persoonsgegevens (WBP) de opvolger van de Registratiekamer – houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Bij het CBP moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt.

Advies, bemiddeling, onderzoek en interventie
Het CBP adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Het CBP toetst gedragscodes en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan het CBP onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet en daaraan zonodig gevolgen verbinden. Voor in gebreke blijven bij de melding kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het CBP overgaan tot bestuursdwang of een dwangsom opleggen.

Over zijn werkzaamheden en bevindingen brengt het CBP jaarlijks een openbaar verslag uit. Het CBP is bij de uitvoering van zijn bevoegdheden gehouden aan de normen die worden gesteld in de Algemene wet bestuursrecht. Beslissingen van het CBP zijn vatbaar voor bezwaar en beroep. Het gedrag van het CBP kan onderzocht worden door de Nationale Ombudsman.

Informatie
Voor meer informatie kunt u kijken op de website: www.cbpweb.nl. Alle publicaties kunt u via de website bestellen of elektronisch binnen halen; telefonisch bestellen is ook mogelijk. Voor eerste advies kunt u gebruik maken van het telefonisch spreekuur, op werkdagen van 9.00 ñ 12.00 uur, telefoon 070 888 85 00.