Privacy Enhancing Technologies
Witboek voor beslissers

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

December 2004

Privacy Enhancing Technologies
Witboek voor beslissers

Geschreven in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Directie Innovatie en Informatiebeleid Openbare Sector (DIIOS)

Auteurs KPMG Information Risk Management:

Drs. ing. Ronald Koorn RE (eindverantwoordelijk)
Drs. Herman van Gils RE RA
Drs. Joris ter Hart
Dr. ir. Paul Overbeek RE
Drs. Raúl Tellegen

In samenwerking met drs. John Borking (Borking Consultancy)

Inhoudsopgave

Bijlagen:

1 Managementsamenvatting

Dit Witboek over Privacy Enhancing Technologies (PET) is geschreven om u te stimuleren PET toe te passen om persoonsgegevens veilig te verwerken. PET is de verzamelnaam voor verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen. Voordelen van PET zijn:

- PET maakt toepassingen mogelijk die anders onmogelijk zouden zijn;
- Het automatiseren van privacymaatregelen is veelal effectiever en efficiënter dan het louter steunen op organisatorische procedures en handmatige activiteiten. Processen zijn derhalve te optimaliseren door toepassing van PET;
- De inzet van PET heeft een positieve uitstraling en geeft burgers vertrouwen in de verwerking van zijn/haar persoonsgegevens in overheidsinformatiesystemen;
- De kosten van PET-toepassing zijn relatief beperkt als reeds in het ontwerpstadium rekening is gehouden met privacyaspecten. De kwantitatieve én kwalitatieve baten van PET voor de betrokken organisaties, de maatschappij en de burgers zijn aanzienlijk.

Is PET geschikt voor alle vormen van overheidsinformatisering?

Voor de uitvoering van publieke taken is sprake van verdergaande informatisering, zowel binnen organisaties als in ketenverband. Het is duidelijk dat steeds meer (authentieke) registraties in backoffice-systemen gekoppeld worden – al dan niet ontsloten via één loket – om klantvriendelijkheid te vergroten, fraude te reduceren en de kwaliteit van de persoonsgegevens te verbeteren.

PET is een geschikt middel om geavanceerde vormen van informatisering binnen privacy-kaders te realiseren.

PET blijkt goed toepasbaar te zijn voor alle type informatiesystemen. De in dit Witboek besproken typen zijn: centrale database, gekoppelde backoffices, routerings-instituut, keteninformatisering en decentrale databases. Daarbij geldt dat niet alle PET-vormen bruikbaar zijn voor alle type systemen.

PET is toepasbaar in alle typen informatiesystemen.

Welke PET-vormen zijn toepasbaar?

Bekende en breed toegepaste basisvormen van PET zijn versleuteling en logische toegangsbeveiliging. Binnen logische toegangsbeveiliging zijn met name het goede beheer van uniek identificerende persoonsgegevens en bijbehorende autorisatie-gegevens van belang.

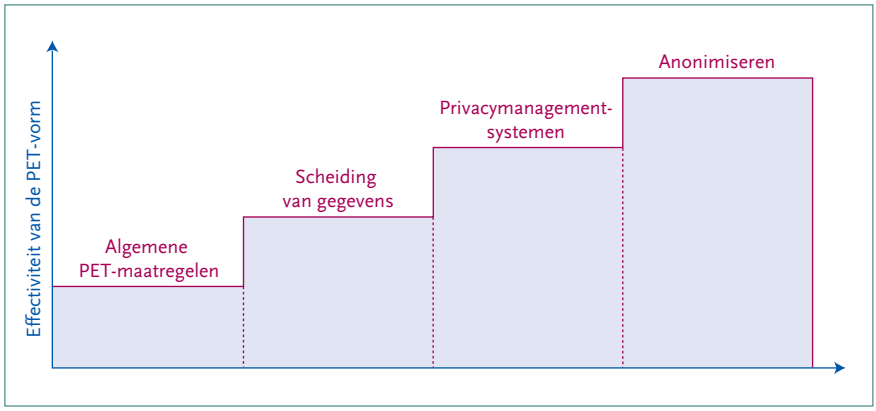
Een belangrijke vorm van PET betreft de scheiding van gegevens in meerdere domeinen. Het ene domein bevat de identificerende persoonsgegevens, het andere de overige persoonsgegevens. De financiële, justitiële of medische gegevens zijn dan in één of meer domeinen opgenomen – los van het domein met de identiteitsgegevens. De gegevens in ieder afzonderlijk domein zijn niet privacygevoelig, omdat ze niet herleidbaar zijn naar een natuurlijk persoon. In deze PET-vorm zorgt programmatuur ervoor dat uitsluitend geautoriseerde systeemgebruikers de verschillende gegevensdomeinen kunnen koppelen. Een variant op de gegevensscheiding is de systeemfunctie die wel verifieert welke detailgegevens in de database zijn opgeslagen, maar die details niet vrijgeeft. De functie antwoordt bijvoorbeeld slechts bevestigend of ontkennend op een bevraging.

Met alle PET-vormen zijn succesvolle praktijkervaringen opgedaan.

Een verdergaande integratie van gegevens en programmatuur wordt gevormd door een PET-vorm waarin de persoonsgegevens uitsluitend te benaderen zijn via specifieke programmatuur – het zogenaamde privacymanagementsysteem. Hierin is de vertaling van het privacyreglement geautomatiseerd. Voor ieder gegevenselement en iedere systeemfunctie wordt direct gecontroleerd of een activiteit in overeenstemming is met de regels in het privacy-reglement.

De ultieme vorm van PET betreft het anonimiseren van persoonsgegevens. Het gaat hierbij om programmatuur die de identificerende persoonsgegevens geheel niet registreert of direct vernietigt nadat die gegevens niet meer nodig zijn – bij voorkeur direct na het verzamelen. Idealiter worden deze persoonsgegevens dan niet eens meer opgeslagen. Dit is de sterkste vorm van bescherming van persoonsgegevens waarbij direct aan de wettelijke privacyeisen is voldaan. Anonimisering is natuurlijk niet altijd toepasbaar; in de situaties waarin persoonsgegevens noodzakelijk zijn kunt u beter één van de voorgaande PET-vormen toepassen.

In nevenstaand figuur is in de PET-trap aangegeven dat de effectiviteit van de bescherming van persoonsgegevens wordt bepaald door de toegepaste PET-vorm. De geschiktheid van de verschillende PET-vormen is met name afhankelijk van het type informatiesysteem, het nagestreefde ambitieniveau en de gevoeligheid van de persoonsgegevens.



Figuur 1: PET-trap

Wat zijn de kosten en baten van PET?

Om te onderzoeken of in uw organisatie een positieve businesscase bestaat voor de toepassing van PET zijn drie aspecten van belang, namelijk:

- de eenmalige en structurele kosten die aan de toepassing van PET zijn verbonden;
- kostenreductie en kwaliteitsverbetering;
- de bijdrage aan de beleidsdoelstellingen.

De kosten van PET-toepassing bedragen bij de meeste projecten slechts enkele procenten van het totaalbudget en laten zich derhalve snel terugverdienen.

Hoe is PET toe te passen?

Een belangrijke les uit eerdere PET-projecten is het in een zo vroeg mogelijk stadium nadenken over de noodzaak van vastlegging van persoonsgegevens, de wijze van gegevensbescherming, de oplossingsrichtingen en de bijbehorende kosten en baten. Dit zorgt ervoor dat gegevensbescherming gewoon als één van de eisen wordt geformuleerd en derhalve op een natuurlijke wijze in de bouw wordt betrokken. Hierbij kunnen PET-strategieën worden toegepast, de drie belangrijkste strategieën betreft:

- het voorkomen van identificatie;
- het waarborgen tegen onrechtmatige verwerking van persoonsgegevens;
- het toepassen van specifieke privacyondersteunende technologieën.

Het later toevoegen van PET in een informatiesysteem is zeker mogelijk gezien enkele praktijkervaringen, maar kan soms dieper in het informatiesysteem ingrijpen. Overigens geldt dat met name voor de geavanceerde PET-vormen en -maatregelen.

PET kan het beste al bij de projectstart of bij een grote systeemaanpassing in de specificatie- en ontwerpfase worden meegenomen. Privacy by design is een belangrijk uitgangspunt voor een succesvolle PET-toepassing.

Zijn er organisatorische implicaties?

Daar programmatuur en ICT-infrastructuur geautomatiseerde voorzieningen bevatten zal door de toepassing van PET de inspanning voor het intern en extern verantwoorden van een goede gegevensbescherming geringer zijn dan zonder PET. PET zal een plaats moeten krijgen in de managementcyclus van het ontwikkelen en beheren van informatie-systemen met persoonsgevoelige gegevens. Dit betekent dat naast ontwerp en implementatie ook aandacht besteed moet worden aan zaken als risicoanalyse, toetsing, toezicht en bijstelling van PET-maatregelen.

Het denken over PET door proceseigenaren, beleidsmedewerkers en projectleiders is een essentiële randvoorwaarde om PET succesvol in een informatiesysteem en een organisatie in te voeren.

Samengevat:

PET is meer dan een manier om persoonsgegevens te beschermen:

- **PET willen!**
  - PET bevordert de informatiekwaliteit.
  - De afhankelijkheid van de goede naleving van processen en procedures vermindert door het automatisch afdwingen van privacyregels.
  - Het toepassen van PET kan een middel zijn om burgers betere inzage- en controle-mogelijkheden over hun persoonsgegevens te geven.
- **PET moet!**
  - Met PET kan eenvoudiger worden voldaan aan de Wet bescherming persoonsgegevens.
  - PET is voorwaardenscheppend voor het vertrouwen van de burger.
  - PET maakt werken met gevoelige persoonsgegevens mogelijk.
- **PET kan!**
  - PET is al vele malen succesvol geïmplementeerd, dit Witboek is gelardeerd met diverse voorbeelden daarvan.
  - PET heeft slechts een beperkte invloed op de ontwikkelkosten van een nieuw informatiesysteem aangezien de technieken voorhanden zijn en het voornamelijk het toepassen ervan betreft. Het 'kost' met name denk- en ontwerpwerk.
  - Het opnemen van PET in uw informatiearchitectuur biedt een basis om PET in verschillende informatiesystemen efficiënt toe te passen.

Figuur 2: Redenen voor PET

2 Waarom PET?

Dit hoofdstuk behandelt de redenen om PET op dit moment toe te passen. Het bestaat uit de volgende paragrafen:

- PET als middel voor gegevensverwerking die anders onmogelijk zou zijn (§ 2.1);
- Technische invulling van wettelijke vereisten (§ 2.2);
- Privacy Enhancing Technologies (§ 2.3);
- Wat heb ik aan PET? (§ 2.4);
- Waarom nu PET? (§ 2.5).

2.1 PET als middel voor gegevensverwerking die anders onmogelijk zou zijn

Alles wijst in de onomkeerbare richting van meer, efficiëntere en gebruikersvriendelijkere dienstverlening. Voorbeelden zijn de 'één-op-één'-benadering in de marketing en de 'één-loket'-gedachte binnen overheidsorganisaties en zelfstandige bestuursorganen. Er zijn inmiddels diverse voorstellen gespecificeerd in verschillende beleidsnotities, zoals Stroomlijning Basisgegevens, het Burger Servicenummer, PKIoverheid en E-gem (Elektronische Gemeente). Op de oude manier doorgaan met gegevensverwerking zonder stroomlijning, integratie en afstemming met overige overheidsonderdelen zal spoedig niet meer kunnen. Efficiëntieverbetering en kostenbeheersing zullen belangrijke aanjagers van vernieuwing zijn. De overheid moet zich daarvoor gereedmaken. Aangezien het handhaven van een hoog niveau van vertrouwen in de overheid de sleutel is tot het welslagen van nieuwe initiatieven als keteninformatisering en e-government, zal een aantal voorzorgsmaatregelen noodzakelijk zijn. Vertrouwen maakt immers communicatie en samenwerking met elkaar mogelijk. In onze tastbare wereld hebben wij langzaam maar zeker geleerd welke signalen leiden tot vertrouwen. Dit is vaak een kwestie van non-verbale lichaamssignalen. In de virtuele wereld zijn er geen tastbare signalen. Bescherming van persoonsgegevens van de burger is een uiterst belangrijke hoeksteen van het beleid dat beoogt dat de burger vertrouwen heeft in de overheid en dient te houden. Zonder dat vertrouwen zal de weerstand tegen een efficiënte en persoonsgerichte dienstverlening toenemen en zal die dienstverlening met achterdocht worden bekeken.

FAQ 1: Werkt gegevensbescherming beknellend?

Gegevensbescherming wordt vaak als knellend gezien door organisaties. Reden hiervoor is dat pas in een laat stadium over de praktische aspecten van de bescherming van persoonsgegevens wordt nagedacht. Vervolgens blijkt het uiterst lastig om PET-maatregelen in dat stadium of zelfs achteraf nog toe te voegen. Wanneer vroegtijdig over gegevensbescherming wordt nagedacht en dit wordt meegenomen in de systeemontwikkeling, gaan gegevensbescherming en functionaliteit van het informatiesysteem hand in hand, zonder dat het ene aspect concessies hoeft te doen aan het andere.

Vanwege de immer toenemende technologische mogelijkheden worden steeds meer gegevens vastgelegd, waaronder persoonsgegevens. Veelal hebben vastleggingen een directe binding met het uit te voeren primaire proces, maar soms heeft het vastleggen van persoonsgegevens een ander of geen duidelijk doel. Hierbij kan worden gedacht aan de formulieren die ingevuld moeten worden op het internet als de burger bijvoorbeeld alleen maar een document wil downloaden. Op de formulieren moeten soms NAW-gegevens worden ingevoerd alsmede aanvullende informatie zoals beroep of werkgever. Deze gegevens zijn echter niet nodig voor het downloaden van het document, maar hebben als doel het profiel van de bezoeker van de website in kaart te brengen. Ook de overheid legt veelvuldig persoonsgegevens vast. Weliswaar niet met het doel commerciële marketingactiviteiten te ontplooien, maar met het doel de burger beter van dienst te zijn of uit gewoonte. Vooral met de opkomst van de elektronische overheid en de administratieve lastenverlichting vinden er in toenemende mate elektronische vastleggingen plaats. Daardoor kan een bepaald beeld van personen worden verkregen. Potentieel zijn er, zo blijkt uit onderzoek naar de bescherming van persoonsgegevens, onbedoeld veel risico's op privacyinbreuken. De makkelijkste manier om dat te voorkomen is uitsluitend die gegevens te verzamelen en te verwerken die strikt noodzakelijk zijn voor het doel waarvoor de verwerking plaats moet vinden. Niet meer en niet minder. Gegevensbescherming is dus in ons eigen belang.

Om de persoonsgegevens te beschermen zijn er nationale en internationale richtlijnen en wetten opgesteld. De belangrijkste in het kader van de gegevensbescherming is de Wet bescherming persoonsgegevens (Wbp). Deze wet is sinds 1 september 2001 van kracht en na een overgangsjaar zijn sinds 1 september 2002 organisaties verplicht om de Wbp geheel na te leven. Dit betekent dat bijna alle organisaties aan alle relevante Wbp-eisen moeten voldoen. Uit ervaring is gebleken dat dit geen eenvoudige opgave is, aangezien dit grote delen van de organisatie raakt waar persoonsgegevens worden gebruikt.

2.2 Technische invulling van wettelijke vereisten

Gegevensbescherming speelt zich op dit moment vaak af in de juridische en administratieve sfeer, waarbij het management veel tijd kwijt is aan de voorbereiding en bewaking. Het toch al druk bezette management kan deze tijd beter aan andere activiteiten besteden. Stel dat de bescherming van persoonsgegevens verdergaand geautomatiseerd zou kunnen worden dan tot nu het geval is. Dat zou tijd vrijmaken voor de primaire processen waar u verantwoordelijk voor bent. En daarnaast gegevensbescherming beter afdwingen. Kan dat? Tijdens de behandeling in het parlement van de Wbp is gebleken dat informatie- en communicatietechnologie (ICT) een belangrijke rol kan spelen in het waarborgen van de gegevensbescherming van burgers. Naast organisatorische maatregelen kan ter bescherming van persoonsgegevens ook technologie worden aangewend. De term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen (zie woordenlijst in bijlage C voor een definitie van het begrip PET). Dit begrip omvat mede de inrichting van de architectuur van informatiesystemen. Met PET wordt het vertrouwen van de burger vergroot en kan nieuwe technologie door de overheid worden aangewend om de service aan de burger te verbreden, te verdiepen en te verbeteren.

FAQ 2: Is PET een onderwerp van en voor automatiseerders?

Nee, PET vraagt in eerste instantie om beleid inzake gegevensbescherming en is na de keuze voor de geëigende PET-vorm een kwestie van de juiste uitvoering. De PET-vorm wordt veelal aangevuld met organisatorische en procedurele maatregelen, zodat de privacyrisico's toereikend worden gedekt. Automatiseerders kunnen aangeven welke technische mogelijkheden beschikbaar zijn en kunnen deze na besluitvorming verder ontwerpen, ontwikkelen en implementeren. Het streven naar een 100% PET-oplossing is niet noodzakelijk, het gaat erom op een goede manier persoonsgegevens te beschermen.

De Wbp is de vervanger van de Wet persoonsregistraties (Wpr) uit 1988 en is de implementatie van de Europese richtlijn 95/46. In de Wbp worden de rechten en plichten van alle betrokken organisaties en personen bij de verwerking van persoonsgegevens gedefinieerd. Onder verwerking wordt het gehele proces vanaf verzamelen, vastleggen tot en met vernietigen verstaan. In de Wbp wordt een aantal privacybeginselen gedefinieerd. De voor dit Witboek relevante beginselen zijn in figuur 3 beschreven.

1. Transparantie	De betrokkene moet voorafgaand aan de (eerste) registratie op de hoogte worden gesteld van de identiteit van de organisatie en het doel waarvoor de gegevens worden verwerkt.
2. Doelbinding	De verzamelde persoonsgegevens worden alleen verder verwerkt als dit verenigbaar is met het doel waarvoor ze zijn verkregen.
3. Rechtmatige grondslag	De Wbp geeft limitatief aan in welke gevallen persoonsgegevens mogen worden verwerkt. Voor gevoelige gegevens - de bijzondere gegevens als bedoeld in de Wbp – geldt dat verwerking onrechtmatig is tenzij aan specifieke voorwaarden is voldaan.
4. Kwaliteit	Voor het doel behoren de persoonsgegevens toereikend, terzake dienend en niet bovenmatig te zijn.
5. Rechten betrokkenen	De betrokkene heeft recht op inzage, verbetering, aanvulling, verwijdering of afscherming van diens persoonsgegevens.
6. Beveiliging	De verantwoordelijke treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
7. Verstrekking aan niet EU-landen	Doorgifte van persoonsgegevens aan landen buiten de EU is niet toegestaan als er geen vergelijkbaar privacyregime heerst.

Figuur 3: Beschrijving van essentiële privacybeginselen

De in dit figuur genoemde privacybeginselen bepalen de benodigde waarborgen voor de bescherming van persoonsgegevens. Iedere verwerker van persoonsgegevens moet rekening houden met deze beginselen en dus voldoen aan de Wbp. Dit is echter niet de enige reden om de informationele privacy van burgers te respecteren. Het is ook een maatschappelijke verwachting dat de persoonsgegevens van burgers worden beschermd. Daarbij heeft de overheid een voorbeeldfunctie met het naleven van wetten die zij zelf heeft opgesteld.

2.3 Privacy Enhancing Technologies

In functionele zin is het toepassen van PET niet moeilijk. Met behulp van PET kan informatie over een persoon, zoals de identiteit en persoonlijke gegevens, worden beschermd. PET omvat alle technische maatregelen om de privacy te waarborgen. PET kan bijvoorbeeld worden gebruikt om de identiteitsgegevens los te koppelen van de overige gegevens die zijn vastgelegd over een persoon. Alleen met bepaalde hulpmiddelen kan dan de koppeling worden gemaakt tussen de identificerende gegevens en de overige persoonsgegevens. Een andere mogelijkheid van PET is het voorkomen dat er überhaupt persoonsgegevens worden vastgelegd, nadat bijvoorbeeld eenmaal de identiteit is vastgesteld. Ook kan door middel van programmatuur worden afgedwongen dat het verstrekken van gegevens altijd voldoet aan het vigerende privacybeleid ('privacy policies'). In hoofdstuk 4 worden de verschillende PET-vormen verder uitgewerkt. In casus 1 wordt een voorbeeld gegeven van een PET-vorm zoals toegepast bij het project Clearinghouse Hoger Onderwijs [2].

Casus 1: Clearinghouse Hoger Onderwijs

De gegevensuitwisseling in het hoger onderwijs gaat worden ondersteund door het Virtual Clearing-house Hoger Onderwijs (VCH). Het VCH wordt ontwikkeld door de Stichting SURF. Hierbij zal het Onderwijsnummer en een ander sectornummer als unieke identificatie van studenten worden gehanteerd. Doelstelling van de VCH is om een eenvoudige ICT-infrastructuur, gemeenschappelijke gegevensdefinities en stroomlijning van gegevensuitwisseling te bewerkstelligen. Hiermee is verbeterde en versnelde gegevensuitwisseling alsmede administratieve lastenverlichting te realiseren. De gegevens van onderwijsinstellingen zijn op die manier efficiënt uit te wisselen tussen onderwijsinstellingen, de Informatie Beheer Groep (IB-Groep), het CBS, het ministerie van OCW, en dergelijke.

PET-toepassing

- beperken van het gebruik van het Onderwijsnummer, dat in de meeste gevallen identiek is aan het sofi-nummer, tot de wettelijk voorgeschreven uitwisseling tussen het VCH (namens de betreffende instelling) en de IB-groep. Zodra een student het hoger onderwijs domein binnentreedt wordt door het VCH een ander sectornummer toegekend. Het sectornummer wordt verder binnen de instellingen en door het VCH gebruikt. Het is derhalve niet mogelijk het onderwijsnummer in allerlei administratieve processen te gebruiken. De koppeling tussen Onderwijsnummer en sectoraal nummer is geregistreerd in een beveiligde tabel;

2 In dit Witboek zijn op verschillende plaatsen voorbeeldcasussen opgenomen ter illustratie van de mogelijke PET-toepassingen. Vanwege het feit dat de eerste toepassingen van PET plaatsvonden in de zorgsector zijn er meer casussen uit deze sector vermeld dan uit andere sectoren. Ook de casussen uit de zorgsector laten PET-toepassingen zien die eveneens in andere sectoren kunnen worden benut of al zijn benut.

- direct verifiëren van ingevoerde gegevens via een GBA [3] -koppeling voor betrouwbare gegevensregistratie;
- hanteren van standaarden en protocollaire afspraken over de gegevensverwerking en over beveiliging van identificerende nummers binnen instellingen;
- gebruikmaken van authenticatie op basis van kennis (persoonsgegevens, Onderwijsnummer) en bezit (per post opgestuurde code), eventueel aangevuld met andere middelen (bijv. bankpas);
- verdelen van gegevens over drie domeinen: studentgegevens, instellingsgegevens en IB-Groep-gegevens. Deze domeinen bepalen tevens het eigenaarschap en de beveiliging van de gegevens (op rollen gebaseerde autorisaties);
- door studenten on-line laten raadplegen en wijzigen van eigen persoonsgegevens.

Baten

Zonder PET-toepassing kan een dergelijk clearinghouse nauwelijks betrouwbaar functioneren. De PET-maatregelen vergroten de transparantie en gegevenskwaliteit en gaan fraude met diploma's en studieresultaten tegen.

Naast het inzetten van PET is het van belang dat iedereen die betrokken is bij de gegevensverwerking, het belang van gegevensbescherming onderkent. De organisatie moet zich bewust worden van het feit dat het hebben van meer persoonsgegevens niet altijd beter is. Alvorens PET wordt toegepast, is het raadzaam om na te gaan welke persoonsgegevens noodzakelijk zijn voor de dienstverlening. Gegevensminimalisatie is een belangrijk uitgangspunt. Voordeel hiervan is dat gegevens die niet zijn vastgelegd, ook niet beschermd hoeven te worden. Voorkomen is beter dan genezen. Een ander voordeel is dat gegevens die niet zijn vastgelegd, ook niet beheerd hoeven te worden. De beheer- en onderhoudsinspanning neemt derhalve af.

Bewustwording van de organisatie omtrent gegevensbescherming en geschikte technische maatregelen hiervoor gaat vooraf aan het ontwikkelen en invoeren van PET. Het goed vooraf nadenken over PET verbetert de toepassing van PET.

PET is een onderdeel van het effectiever en efficiënter met gegevensbescherming omgaan. Ook wanneer PET niet strikt noodzakelijk is vanuit wettelijk perspectief kan PET de organisatie van nut zijn. De invoering van PET vraagt namelijk om kritisch na te denken over persoonsgegevens en de noodzaak en de bescherming ervan. Deze aanpak verhoogt de integriteit en vertrouwelijkheid van de gegevens.

3 GBA: Gemeentelijke Basisadministratie

PET is derhalve ook een hulpmiddel om uw informatiesystemen hygiënisch te houden en de kwaliteit van de informatie te verhogen.

Gebruik van PET verhoogt de hygiëne van het informatiesysteem.

2.4 Wat heb ik aan PET?

Uit de voorgaande paragraaf is gebleken dat u PET kunt inzetten om de gegevensbescherming van de burger te waarborgen. Daarnaast kan die inzet uw organisatie in staat stellen de risico's van inbreuken op de bescherming van persoonsgegevens beter te voorkomen en te managen. Natuurlijk zijn er ook 'gewone' privacyoplossingen, maar deze steunen vaak sterk op organisatorische en procedurele maatregelen. De gegevensbescherming is daarbij zo sterk als de zwakste schakel in het proces. Uit vele beveiligings- en privacyaudits is gebleken dat mensen vaak vergeten of nalatig zijn de geëigende beveiligingsmaatregelen consequent toe te passen en te blijven toepassen. Algemene informatiebeveiliging werkt niet altijd waardoor privacyrisico's ontstaan. Men bouwt dikke en dure muren rond gegevens, maar zonder organisatorische naleving van richtlijnen en procedures voorkomt dat niet het lekken van gegevens. Het risico wordt niet uitgesloten dat ongeautoriseerde personen toegang krijgen tot persoonsgegevens met alle gevolgen van dien.
Met behulp van PET kan een organisatie aan de bron al technische maatregelen treffen en het aantal identificerende gegevens tot het absolute minimum beperken. Daar waar het niet nodig is, wordt de identiteit niet vastgelegd of wordt de identiteit losgekoppeld van de overige persoonsgegevens.

Casus 2: Landelijke Centrale Middelen Registratie

De Landelijke Centrale Middelen Registratie (LCMR) van Prismant en de Stichting Informatievoorziening Zorg (IVZ) is een informatiesysteem dat hulpverleners ondersteunt om aan verslaafde patiënten de juiste dosering van het voorgeschreven geneesmiddel – waaronder bijvoorbeeld methadon – te verstrekken. Nevendoelstellingen voor de opdrachtgevers, de ministeries van VWS en Justitie, zijn ook het tegengaan van diefstal en onjuist gebruik van verslavende middelen en het beschikbaar stellen van beleidsinformatie. Het centrale LCMR-systeem wordt gevoed met informatie uit verschillende lokale registratiesystemen met gegevens over patiënten, medicatieverstrekking en hulpverlening.

PET-toepassing

De volgende PET-maatregelen zijn in het LCMR-systeem opgenomen:

- minimaliseren van centraal vastgelegde gegevens, centraal is vrijwel alleen een verwijsindex opgeslagen;

- beperken van toegang tot persoons- en medicatiegegevens tot uitsluitend geautoriseerde hulpverleners door met biometrie beveiligde chipkaarten en verfijnde autorisatiestructuur. De gekozen biometrische vorm betreft de vingerafdruk, waarbij van iedere persoon vier vingerscans worden afgenomen. Dankzij de gekozen techniek is het niet meer mogelijk van de vingerscans een visuele vingerafdruk te maken;
- registreren van recepten op de chipkaart van patiënten waarmee zij bij de door hen gewenste apotheek de medicatie kunnen verkrijgen;
- anonimiseren van gegevens voor onderzoek en voor de bijstelling van medicatievoorschriften.

Baten

Het LCMR-systeem biedt door de PET-toepassing sterke waarborgen voor de identiteit van de patiënt die medicatie ontvangt en de hulpverlener die gevoelige persoonsgegevens gebruikt. Verder kunnen er op ieder willekeurig tijdstip actuele gegevens worden opgevraagd in plaats van uitsluitend tijdens openingstijden van de zorginstelling. De chipkaart maakt mobiliteit mogelijk voor patiënten.

De belangrijkste voordelen van een structurele inpassing van PET in informatiesystemen zijn:

- Dankzij PET zijn bepaalde gegevenswerkende processen mogelijk die zonder PET onmogelijk of onrechtmatig zouden zijn. Zonder de toepassing van PET ontbreekt het namelijk aan adequate gegevensbescherming en zou de verwerking in strijd zijn met de Wbp.
- Het toepassen van PET zorgt voor een positieve uitstraling, waardoor zowel uw medewerkers als uw klanten er vertrouwen in hebben dat uw organisatie goed omgaat met persoonsgegevens. Privacycertificering kan dat vertrouwen verder versterken. Voordeel is dat de overheid haar takenpakket zo efficiënt en effectief mogelijk kan uitvoeren.
- Door de toepassing van PET en het uitgangspunt van gegevensminimalisatie verbetert de kwaliteit van de informatie. Er worden namelijk minder gegevens dan normaal verwerkt en gebruikers hebben uitsluitend toegang tot de voor hen noodzakelijke gegevens. De kans op vervuiling van persoonsgegevens in uw organisatie daalt daardoor. Tevens neemt in het algemeen de beheer- en onderhoudsinspanning af aangezien persoonsgegevens niet of op een zorgvuldigere wijze worden verwerkt.
- U hoeft zich minder zorgen te maken over de bescherming van persoonsgegevens. U hoeft zich niet telkens af te vragen of u aan de Wbp voldoet op het moment dat u geen persoonsgegevens meer registreert [4]. Voordeel hiervan is dat u diverse organisatorische maatregelen niet hoeft te treffen en geen risico loopt op boetes en

sancties van het College Bescherming Persoonsgegevens (CBP). Daar waar uw organisatie wel persoonsgegevens moet verwerken, kan het verwerkingsproces 'Wbp-proof' worden gemaakt.

- PET zorgt niet alleen voor bescherming van persoonsgegevens, maar geeft ook hulpmiddelen die nodig zijn indien de burger meer inzage in de van hem of haar vastgelegde gegevens wenst. Dat leidt weer tot een hogere kwaliteit van de vastgelegde gegevens. Dit is een belangrijk privacybeginsel en sluit aan op de gewenste transparantie.

FAQ 3: Is PET te duur voor mijn organisatie?

Nee, er zijn verschillende PET-vormen mogelijk met ieder een eigen kostenniveau. Het is van belang om na te gaan of de kosten die met de oplossing zijn gemoeid in verhouding staan tot de risico's. Eenvoudige, maar krachtige PET-maatregelen kunnen zelfs met geringe kosten een wezenlijke verbetering van de gegevensbescherming opleveren. In hoofdstuk 5 wordt beschreven hoe u een businesscase voor een PET-vorm kunt opstellen. Hierin zijn zowel kwalitatieve als kwantitatieve aspecten beschouwd.

2.5 Waarom nu PET?

In tijden van bezuinigingen en in het kader van de administratieve lastenverlichting streeft de overheid naar een zo efficiënt mogelijke dienstverlening. Dit uit zich bijvoorbeeld in het meervoudig gebruik van eenmalig vastgelegde persoonsgegevens. Hierbij wordt gebruikgemaakt van authentieke registraties zoals de GBA. Hierover is de notitie 'Stroomlijning Basisgegevens' verschenen [5]. Daarnaast digitaliseert de overheid haar dienstverlening in belangrijke mate [6] en worden steeds meer registers elektronisch ontsloten. Een voorbeeld hiervan is het kentekenregister van de RDW (Centrum voor voertuigtechniek en informatie).

4 Dit is afhankelijk van de plaats van de PET-oplossing in het informatiesysteem. Hierop zal in hoofdstuk 4 verder worden ingegaan.
5 Zie hiervoor www.stroomlijningbasisgegevens.nl.
6 Zie bijvoorbeeld www.elo.nl.

In figuur 4 is een passage uit de Troonrede 2003 weergegeven waaruit blijkt dat de authentieke registratie en de elektronische overheid sterk in opkomst zijn.

> De regering streeft ernaar dat in 2004 ongeveer de helft van de publieke informatie ook op internet beschikbaar zal zijn, om zo de toegankelijkheid van de overheid te verbeteren. Daarenboven zal de burger in de toekomst niet steeds opnieuw, maar slechts één keer zijn persoonsgegevens aan de overheid hoeven te verstrekken.

Figuur 4: Fragment uit Troonrede 2003

Vanwege deze toenemende digitalisering worden steeds meer persoonsgegevens van burgers door de overheid elektronisch verwerkt en worden er databases gekoppeld, waardoor persoonsgegevens gemakkelijker benaderbaar zijn. Dit kan op gespannen voet staan met de eerdergenoemde privacybeginselen. Het is daarom van belang dat de gegevensbescherming en de efficiëntie en effectiviteit van de gegevensverwerking met elkaar in evenwicht zijn. Het waarborgen van de gegevensbescherming moet een efficiënte en effectieve overheid niet in de weg staan. PET maakt het mogelijk de gegevensbescherming te waarborgen zonder een te grote aanslag te plegen op het verwerkingsproces. Door middel van het toepassen van PET en het stroomlijnen van de gegevensverwerking van personen kan de overheid blijven voldoen aan de hoge verwachtingen die de burgers hebben omtrent de kwaliteit van de dienstverlening en de omgang met persoonsgegevens. Met PET bent u klaar voor de nieuwe wijze van gegevensverwerking.

Casus 3: Routeringsinstituut RINIS

RINIS faciliteert de gegevensuitwisseling tussen overheidsorganisaties in de sociale zekerheidssector via een gesloten EDI-netwerk. Deze uitwisseling vermijdt het doorgeven van mutaties voor burgers en instellingen aan alle afzonderlijke partijen. Instellingen als de Uitvoeringsinstituut Werknemersverzekeringen (UWV), Sociale Verzekeringsbank (SVB), Belastingdienst, diverse ministeries (Justitie, BZK, Financiën), zorgverzekeraars, Informatie Beheer Groep en andere uitvoeringsinstanties wisselen hier (bulk)berichten uit tussen backoffice-systemen, bijvoorbeeld het informeren van de SVB van nieuwe registraties bij de UWV. RINIS verzorgt de koppeling tussen meerdere sectoren, waarbij de Sectorale Aanspreekpunten van een RINIS-server zijn voorzien.

PET-toepassing

Uitwisseling vindt plaats over een gesloten netwerk, waarbij de aangesloten partijen onomstotelijk vaststaan door gebruikmaking van digitale certificaten. De volgende PET-maatregelen zijn in RINIS toegepast:

- minimaliseren van persoonsgegevens door uitsluitend sofi-nummers en berichtencodes uit te wisselen;
- sterke beveiliging door het versleutelen van de uitgewisselde berichten, welke op berichtniveau worden geautoriseerd voor verzending en worden voorzien van een elektronische handtekening. Onbevoegden of beheerders hebben geen toegang tot de berichtinhoud. De sleutels worden uitgegeven en beheerd door een vertrouwde derde partij (zg. Certification Service Provider);
- verbeteren van gegevenskwaliteit door valideren van berichten op de centrale server zodat uitsluitend toegestane codes worden verwerkt. Tevens worden de berichten slechts enkele minuten vastgehouden voor het eventueel opnieuw moeten verzenden bij storingen;
- loggen op berichtniveau, niet op berichtinhoud, zodat een rechtmatigheidstoets achteraf mogelijk blijft.

Baten

De PET-toepassing binnen RINIS heeft gezorgd voor een veilige uitwisseling van berichten tussen partijen die zekerheid hebben over elkaars identiteit en over de betrouwbaarheid van de gegevensverwerking. Het minimaliseren van de persoonsgegevens en de centrale rol van RINIS vergroten het succes van de RINIS-oplossing.

Zoals uit dit hoofdstuk is gebleken, heeft PET voordelen te bieden.
Om misverstanden te voorkomen: PET is geen losse component uit een informatiesysteem die altijd kant-en-klaar is toe te voegen en is ook niet altijd in een handomdraai ingevoerd. Om een optimaal resultaat te bereiken moet PET zowel bij de ontwikkeling als in het informatiesysteem zelf als integraal onderdeel worden opgenomen. Het verdient dan ook de voorkeur om de invoering van PET onderdeel te laten zijn van de reguliere systeemontwikkeling. In de navolgende hoofdstukken wordt inzicht gegeven hoe PET in uw organisatie kan worden toegepast, wordt vermeld welke PET-vormen het meest voorkomen en wordt een raamwerk gegeven voor het opstellen van een businesscase. Vervolgens is een stappenplan gedefinieerd om tot de daadwerkelijke PET-invoering te komen.

3 Toepassing in informatiesystemen

In dit hoofdstuk treft u hoe u een geschikte PET-vorm kunt kiezen en welke type informatiesystemen zijn te onderscheiden. Het bevat de volgende paragrafen:

- Bepalende factoren voor keuze van een PET-vorm (§ 3.1);
- Mogelijke structuren van een informatiesysteem (§ 3.2).

3.1 Bepalende factoren voor keuze van een PET-vorm

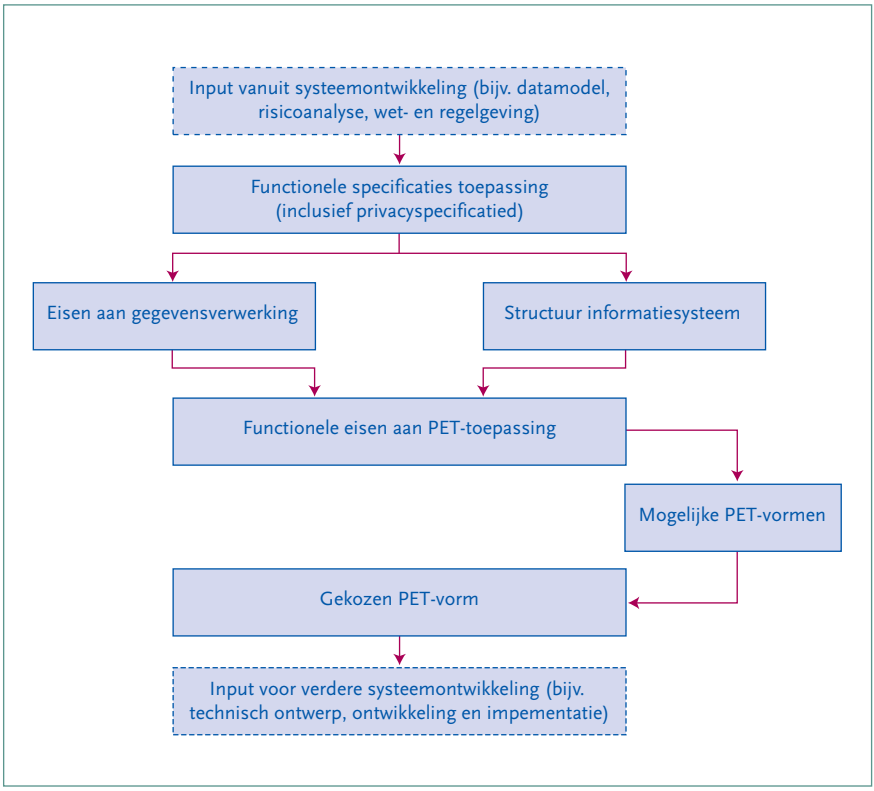
Wanneer u een nieuw informatiesysteem gaat invoeren, worden er allereerst functionele eisen opgesteld. Deze eisen of specificaties omvatten natuurlijk ook de eisen die gesteld moeten worden aan het niveau van bescherming van persoonsgegevens. Deze specificaties leiden uiteindelijk tot een keuze voor een bepaalde opzet of structuur van het informatiesysteem, bijvoorbeeld een zelf te onderhouden centrale database of gebruikmaken van databases van andere organisaties. Een belangrijk aspect hierbij is dat moet worden vastgesteld of het verwerken van persoonsgegevens [7]:

- noodzakelijk is: 'identiteitsrijk';
- beperkt noodzakelijk is: 'identiteitsarm';
- vermijdbaar is (anonieme dienst): 'identiteitsloos'.

De structuur van het informatiesysteem en de eisen aan de gegevensverwerking stellen functionele eisen aan de toepassing van PET. Op basis van deze functionele eisen kan een PET-vorm worden gekozen die optimaal aansluit bij de wensen en verwachtingen van zowel de overheid als de burger. Tevens kan in deze fase worden bepaald welke procedurele en organisatorische maatregelen gewenst zijn.
In hoofdstuk 4 worden de mogelijke PET-vormen beschreven en in hoofdstuk 6 wordt nader ingegaan op de balans tussen PET en organisatorische en procedurele maatregelen. In figuur 5 is het zojuist beschreven proces schematisch weergegeven. Dit betreft een onderdeel van het systeemontwikkelingsproces.

Alvorens tot de functionele specificaties te komen, moet nog een aantal stappen worden uitgevoerd. Vervolgens moet nog een aantal stappen worden doorlopen om vanuit de keuze voor een PET-vorm te komen tot de implementatie en ingebruikname van het informatiesysteem. In hoofdstuk 7 wordt in het stappenplan uitgebreider stilgestaan bij het kiezen, ontwerpen en invoeren van PET-vormen.

7 Zie ook: Taskforce PKIoverheid, PET en de PKI voor de overheid, november 2002.



Figuur 5: Bepalende factoren voor keuze van een PET-vorm

Om u te ondersteunen bij het kiezen van een PET-vorm wordt in de volgende paragraaf allereerst een beknopte beschrijving gegeven van de in dit Witboek gehanteerde structuren van informatiesystemen. Vervolgens worden in hoofdstuk 4 de verschillende PET-vormen beschreven en wordt de koppeling gemaakt tussen de beschreven PET-vormen en de verschillende structuren van de informatiesystemen.

Voor een succesvol gebruik van PET moet de ontwikkeling en invoering van PET een integraal onderdeel uitmaken van het systeemontwikkelingsproces en reeds in het begin van het project worden meegenomen.

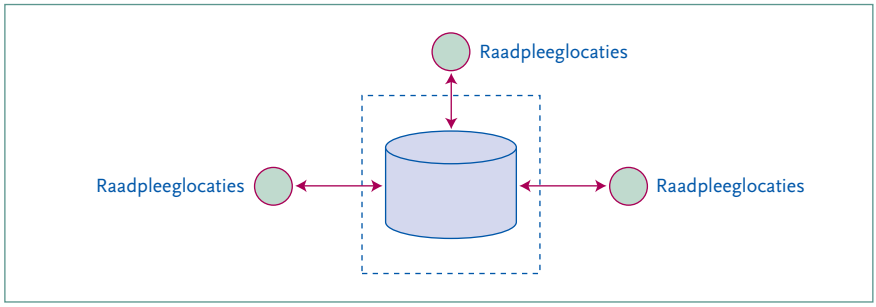
3.2 Mogelijke structuren van informatiesystemen

3.2.1 *Centrale database*

In een 'centrale database' wordt één database gebruikt voor de gegevensverwerking. De centrale database kan door verschillende personen vanaf verschillende locaties worden benaderd. Voorbeelden van centrale databases zijn de authentieke registraties

zoals het GBA, het handelsregister van de Vereniging van Kamers van Koophandel, het Beroepen Individuele Gezondheidszorg (BIG)-register van het ministerie van VWS, de registers van de Informatie Beheer Groep (IB-Groep) en de polisadministratie van het UWV.

Lokaal worden er geen gegevens opgeslagen en verwerkt anders dan direct in de centrale database. De bewerkingen die op de centrale database worden uitgevoerd, worden vanuit één of meer locaties geïnitieerd. In figuur 6 is de structuur van de centrale database weergegeven.



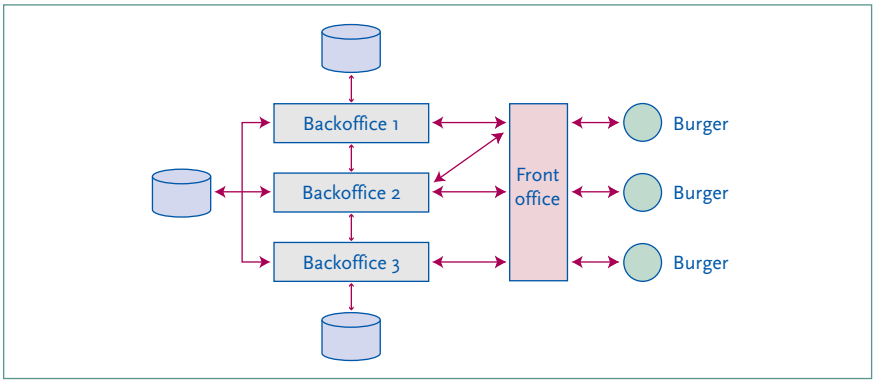
Figuur 6: Centrale database

De casussen in dit Witboek met een centrale database zijn het LCMR-systeem (casus 2), het LADIS-systeem (casus 9), het X/MCare-systeem (casus 12) en het Digitale Ervaringen Dossier (casus 14).

3.2.2 *Gekoppelde backoffices*

In de structuur van gekoppelde backoffices worden de databases van een aantal backoffices benaderd vanuit één frontoffice. De burger hanteert één toegangsportaal om gegevens uit verschillende organisaties te benaderen. De backoffices zijn ook onderling aan elkaar gekoppeld, zodat gegevens uit meerdere bestanden kunnen worden betrokken. Een voorbeeld hiervan is de koppeling van de gegevens van IB-Groep aan die van de Gemeentelijke Basisadministratie. Op basis van de koppeling wil de IB-Groep nagaan of studenten ingeschreven staan in de woonplaats die ze aan de IB-Groep hebben opgegeven.

De koppelingen tussen de backoffices kunnen tijdelijk van aard zijn. Een centrale database kan bijvoorbeeld tijdelijk gekoppeld worden aan een backoffice van een andere organisatie. Daarnaast kan één van de backoffices ook als authentieke registratie dienen. In figuur 7 is de structuur van de gekoppelde backoffices weergegeven.



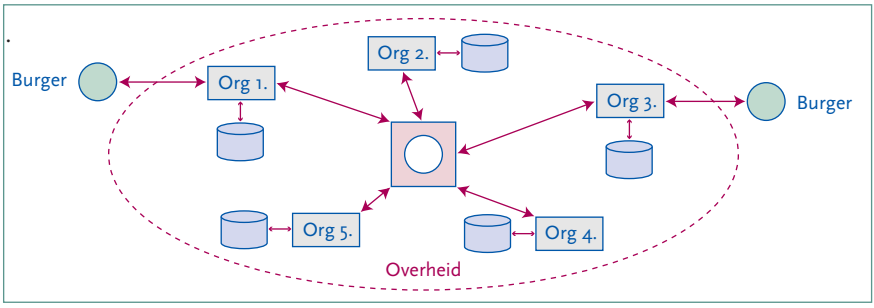
Figuur 7: Gekoppelde backoffices

De casussen in dit Witboek met gekoppelde backoffices zijn NTIS-systeem (casus 4), het Suwinet (casus 5) en de Alberta-systemen (casus 11).

3.2.3 *Routeringsinstituut*

Een routeringsinstituut is het centrale punt in de communicatie tussen en met de aangesloten organisaties. De onderlinge gegevensuitwisseling tussen de aangesloten organisaties wordt ook afgehandeld via het routeringsinstituut. Andere instanties kunnen alleen via het routeringsinstituut gegevens uitwisselen met de aangesloten organisaties. Burgers hebben meestal geen direct contact met het routeringsinstituut, maar alleen met de daarbij aangesloten (uitvoerings)instanties.

Bij het routeringsinstituut vindt geen gegevensopslag plaats, het is alleen een doorgeefluik. Om de gegevensuitwisseling effectief en efficiënt te laten verlopen, wordt meestal gebruikgemaakt van verwijzingsindices in de databases van de aangesloten organisaties. Een andere mogelijkheid is om met centrale of sectorale verwijzingsindices te werken. Voorbeelden van routeringsinstituten zijn RINIS, Suwinet van het Bureau Keteninformatisering Werk en Inkomen (BKWI), het Virtual Clearinghouse Hoger Onderwijs (VCH) en het Sectoraal Aanspreekpunt

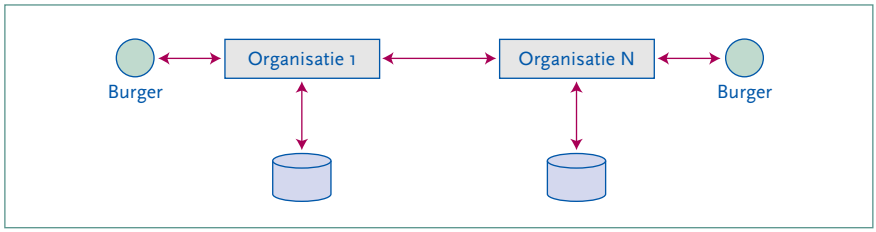


Figuur 8: Routeringsinstituut

ZIN (SAP-ZIN). In figuur 8 is de structuur van het routeringsinstituut weergegeven De casussen in dit Witboek met een routeringsinstituut zijn het Clearing House Hoger Onderwijs (casus 1), het RINIS-systeem (casus 3) en Suwinet (casus 5).

3.2.4 *Keten*

In een keten worden gegevens uitgewisseld of doorgegeven tussen minimaal twee organisaties. Een kenmerk van een keten is dat de ketenorganisaties zelf databases hebben waarin gegevens worden opgeslagen. Voorbeeld van een keten is de RDW-keten. Hierin communiceren de erkenninghouders (dit zijn vaak garagehouders of APK-keuringsstations) via een communicatieprovider met de RDW. De providers verzamelen een gedeelte van de informatie die de erkenninghouders via hen aan de RDW verstrekken. Andere voorbeelden van ketens met een hoge informatiserings-graad zijn te vinden in de zorg (bijv. CVA Ketenzorg), Verkeer & Waterstaat (bijvoorbeeld de gegevensuitwisseling in de Rotterdamse haven) en bij de relatie Politie – Justitie (bijv. elektronische aangifte, proces-verbaal en dossier).
Figuur 9 geeft een gesimplificeerde structuur van de keten.



Figuur 9: Keten

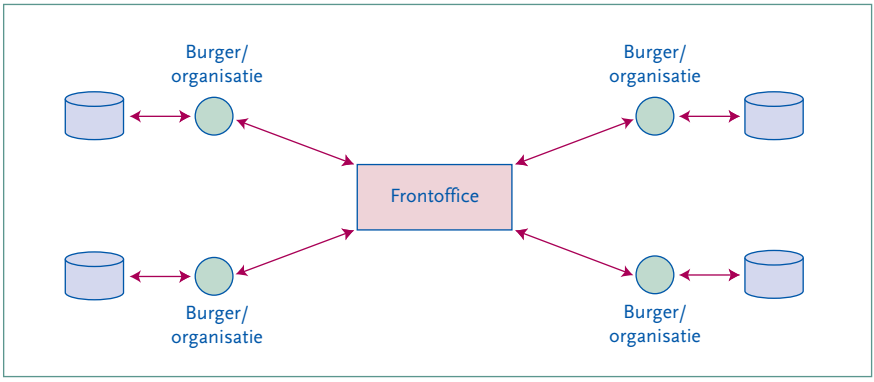
De casus in dit Witboek met keteninformatisering is het NTIS-systeem in combinatie met de toekomstig gekoppelde informatiesystemen (casus 4).

3.2.5 *Decentrale databases*

In deze structuur zijn de gegevens verspreid over verschillende decentrale databases, waarbij het mogelijk is dat de centrale frontoffice / backoffice ook een eigen database heeft. De decentrale databases bevatten onderling niet dezelfde gegevens, terwijl de frontoffice / backoffice niet dezelfde gegevens bevatten als de decentrale databases. In de decentrale databases worden alleen dezelfde soort gegevens opgeslagen.
Er worden geen databases van verschillende organisaties gekoppeld. Een ander voorbeeld van decentrale databases betreft het gebruik van chipkaarten zodat burgers hun eigen gegevens beheren en bewaren.

Voorbeelden van decentrale databases zijn het GBA, de OV-chipkaart, de digitale tachograaf (waarbij iedere vrachtwagen wordt uitgerust met een lokaal registratie-

systeem voor rij- en rusttijden, zie verder paragraaf 4.4) en de oplossing voor rekeningrijden ('kilometerheffing', zie ook paragraaf 4.4). In figuur 10 is de structuur van de decentrale databases weergegeven.



Figuur 10: Decentrale databases

De casussen in dit Witboek met decentrale databases zijn het rekeningrijden en de digitale tachograaf (casus 7), de AgeKey (casus 8), Kiezen op Afstand (casus 10) en de OV-chipkaart (casus 13).

4 PET-vormen

In de navolgende paragrafen worden mogelijke PET-vormen op een functionele wijze beschreven [8]. Dit betreft de volgende vier hoofdvormen:

- algemene PET-maatregelen (§ 4.1);
- scheiden van gegevens (§ 4.2);
- privacymanagementsystemen (§ 4.3);
- anonimiseren (§ 4.4).

Vervolgens wordt behandeld hoe een organisatie met logging en controle kan verifiëren dat de ingevoerde PET-maatregelen adequaat functioneren. Daarnaast treft u in dit hoofdstuk een PET-trap aan waarop de mogelijke PET-vormen op het punt van effectiviteit tegen elkaar zijn afgezet. Ten slotte wordt de koppeling gemaakt tussen de beschreven PET-vormen en de besproken structuren van informatiesystemen.

4.1 Algemene PET-maatregelen

Voordelen:

- Algemene PET-maatregelen zijn relatief eenvoudig te implementeren.
- Met de juiste combinatie van algemene PET-maatregelen is een behoorlijk basisniveau van effectieve bescherming van persoonsgegevens te bereiken.

Veel organisaties passen algemene beveiligingsmaatregelen toe, zoals versleuteling en logische toegangsbeveiliging. Deze algemene beveiligingsmaatregelen hebben bij de juiste toepassing ook een 'privacy enhancing'-functie. Een voorbeeld hiervan is dat een gebruiker toegang krijgt tot een bepaalde gegevensverzameling op basis van zijn organisatorische functie of rol. Niet iedere gebruiker hoeft namelijk de volledige gegevensverzameling te zien. Iemand die bijvoorbeeld adreswijzigingen verwerkt, hoeft niet alle overige gegevens van die persoon te zien. Op basis van zijn functie/rol krijgt hij dan alleen het recht om de adresgegevens te bewerken. De functie/rol wordt dus gekoppeld aan de soort handelingen die hij of zij mag uitvoeren.

Gegevensminimalisatie

Daarnaast bestaat nog een aantal technieken om de persoonsgegevens te transformeren tot gegevens, waaruit de identiteit niet direct herleidbaar is. Wanneer

8 In de literatuurlijst in bijlage A is documentatie opgenomen met aanvullende beschrijving van PET-vormen.

een gebruiker wel persoonsgegevens nodig heeft, maar niet noodzakelijk de identificerende gegevens, dan kan een aantal identificerende gegevens worden verwijderd. Een andere oplossing is om een deel van de gegevens van een veld te verwijderen, bijvoorbeeld de laatste drie cijfers van de postcode, waardoor het unieke adres onbekend blijft, maar de ontvanger wel een indicatie heeft van de buurt. Wanneer wel de complete gegevensverzameling noodzakelijk is, maar niet de exacte waarde van een veld, kan volstaan worden met het categoriseren van de gegevens. Wil een gebruiker bijvoorbeeld weten of een persoon meerderjarig is, dan geeft de applicatie niet de leeftijd of de geboortedatum, maar alleen ja of nee. De vraag van de gebruiker is dan beantwoord, maar de betreffende systeemgebruiker weet niet de exacte leeftijd van de persoon in kwestie. Wanneer de gebruiker niet de exacte waarde van een veld hoeft te weten, kan de bandbreedte van de vastgelegde gegevens worden vergroot. Bij de leeftijd kan bijvoorbeeld een willekeurig getal worden opgeteld.

In ketenverband is gegevensminimalisatie ook bruikbaar in de vorm van gegevensfiltering, waarbij achtereenvolgende ketenpartijen steeds minder persoonsgegevens ontvangen. Of waarbij voor verschillende typen partijen een verschillende mate van filtering wordt toegepast. Hierdoor kan slechts één partij of geen enkele partij een volledig beeld van een persoon opbouwen. Een praktijktoepassing is vermeld bij de OV-chipkaart (casus 13).

Een aantal van deze minimalisatietechnieken gecombineerd lijkt op het volledig anoniem verwerken van gegevens, maar dit is echter niet het geval. Volledige anonimisering wordt in paragraaf 4.5 behandeld.

Casus 4 betreft een voorbeeld van de PET-toepassing bij het Nationaal Trauma Informatie Systeem (NTIS). Naast de algemene PET-maatregelen wordt binnen het NTIS ook scheiding van gegevens toegepast. Deze PET-vorm wordt in paragraaf 4.4 behandeld. In een afzonderlijke casusbeschrijving [9] wordt in meer detail ingegaan op de toepassing van PET bij het NTIS.

9 'Casusbeschrijving Nationaal Trauma Informatie Systeem: Toepassing van Privacy Enhancing Technologies bij traumacentra', Universitair Medisch Centrum Utrecht en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004.

Casus 4: Nationaal Trauma Informatie Systeem (NTIS)

Het NTIS is een digitaal registratiesysteem voor traumapatiënten met zwaar acuut letsel die geholpen worden op de afdeling Spoed Eisende Hulp. Artsen, verpleegkundigen en assistenten hebben toegang tot dit systeem. Door de elektronische vastlegging en uitwisseling van medische gegevens kan een efficiëntere en effectievere hulpverlening aan de patiënt worden geboden. Tevens worden de uiterst gevoelige medische patiëntgegevens en behandelmethodieken anoniem geanalyseerd zodat men de behandelmethodieken kan verbeteren en de patiënten beter kunnen worden geholpen en de kans op overleven groter wordt.

PET-toepassing

- sterke beveiliging door een verfijnde autorisatiestructuur, waarbij de rol van de gebruiker bepaalt tot welk deel van het systeem hij of zij toegang heeft. Geautoriseerde zorgverleners maken gebruik van digitale certificaten die op chipkaarten zijn opgeslagen of van chipkaarten met biometrische gegevens om zich uniek te identificeren. Andere gebruikers maken gebruik van softwarecertificaten, maar daarmee krijgt men geen toegang tot de medische gegevens;
- scheiden van gegevens, waarbij de medische gegevens en NAW-gegevens in verschillende tabellen zijn opgeslagen. De NAW-gegevens zijn versleuteld, zodat de medische gegevens voor ongeautoriseerde personen (bijvoorbeeld systeembeheerders) niet zijn te herleiden tot een natuurlijk persoon. De database is opgeslagen bij een vertrouwde derde partij, de zogenaamde Trusted Third Party (TTP), die stringente fysieke en logische beveiligingsmaatregelen heeft getroffen en hierop wordt geaudit;
- minimaliseren van gegevens die worden uitgewisseld met andere informatiesystemen. Vanuit het NTIS worden er gegevens verstrekt aan een systeem waarmee de Regionaal Geneeskundig Functionaris kan zien welke personen uit zijn gemeente betrokken zijn bij een ramp. Naast de NAW-gegevens wordt uitsluitend een classificatiecode verstrekt. De classificatiecode geeft informatie over de zwaarte van het letsel, maar de RGF krijgt geen inzage in de medische gegevens. Dit systeem bevat een tijdelijke database en de NAW-gegevens blijven hierin niet bewaard. De functionaris kan de gegevens wel exporteren naar zijn eigen computer.

Baten

Met het toepassen van PET is dit systeem uiteindelijk mogelijk geworden, zonder dit systeem zou de kwaliteit van de hulpverlening door traumacentra lager zijn. Door dit succes is een landelijke uitrol van het NTIS gaande.

Authenticatie en autorisatie

Een voorwaarde voor de meeste vormen van PET is dat authenticatie en autorisatie van personen betrouwbaar zijn ingericht. De PET-vormen steunen namelijk sterk op

authenticatie- en autorisatiemanagement. Wanneer het toekennen (autoriseren) en het uitreiken van de authenticatiemiddelen niet zorgvuldig gebeuren, kunnen ongeautoriseerde personen onrechtmatig toegang verkrijgen tot de persoonsgegevens. Hiermee wordt het voordeel van PET geheel tenietgedaan.
Een betrouwbaar authenticatie- en autorisatieproces staat veelal aan de basis van een succesvolle PET-implementatie. Het zal bijvoorbeeld duidelijk zijn dat de identiteitsbeschermer alleen werkt als het hiervoor benodigde authenticatiemiddel (bijvoorbeeld een chipkaart) op een zorgvuldige wijze aan gebruikers wordt uitgegeven. Daarnaast biedt juist authenticatie- en autorisatiemanagement de organisatie ook voordelen op het gebied van algemene informatiebeveiliging en efficiency en helpt het de organisatie om 'in control' te zijn over de geautomatiseerde gegevensverwerking.

Quality Enhancing Technology

Een onderdeel van PET is het gelijksoortige begrip Quality Enhancing Technology (QET). Met behulp van QET is de kwaliteit (volledigheid, juistheid en actualiteit) van de vastgelegde gegevens te bewaken en te verbeteren. De kwaliteit van de persoonsgegevens is van sterke invloed op de kwaliteit van de diensten die de overheid verleent. Bovendien is hiermee ook het privacybeginsel inzake kwaliteit gediend (zie hoofdstuk 2), omdat bij betrouwbare persoonsgegevens de juiste beslissingen worden genomen. Deze technieken kunnen onder andere worden ingezet om redundantie uit databases te verwijderen en de gegevenskwaliteit te verbeteren.

Casus 5: Suwinet

Het Suwinet is opgezet voor het verbeteren van de samenwerking in het Werk en Inkomen domein van de sociale zekerheid. Voor deze samenwerking moeten de ketenpartners: Uitvoeringsinstantie Werknemers-verzekeringen (UWV), Sociale Verzekeringsbank (SVB), Centra voor Werk en Inkomen (CWI) en de gemeentelijke sociale diensten kunnen beschikken over elkaars gegevens. Op Suwinet zijn inmiddels meer dan 18.000 medewerkers van deze ketenpartijen aangesloten. Door gebruik te maken van de informatie die ketenpartners al hebben, hoeven gegevens niet opnieuw te worden opgevraagd bij burgers of bedrijven.
De gegevens worden onder stringente beveiligings- en privacyvoorwaarden uitgewisseld tussen de aangesloten partijen. Dit is in specifieke wetgeving geregeld. Suwinet wordt meestal in de frontoffice (bijv. balie) gebruikt, in tegenstelling tot RINIS dat een systeem is dat in de backoffice wordt toegepast.

PET-toepassing

Naast algemene beveiligingsmaatregelen als het gebruikmaken van een besloten netwerk zijn de volgende privacywaarborgen aangebracht:

- minimaliseren van de uitgewisselde set van persoonsgegevens voor het betreffende doel.

Bij het opvragen van een status van een paspoort wordt uitsluitend teruggekoppeld dat het ongeldig is, niet wat de oorzaak daarvan is (bijv. gestolen). Tevens vindt geen centrale gegevensopslag of -verwerking plaats zodat beheerders geen inzage hebben;

- gedetailleerd autoriseren van gebruikers door toepassing van organisatorische rollen en directe koppeling van type bevraging aan de op te vragen persoonsgegevens (en volgorde van tonen). Partijen hebben geen aanvullende autorisaties op de backoffice-systemen van de andere partijen en de aangesloten partijen kunnen verdere kanalisering en beperkingen op bevraging van gevoelige persoonsgegevens aanbrengen. Vrije zoekmogelijkheden zijn niet toegestaan;
- verbeteren van gegevenskwaliteit door on-line bevragingen en door het aan de balie 'confronteren' van burgers met de gegevens van andere instanties om inconsistenties te verwijderen en betrouwbare gegevens vast te leggen. Deze kwaliteit wordt verder gewaarborgd door de gebruiksonderzoeken en ICT- en privacyaudits die jaarlijks centraal en bij ketenpartijen plaatsvinden;
- loggen van opgevraagde gegevens per sofi-nummer per medewerker, niet de inhoud van die berichten. Deze logging is alleen door geautoriseerde auditors of gerechtelijke onderzoeken in te zien. Daarnaast worden geavanceerde statistieken per rol en profiel bijgehouden met gebruikmaking van heuristische technieken om eventuele onregelmatigheden in de gegevensverwerking te ontdekken.

Baten

Met het ontwerp van het Suwinet is de uitwisseling van persoonsgegevens op geautomatiseerde wijze aan stringente privacyregels gebonden, waarbij het transparant is dat iemands persoonsgegevens slechts in beperkte mate worden uitgewisseld tussen overheidsorganisaties. De eenmalige registratie, de gestructureerde gegevensuitwisseling en de controle door de burger verbeteren alle de kwaliteit van de persoonsgegevens.

Aandachtspunten algemene PET-maatregelen:

- Persoonsgegevens worden nog steeds verwerkt.
- Algemene PET-maatregelen betreffen voornamelijk identificatie, authenticatie, autorisatie en versleuteling.
- Algemene PET-maatregelen zijn heel goed toe te passen in combinatie met specifieke PET-vormen.

4.2 Scheiding van gegevens

Voordelen:

- Identificerende gegevens worden losgekoppeld van de overige persoonsgegevens.
- Het effect is niet afhankelijk van algemene beveiligingsmaatregelen.
- Uitwisseling van gegevens tussen organisaties is mogelijk met inachtneming van de gegevensbescherming.

Scheiding van gegevens houdt in dat persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens worden losgekoppeld van de overige persoonsgegevens. Er worden ten minste twee domeinen gecreëerd: een identiteitsdomein waarin bijvoorbeeld de naam en adresgegevens worden verwerkt en één of meer pseudo-identiteitsdomeinen waarin overige gegevens als lidmaatschap of opsporingsgegevens worden verwerkt. De scheiding tussen beide domeinen wordt aangebracht en beheerd door een identiteitsbeschermer.

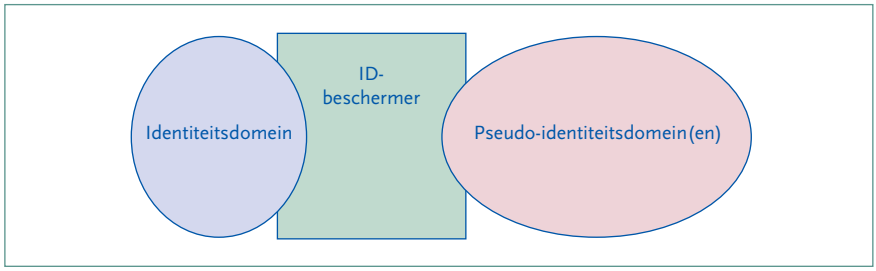
In de praktijk is een identiteitsbeschermer een stukje software dat op een server kan staan. Ook een chipkaart kan als identiteitsbeschermer dienen, maar dit is niet noodzakelijk. De identiteitsbeschermer zet de echte identiteit om in een pseudo-identiteit, meestal door het toekennen van niet-herleidbare identificatiecodes. Alleen met behulp van de identiteitsbeschermer kan de koppeling worden gelegd tussen de twee domeinen. Personen die geautoriseerd zijn de identiteitsbeschermer te gebruiken, kunnen hiermee toegang verkrijgen tot beide domeinen en de relatie tussen de twee domeinen zien. Personen die voor hun functie niet de beschikking hoeven te hebben over alle persoonsgegevens, krijgen alleen toegang tot die pseudo-identiteitsdomeinen waartoe zij gerechtigd zijn.

Samenvattend heeft de identiteitsbeschermer de volgende functies:

- genereren van een pseudo-identiteit op basis van een echte identiteit;
- koppelen van de pseudo-identiteit en de echte identiteit. De koppeling tussen beide domeinen kan worden gemaakt indien dit noodzakelijk is voor het verwerkingsproces;
- converteren van een pseudo-identiteit in een andere pseudo-identiteit. Door het vele gebruik van een en dezelfde pseudo-identiteit kan de ware identiteit toch achterhaald worden. Wanneer verschillende pseudo-identiteiten worden gebruikt, valt er geen patroon te ontdekken in de activiteiten die op basis van de pseudo-identiteit worden uitgevoerd.

Gezien de belangrijke functies van de identiteitsbeschermer is het van groot belang dat er zorgvuldig met de identiteitsbeschermer wordt omgesprongen. De autorisatie en authenticatie van personen is dan ook een kritisch proces om de effectieve werking van de identiteitsbeschermer te waarborgen. Het authenticeren kan bijvoorbeeld gebaseerd worden op een digitaal certificaat.

In veel gevallen kent een informatiesysteem verschillende typen gebruikers en mag iedereen maar een beperkt aantal gegevens inzien. In dat geval kunnen verschillende pseudo-identiteitsdomeinen worden ingericht. In ieder pseudo-identiteitsdomein wordt dan een deel van de informatie over een persoon verwerkt.
In figuur 11 wordt de zojuist beschreven PET-vorm schematisch weergegeven.



Figuur 11: Scheiding van gegevens

Casus 6: Identiteitsbeschermer in een ziekenhuisinformatiesysteem

Om de privacy van patiënten te waarborgen, kunnen de patiëntgegevens in twee domeinen worden gesplitst. In het identiteitsdomein worden de persoonsgegevens inclusief een patiëntnummer opgeslagen. In het pseudo-identiteitsdomein worden de diagnostische en behandelgegevens opgeslagen. Ook in dit domein wordt een patiëntnummer gebruikt. De patiëntnummers uit de beide domeinen mogen niet aan elkaar gelijk zijn, omdat iedereen dan de koppeling kan maken. Om dit op te lossen wordt het patiëntnummer uit het identiteitsdomein versleuteld. Dit versleutelde nummer wordt als patiëntnummer gebruikt in het pseudo-identiteitsdomein. Met behulp van de identiteitsbeschermer kan het versleutelde patiëntnummer worden ontsleuteld en wordt de koppeling met het identiteitsdomein gemaakt. Op deze wijze kunnen alleen mensen die de beschikking hebben over de identiteitsbeschermer, de twee domeinen met elkaar in verband brengen.

Wanneer een organisatie statistisch onderzoek wil doen, ontbreekt veelal de noodzaak om de identiteit van de individuele burgers vast te leggen, ook al wil men wel aan de burger gerelateerde gegevens gebruiken. In dat geval kan worden volstaan met het verwerken van de gegevens uit het pseudo-identiteitsdomein. De burger beheert zelf de identiteitsbeschermer en daarmee de koppeling tussen de domeinen. Deze vorm

van scheiding van gegevens kan worden gebruikt in het geval de overheid wel zekerheid wil hebben over iemands identiteit, maar deze identiteit niet wil of mag vastleggen. Dit is bijvoorbeeld het geval bij Kiezen op afstand (zie casus 10). Wanneer burgers hun stem elektronisch uitbrengen wil de overheid wel de zekerheid hebben dat de burger stemgerechtigd is en slechts eenmaal stemt, maar mag de identiteit van de burger in relatie tot de uitgebrachte stem absoluut niet worden vastgelegd om te voorkomen dat de vereiste anonimiteit van de stem verloren gaat.

Deze PET-vorm kan ook andersom worden gebruikt. De overheid legt alleen het identiteitsdomein vast en alleen de burger beschikt over het pseudoidentiteits-domein. Ook nu beslist de burger over het feit of de overheid de koppeling kan en mag maken tussen de twee domeinen. Hierbij moet wel worden opgemerkt dat een chipkaart een beperkte opslagcapaciteit heeft en dat daar bijvoorbeeld geen complete gegevensverzameling op bewaard kan worden. In veel gevallen zal op de chipkaart een verwijzing zijn opgenomen naar de locatie waar de gegevensverzameling wordt bewaard of de instelling die de gegevens in bewaring heeft. Een voorbeeld hiervan is dat een burger geen Elektronisch Patiënt Dossier bij zich draagt, maar dat op zijn chipkaart is opgeslagen wie zijn huisarts is. Bij een ongeval kan de behandelend arts contact opnemen met de huisarts over medische bijzonderheden uit het verleden.

Persoonsgegevens in eigen beheer

Maximale gegevensbescherming wordt gerealiseerd wanneer de identiteitsbeschermer wordt beheerd door de persoon wiens gegevens zijn vastgelegd. Alleen hij bepaalt dan wanneer en aan wie zijn ware identiteit bekend wordt gemaakt. De situatie waarbij de identiteitsbeschermer onder controle staat van de betrokkene zelf wordt 'persoonsgegevens in eigen beheer' genoemd en is in feite een specifieke ver-schijningsvorm van scheiding van gegevens. Een persoonlijke chipkaart en (on-line) gegevenskluisje zijn voorbeelden hiervan. In de voorafgaande casus kan een arts in het ziekenhuis een patiënt om zijn chipkaart vragen waarmee hij/zij het elektro-nische medische dossier kan inzien. Dit biedt een goede beveiliging maar is praktisch moeilijk uitvoerbaar, omdat de arts dan alleen in het bijzijn van een – bij bewustzijn zijnde – patiënt het medisch dossier kan raadplegen. Daarom zou de arts zelf (ook) over een chipkaart moeten beschikken om toegang te verkrijgen tot het medische dossier. Die chipkaart wordt idealiter niet uitgegeven door het ziekenhuis zelf; het is hierin niet gespecialiseerd en het risico bestaat dat hierdoor ongeautoriseerde personen toch een chipkaart krijgen. Daarom is het verstandiger om de chipkaart uit te laten geven door een onafhankelijke derde partij [10]. Deze partij is hierin gespe-cialiseerd en stelt de identiteit van een systeemgebruiker op de vereiste wijze vast.

10 Leverancier van vertrouwensdiensten, zogenaamde Trusted Third Party.

Casus 7: Rekeningrijden & Digitale Tachograaf

Bij de toepassing van rekeningrijden legt de overheid persoonsgegevens vast ten behoeve van de afrekening van het weggebruik. De overheid hoeft niet te weten waar en wanneer de weggebruiker gereden heeft. De overheid wil alleen weten welk bedrag in rekening moet worden gebracht. Om dit te bereiken heeft de gebruiker een kaartje in zijn auto waarop automatisch een gedetailleerde rittenadministratie wordt bijgehouden. Wanneer de weggebruiker langs een uitleespunt komt wordt zijn rittenadministratie in geaggregeerde vorm aangeboden. Nu weet de overheid welk bedrag ze in rekening moet brengen, maar beschikt alleen de weggebruiker over de gedetailleerde rittenadministratie.

Een soortgelijke PET-vorm wordt toegepast bij de digitale tachograaf, waarbij in de vrachtauto de reis- en rusttijden op een chipkaart worden vastgelegd. Aanvullend zijn er mogelijkheden gecreëerd om de chauffeur de registratie op de chipkaart elektronisch te laten tekenen en om toezichthouders specifieke raadpleegmogelijkheden te bieden.

FAQ 4: Wat is het verschil tussen afschermen van gegevens door middel van algemene logische toegangsbeveiliging en de identiteitsbeschermer?

Hoewel het gebruik van algemene logische toegangsbeveiligingsmaatregelen belangrijk is om ongeautoriseerde toegang tot persoonsgegevens te voorkomen, kent deze beveiliging beperkingen. Een nadeel van algemene logische toegangsbeveiliging is dat de gegevens nog steeds identificeerbaar en bij elkaar worden opgeslagen. Verdere beperkingen zijn dat de gegevens buiten de applicatie om kunnen worden benaderd en het feit dat er vaak onvoldoende functieprofielen gedefinieerd zijn in de applicatie. Deze laatste beperking heeft tot gevolg dat personen vaak te ruime autorisaties hebben.

Bij de identiteitsbeschermer worden de persoonsgegevens ontkoppeld van de overige gegevens. De koppeling tussen de verschillende domeinen kan alleen worden gelegd door de identiteitsbeschermer. Het grote verschil is dat de gegevens niet direct identificeerbaar worden verwerkt en opgeslagen. Voordeel hiervan is dat wanneer de algemene maatregelen worden doorbroken en personen de beschikking krijgen over de verschillende domeinen, de koppeling tussen de persoonsgegevens en de overige gegevens niet kan worden gelegd. De identiteitsbeschermer biedt dus een betere privacybescherming dan de algemene logische toegangsbeveiliging.

Een algemeen verschil tussen de algemene informatiebeveiliging en het toepassen van PET is het verschil tussen de uitgangspunten. Informatiebeveiliging is veelal gericht op het in toenemende mate beschermen van een steeds omvangrijker wordende gegevensverzameling. PET is er juist op gericht om minder gegevens te verzamelen, waardoor minder dikke muren nodig zijn om de gegevens te beschermen. Een toepassing als Kiezen op afstand is bijvoorbeeld niet mogelijk op basis van de algemene informatiebeveiliging, maar wel met de toepassing van PET.

Aandachtspunten:

- Beveiliging van de identiteitsbeschermer is van groot belang.
- Scheiding van gegevens in een bestaand informatiesysteem vergt vaak een grondige herziening van het gegevensmodel.

4.3 Privacymanagementsystemen

Voordelen:

- Transparantie voor de burger wordt verhoogd.
- Naleving van het privacyreglement wordt technisch afgedwongen.

Een bijzondere vorm van PET wordt gevormd door privacymanagementsystemen die zorgen voor de geautomatiseerde toepassing van privacybeleid. Dit betreft programmatuur die als het ware als een schil om de persoonsgegevens heen ligt en alle transacties die met die gegevens plaatsvinden automatisch toetst aan het privacyreglement. Deze toetsing is gebaseerd op elektronische privacyregels (in het Engels veelal aangeduid als 'privacy policies') die zijn afgeleid uit het privacyreglement voor de betreffende database of het betreffende informatiesysteem. Door middel van een privacycodering of privacytaal worden die privacyregels in de PET-software ingevoerd.

Een operationeel voorbeeld daarvan is het Platform for Privacy Preferences Project (P3P), ontworpen door het World Wide Web -Consortium (W3C). P3P [11] is een hulpmiddel om op eenvoudige en gestandaardiseerde wijze over de privacyvoorkeuren van de internetgebruiker te communiceren in een door het informatiesysteem leesbare vorm. Binnen P3P wordt aangegeven:

- wie de gegevens verzamelt, verwerkt en opslaat;
- welke gegevens worden verzameld en met welk doel ze worden verwerkt;
- of er opt-in en opt-out alternatieven zijn;
- aan wie de gegevens worden verstrekt;
- tot welke gegevens de verantwoordelijke toegang heeft;
- welke bewaarperiode voor de persoonsgegevens van kracht is;
- hoe conflicten over het privacybeleid van de verwerkende organisatie worden opgelost of beslecht;
- waar het privacybeleid op de website te vinden is.

11 Zie http://www.w3.org/P3P/ en P3P and Privacy – Center for Democracy & Technology / IPC Ontario – zie http://www.cdt.org/privacy/pet/p3pprivacy.shtml.

Op deze wijze wordt de transparantie inzake de gegevensverwerking voor de gebruiker sterk verhoogd. De internetgebruiker vult on-line een formulier in waarin de gebruiker zijn/haar voorkeuren inzake gegevensbescherming vastlegt. Vervolgens kan deze gebruiker bij ieder websitebezoek automatisch vaststellen of zijn/haar preferenties door het privacyreglement van de organisatie worden gerespecteerd en op grond daarvan beslissen of hij/zij inderdaad de website gaat bezoeken. Overigens is een dergelijke toepassing ook bruikbaar voor toepassingen die niet via internet verlopen, maar wel gebruikmaken van internettechnologie [12].

Voor het definiëren van elektronische privacytaal zijn inmiddels praktische hulpmiddelen verkrijgbaar, bijvoorbeeld de Enterprise Privacy Authorisation Language (EPAL). Verschillende leveranciers hebben inmiddels privacymanagementsystemen ontwikkeld of zijn daarmee bezig. Deze systemen dwingen af dat verwerkingen zich aan de gedefinieerde privacyregels houden. In het privacymanagementsysteem wordt in de eerste plaats het vastgestelde privacybeleid van de organisatie ingevoerd en vervolgens geïntegreerd met de verwerkingsprocessen. Bij invoer van nieuwe verwerkingsprocessen en gegevens wordt automatisch geanalyseerd of het verwerkingsproces wordt gedekt door een van tevoren vastgestelde norm of regel voortvloeiende uit het privacybeleid. Bovendien wordt vastgesteld of de verwerkingsprocessen van de verschillende organisatieonderdelen consistent zijn. De functionaliteiten kunnen zelfs worden uitgebreid naar de bewerkers [13], opt-in management en geautomatiseerde handhaving.

Uit ervaring in het buitenland (zie ook casus 11 uit Canada) blijkt dat privacymanagementsystemen het vertrouwen van de burger aanmerkelijk vergroten en het inzicht van het management in de verwerking en controle van gegevens doen toenemen. Vooral de geautomatiseerde handhaving is een belangrijk pluspunt en voorkomt kostbare privacy-audits naar de organisatorische naleving [14].

Aandachtspunten:

- De toepasbare technieken zijn recent ontwikkeld en worden nog niet op grote schaal toegepast.
- Dergelijke PET-maatregelen zijn ook zelf in te voeren op het niveau van de database door gebruikmaking van moderne producten.

12 Bijvoorbeeld door gebruik van het internet TCP/IP-protocol binnen de organisatie of over gesloten netwerken tussen organisaties.

13 Derde partij die in een uitbestedingssituatie (een deel van) de gegevensverwerking uitvoert voor de organisatie die voor de persoonsregistratie verantwoordelijk is.

14 J.de Rooij, Privacymanagement en Enterprise Privacy manager, Privacy & Informatie, 6e jaargang nummer 5, oktober 2003, blz. 206-212.

4.4 Anonimiseren

Voordelen:

- Na volledige anonimisering worden geen persoonsgegevens meer verwerkt en hoeven geen beveiligingsmaatregelen vanwege privacyredenen meer te worden getroffen.
- Minder gegevens worden vastgelegd en minder gegevens hoeven beheerd en onderhouden te worden.

Anonimiseren kan in twee stadia van de gegevensverwerking worden toegepast. Ten eerste kan worden voorkomen dat persoonsgegevens van de burger worden vastgelegd door de overheid. In het geheel worden er geen persoonsgegevens verwerkt. Deze oplossing is alleen mogelijk indien voor het doeleinde van de dienstverlening het verwerken van persoonsgegevens niet noodzakelijk is.

De tweede vorm is dat wanneer de persoonsgegevens tijdelijk nodig zijn, de gegevens in eerste instantie worden verwerkt en na deze verwerking worden vernietigd of losgekoppeld van de overige gegevens. Het vernietigen en/of loskoppelen moet onomkeerbaar gebeuren. Wanneer dit niet het geval is kunnen de persoonsgegevens en overige gegevens weer gekoppeld worden en is geen volledige anonimiteit bereikt. Indien de gegevens ook van indirect identificerende kenmerken zijn ontdaan, zijn er helemaal geen persoonsgegevens meer aanwezig.

Het voordeel van anonimiseren is dat gegevens die niet zijn vastgelegd, ook niet beschermd en beheerd hoeven te worden. De beheer- en onderhoudsinspanning neemt af. Daarnaast is ook niet langer de Wbp van toepassing omdat er geen persoonsgegevens verwerkt worden. Het vernietigen en/of loskoppelen kan uitkomst bieden indien bijvoorbeeld statistische analyses moeten worden uitgevoerd, waarbij de identiteitsgegevens niet van belang zijn of niet verwerkt mogen worden. Een anonimiseerder is een technisch hulpmiddel, bijvoorbeeld een softwareprogramma, dat wordt ingezet om persoonlijke informatie van de gebruiker weg te filteren wanneer hij gebruikmaakt van internetdiensten.

Casus 8: Anonieme dienstverlening: AgeKey

De overheid wil het roken ontmoedigen en heeft het verkopen van sigaretten aan jongeren onder de zestien jaar verboden. De handhaving van dit verbod was echter een probleem. Hiervoor is de AgeKey ontwikkeld. De AgeKey kan worden opgeslagen op een bank- of chippas. Sigarettenautomaten werken alleen als iemand de beschikking heeft over een dergelijke AgeKey. Om een AgeKey te bemachtigen moet een persoon een postkantoor gaan en aantonen dat hij/zij zestien jaar of ouder is. Vervolgens wordt de AgeKey op de pas geactiveerd en kan

iemand sigaretten uit de automaat kopen. De automaat controleert alleen of de AgeKey op de pas staat. Het kopen gebeurt volledig anoniem. Er wordt nergens geregistreerd dat de AgeKey is geactiveerd. Niemand weet dan ook wie er een geactiveerde AgeKey heeft en hoe de AgeKey wordt gebruikt. Zie www.agekey.nl voor aanvullende informatie.

Casus 9: Landelijk Alcohol en Drugs Informatiesysteem (LADIS)

Het Landelijk Alcohol en Drugs Informatiesysteem (LADIS) is een systeem waarin wordt bijgehouden wat de omvang en inhoud is van de landelijke hulp aan verslaafden. Alle verslavingszorginstellingen in Nederland leveren viermaal per jaar gegevens per diskette of beveiligde e-mail aan het LADIS-systeem aan, op basis waarvan beleidsinformatie wordt opgesteld en epidemiologisch onderzoek wordt uitgevoerd. Sinds 1994 zijn 150.000 individuen anoniem in LADIS geregistreerd. De gebruikers van LADIS-gegevens zijn legio; naast de instellingen zelf variëren die van onderzoeksinstituten en overheidsorganisaties tot farmaceutische bedrijven, mediabedrijven, producenten van gokmachines, casino's en ambassades.

PET-toepassing

- gebruik van unieke codes op basis van de persoonsgegevens, waarbij onder andere de naam, geslacht en geboortedatum worden versleuteld. De software bij de aanleverende instelling maakt deze code aan en is hiervoor gecertificeerd. De unieke code wordt na aanlevering omgezet in een tweede anonieme cliëntcode (door zogenaamde 'hashing'), waarbij de oorspronkelijke gegevens niet meer zijn te herleiden;
- veilige aanlevering van gegevens door gebruikmaking van versleuteling en wachtwoordbeveiliging;
- direct vernietigen van de door instellingen aangeleverde gegevens.

Baten

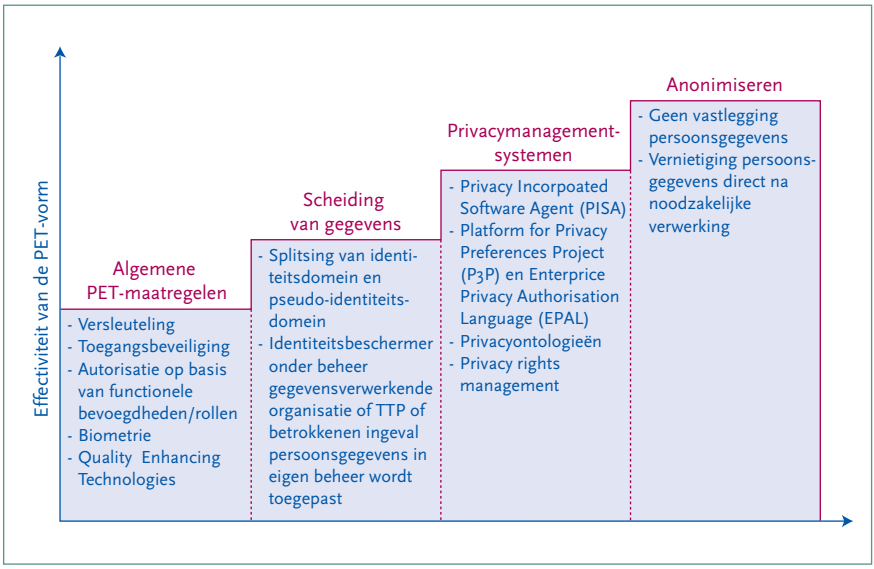
Door de jarenlange toepassing is met LADIS een anoniem cliëntvolgsysteem ontstaan. LADIS is door de getroffen maatregelen in feite geen persoonsregistratie meer, waardoor gegevensverstrekking aan een brede doelgroep voor beleidsvorming en onderzoek mogelijk is. Ondanks een zekere foutmarge (cliëntcode meer dan 90% uniek) vanwege de grofmazigheid van de in 1994 ontwikkelde techniek kunnen de gegevens toch worden gebruikt voor onderzoek door een geprogrammeerde correctie. De grofmazigheid kan namelijk worden gecorrigeerd.

Aandachtspunt:
Anonimisering kan alleen in identiteitsarme of identiteitsloze processen worden toegepast [15].

15 Zie ook: Taskforce PKIoverheid, PET en de PKI voor de overheid, november 2002.

4.5 De PET-trap

Uit de beschrijving van de vier mogelijke PET-vormen blijkt dat iedere PET-vorm specifieke functies heeft met betrekking tot gegevensbescherming. De ene vorm biedt meer bescherming dan de andere. In figuur 12 zijn de verschillende PET-vormen gepositioneerd ten opzichte van de effectiviteit van de gegevensbescherming. Daarnaast zijn in de figuur de belangrijkste eigenschappen van de PET-vormen weergegeven. De PET-trap is geen groeimodel en behoeft niet geheel 'tot de overloop' te worden opgelopen. Wanneer een organisatie algemene PET-maatregelen heeft toegepast, wil dit niet zeggen dat de organisatie door moet groeien naar 'hogere' PET-vormen. De geschiktheid van de verschillende PET-vormen is situatieafhankelijk.



Figuur 12: PET-trap: de effectiviteit van PET-vormen

4.6 Koppeling PET-vormen met structuur van het informatiesysteem

In figuur 13 wordt weergegeven welke PET-vormen in welke structuur gebruikt kunnen worden. Daarnaast worden de kenmerken van iedere combinatie kort behandeld. Er is niet in detail ingegaan op de combinaties. De beschrijving van de PET-vormen in dit hoofdstuk en de in de figuur genoemde kenmerken geven voldoende inzage in hoe de verschillende PET-vormen in de verschillende structuren toegepast kunnen worden.

De toepassing van de algemene PET-maatregelen en privacymanagementsystemen is niet in deze figuur beschreven, aangezien deze vormen generiek zijn toe te passen op de verschillende structuren van informatiesystemen. Aansluitend wordt de subcategorie 'Persoonsgegevens in eigen beheer' afzonderlijk besproken.

	Anonimiseren	Scheiding van gegevens
Centrale database	■ Anonimiseren voordat gegevens in database worden vastgelegd, indien geen persoonsgegevens benodigd zijn; of ■ Persoonsgegevens tijdelijk vastleggen en na verwerking in database gegevens anonimiseren.	■ Identiteitsdomein en pseudoidentiteitsdomein(en) beide in centrale database; ■ Geautoriseerde gebruiker verkrijgt toegang tot persoonsgegevens door authenticatie aan identiteitsbeschermer in centrale database.
Gekoppelde backoffices	■ Anonimiseren aan frontoffice indien gekoppelde backoffices geen persoonsgegevens nodig hebben; of ■ Anonimiseren na verwerking in backoffice indien aantal backoffices persoonsgegevens tijdelijk nodig heeft. Anonimiseren is verantwoordelijkheid aangesloten organisaties.	■ Identiteitsdomein en pseudoidentiteitsdomein(en) beide bij iedere backoffice; ■ Geautoriseerde gebruiker verkrijgt toegang tot persoonsgegevens door authenticatie aan identiteitsbeschermer in database backoffice.
Routeringsinstituut	■ Anonimiseren door routeringsinstituut indien aangesloten organisaties geen persoonsgegevens nodig hebben; of ■ Anonimiseren na verwerking door aangesloten organisaties indien deze organisaties tijdelijk persoonsgegevens nodig hebben. Anonimiseren is verantwoordelijkheid aangesloten organisaties.	■ Identiteitsdomein en pseudoidentiteitsdomein(en) beide bij iedere aangesloten organisatie; ■ Geautoriseerde gebruiker verkrijgt toegang tot persoonsgegevens door authenticatie aan routeringsinstituut.

Figuur 13: Koppeling PET-vormen met structuur van het informatiesysteem

	Anonimiseren	Scheiding van gegevens
Keten	■ Anonimiseren door eerste organisatie in keten indien ketenorganisaties geen persoonsgegevens nodig hebben; of ■ Anonimiseren na verwerking door één van de ketenorganisaties indien deze en de achterliggende organisaties geen persoonsgegevens nodig hebben. Anonimiseren is verantwoordelijkheid ketenorganisaties.	■ Identiteitsdomein en pseudoidentiteitsdomein(en) beide bij iedere ketenorganisatie; ■ Identiteitsdomein bij één organisatie en pseudo-identiteitsdomeinen bij andere ketenorganisaties; ■ Geautoriseerde gebruiker verkrijgt toegang tot persoonsgegevens door authenticatie aan identiteitsbeschermer in database van iedere ketenorganisatie waartoe hij toegang wil verkrijgen.
Decentrale databases	■ Niet van toepassing aangezien de burger zelf de beschikking heeft over de gegevens.	■ In eventueel aanwezige centrale database al gerealiseerd aangezien de burger zelf de beschikking heeft over de gegevens.

Figuur 13: Koppeling PET-vormen met structuur van het informatiesysteem

De PET-vorm 'Persoonsgegevens in eigen beheer' is een subcategorie van 'Scheiding van gegevens' en is daarom niet afzonderlijk in de figuur opgenomen. Er is echter wel een aantal verschillen in de toepasbaarheid van beide vormen. Deze betreffen:

- De vorm 'Persoonsgegevens in eigen beheer' is niet eenvoudig toepasbaar voor gekoppelde back-offices, het routeringsinstituut en de keten. Vanwege de aard van het gegevens-verwerkende proces is het bijvoorbeeld momenteel nog niet mogelijk om burgers controle te geven over de eigen persoonsgegevens in de gehele keten. Dit zou namelijk een geautomatiseerde oplossing vergen die de persoonsgegevens op meerdere registratielocaties tegelijkertijd beschermt tegen ongeautoriseerde verwerkingen en daarbij feitelijk meereist met die persoonsgegevens. Hiervoor dienen alle systemen in de betreffende keten op dezelfde wijze te kunnen omgaan met persoonsgegevens die door de betrokkene zelf worden beheerd.
- In de centrale database staat het identiteitsdomein onder controle van de burger en staat het pseudo-identiteitsdomein in de centrale database (of andersom).

Een geautoriseerde gebruiker verkrijgt toegang door authenticatie aan de identiteitsbeschermer van de burger.

- In de decentrale databases staan het identiteitsdomein en de pseudo-identiteitsdomeinen onder controle van de burger. Een geautoriseerde gebruiker verkrijgt toegang door authenticatie aan de identiteitsbeschermer van de burger.

FAQ 5 : Is PET alleen geschikt voor processen waarin geen identiteit wordt verwerkt?

Nee, het is een misverstand dat PET alleen kan worden toegepast bij identiteitsarme processen. Dit zou de toepasbaarheid van PET ernstig beperken. Een identiteitsbeschermer kan bijvoorbeeld aan de invoer- of uitvoerzijde van het informatiesysteem worden geplaatst. Wanneer het noodzakelijk is dat de identiteit aan het begin en aan het einde van het proces bekend is, is dit vaak voor de tussenliggende interne verwerkingsprocessen niet het geval. PET kan worden ingezet om de gegevensbescherming in deze tussenliggende processen te realiseren.

4.7 Aandachtspunten

4.7.1 Logging en controle

Met behulp van logging en controle kan achteraf worden vastgesteld of de PET-maatregelen adequaat functioneren. Hiervoor is het belangrijk om elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens die onder verantwoordelijkheid van de verantwoordelijke plaatsvindt, vast te leggen en te controleren. Een voorbeeld is om op persoonsniveau vast te leggen aan welke organisaties gegevens zijn verstrekt (inclusief waarom en wanneer). Er ontstaat een audit-trail (wie deed wat, wanneer, waar en waarom) waardoor de bewerkingen controleerbaar zijn en kan worden vastgesteld of de PET-maatregelen adequaat werken.

Omdat logging en controle een middel is om te controleren of de maatregelen ten behoeve van de gegevensbescherming worden nageleefd, wordt logging en controle altijd in combinatie met één van de overige PET-vormen ingezet. De analyse van de logbestanden kan er wel toe leiden dat 'lekken' in de PET-vorm worden opgespoord en gedicht kunnen worden. Op deze wijze draagt logging en controle ook bij tot het voorkomen van onrechtmatige verwerking van persoonsgegevens.

Een bijkomend voordeel van logging en controle is dat voldaan kan worden aan de informatieplicht richting de burger. Een burger kan namelijk aan een organisatie vragen welke gegevens de organisatie over hem heeft vastgelegd en aan wie deze informatie allemaal is verstrekt. Met behulp van de logbestanden kan de organisatie

aantonen dat de informatie in het geheel niet is verstrekt of dat de informatie alleen maar is verstrekt aan geautoriseerde instanties of personen.

Het is uiteraard van belang dat de logbestanden niet gemanipuleerd kunnen worden, waardoor onbevoegden sporen zouden kunnen uitwissen. Daarnaast moeten de logbestanden periodiek worden beoordeeld door bijvoorbeeld de beveiligingsfunctionaris of de functionaris gegevensbescherming, en moet het management periodiek worden geïnformeerd (zie ook paragraaf 6.2). Een belangrijk aandachtspunt bij logging en controle is dat de logbestanden natuurlijk ook PET-proof moeten zijn. Men moet ervoor waken dat de logbestanden persoonsgegevens bevatten, waarvan men met PET juist de verwerking probeert te voorkomen.

Casus 10: Kiezen op Afstand

Politiek is bepaald dat stemmen op afstand en elektronisch stemmen mogelijk moeten zijn. Op deze wijze kunnen Nederlandse staatsburgers in een willekeurig stemlokaal in Nederland of zelfs in het buitenland stemmen. De elektronische wijze betreft het stemmen per telefoon of per internet, waarbij de burger de flexibiliteit heeft deze keuze op het laatste moment te maken.

PET-toepassing

De wet stelt strenge eisen aan het kiezen op afstand, zodat de volgende PET-maatregelen zijn getroffen:

- ontkoppelen van de stemmogelijkheid van het daadwerkelijke stemmen. Hiervoor is een scheiding aangebracht tussen de registratie (bij gemeente), het mogelijk maken te kunnen stemmen met de stembescheiden (bij Kiezen op Afstand-instantie) en de uitgebrachte stem (bij stemdienst bij derde vertrouwde partij). Ook in het drukproces is een scheiding aangebracht tussen de productie van kandidatenlijsten en die van gepersonaliseerde toegangscodes;
- sterk beveiligen van de gebruikte toegangs- en stemcodes. De toegangscode van de burger wordt via een eenwegsversleuteling omgezet in een niet-herleidbare code ('hash') die kan worden gebruikt om af te dwingen dat slechts eenmaal wordt gestemd. De uitgebrachte stem wordt niet op de pc van de kiezer opgeslagen. Tevens wordt de database van de 'elektronische stembus' zodanig versleuteld met cryptografische technieken dat alleen personen van het stembureau die door de burgemeester zijn geautoriseerd deze kunnen ontsleutelen. Aan een kandidaat is een groot aantal kandidaat-codes gekoppeld. Hiermee wordt voorkomen dat met afluisteren c.q. aftappen van de verbinding een stem openbaar zou worden;
- waarborgen van de gegevensintegriteit. Hiervoor worden transactiemechanismen toegepast die ervoor zorgdragen dat een stemhandeling alleen als volledige handeling kan worden uitgevoerd;

- logging van acties en gebeurtenissen vindt gedurende het stemproces plaats, dit stelt een toezichthouder in staat om achteraf het verloop van de stemming te controleren;
- vernietiging van stemcodes en uitgebrachte stemmen enkele dagen na de stemming (na onherroepelijk worden van de uitslag van de verkiezingen);
- diepgaande audits op gehele proces, drukkers, stemdienst en programmatuur van stemdienst voorafgaand en rond de stemdag/-periode.

Baten

Met de gebruikte PET-maatregelen is een uitgebrachte stem volstrekt anoniem en kan deze niet worden herleid tot de stemmende burger. Daarbij is de stemmer eenduidig en uniek geïdentificeerd alvorens hij/zij stemt. Tevens is het stemproces transparant voor de burger, het stembureau en de beheerorganisatie, zonder dat er te veel concessies moeten worden gedaan aan de veiligheid en betrouwbaarheid van het proces.

FAQ 6: Kan fraude nog wel worden opgespoord na de toepassing van PET?

Fraudeopsporing is ook na de toepassing van PET mogelijk. Zoals uit de beschrijving van de PET-vormen is gebleken, is er maar één vorm waarbij de gegevensverwerking volledig anoniem plaatsvindt. In dat geval is fraude moeilijker op te sporen. Bij de toepassing van algemene PET-maatregelen en het geautomatiseerde afdwingen van het privacybeleid wordt de identiteit verwerkt en is de identiteit van een persoon redelijk eenvoudig te achterhalen. Het uitgangspunt bij scheiding van gegevens is dat de identiteit wordt losgekoppeld van de overige gegevens. In beginsel in fraudeopsporing dus niet direct uitvoerbaar. Wanneer er een vermoeden van fraude bestaat kan de identiteitsbeschermer worden ingezet om iemands ware identiteit te achterhalen. Het gebruiken van de identiteitsbeschermer ten behoeve van fraudeonderzoek moet wel onder strikte voorwaarden en toezicht gebeuren, omdat anders de gegevensbescherming in gevaar komt en het vertrouwen van de burger sterk zal afnemen.

5 De businesscase van PET

Inzicht in de kosten en de – kwantitatieve en kwalitatieve – baten is een essentiële stap in het besluitvormingstraject bij toepassing van PET. Dit hoofdstuk gaat in op:

- Wenselijkheid van PET (§ 5.1);
- Elementen van de businesscase ((§ 5.2);
- Hoe kom ik tot een positieve businesscase? (§ 5.3).

5.1 Wenselijkheid van PET

In de vorige hoofdstukken is een functionele classificatie gegeven van PET-vormen. Ook is mede aan de hand van de verschillende structuren van informatiesystemen een aantal mogelijkheden gegeven voor de toepassing van PET in een organisatie. Om te onderzoeken of er voor uw organisatie een positieve businesscase bestaat voor de toepassing van PET, moeten drie kernvragen worden beantwoord. Deze vragen zijn:

1. Levert PET een wezenlijke bijdrage aan de beleidsdoelstellingen van de organisatie?
2. Welke kwalitatieve en kwantitatieve baten kan PET in onze organisatie realiseren?
3. Welke kosten brengt PET eenmalig en structureel met zich mee?

Indien de beantwoording van deze vragen leidt tot de conclusie dat de toepassing van PET in uw organisatie wenselijk én vanuit een kosten- batenperspectief rationeel is, dan heet het dat er een positieve businesscase bestaat voor de toepassing van PET. De positieve businesscase is de zakelijke rechtvaardiging van de toepassing van PET. De term businesscase verwijst dan tevens naar de uitwerking hiervan in een beleidsdocument. Dit document zal de primaire verantwoording en de aanleiding vormen voor het opnemen van PET-activiteiten in het totale project. Ook zal het bij de uitvoering fungeren als communicatiemiddel rondom de aanleiding van het project en als vastlegging van de overeenstemming over de nettobaten aan belanghebbenden. Het is belangrijk hierbij tevens de aannames zo gedetailleerd mogelijk vast te leggen.

Het blijft overigens niet bij het eenmalig opstellen van de businesscase. Tijdens de uitvoering van het project dient deze te worden bewaakt. Gaande het project zal meer inzicht worden verkregen in de te realiseren baten en de te maken kosten. Continu moet worden bekeken of de businesscase nog positief is.

In dit hoofdstuk zal u ondersteuning worden geboden bij het opstellen van de businesscase voor PET en worden bouwstenen aangereikt voor de verdere detaillering tijdens de projectuitvoering.

5.2 Elementen van de businesscase

5.2.1 *Beleid*

De belangrijkste overweging in het opstellen van een businesscase is in welke mate een bijdrage wordt geleverd aan de beleidsdoelstellingen van de organisatie. Deze overweging zal in de praktijk vaak doorslaggevend zijn en vormt daarom het startpunt van de businesscase. De in hoofdstuk 2 genoemde belangrijkste voordelen kunnen als uitgangspunt dienen om te bepalen of PET een bijdrage aan de beleidsdoelstellingen van de organisatie levert. Wordt er een bijdrage geïdentificeerd, dan kan worden doorgegaan met de kosten- batenanalyse. Kernvraag is dan of deze bijdrage(n) opweegt (opwegen) tegen de kosten die ermee gemoeid zijn. Indien geen bijdrage wordt geleverd, kan de opstelling van de businesscase worden stopgezet. Indien de bescherming van persoonsgegevens een absolute vereiste is – denk aan elektronisch stemmen voor de kamerverkiezingen – dan zullen te hoge kosten zelfs het gehele project onmogelijk maken.

5.2.2 *Baten*

De baten van PET kunnen kwantitatief en kwalitatief van aard zijn. Indien de invoering van PET aantoonbare kostenreducties met zich meebrengt, dan zijn de baten meetbaar en dus kwantitatief. Kwalitatieve baten zijn slecht meetbaar en lastig in geld uit te drukken, ze kunnen echter de kwantitatieve baten overtreffen. Een voorbeeld hiervan is de positieve uitstraling wanneer PET wordt toegepast. Een andere kwalitatieve baat is dat door invoering van PET koppelingen tussen verschillende instanties mogelijk zijn die zonder PET niet mogelijk zijn. Hierdoor neemt de kwaliteit van de dienstverlening aan de burger toe, maar zij is moeilijk in cijfers uit te drukken. In figuur 14 is een overzicht gegeven van mogelijke baten.

Kwalitatieve baten	Kwantitatieve baten
■ PET maakt toepassingen mogelijk die anders onmogelijk zouden zijn; ■ Positieve uitstraling richting burger. Burgers hebben hierdoor meer vertrouwen in de overheid en haar elektronische dienstverlening. Dit vertrouwen is noodzakelijk voor het welslagen van dit dienstverleningskanaal; ■ Voldoen aan de Wbp; ■ Toegenomen controle van betrokkene over zijn persoonsgegevens; ■ Verbetering van de kwaliteit van informatie; ■ Versterking van innovatieve imago van organisatie die PET toepast; ■ PET en de daarmee verband houdende privacy-managementsystemen zorgen ervoor dat voor de organisatie de risico's op privacy-schendingen beheersbaar zijn.	■ Verbetering van de klanttevredenheid; ■ PET maakt het mogelijk databases te koppelen, de gegevensverwerking te stroomlijnen en de privacy te waarborgen. De dienstverlening van de overheid en de bijbehorende gegevensverwerking kunnen daarom efficiënter worden uitgevoerd en administratieve lastenverlichting kan worden bereikt; ■ Men hoeft minder persoonsgegevens op te vragen, in te voeren, te corrigeren en te verwerken; ■ Door de inzet van PET wordt minder gesteund op procedurele/organisatorische maatregelen. Dit is een verlichting voor de organisatie en geeft meer zekerheid over privacybescherming; ■ Internet kan worden gebruikt als communicatiemedium in plaats van duurdere vaste netwerken; ■ Vermindering van audit-, toezicht- en managementkosten en van eventuele boetes van toezichthouders; ■ Vermindering van kosten voor informatie-verstrekking aan betrokkenen.

Figuur 14: De baten van PET

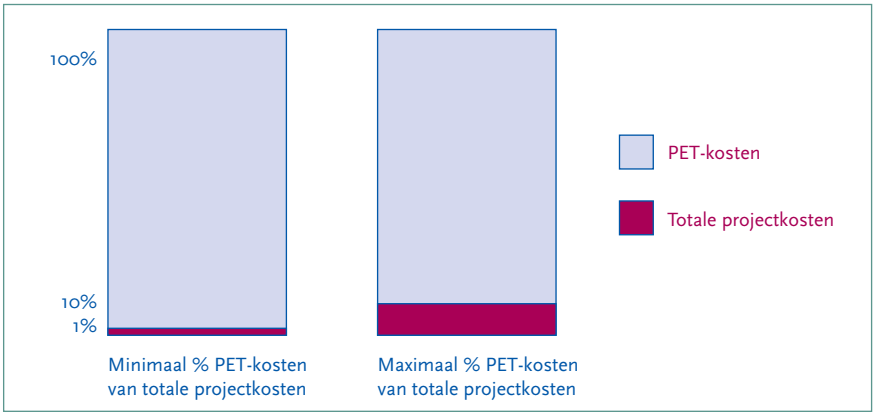
Het niet kunnen kwantificeren van baten hoeft geen belemmering te zijn voor een positieve businesscase. De kwalitatieve baten kunnen namelijk van groot belang zijn voor een succesvolle dienstverlening en zodoende de doorslag geven.

Businesscase bij Nationaal Trauma Informatie Systeem

Het huidige NTIS was niet mogelijk geweest zonder de toepassing van PET. Om de kosten laag en beheersbaar te houden, moest namelijk gebruik worden gemaakt van internet. Het gebruik van internet betekende automatisch dat stringente gegevensbeschermende maatregelen toegepast moesten worden.

5.2.3 *Kosten*

In deze paragraaf is een overzicht van kostenposten gegeven dat kan worden gebruikt tijdens het opstellen van de businesscase. Allereerst wordt in figuur 15 een overzicht gegeven van het percentage PET-kosten ten opzichte van de totale projectkosten van het ontwikkelen van een systeem. Uit de interviews met personen die betrokken zijn geweest bij de ontwikkeling van een systeem met PET is gebleken dat de kosten tussen de 1 en 10% van de totale projectkosten bedragen.



Figuur 15: Percentage PET-kosten van de totale projectkosten

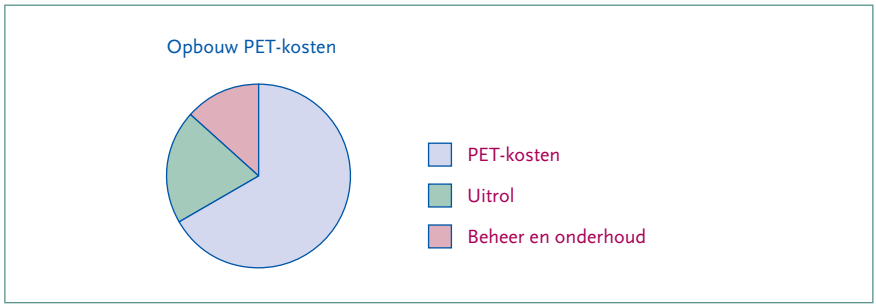
De bandbreedte wordt veroorzaakt doordat de kosten afhankelijk zijn van de gekozen PET-vorm. Bij anonimiseren ligt het accent van de kosten op de eenmalige investeringen en minder op de structurele kosten. Er hoeven bijvoorbeeld geen authenticatiemiddelen worden uitgerold. Daarnaast verminderen de kosten van de algemene beveiligingsmaatregelen. Er worden namelijk geen persoonsgegevens meer verwerkt en daarom kunnen ten aanzien van de gegevensbescherming minder strenge eisen aan de beveiliging worden gesteld [16].

Bij scheiding van gegevens worden er verschillende domeinen ingericht, moet meestal het gegevensmodel worden gewijzigd en is vaker maatwerk nodig om de PET-vorm te implementeren. Juist doordat bij anonimiseren geen persoonsgegevens worden verwerkt, zijn het gegevensmodel en de implementatie eenvoudiger. Ook zijn er meer standaardoplossingen beschikbaar voor anonimiseren.

16 Vanuit het oogpunt van beschikbaarheid kan het bijvoorbeeld wel noodzakelijk om een hoger algemeen beveiligingsniveau te handhaven.

De kosten van de algemene PET-maatregelen zijn variabel vanwege de verscheidenheid van de mogelijke maatregelen. Versleuteling is bijvoorbeeld goedkoper dan het toepassen van biometrie met PKI.

Om inzicht te krijgen in de opbouw van de specifieke PET-kosten, zijn de kosten uitgesplitst in de categorieën ontwikkeling, uitrol, en beheer en onderhoud. Ontwikkeling en uitrol zijn eenmalige kostencategorieën en beheer en onderhoud is een structurele kostencategorie. In figuur 16 wordt een schatting van de verhouding tussen de drie categorieën weergegeven. De drie categorieën samen vormen de totale PET-kosten, waarbij moet worden opgemerkt dat de exacte verhouding kan verschillen voor de verschillende PET-vormen en -toepassingen.



Figuur 16: Verdeling van de totale PET-kosten

Figuur 17 geeft aan uit welke kostenposten de zojuist genoemde categorieën bestaan. Standaardkosten die voor ieder ICT-project van toepassing zijn, zoals haalbaarheidsstudie en functioneel ontwerp van het informatiesysteem, zijn niet opgenomen in dit overzicht. In de figuur zijn alleen de PET-specifieke kosten opgenomen. Daarnaast is op een schaal van laag/midden/hoog aangegeven wat het gewicht is van iedere kostenpost in het totale kostenplaatje van de PET-specifieke kosten.

	Kostensoort	Gewicht in het PETtotaal [17]
Eenmalig	**Ontwikkeling**	
	Analyseren noodzaak verwerking persoonsgegevens	Midden
	Ontwerpen gegevensmodel	Hoog
	Functioneel ontwerp PET-vorm	Midden
	Technisch ontwerp PET-vorm	Midden
	Eventuele aanpassingen aan infrastructuur	Laag
	Ontwikkelen van PET-vorm of kopen PET-product [18]	Laag/hoog
	Ontwikkelen of kopen van logging- en monitoring-hulpmiddel	Laag
	Uitrol	
	Opleiding gebruikers / beheerders	Laag
	Uitrol van eventuele authenticatiemiddelen	Laag/midden
	Communicatie [19]	Laag/midden
Structureel	**Beheer en onderhoud**	
	Beheer van eventueel gebruikte authenticatiemiddelen	Laag
	Onderhoud van de specifieke PET-vorm	Laag/midden

Figuur 17: Overzicht van specifieke PET-kosten

Bij gebruik van dit overzicht is het belangrijk om te onthouden dat dit een generiek overzicht is, dat moet worden aangepast aan de specifieke kenmerken van uw organisatie en de structuur van het informatiesysteem (zie hoofdstuk 3).

Professor Boasson (Universiteit van Amsterdam, Kilometerheffing): 'De meeste tijd en kosten zitten in het ontwerpen van het gegevensmodel. Dit is één van de belangrijkste stappen uit het gehele ontwikkeltraject.'

17 Op basis van de interviews en onderzoek is het niet mogelijk een exacte inschatting van de verschillende kostenposten te geven.

18 De PET-vorm kan simpel tot complex zijn; met bijvoorbeeld de toepassing van biometrie en PKI zijn relatief hogere kosten gemoeid dan met een oplossing in de database of met rolautorisaties.

19 Communicatie wordt in dit geval als PET-specifiek gezien, omdat de manier van werken anders kan worden. Het creëren van draagvlak is om die reden dan ook uiterst belangrijk.

BKWI-directeur Kinkhorst: 'Voor het realiseren van veilige gegevensuitwisseling in de sociale sector hebben we gebruikgemaakt van een besloten netwerk en een verfijnde rol-gebaseerde autorisatiestructuur 20. Uitgaande van de huidige omvang van de gebruikersgroep bedragen de kosten voor deze PET-toepassing circa 10% van de totale kosten'.

Verantwoordelijk systeemarchitect bij de ontwikkeling van de PET-toepassing bij psychiatrisch ziekenhuis Meerkanten, Van Blarkom: 'De kosten van een nieuw PET-proof ziekenhuisinformatiesysteem met elektronische patiëntendossiers bedragen slechts enkele procenten extra van de totale kosten, mits bij de bouw grondig over PET is nagedacht.'

Het feit of PET wordt toegepast op bestaande of nieuw te ontwikkelen systemen is ook van invloed op de hoogte van de kosten. Wanneer PET wordt toegepast op bestaande systemen liggen de kosten hoger dan bij nieuwe systemen. De oorzaak hiervan is dat de meeste kostenposten van PET eenmalig zijn en de eenmalige activiteiten onderdeel uitmaken van het gehele systeemontwikkelingtraject. Wanneer de PET-specifieke activiteiten achteraf worden uitgevoerd, moet het bestaande systeem eventueel worden aangepast. Als gevolg hiervan moeten bepaalde activiteiten dubbel worden uitgevoerd en nemen de kosten van de invoering van PET toe.
In hoofdstuk 7 wordt verder ingegaan op PET bij bestaande systemen.

Stor, directeur RINIS: 'Bij de ontwikkeling van RINIS betroffen de PET-kosten met name het denkwerk over de architectuur. De kosten van de diverse toegepaste PET-maatregelen vormden 2 à 3% van de totale ontwikkelkosten.'

Taal, Projectmanager NTIS: 'De kosten voor de PET-specifieke onderdelen van het NTIS bedragen ongeveer 8 à 10% van de totale kosten, voornamelijk vanwege het gebruik van sterke authenticatie op basis van digitale certificaten, die zijn opgeslagen op met pincode of biometrie beveiligde chipkaarten.'

Uit de interviews met personen in organisaties waar PET wordt toegepast, is gebleken dat altijd wel een globale schatting kan worden gegeven van de additionele kosten van PET. Een nauwkeurige schatting blijkt lastiger komt doordat PET-gerelateerde

20 Voor verdere uitleg over rolgebaseerde autorisaties zie: Mienes, P. en Bokhorst, B., De (on)beheersbaarheid van logische toegangsbeveiliging, Compact, nummer 1, 2003.

activiteiten vanaf de ontwerpfase een integraal onderdeel vormt van het gehele systeem-ontwikkelingtraject.

5.3 Hoe kom ik tot een positieve businesscase?

De vereiste kennis voor het opstellen van de businesscase ligt vaak verspreid in uw organisatie, waarbij er ook verschillende visies kunnen bestaan op de baten en de kosten. Vaak kan ook externe informatie gewenst zijn van bijvoorbeeld leveranciers en overheidsorganisaties met vergelijkbare informatiesystemen en met langere ervaring in de toepassing van PET. Om deze redenen kan het nuttig zijn om de bepaling van de businesscase in de vorm van een workshop te organiseren. Ook vanuit het perspectief van projectmanagement is dit wenselijk, omdat op deze wijze een gedeelde visie kan worden ontwikkeld omtrent de aard van de problematiek, het doel van het project, verwachte baten en kosten en de aansluiting op de organisatiedoelstellingen.

Voor een effectieve workshop wordt vooraf een inventarisatie gemaakt van de te beantwoorden vragen, de reeds beschikbare informatie en documenten rondom de eigen organisatie en de te evalueren PET-vormen. Deze inventarisatie wordt vooraf aan de deelnemers beschikbaar gesteld. Aspecten die in de workshop worden behandeld, zijn:

- behoefte aan gegevensbeschermende maatregelen voor het behalen van de beleidsdoelen van de organisatie;
- doelgroep van de dienstverlening;
- mogelijke baten en kwantificeerbaarheid van de baten;
- mogelijke PET-vormen die toegepast kunnen worden en de bijbehorende (eenmalige) investeringskosten en structurele kosten (onderhoud, beheer, licenties) voor ieder alternatief;
- toepassing van bestaande middelen;
- impact op de processen en de manier van werken voor de betrokken medewerkers;
- creëren van draagvlak in de organisatie voor het toepassen van PET;
- aanwezigheid en beschikbaarheid van de noodzakelijke kennis en expertise;
- overeenstemming of de toepassing van PET wenselijk is en de te nemen vervolgstappen.

Op basis van de uitkomsten van de workshop kan vervolgens de businesscase definitief worden opgesteld en wordt de beslissing genomen of PET toegepast gaat worden in de geautomatiseerde gegevensverwerking.

In figuur 18 is een cijfervoorbeeld opgenomen van de kosten en baten van de invoering van een privacymanagementsysteem (PMS).

Voorbeeld Return on Investment van een privacymanagementsysteem (PMS)

Stel dat een organisatie besluit een PMS in te voeren. Een mogelijke onderbouwing van de businesscase kan er als volgt uitzien:

Indien geen PMS wordt aangeschaft, worden de minimale jaarlijkse privacyhandhavings-kosten voor een organisatie van meer dan 1.000 medewerkers als volgt geschat:

	Jaarlijkse kosten
Salariskosten Functionaris Gegevensbescherming (100% tijdbesteding)	100.000
Salariskosten management en secretariaat	40.000
Kosten privacyaudit	30.000
Beveiligingskosten i.v.m. privacyhandhaving (los van de noodzakelijke informatiebeveiliging)	20.000
Onderhoud meldingen, reglementen, afhandeling rechten geregistreerden, voorlichting, imago- en andere schade, etc.	20.000
TOTAAL	**210.000**

Bij gebruikmaking van een PMS:	
	Ontwikkeling en invoering Jaarlijkse kosten
Aanschaf PMS	150.000
Consultancy voor PMS-implementatie (60 dagen)	80.000
Aanloopkosten na implementatie	20.000
Operationele kosten PMS	30.000
Onderhoud ± 15% aanschafprijs per jaar	22.000
Kosten privacyaudit	10.000
Salariskosten Functionaris Gegevensbescherming (50% tijdbesteding)	50.000
	50.000
TOTAAL	300.000
	112.000
Uit dit overzicht blijkt dat al na drie jaar de extra ontwikkelingskosten voor PET geheel zijn terugverdiend.	

Figuur 18: Voorbeeld ROI van een privacymanagementsysteem

6 Organisatorische en juridische aspecten

PET betreft technologie voor het realiseren van wetgeving, maar is voor een goede toepassing afhankelijk van juridische, maar met name organisatorische randvoorwaarden en implicaties. Dit hoofdstuk behandelt:

- Managementbewustzijn en –betrokkenheid (§ 6.1);
- PET als onderdeel van de managementcyclus (§ 6.2);
- De duivelsdriehoek (§ 6.3);
- PET-strategieën (§ 6.4);
- De normatieve kant van PET (§ 6.5);
- Toetsing en toezicht (§ 6.6).

6.1 Managementbewustzijn en -betrokkenheid

De invoering van de toepassing van PET vereist een doelgerichte implementatie en een bewustwordingsproces ten aanzien van gegevensbescherming en PET. Het stelsel van reeds getroffen maatregelen en procedures voor het beheer, de beveiliging en de verwerking van gegevens zal getoetst moeten worden aan de doelstellingen van de invoering van PET en zo nodig moeten worden heroverwogen. Het implementeren van PET is niet alleen een technisch maar ook een organisatievraagstuk en behoort derhalve ook tot de primaire verantwoordelijkheid van het management van een organisatie. Daarnaast is van belang dat de implementatie van PET geen losse component of los project is, maar als deelgebied geïntegreerd moet worden in systeemontwikkelings- en onderhoudstrajecten.

> Directeur Kok (Trans Link Systems/OV-chipkaart): "We hebben bij de aanbesteding en het systeem-ontwerp direct rekening gehouden met de privacyeisen. Daarnaast hebben wij gekozen voor de optie van anonieme kaarten om de gebruikersacceptatie zo hoog mogelijk te laten zijn."

Implementatie van PET gaat niet van vandaag op morgen. Een organisatie heeft tijd nodig om het bewustwordingsproces daaromtrent op gang te brengen. Er zit dan ook een verschil tussen de bewustwording en het nadenken over gegevensbescherming en het ontwikkelen en implementeren van PET. Het is voor het management dat belast is met de implementatie van PET raadzaam één of meer contactpersonen aan te stellen die verantwoordelijk zijn voor onder meer de coördinatie van de te treffen PET-voorzieningen en de evaluatie van de getroffen voorzieningen. Behalve voor de ICT-manager en de projectmanager is hier een belangrijke rol weggelegd voor de functionaris voor de gegevensbescherming en de beveiligingsfunctionaris.

6.2 PET als onderdeel van de managementcyclus

De invoering van PET stelt eisen aan de verwerking van persoonsgegevens en heeft gevolgen voor de procedures en maatregelen die een organisatie heeft genomen om haar gegevensverwerking goed te beheersen en te beveiligen (betrouwbaar, efficiënt, effectief, exclusief, integer, continu en controleerbaar). Om PET te implementeren is een belangrijke voorwaarde dat er een adequaat stelsel van algemene verwerkingsmaatregelen en procedures wordt gerealiseerd waarbij rekening wordt gehouden met de specifieke beschermingsmaatregelen die voor de verwerking van persoonsgegevens noodzakelijk zijn.

Wil men een evenwichtig verwerkingsbeleid voor persoonsgegevens implementeren en onderhouden, waarin PET als hoeksteen van dat beleid wordt toegepast, dan zal PET een belangrijke plaats in de managementcyclus moeten innemen.

Het realiseren van bedrijfsdoelstellingen, via de managementcyclus, verloopt in het algemeen via de volgende drie fasen: de organisatie van de processen (inclusief de beleidsvoering), de processen zelf, en een evaluatie en bijsturing van de processen. Daarbij is het van belang, voorzover dat nog niet is gedaan, de administratieve organisatie in kaart te brengen.

PET is onderdeel van de managementcyclus en daarom zal eens per jaar onderzoek moeten worden gedaan of de PET-toepassingen het gewenste effect sorteren. Dat onderzoek kan een onderdeel zijn van een privacyaudit waarin wordt vastgesteld of de organisatie haar privacybeleid heeft nageleefd. De privacyaudit is noodzakelijk om vast te stellen of PET het gewenste effect heeft en om terugkoppeling te geven aan de ontwerpers van de met PET versterkte systemen.

Noodzaak van een risicoanalyse
Uitgangspunt is om vanuit het privacybeleid de verwerking van persoonsgegevens te analyseren en te evalueren, en vervolgens in kaart te brengen hoe een PET-implementatie de Wbp-eisen realiseert. Een privacyrisicoanalyse vooraf is noodzakelijk en nuttig voor het treffen van de juiste maatregelen. Dit kan gebeuren op een wijze analoog aan een Afhankelijkheids- en Kwetsbaarheidsanalyse zoals vermeld in het Voorschrift Informatiebeveiliging Rijksoverheid (VIR).

PET kan alleen maar met succes geïmplementeerd worden na een grondige risicoanalyse, waarin de bedreigingen worden geïnventariseerd waaraan de

verwerking van persoonsgegevens blootstaat. In dit verband worden ook de sterke en zwakke punten van de gegevensverwerking vastgelegd. Concreet betekent dit dat het inzichtelijk moet zijn welke persoonsgegevens een organisatie verzamelt en verwerkt, wie toegang tot de gegevens heeft, wie verantwoordelijk voor de verwerking is en of in de organisatie controlemaatregelen zijn getroffen om na te gaan of het privacybeleid wordt nageleefd.

De risico's tezamen met de sterke en zwakke punten van de verwerkingsorganisatie en een kosten- batenanalyse leiden, op basis van het gedefinieerde privacybeleid, tot een afgewogen keuze voor de te treffen voorzieningen van organisatorische en technische aard. Het management dient vervolgens zorg te dragen voor implementatie van de gekozen voorzieningen op een toereikend niveau.

Met behulp van een systeem van logging en controle (zie paragraaf 4.8.1) dient het management na te gaan in hoeverre de getroffen voorzieningen de doelstelling van het geformuleerde privacybeleid realiseren. Het management moet aangeven op welke wijze en met welke intensiteit het gegevens over de logging en controle wil ontvangen. De resultaten van de uitgevoerde logging en controle vormen de basis voor eventuele correctieve acties, aanpassing van getroffen technische maatregelen en procedures dan wel bijstelling van het geformuleerde beleid.

6.3 De duivelsdriehoek

Een specifiek probleem bij het ontwikkelen van informatiesystemen met privacygevoelige gegevens vormen de verschillende privacyperspectieven van de betrokken partijen. Bij privacygevoeligheid van gegevensverwerking zal de privacyfunctionaris eisen stellen aan de beveiliging van de persoonsgegevens. Vaak heeft de privacyfunctionaris een juridische achtergrond en is hij minder geschoold in technologische oplossingen. Daarvoor is een ICT-medewerker in het project betrokken, die heeft echter veelal weinig juridische kennis in het algemeen of van privacybescherming in het bijzonder.

Feitelijk zal de privacyfunctionaris primair geschoold zijn in het 'PET-denken' en veel minder in PET als technologie oftewel de informatietechnische oplossingen. Voor de ICT-medewerker geldt dat juist omgekeerd.

Het komt er dus op neer dat bijvoorbeeld beleidsmedewerkers of proceseigenaren een brugfunctie moeten vervullen tussen 'PET-denken' en 'PET-technologie' om beide typen functionarissen een effectieve en efficiënte bijdrage aan het project te kunnen laten leveren. Zonder deze brugfunctie kunnen in de praktijk veel miscommunicatie

en gemiste PET-kansen optreden. Hopelijk biedt dit Witboek goede ondersteuning aan beleidsmedewerkers en proceseigenaren om voor beide disciplines de brugfunctie te kunnen vervullen.

6.4 PET-strategieën

Nadat de risicoanalyse is uitgevoerd en de privacybedreigingen in kaart zijn gebracht, dient het management een keuze te maken uit de verschillende strategieën om PET in te zetten ter bescherming van de gegevens. Uit de volgende strategieën kan worden gekozen:

- De organisatie richt zich op het voorkomen of verminderen van de identificeerbaarheid.
- De organisatie zet in op het voorkomen van onrechtmatig verwerken van persoonsgegevens.
- De organisatie gebruikt specifieke technologieën die de gegevensbescherming ondersteunen.

Een combinatie van deze strategieën is natuurlijk ook denkbaar. In de navolgende paragrafen zijn deze drie PET-strategieën nader uitgewerkt. In hoofdstuk 7, waarin het stappenplan wordt besproken, is in dat stappenplan een plaats toegewezen aan de PET-strategieën.

6.4.1 Eerste PET-strategie: het voorkomen van identificatie

Voor de eerste strategie is het van belang om te bepalen of er sprake is van identificeerbare gegevens. Een natuurlijk persoon kan direct of indirect identificeerbaar zijn. Direct identificeerbaar is men aan de hand van naam, adres en woonplaats (NAW-gegevens), een persoonsnummer, een pseudo-identiteit die in brede kring bekend is of een biometrisch kenmerk (zoals een vingerafdruk). 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.

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 ook niet langer de Wbp van toepassing omdat er geen persoonsgegevens beschermd hoeven te worden.

6.4.2 *Tweede PET-strategie: het waarborgen tegen onrechtmatige verwerking van persoonsgegevens*

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

> 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 men ze zou willen gebruiken voor een ander doel dan waarvoor ze verzameld zijn. PET kan ook uitstekend worden ingezet in het kader van de informatiebeveiliging.

6.4.3 *De derde PET-strategie: het toepassen van specifieke privacyondersteunende technologieën*

Omdat de hiervoor besproken PET-strategieën niet overal ingezet kunnen worden, kan gebruik worden gemaakt van andere technologieën die kunnen bijdragen tot een betere gegevensbescherming. Daarbij kan men denken aan het toepassen van privacymanagementsystemen zoals die door diverse fabrikanten op de markt worden gebracht. In deze systemen wordt consequent op alle gegevensverwerkingen het van tevoren vastgestelde privacybeleid toegepast.

> **Een voorbeeld van zo'n privacyregel kan zijn [21]:**
> [Instelling] [mag] [klant adres] [telefonisch doorgeven] aan [externe relatie] voor [doeleinden] als [klant toestemming heeft gegeven]
> Tussen de vierkante haken wordt bij een verwerkingsverzoek steeds een concrete naam of conditie ingevuld op basis waarvan het privacymanagementsysteem beslist of het verzoek wordt gehonoreerd of niet. Daartoe zijn dan vooraf door de privacy-functionaris de mogelijke condities ingevuld; het privacymanagementsysteem biedt daarvoor praktische ondersteuning.

21 In overeenstemming met: J. de Rooij, Privacymanagement en Enterprise Privacymanager, Privacy & Informatie, nummer 5, oktober 2003.

Voorts kan een sandwich van technologieën gezamenlijk een privacyveilige gegevensverwerking realiseren.

Privacybevorderende technologieën

Enkele voorbeelden van het inzetten van technologieën ter bevordering van privacy zijn:

- Transparantie wordt bevorderd door het gebruik van P3P (een technologie om het privacybeleid van websites te toetsen).
- Een statistische- en taalkundige analyse op de juistheid van de naam of het adres binnen een adressensysteem kan de kwaliteit van de gegevens verbeteren.
- De rechten van betrokkenen kunnen beter worden bewaakt door feedback en controle. Deze ontwerpbeginselen zorgen ervoor dat informatiesystemen op elk gewenst moment terugkoppelen naar het individu over datgene wat de betrokkene aan persoonsgegevens heeft afgestaan aan het informatiesysteem, met als reactiemogelijkheid de inzage, aanvulling, wijziging en verwijdering van persoonsgegevens.
- 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 is het eveneens mogelijk technische maatregelen te treffen om onrechtmatige handelingen in de zin van de Wbp tegen te gaan. Dit kan bijvoorbeeld door IP-adressen te scannen op bestemming. Wanneer de bestemming buiten de EU is blokkeert het privacymanagementsysteem de verzending. Vervolgens vraagt het systeem toestemming van het management en wordt de eventuele verzending uiteraard gelogd.

Figuur 19: PET-technologieën

6.5 De normatieve kant van PET

Artikel 13 Wbp vormt de wettelijke grondslag voor de inzet van PET. Dit artikel schrijft 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 criteria:

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

De eis om PET toe te passen wordt in artikel 11 van de Wbp versterkt. Dit artikel bepaalt dat er niet meer, maar ook niet minder persoonsgegevens mogen worden verzameld en verwerkt dan voor de doeleinden noodzakelijk is. Daarnaast moet de verantwoordelijke de nodige maatregelen treffen opdat de onderhavige gegevens juist en nauwkeurig in het licht van de doeleinden worden verzameld en verwerkt.

Voor alle duidelijkheid: onder persoonsgegevens verstaat de Wbp: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.'

Het gebruik van de slogan 'PET INSIDE' bij informatiesystemen kan de bewustwording over PET positief beïnvloeden.

PET houdt de vertaling in van 'zachte' juridische normen in 'harde' systeemspecificaties. Dat betekent, dat het inbouwen van PET in systemen niet alleen een technische opgave, maar ook een normatieve opgave is. Voordat 'PET INSIDE' (de term is 'geleend' van de reclame 'INTEL INSIDE') in informatiesystemen zit, moet duidelijk zijn welke eisen de Wbp aan een informatiesysteem stelt. Technologen en juristen zullen die normen moeten vertalen in technische systeemeisen.

6.6 Toetsing en toezicht

Het CBP kan de verantwoordelijke en de bewerker aanspreken op het door de organisatie gevoerde privacybeleid, de beveiliging en de verwerking van persoonsgegevens en de wijze waarop het stelsel van genomen maatregelen is geïmplementeerd en wordt nageleefd. Het CBP heeft de bevoegdheid ambtshalve of op verzoek van belanghebbende (rechts)personen een onderzoek in te stellen naar de manier waarop de Wbp wordt nageleefd (artikel 60 Wbp). De auditors van het CBP zullen dan in de privacyaudit de opzet, het bestaan en de werking van het stelsel van procedures en maatregelen om de gegevensbescherming te waarborgen conform de wettelijke normen, toetsen. De implementatie van PET voorkomt dat de organisatie voor onverwachte en onaangename verrassingen komt te staan en schept het noodzakelijke vertrouwen van de burger in de overheid.

Naast toetsing door het CBP of andere externe partijen kunnen ook interne reviews en audits worden uitgevoerd. Hiermee kan eventueel worden aangetoond dat verdere verbeteringen van de geïmplementeerde privacymaatregelen wenselijk of zelfs noodzakelijk zijn om te kunnen voldoen aan wettelijke en interne vereisten. Hiervoor zijn standaardaanpakken en checklisten beschikbaar.

7 Stappenplan

In dit hoofdstuk is een stappenplan opgenomen voor het invoeren van PET. Hierbij wordt zowel ingegaan op nieuwe als op bestaande informatiesystemen. Aan bod komen de navolgende onderwerpen:

- PET als ontwerpkeuze (§ 7.1);
- PET bij bestaande keuze (§ 7.2);
- De stappen (§ 7.3).

7.1 PET als ontwerpkeuze

In het PET-stappenplan worden alleen de PET-specifieke onderdelen behandeld en wordt niet ingegaan op de algemene stappen rondom de ontwikkeling van informatiesystemen. Voorafgaand aan het uitvoeren van het stappenplan moet de organisatie zich reeds bewust zijn van het belang van gegevensbescherming. Tijdens gesprekken met projectleiders die betrokken zijn bij grote projecten waarbij de toepassing van PET is overwogen en/of is ingevoerd, bleek steeds zeer nadrukkelijk de volgende regel:

Privacy by design
Gegevensbescherming inclusief PET dient van meet af aan een onderdeel te zijn van het ontwerp van de architectuur van het informatiesysteem.

Alvorens het stappenplan wordt behandeld, wordt in paragraaf 7.2 eerst aangegeven waarom het belangrijk is om de implementatie van PET integraal mee te nemen in de systeemontwikkeling.

Casus 11: Privacy by design in Canada: ICT kan niet alleen privacyproblemen veroorzaken maar ook oplossen!

Uit onderzoek van de overheid van Alberta was gebleken dat de inhoud van haar gegevensbanken voor ongeveer 57% bestond uit direct of indirect identificeerbare persoonsgegevens. Vandaar dat een privacyarchitectuur binnen de Centrale Overheid van de Provincie Alberta (Canada) als een logische stap werd gezien. Dit vormt een uitbreiding op de reeds bestaande ICT-infrastructuur en de Government of Alberta Enterprise Architecture (GAEA). Met deze privacyarchitectuur kan de overheid van Alberta haar privacybeleid met ICT realiseren en ervoor zorgdragen dat het gebruik van geavanceerde technieken voldoet aan de wettelijke privacyvereisten.

De vereisten voor de privacyarchitectuur werden in detail vastgelegd in oktober 2002

door middel van overheidsbreed georganiseerde werkvergaderingen met de betrokken beleidsambtenaren, ambtenaren verantwoordelijk voor de ICT-infrastructuur en vertegenwoordigers van het bedrijfsleven. Het resultaat van deze workshops leidde tot een lijst van twaalf vereisten, die gedetailleerd werden vastgelegd in het beleidsstuk over de GAEA Privacy Architecture Requirements. Niet alleen werd een afspraak gemaakt over de gemeenschappelijke privacyterminologie, de noodzakelijke gebruikers-interfaces en het gebruik van technologie om het privacybeleid af te dwingen, maar ook over een identiteitssysteem gebaseerd op betekenisloze maar unieke nummers (MBUNs)[22]. Deze nummers dienen als referentie naar bewust gefragmenteerde en aldus slechts per deel benaderbare domeinen van persoonsgegevens. Het concept van identificatie-sleutelnummers is gebaseerd op het inzetten van identiteitsbeschermers en gelaagde identiteitsdomeinen. Na de specificatie van de vereisten voor de privacyarchitectuur werd een testmodel ontwikkeld, dat vervolgens in dezelfde werkgroepen werd becommentarieerd. Met de verkregen informatie werd ten slotte het privacymanagementsysteem gerealiseerd. Dit systeem ontving de HP Privacy Innovation Award in 2003.

7.2 PET bij bestaande systemen

PET is geen black box die men koopt en achteraf gemakkelijk aan een bestaand informatiesysteem kan worden toegevoegd.

PET toepassen op bestaande systemen blijkt in de praktijk een lastige opgave. Wanneer bijvoorbeeld wordt overgegaan op het vastleggen van gegevens verdeeld over verschillende domeinen, moet het gegevensmodel worden aangepast aan de domeinen en de nieuwe gegevensstroom. Een bestaand informatiesysteem, zowel de applicatieprogrammatuur als de databasearchitectuur, moet daarop worden aangepast. Veelal is dat een ingrijpende systeemaanpassing en derhalve betrekkelijk kostbaar. Overigens hoeft de gebruiker daar maar weinig van te merken omdat het vooral technische aanpassingen aan het systeem betreft.

Casus 12: Psychiatrisch Ziekenhuis Meerkanten

Uit een diepgaande privacyaudit was gebleken dat een psychiatrisch ziekenhuis op bijna alle onderdelen voldeed aan de privacywetgeving, behalve dat de logische toegangsbeveiliging te ruime inzage- en mutatiemogelijkheden bood. Voor het goed afschermen van gegevens over de geestelijke gesteldheid van personen wilde dit psychiatrische ziekenhuis ook de behandelrelatie tussen zorgverlener en patiënt met autorisatie geautomatiseerd afdwingen.

22 De MBUNs zijn niet gebaseerd op reeds bestaande identificerende nummers.

Men had echter te maken met een al bestaand ziekenhuisinformatiesysteem (X/MCare) en al bestaand gegevensmodel.

PET-toepassing

- scheiden van identificerende gegevens en medische gegevens door gebruikmaking van pseudo-identiteiten. Op deze wijze kunnen alleen geautoriseerde personen bepaalde gegevensgroepen combineren, anderen zien alleen de identificatiegegevens of alleen anonieme medische gegevens. De medische gegevens zijn wederom ondergebracht in verschillende domeinen om per zorgverlener specifieke toegang te verstrekken. Deze PET-toepassing staat bekend onder de naam Privacy Incorporated Database. Door de anonimisering is goede detailinformatie beschikbaar voor wetenschappelijk onderzoek;
- gedifferentieerde beveiliging van systeemtoegang door medewerkers. ICT-beheerders hebben geen toegang tot de medische gegevens van patiënten. Toegang door medewerkers van buiten de organisatie vindt plaats door sterke authenticatie met een mobiele telefoon en versleuteling van het gegevensverkeer;
- registratie van verstrekkingen van persoonsgegevens aan derden per betreffende patiënt in de database.

Baten

Het informatiesysteem beschikt door PET over verdergaande mogelijkheden tot afscherming van persoonsgegevens. Hiermee wordt niet alleen aan de Wbp voldaan, maar ook aan andere zorgspecifieke wetgeving met gedetailleerde privacyeisen (WGBO, BOPZ). De gebruikers merken de toevoeging van PET niet tenzij ze bepaalde persoonsgegevens ongeautoriseerd willen benaderen. Het systeem is door de PET-toepassing toepasbaar voor aansluiting op een eventueel ontwikkeld landelijk cliëntvolg-systeem; hiervoor zal dan een vertrouwde derde partij de authenticatie van de gebruikers moeten realiseren.

Daarentegen kan anonimiseren eenvoudiger worden toegepast op bestaande informatiesystemen. Anonimiseerders kunnen in een aantal gevallen als 'accessoire' worden toegevoegd aan het informatiesysteem. Dit is redelijk goed mogelijk bij front-end systemen, zoals de website van de organisatie. Het feit dat nu gewerkt wordt met anonieme gegevens heeft wel gevolgen voor het informatiesysteem en de uit te voeren processen. Waarschijnlijk zullen de processen wel aangepast moeten worden omdat men geen persoonsgegevens meer verwerkt. Daarnaast is het goed mogelijk naast een bestaand informatiesysteem een datawarehouse toe te voegen voor het verzorgen van selecties, rapportages en andere bewerkingen. Dit datawarehouse ontvangt dan op periodieke basis een selectie van gegevens uit de productiedatabase en bevat derhalve geanonimiseerde gegevens voor statistische doeleinden.

Naar verwachting zal het invoeren van een privacymanagementsysteem dat het volgen van privacyregels afdwingt, enige investering vergen, waarvan een belangrijk deel de aanschaf van het ondersteunende pakket betreft. Wel is het zo dat de nu beschikbare pakketten functionaliteiten bezitten om bestanden en processen te inventariseren en zichtbaar te maken, waardoor het implementeren van privacyregels zal worden vereenvoudigd. Praktische ervaring is er in Nederland nog niet, dus kan er ook nog weinig gezegd worden over de inspanning in de praktijk en de te verwachten kosten bij bestaande informatiesystemen.

Algemene PET-maatregelen kunnen veelal effectief en efficiënt worden geïmplementeerd na ingebruikname van een informatiesysteem. Dit betreft dan bijvoorbeeld het overstappen naar zwaardere authenticatiemiddelen, zoals het gebruiken van chipkaarten, biometrische technieken of certificaten voor het verkrijgen van toegang tot een systeem.

Het verder verfijnen van de autorisatiestructuur gebaseerd op rollen of het afschermen van de toegang tot bepaalde gegevens is in een later stadium bij een systeem aan te brengen aangezien deze aspecten overwegend de buitenkant van het systeem beïnvloeden. Maar de inspanning die daarvoor vereist is, is sterk afhankelijk van de wijze waarop die functionaliteit in het bestaande informatiesysteem is opgenomen.

Dynamische verantwoordelijkheden en autorisaties voor een bepaald dossier, zoals voorkomend in de zorg en bij politie en justitie, kunnen met enige moeite ook als element in een bestaand systeem worden geïmplementeerd.

PET-maatregelen die het systeem inwendig wijzigen zijn mogelijk als de maatregel redelijk geïsoleerd valt toe te passen. Hierbij valt te denken aan het versleutelen van gegevens in de database. Dit is technisch te realiseren zonder dat het de applicatie aantast. Het selectief versleutelen, zoals vermeld bij de NTIS-casus, vergt meer inspanning omdat hierbij in functionele zin wijzigingen moeten worden doorgevoerd.

Financieel directeur en rentmeester van Meerkanten, Ter Avest: 'De succesfactor van de PET-toepassing is dat je PET-technologie in de praktijk niet merkt als gebruiker, tot je bij persoonsgegevens wilt die niet bij je bevoegdheidsgebied horen. Daarmee voldoet PET precies aan onze doelstelling.'

In figuur 20 is per PET-vorm aangegeven of het mogelijk is de PET-vorm achteraf toe te voegen aan het informatiesysteem.

	Vooraf	Achteraf
Algemene PET maatregelen	Eenvoudig mogelijk	Sterk maatregel- en situatieafhankelijk
Privacymanagement-systeem	Mogelijk	Mogelijk
Anonimiseren	Mogelijk	Redelijk mogelijk
Scheiding van gegevens	Eenvoudig mogelijk	Lastig/kostbaar om te realiseren

Figuur 20: Toepasbaarheid van PET in bestaande systemen

7.3 De stappen

7.3.1 *Doelbinding en noodzaak*

De precieze uitwerking van de privacymaatregelen in de programmatuur en technische infrastructuur komt vooral naar voren in de fasen functioneel en technisch ontwerp23. Echter, in de praktijk blijkt dat daar een essentiële fase aan voorafgaat waarin de noodzaak en de diepgang van gegevensbescherming moet worden geanalyseerd.

Allereerst moet worden bepaald welke persoonsgegevens noodzakelijk zijn om de dienst te kunnen verlenen. Bij het vaststellen van de noodzaak tot het verwerken van persoonsgegevens moet u uitgaan van de gedachte 'hoe minder persoonsgegevens we verwerken, hoe beter'. Per slot van rekening kan geen misbruik worden gemaakt van gegevens die niet worden verzameld en is er minder inspanning nodig voor het beheer en de beveiliging van de persoonsgegevens. In diverse projecten is gebleken dat na een goede analyse een behoorlijk aantal persoonsgegevens niet (centraal) hoefde te worden verwerkt.

In deze fase moet u rekening houden met feit dat bij de gegevensverwerking meerdere organisaties en organisatieonderdelen betrokken kunnen zijn.

23 Ook wel: basis- en detailontwerp.

Ieder belanghebbend onderdeel zal inspraak willen hebben in de bepaling welke persoonsgegevens moeten worden verzameld.

Deze fase levert een overzicht op waarin uiteen is gezet welke persoonsgegevens om welke reden moeten worden verwerkt.

Prof. Boasson (Universiteit van Amsterdam): 'Bij deze analyse is soms wel een rechte rug nodig; er is nog steeds een weerstand om bepaalde gegevens niet te verzamelen of niet op te slaan met de gedachte dat je maar beter de gegevens beschikbaar kunt hebben voor het geval dat het eens handig kan blijken.'

7.3.2 *Gegevensanalyse en -classificatie: PET gewenst?*

Voordat een informatiesysteem daadwerkelijk wordt ontworpen, vindt eerst een globale verkenning (definitiestudie) plaats van de belangrijkste kenmerken van het te ontwikkelen informatiesysteem. De mate waarin bescherming van persoonsgegevens noodzakelijk is, is een dergelijk kenmerk.

Gebaseerd op de globale verkenning kan de organisatie een analyse uitvoeren om in kaart te brengen welke bedreigingen en risico's aanwezig zijn in het verwerkingsproces. Op grond van de resultaten van de risicoanalyse en een in de organisatie aanwezige gegevensclassificatie kan worden bepaald welke mate van bescherming van de te verwerken persoonsgegevens gewenst is. Als hulpmiddel kan hierbij de indeling van risicoklassen van het CBP worden gebruikt.

Casus 13: OV-chipkaart

In Nederland is besloten tot het toepassen van de OV-chipkaart als vervanger van de strippenkaart in het openbaar vervoer om een aantal redenen, te weten:

- *gebruikers:* verhogen gebruiksgemak en verhogen veiligheid (door ontbreken noodzaak van contant geld);
- *vervoersorganisaties:* verbeteren doelmatigheid, beschikbaar komen van betrouwbare en actuele managementinformatie, het verlagen van het percentage zwartrijders en het vergroten van de veiligheid van het personeel.

Dit elektronische betaalsysteem wordt opgezet en beheerd door Trans Link Systems en omvat de gehele financiële backoffice-afhandeling ten behoeve van haar aandeelhouders, de openbaar vervoerorganisaties.

23 College Bescherming Persoonsgegevens, Achtergrondstudies en Verkenningen 23: Beveiliging van persoonsgegevens, april 2001.

Tevens zullen – waar mogelijk – de trein-, bus- en metrostations worden uitgerust met toegangspoorten voor deze OV-chipkaart. De chipkaart is geschikt voor alle vormen van openbaar vervoer en kan in een later stadium worden uitgebreid met gerelateerde diensten. Voor de financiële afwikkeling van gebruik met gepersonaliseerde kaarten zijn gegevens (NAW) van de openbaar vervoer gebruikers noodzakelijk, dit kan door middel van automatische incasso of vooraf een reistegoed storten via de opwaardeerautomaat. In het andere geval, reizen met anonieme kaarten is alleen de mogelijkheid om een reistegoed te storten via de opwaardeerautomaat.

Het Nederlandse systeem is gebaseerd op dat van Hong Kong, waar inmiddels meer dan negen miljoen OV-chipkaarten zijn uitgegeven waarmee enkele miljoenen transacties per dag plaats-vinden. Hong Kong heeft een privacywetgeving die vergelijkbaar is met die van Nederland, aangezien beide zijn afgeleid van de Europese richtlijnen. Het systeem heeft zich hier succesvol in de praktijk bewezen. Hierbij heeft net als in Nederland een organisatie de verantwoordelijkheid voor het eenduidig formuleren van het privacy- en beveiligingsbeleid en voor het toezien op implementatie en naleving.

PET-toepassing

- indelen in lagen van het gehele informatiesysteem (chipkaart, toegangspoortjes, lokale verwerking, vervoersorganisatieverwerking en een centraal clearing house), waarbij er onderscheid is gemaakt tussen de persoonsgegevens die op de verschillende lagen mogen worden geregistreerd. Op veel lagen zijn louter chipkaart- en reisgegevens geregistreerd en geen verdere persoonsgegevens. Door gebruikmaking van een gegevensfilter worden slechts beperkte persoonsgegevens opgeslagen;
- versleutelen van de gevoelige persoonsgegevens, zoals reis- en financiële gegevens. Tevens wordt – waar mogelijk – gebruik gemaakt van een gesloten netwerk;
- gebruikmaken van anonieme chipkaarten die handmatig worden geladen met een geldwaarde als reistegoed;
- toepassen van fraude- en foutdetectiefuncties op alle hiervoor genoemde lagen. Bij opsporing dienen de (reis)transactiegegevens van een persoon van de verschillende vervoersorganisaties te worden gecombineerd;
- regelmatig uitvoeren van een privacyaudit om te kunnen aantonen dat in continuïteit aan alle privacyeisen uit de policy en het contract wordt voldaan. Op basis van de uitkomsten uit de privacyaudits zijn diverse verbeteringen aan beheersings- en beveiligingsmaatregelen doorgevoerd.

Baten

Dankzij de PET-toepassing kan geen enkele partij een volledig reisprofiel van een persoon opbouwen en biedt het systeem een basis voor vervolgstappen voor derde partijen om commerciële diensten aan te bieden met voldoende privacywaarborgen (zg. 'opt-in' regeling).

Overkoepelend resulteren de toegepaste PET-maatregelen in het vertrouwen bij openbaar vervoergebruikers, politiek, toezichthouders, media en andere belanghebbenden. Bij het ontbreken van vertrouwen bij een van deze groepen zou de slagingskans van een dergelijk complex project substantieel lager zijn. Daarnaast zijn in Hong Kong geen (gegronde) klachten geweest over de bescherming van de persoonsgegevens.

Nu is vastgesteld welke mate van gegevensbescherming gewenst is kan, mede op basis van de reeds getroffen privacymaatregelen, worden bepaald of de toepassing van PET gewenst is en hoe PET kan bijdragen aan de gegevensbescherming. Een balans moet worden gevonden tussen enerzijds de organisatorische en procedurele maatregelen en anderzijds de toepassing van PET. Hierbij kunt u de PET-trap uit paragraaf 4.6 hanteren om te bepalen welke PET-maatregelen nodig zijn gezien het risicoprofiel van gegevensverwerking en om te bepalen welk ambitieniveau op PET-gebied wenselijk is.

Hier kan een driedeling worden gemaakt in identiteitsrijke (identificerende persoonsgegevens vereist), identiteitsarme (identiteit eenmalig benodigd, maar één persoonskenmerk zoals leeftijd of beroep volstaat) en identiteitsloze processen (geen identiteit benodigd)[25]. Bij identiteitsrijke processen zijn met name de algemene PET-maatregelen en privacymanagementsystemen toepasbaar. Bij identiteitsarme processen zijn scheiding van gegevens in domeinen, algemene PET-maatregelen en privacy-management-systemen goed inzetbaar. Bij identiteitsloze processen zijn scheiding van gegevens en anonimiseren de aangewezen PET-vormen.

In deze fase moet tevens de uitwerking van de businesscase plaatsvinden (zie hoofdstuk 5). Daarnaast moet de doelstelling van het toepassen van PET duidelijk zijn vastgesteld en zijn gecommuniceerd in het project en in de gebruikers-organisatie.

7.3.3 *Basisontwerp*

In deze fase wordt het procesmodel gemaakt van de gegevensstromen binnen het informatiesysteem inclusief koppelingen/uitwisselingen met andere instanties. Ook het gegevensmodel moet voor iedere gegevensstroom in het verwerkingsproces van verzamelen, opslaan, bewaren tot aan vernietigen worden weergegeven. Belangrijke aspecten bij het opstellen van het proces- en het gegevensmodel voor de verwerking van persoonsgegevens zijn:

25 Zie verder Taskforce PKIoverheid, PET en de PKI voor de overheid, november 2002.

- herkomst van de persoonsgegevens (eventueel gebruik van authentieke registraties en koppelingen met andere gegevensbestanden);
- type persoonsgegevens (eventuele bijzondere gegevens);
- type verwerkingsprocessen (eventuele geautomatiseerde beslissingen);
- gebruikers(groepen) aan wie de gegevens worden verstrekt (eventuele ontvangers buiten de organisatie of zelfs buiten de EU);
- het vereiste niveau van zelfbeschikking door de burger en informatieplicht aan de burger;
- beheerder en verantwoordelijke van de gegevens (eventuele uitbesteding);
- bewaartermijnen (eventuele verplichte vernietiging);
- betrokkenen bij de gegevensverwerking (eventuele gemachtigden en bewindvoerders).

Het zal duidelijk zijn dat de te kiezen PET-vorm hierop grote invloed kan hebben. Zo zal het scheiden van domeinen, één van de PET-vormen, directe gevolgen hebben voor het gegevensmodel en voor koppelingen tussen de domeinen en eventuele andere informatiesystemen die gegevens onttrekken aan de gegevens van de onderhavige toepassing. Het anonimiseren zal zowel van invloed zijn op het gegevensmodel (minder gegevens vast te leggen) als op de processen. Ook het toepassen van allerlei afzonderlijke PET-maatregelen zal nu al moeten plaatsvinden om systeemwijzigingen in een later stadium te vermijden. En het toepassen van privacymanagementsystemen mag dan beperkte invloed hebben op het gegevensmodel of de functionele processen, op de technische opzet van het informatiesysteem zal de invloed groter zijn (zie volgende fase, detailontwerp).

7.3.4 *Detailontwerp*

In deze fase wordt het basisontwerp verder uitgewerkt en in meer technische zin gedetailleerd. Een belangrijk aspect hierbij is dat het technisch ontwerp van de PET-vorm geïntegreerd moet worden in het volledige technisch ontwerp van het informatiesysteem. De PET-vorm is immers geen los toe te voegen component en daarom kan het technisch ontwerp van PET niet los worden gezien van het technisch ontwerp van het gehele informatiesysteem. In bijlage B is een overzicht opgenomen van welke PET-technieken voor welke PET-vormen zijn in te zetten. Uiteraard kan ook een combinatie van PET-vormen en -technieken of kunnen losse PET-maatregelen als versleuteling of rolgebaseerde autorisaties worden gebruikt.

7.3.5 *Ontwikkeling*

Tijdens de ontwikkeling moet worden besloten of de gekozen PET-vorm en bijbehorende technieken door de organisatie zelf worden ontwikkeld of dat er een standaardpakket wordt gekocht. Voor anonimiseren en logging en controle zijn al redelijk wat standaardpakketten op de markt. Wanneer de vorm 'scheiding van gegevens' wordt toegepast en verschillende domeinen worden gecreëerd, is het waarschijnlijk dat er een behoorlijke component maatwerk ontwikkeld moet worden. Voor het toepassen van privacymanagementsystemen is standaardsoftware op de markt verkrijgbaar. Wel moet rekening worden gehouden met een inspanning om privacybeleid te vertalen in specifieke privacyregels, die op hun beurt weer in het gekozen privacymanagementsysteem moeten worden geprogrammeerd. Helaas zijn op dit moment nog geen kant-en-klare ontologieën beschikbaar (zie paragraaf 4.3). Behalve het overzicht van PET-vormen en -technieken is in bijlage B ook aangegeven welke technieken reeds beschikbaar zijn en welke technieken zelf ontwikkeld moeten worden.

7.3.6 *Testen*

Na ontwikkeling van het informatiesysteem moet uiteraard worden getest of het systeem functioneel voldoet en of de gebruikers het nieuwe systeem accepteren. In de tests moet ook de functionaliteit en de gebruikersvriendelijkheid van PET aan de orde komen. Gezien het stadium van volwassenheid van PET is het raadzaam om eerst een kleinschalige pilot te starten. Vervolgens kan op basis van de resultaten van de pilot het PET-proof informatiesysteem eventueel worden aangepast en verder worden uitgerold in de gehele organisatie. Het is ook raadzaam om bij het testen rekening te houden met de schaalbaarheid van het systeem. Uit een buitenlandse implementatie is gebleken dat het systeem niet helemaal correct functioneerde bij grootschalige implementatie, terwijl het systeem wel correct functioneerde bij kleinschaliger gebruik.

Zeker wanneer gekozen is voor de oplossing via een privacymanagementsysteem zal bij het testen gerichte aandacht nodig zijn voor de privacyregels die in dit systeem zijn ingebracht. Met het gebruik van de specifieke syntax (vaak lijkend op XML) is weinig ervaring opgedaan en deze syntax zal waarschijnlijk zijn opgesteld door de privacyfunctionaris, die daar ook nog weinig ervaring mee zal hebben.

7.3.7 *Implementatie*

In deze fase wordt het informatiesysteem inclusief de PET-vorm geïmplementeerd en gaat de organisatie gebruikmaken van het PET-proof systeem. Naast de reguliere implementatiewerkzaamheden is het van belang na te gaan welke activiteiten er moeten worden uitgevoerd om PET te laten werken. In het geval van scheiding van

gegevens moeten bijvoorbeeld authenticatiemiddelen worden uitgegeven, zodat gebruikers de identiteits-beschermer kunnen gebruiken. Het uitgeven en vooral het toekennen (autoriseren) van authenticatiemiddelen moet niet worden onderschat. Dit is de basis voor het juist werken van de PET-vorm. Uiteraard speelt de communicatie rondom het nieuwe systeem en de toepassing van PET een belangrijke rol tijdens de implementatie. Onderdeel van de communicatie is de opleiding van de gebruikers en beheerders met betrekking tot het gebruik van PET.

In de voorbereiding tot de implementatie is het van belang na te gaan of de gekozen PET-hulpmiddelen, bijvoorbeeld een chipkaart, in voldoende mate binnen de gestelde termijn kunnen worden uitgeleverd.

7.3.8 *Beheer en onderhoud*

Naast de beheertaken en onderhoudstaken die standaard aan de orde zijn bij een informatiesysteem en dus ook bij de PET-vorm is er ook PET-specifiek beheer en onderhoud. Indien bijvoorbeeld authenticatiemiddelen worden uitgegeven, zullen deze ook beheerd moeten worden. Mensen raken het middel kwijt, vergeten de eventuele bijbehorende pincode. Rondom het authenticatiemiddel en de autorisatie van mensen moet daarom een beheerproces worden ingericht.

7.3.9 *Evaluatie*

Het project moet worden geëvalueerd. Hiervoor kunnen een evaluatieplan en evaluatiecriteria worden opgesteld. Op basis van de evaluatie kan onder andere worden bepaald of de PET-maatregelen effectief zijn en kunnen de noodzakelijke aanpassingen aan het informatie-systeem en de PET-vorm worden verricht. Het (laten) uitvoeren van een privacyaudit biedt hierbij nuttige ondersteuning als daarbij ook de PET-mogelijkheden aan bod komen. Een organisatie kan ook besluiten haar informatiesysteem te laten certificeren op basis van de Wbp.

Casus 14: On-line medische ervaringen dossier (Digitale Ervaringen Dossier)

De Chronisch zieken en Gehandicaptenraad Nederland (CG-Raad) heeft samen met TNO en Diginotar een on-line medisch ervaringendossier ontwikkeld. Met dit zogenaamde Digitale Ervaringen Dossier (DED) kunnen alle leden van de 140 organisaties die bij de CG-Raad zijn aangesloten, hun medische gegevens bijhouden.

PET-toepassing

- onafhankelijk verstrekken van authenticatiemiddel door vertrouwde derde partij (Diginotar). Hierbij bestaat de keuze uit authenticatie met gebruikers-ID en wachtwoord, mobiele telefoon of met een bankpas, al naargelang de eisen die de internetapplicatie stelt. Voor toegang tot het on-line medisch ervaringen dossier is ten minste een bezitskenmerk nodig (mobiele telefoon of bankpas);
- gebruikmaken van pseudo-identiteiten voor anonieme toegang tot digitale ervaringen dossier. Deze pseudo-identiteiten worden beheerd door dezelfde vertrouwde derde partij. De CG-Raad en TNO kunnen geen koppeling maken tussen de echte identiteit en de pseudo-identiteit. Voor veel serviceapplicaties, zoals zorg- en preventiesites van verzekeraars, zijn geen identiteitsgegevens nodig;
- certificeren van de betrouwbaarheid van de derde partij en van de internetapplicaties die medische gegevens verwerken. Certificatie verloopt via het QMIC®-systeem
- aangeven door gebruikers welke medisch gerelateerde ervaringen ze aan derden beschikbaar willen stellen en aan welke onderzoeksenquêtes ze willen deelnemen.

Baten

Chronisch zieken en gehandicapten kunnen hiermee op een veilige en flexibele wijze hun eigen medische ervaringen dossier bijhouden. Daarnaast zijn ze verzekerd van een betrouwbaar beheer van hun medische ervaringen dossier door TNO en hun persoonsgegevens door DigiNotar. Daarnaast wordt het persoonlijke medische ervaringen dossier uitsluitend gekoppeld aan QMIC® gecertificeerde informatiediensten.

Uiteraard zijn de gebruikerservaringen ook relevant en dienen deze te worden meegenomen in de evaluatie. Daarnaast is het van belang om vanuit de evaluatie leereffecten voor het ontwikkeltraject te identificeren, bijvoorbeeld op het gebied van efficiëntie, projectaanpak en de integratie van PET daarin. Deze leereffecten zijn nuttig voor de organisatie zelf, maar kunnen ook andere overheidsonderdelen ondersteunen die PET willen implementeren. Tijdens de evaluatie kunnen eveneens de gerealiseerde kosten en baten (de toegevoegde waarde van PET) worden vergeleken met de opgestelde begroting en businesscase.

7.3.10 *Deelproducten*

In figuur 21 is in een overzicht aangegeven welke deelproducten met PET-specifieke onderdelen in welke fase moeten worden opgesteld.

Projectfase	Deelproducten met PET-specifieke onderdelen
Doelbinding en noodzaak	■ Overzicht van welke gegevens waarom worden verwerkt.
Gegevensanalyse en -classificatie	■ Gegevensclassificatie; ■ Risicoanalyse inzake gegevens-bescherming; ■ Definitiestudie-rapport, inclusief de businesscase voor PET.
Basisontwerp	■ Basisontwerp, waarin PET is geïntegreerd; ■ Gegevens- en procesmodel.
Detailontwerp	■ Detailontwerp.
Ontwikkeling	■ Beslisdocument inzake aanschaf voorkeursoplossing (welk pakket wordt gekocht) of maatwerkontwikkeling.
Testen	■ Testplan voor specifieke PET-aspecten. Plan moet wel geïntegreerd worden in reguliere testplan.
Implementatie	■ Communicatie- en trainingsplan; ■ Uitrolplan eventuele authenticatie-middelen.
Beheer en onderhoud	■ Handleiding voor beheer en onderhoud specifieke PET-onderdelen. Handleiding en werkzaamheden integreren in reguliere handleiding en werkzaamheden.
Evaluatie	■ Evaluatie- en/of auditrapport.

Figuur 21: Op te leveren PET-specifieke deelproducten per fase

8 Acties

U bent voornemens de mogelijkheden voor PET-toepassing voor de informatiesystemen onder uw verantwoordelijkheid serieus te evalueren. Welke acties kunt u nu op korte termijn nemen om PET in uw organisatie succesvol toe te passen? In onderstaand overzicht is een korte opsomming gegeven van de succesfactoren en tips die de geïnterviewden hebben aangereikt vanuit hun eigen ervaring.

- Identificeer de belangrijkste lopende of nog te starten projecten van systemen met verwerking van persoonsgegevens.
- Organiseer een bewustwordingssessie over PET voor de verantwoordelijke proceseigenaren, beleidsmedewerkers, programma- en projectleiders en privacy- en beveiligingsambtenaren, en verhelp zo snel mogelijk eventueel ontstane misverstanden rondom gegevensbescherming en benodigde PET-maatregelen. Vul dit aan met bewustwordingsmateriaal voor alle betrokken groepen, bestaande uit dit Witboek PET, een flyer en informatie over best practices.
- Zorg dat het 'PET-denken' in de organisatie is verankerd zodat PET een serieuze optie is bij alle (nieuwe) informatiesystemen waarin persoonsgegevens worden verwerkt.
- Redeneer bij de gegevensbescherming en toepassing van PET vanuit de organisatiestrategie en het besturingsmodel.
- Vind een goede balans tussen de anonimiteit van de betrokkene enerzijds en het kennen van de klant, het tegengaan van fraude en het mogelijk maken van opsporing anderzijds. In sommige gevallen is er geen behoefte aan de identiteit van iemand, maar wel aan het gegeven dat het slechts één uniek persoon is, andere keren is er wel een noodzaak om de klant te kennen. Hiervoor is gebruikmaking van een nummer als bescherming tegen naamgebruik een optie. Om de balans te bepalen kunnen de processen worden ingedeeld in identiteitsrijke, identiteitsarme en identiteitsloze processen.
- Bepaal vooraf duidelijk en goed onderbouwd de minimale gegevensset en in welke gevallen eventueel aanvullende gegevens nodig zijn.
- Maak goed onderscheid tussen eisen en wensen met betrekking tot de gegevensbescherming en de daarmee samenhangende PET-maatregelen.
- Verbeter parallel de kwaliteit van de persoonsgegevens (de 11-proef van sofi-nummers is daar een voorbeeld van). Betrouwbare gegevens zijn een solide basis voor de acceptatie van authentieke registraties en gegevensbeschermende maatregelen en het tegengaan van dubbele administraties.
- Om een optimale effectiviteit van de PET-maatregelen te realiseren is het van belang om stapsgewijs de autorisatiestructuur van de organisatie te verfijnen. Hierbij kan worden gedacht aan het definiëren van functies en rollen en het invoeren van rolgebaseerde toegangsbeveiliging.

- Gebruik uitkomsten van uitgevoerde privacyaudits en het patroon van eventuele privacyklachten om de noodzaak voor PET te onderbouwen. Laat ook periodiek een privacyaudit of evaluatie uitvoeren om de PET-maatregelen verder te verbeteren.
- Bespreek de noodzaak en wenselijkheid van mogelijke PET-toepassing met ketenpartners in geval van interorganisatorische koppelingen en gegevens-uitwisseling. Maak tevens duidelijke afspraken met alle betrokken partijen om de effectiviteit van de PET-toepassing te versterken.
- Handhaaf de flexibiliteit van andere betrokken organisaties waarmee gegevensuitwisseling plaatsvindt. Kies voor een minimaal centraal model om decentrale autonomie en verantwoordelijkheden te kunnen handhaven. Er mag slechts beperkte of geen centrale invloed op de wijze van gegevensuitwisseling ontstaan of sprake zijn van centraal inzicht in de inhoud van berichten.
- Selecteer een geschikt informatiesysteem voor een pilot met PET-toepassing en kies een stapsgewijze aanpak die niet te grootschalig of 'te streng in de privacyleer' in één keer is.
- Tracht met name het transparantiebeginsel vanaf het begin in het ontwerpen van de PET-toepassing mee te nemen.
- Positioneer PET-oplossingen als een infrastructurele voorziening die ten goede komt aan meerdere projecten en niet (alleen) ten laste van het budget van het betreffende pilotproject. Neem na het pilotproject de wijze van PET-toepassing op in de systeem-ontwikkelmethode en neem PET-componenten op in de informatiearchitectuur.
- Zorg dat de gebruikers weinig last en met name voordeel hebben van de PET-toepassing.
- Oriënteer u op mogelijke financiële ondersteuning vanuit stimuleringsregelingen.

Ten slotte:

Samengevat

PET is meer dan een manier om persoonsgegevens te beschermen:

- **PET willen!**
  - PET bevordert de informatiekwaliteit.
  - De afhankelijkheid van de goede naleving van processen en procedures vermindert door het automatisch afdwingen van privacyregels.
  - Het toepassen van PET kan een middel zijn om burgers betere inzage- en controle-mogelijkheden over hun persoonsgegevens te geven.

- **PET moet!**
  - Met PET kan eenvoudiger worden voldaan aan de Wet bescherming persoonsgegevens.
  - PET is voorwaardenscheppend voor het vertrouwen van de burger.
  - PET maakt werken met gevoelige persoonsgegevens mogelijk.

- **PET kan!**
  - PET is al vele malen succesvol geïmplementeerd.
  - PET heeft slechts een beperkte invloed op de ontwikkelkosten van een nieuw informatie-systeem aangezien de technieken voorhanden zijn en het voornamelijk het toepassen ervan betreft. Het 'kost' met name denk- en ontwerpwerk.
  - Het opnemen van PET in uw informatiearchitectuur biedt een basis om PET in verschillende informatiesystemen efficiënt toe te passen.

Figuur 22: Redenen voor PET

A Literatuur

De termen die bij een aantal literatuurverwijzingen tussen vierkante haken zijn opgenomen, hebben betrekking op de in bijlage B genoemde PET-technieken.

A.1 Privacy algemeen

- Berenschot, *Werkbare vormen van digitale regie over eigen (persoons)gegevens door de burger, april 2003. [Persoonlijk gegevenskluisje]*
- College Bescherming Persoonsgegevens / Samenwerkingsverband audit aanpak, *Raamwerk Privacy Audit*, december 2000.
- College Bescherming Persoonsgegevens, *Achtergrondstudies en Verkenningen 23: Beveiliging van persoonsgegevens*, april 2001.
- College Bescherming Persoonsgegevens, *Achtergrondstudies en Verkenningen 25: Elektronische overheid en privacy*, juli 2002.
- College Bescherming Persoonsgegevens, *Achtergrondstudies en Verkenningen 26: Privacy bij ICT in de zorg*, november 2002.
- KPMG, Themanummer Privacy, *Compact 2001/3*, augustus 2001.
- Programma Stroomlijning Basisgegevens, *Advies van de Tafel: Persoonsnummerbeleid in het kader van identiteitsmanagement*, juni 2002.
- Programma Stroomlijning Basisgegevens, *Kroniek Stroomopwaarts*, mei 2003.
- Staat der Nederlanden, *Wet bescherming persoonsgegevens*, juli 2000, www.wetten.nl.

A.2 PET algemeen

- Borking, J.J., PET: Het derde spoor. Een terugblik, *Privacy & Informatie*, nummer 5, oktober 2002. *[PISA, Privacy Rights Management]*
- Borking, J.J., Raab, C., Laws, PETS and other technologies for privacy protection, *Journal of Information, Law and Technology*, nummer 1, februari 2001.
- Bos, H. en St. Rekenschap, *Privacy begint in je genen*, 2001.
- College Bescherming Persoonsgegevens, *Achtergrondstudies en Verkenningen 11: Privacy Enhancing Technologies: the path to anonimity*, september 1998. *[Blinde elektronische handtekening, Privacy Incorporated Database, Biometrie]*
- College Bescherming Persoonsgegevens, *PET: presentatie voor de Beveiligingscommissie*, januari 2000.
- College Bescherming Persoonsgegevens, *Symposium voor John Borking: Privacy by design*, mei 2002.

- College Bescherming Persoonsgegevens, *Mag het een bitje minder zijn?*, januari 2002. *[Privacy Incorporated Database, automatische gegevensvernietiging]*
- Gardeniers, H.J.M. Privacy Enhancing Mediaries. Nieuwe mogelijkheden voor privacybescherming. *Privacy & Informatie*, nr. 1, februari 2001.
- Horst, J., van der, To PET or not to PET, *Privacy & Informatie*, nummer 4, augustus 2003.
- Kinkhorst, O.M., Privacybescherming als vertrekpunt voor hygiënische ICT-toepassing, *Informatiebeveiliging*, nummer 5, 2002.
- Lieshout, M.J. van, PET: een zaak van de lange adem, *Privacy & Informatie*, nummer 5, oktober 2002.
- Mienes, P., Bokhorst, B., De (on)beheersbaarheid van logische toegangsbeveiliging, *Compact*, nummer 1, 2003. *[Logische toegangsbeveiliging]*
- Morssink, P.J., De implementatie van PET in informatiesystemen, *Privacy & Informatie*, nummer 5, oktober 2002.
- Prins, C., Consument en het recht op anonimiteit: een oud fenomeen in een nieuw jasje.
- PrivacyPunt, *Privacy beschermende ICT: PET uitgelegd*, KWINT, 2003.
- RAND Europe, *Werkbare vormen van PET*, juli 2003.
- Rooij J., de, Privacymanagement en Enterprise Privacy Manager, *Privacy & Informatie*, nummer 5, oktober 2003.
- Taskforce PKIoverheid, *PET en de PKI voor de overheid*, november 2002. *[Blinde elektronische handtekening]*

A.3 Casussen

- Blarkom, G.W. van, Meer kanten aan PET: PET in de praktijk bij Meerkanten, *Privacy & Informatie*, nummer 5, oktober 2002. *[Versleuteling, Biometrie]*
- Campbell, A., *Privacy architecture*, Government of Alberta, november 2003. *[Privacy Incorporated Database, EPAL, Privacy policy management, Cryptografie gebaseerde ID's]*
- IBM Global Services, Privacy architecture overview of the government of Alberta, mei 2003. *[Privacy Incorporated Database, EPAL, Privacy policy management]*
- Maes, P., *Case: De Kruispuntbank van de Sociale Zekerheid*, presentatie hand-outs congres Overheid & Internet, april 2003. *[Chipkaart]*
- Wijskamp, B., Hart, J. ter en Koorn, R.F., *Casusbeschrijving Nationaal Trauma Informatie Systeem: Toepassing van Privacy Enhancing Technologies bij traumacentra*, Universitair Medisch Centrum Utrecht en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ISBN 90-5414-086-0. Juli 2004. *[PKI, Chipkaart, Biometrie, Logische toegangsbeveiliging, Versleuteling]*

A.4 PET diepgaand

- Borking, J.J., *The status of privacy enhancing technologies, Certification and security in E-services: From e-government to e-business,* ISBN 1-4020-7493-X, Kluwer Acadamic Publishers group, 2003. *[P3P, PISA]*
- Borking, J.J., Kenny, S., The value of privacy engineering, *Journal of Information, Law and Technology,* nummer 1, maart 2003.
- Borking, J.J., Privacy rules for intelligent software agents, *Tilt,* nummer 15, 2003. *[PISA]*
- College Bescherming Persoonsgegevens, *Achtergrondstudies en Verkenningen 13: Intelligent software agents and privacy,* januari 1999.
- Escudero-Pascual, A., To be or not to be in the next generation Internet, *Tilt,* nummer 15, 2003. *[Cryptografie gebaseerde ID's]*
- Karjoth, G., Schunter, M., Waidner, M., Privacy-enabled services for enterprises, *Tilt,* nummer 15, 2003. *[EPAL]*
- Kenny, S., Korba, L., Applying digital rights management systems to privacy rights management, *Computers & Security,* nummer 7, 2002. *[Privacy rights management]*
- PISA consortium, Handbook of Privacy and Privacy-Enhancing Technologies: the case of Inteligent Software Agents, 2003. *[PISA]*
- Reimerink, E., Softwarecomponenten bewaken de kwaliteit van het relatiebestand: Quality Enhancing Technology, *de EDP-auditor,* nummer 2, 2001. *[Quality Enhancing Technologies]*
- TNO, *Privacy Enhancing Technologies en overheidsinformatiesystemen,* februari 2002. *[MIX-routers, Onion-routers, Browser test, Cookie management, File management, Profile management, Biometrie, Chipkaarten, Versleuteling, P3P]*

A.5 Websites

- www.cbpweb.nl
- www.pet-pisa.nl
- www.pkioverheid.nl
- www.privacypunt.nl
- www.agekey.nl
- www.w3.org/P3P
- www.cdt.org/privacy/pet/p3pprivacy.shtml

B PET-technieken

In deze bijlage is een overzicht opgenomen van mogelijke technieken die ingezet kunnen worden om de in dit Witboek behandelde PET-vormen te kunnen realiseren. Hierbij is onderscheid gemaakt naar standaardoplossingen, zelf te realiseren oplossingen en toekomstige oplossingen. Verdere uitleg en informatie over de in de tabel genoemde technieken kan worden gevonden in de in bijlage A genoemde literatuur. In bijlage A is bij een aantal artikelen aangegeven welke technieken in het betreffende document/website worden besproken.

	Standaard	Maatwerk	Toekomst
Algemeen	■ Versleuteling (opslag & communicatie) ■ Logische toegangs-beveiliging (authenticatie en autorisaties)	■ Biometrie ■ Quality Enhancing Technologies	■ Cryptografie-gebaseerde ID's ■ Nationale Authenticatie-voorziening (NAV) ■ Overheids Toegangs-voorziening (OTV)
Scheiding van gegevens	■ Profile management	■ Privacy incorporated database ■ Blinde elektronische handtekening	■ Persoonlijk gegevenskluisje
Anonimiseren	■ MIX-routers ■ Onion-routers ■ Cookie management tools ■ File management tools	■ Chipkaarten ■ Biometrie	
Privacymanagement-systemen	■ P3P (Platform for Privacy Preference Project)	■ Privacy Rights Management (gebaseerd op Digital Rights Management) ■ Automatische gegevensvernietiging (retentiemanagement)	■ PISA (Privacy-Incorporated Software Agent) ■ Privacy-ontologieën ■ EPAL (Enterprise Privacy Authorisation Language) ■ Privacy policymanagement software

Figuur 23: PET-technieken

C Woordenlijst

Authenticatiemiddel

Het authenticatiemiddel wordt gebruikt om vast te stellen of een persoon daadwerkelijk is wie hij beweert te zijn. Dit kan bijvoorbeeld een digitaal certificaat zijn, maar ook een gebruikersnaam in combinatie met een wachtwoord is een vorm van authenticatie.

Burger Service Nummer

Het Burger Service Nummer (BSN) is een algemeen door de centrale overheid aan de burger toe te kennen gebruikersnummer. Met de invoering van het BSN hoeven burgers in alle contacten met de overheid nog maar één nummer te gebruiken. Overheden kunnen op hun beurt met het BSN hun taken beter uitvoeren doordat de gegevensuitwisseling sneller, efficiënter en betrouwbaarder kan plaatsvinden. Het gebruik van persoonsnummers dient drie doelen: de dienstverlening aan klanten verbeteren, de identiteitsfraude bestrijden en de transparantie van de overheid vergroten met als doel de privacy te verbeteren.

Bijzondere gegevens

Op grond van artikel 16 Wwp is de verwerking verboden van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Dit verbod kan slechts worden opgeheven indien aan bepaalde stringente voorwaarden (zie artikel 23 Wbp) wordt voldaan

Digitale handtekening

Een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. (Bron: Wet elektronische handtekeningen.) Een elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat heeft dezelfde juridische waarde als een geschreven handtekening.

EPAL

Enterprise Privacy Authorisation Language (door IBM en Zeroknowledge ontwikkeld) is een taal om de relaties tussen objecten weer te geven (zie privacyontologie) voor gebruik in privacymanagementsystemen teneinde automatisch de verwerking van persoonsgegevens binnen de wettelijke kaders te verwezenlijken.

GBA

De Wet Gemeentelijke Basisadministratie persoonsgegevens geeft onder meer aan wanneer en onder welke omstandigheden gegevens uit de basisadministratie mogen worden verstrekt, bijvoorbeeld voor wetenschappelijk onderzoek, voorzover de persoonlijke levenssfeer daardoor niet onevenredig wordt geschaad en door de ontvanger van de persoonsgegevens de nodige voorzieningen zijn getroffen teneinde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

Identiteitsbeschermer

Systeemelement in een informatiesysteem, dat de identiteit van de gebruiker, burger, consument afschermt en de uitwisseling van de identiteit tussen de verschillende andere elementen van het informatiesysteem regelt. De identiteitsbeschermer, ook wel Identity Protector genoemd, converteert de identiteit van betrokkene in één of meer pseudo-identiteiten. Door het plaatsen van een identiteitsbeschermer ontstaan er minimaal twee soorten domeinen, namelijk domeinen, waar de identiteit bekend of toegankelijk is en domeinen waar dat niet het geval is (zie ook PID).

P3P

Het Privacy Preferences Protocol is een middel (tool) om op gemakkelijke wijze over de eigen privacyvoorkeuren van de gebruiker van internet te kunnen communiceren in een gestandaardiseerde, voor het informatiesysteem leesbare vorm.

Persoonsgegeven

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

PET

Een verzameling van informatie- en communicatietechnologieën die de bescherming van de persoonlijke levenssfeer van individuen binnen een informatiesysteem versterken door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens of door het bieden van middelen en maatregelen tot het vergroten van de controle van de betrokkene over zijn of haar persoonsgegevens. (Bron: TNO.)

PID

In een Privacy Incorporated Database zijn de gegevens gescheiden in een identiteitsdomein en een pseudo-identiteitsdomein. De koppeling tussen de verschillende domeinen wordt gelegd door de zogenaamde identiteitsbeschermer. Wanneer een persoon geen toegang heeft tot de identiteitsbeschermer kan hij de gegevens in de verschillende domeinen niet met elkaar in verband brengen (zie ook identiteitsbeschermer).

PISA

Het Privacy Incorporated Software Agent-project is een door de EU gesubsidieerd researchproject waarin softwareagenten ('digitale butlers') worden gebouwd die de privacy beschermen van de gebruikers van 'personal digital assistants' op het internet. Zie: www.pet-pisa.nl.

PKI

Public Key Infrastructure is de infrastructuur die nodig is om met gebruikmaking van openbare-sleutelcryptografie de betrouwbare koppeling te bewerkstelligen tussen de identiteit en andere attributen van de houder ervan. In een PKI wordt gebruikgemaakt van digitale certificaten, die door een Certification Service Provider (CSP) zijn uitgegeven.

Privacy

Internationaal erkend grondrecht: Eerbiediging en bescherming van de persoonlijke levenssfeer, onder andere door het rechtmatig verwerken van persoonsgegevens. Geregeld in de Grondwet artikel 1:10, in de Wet bescherming persoonsgegevens en in vele andere wetten.

Privacyontologie

Een ontologie is een formele voor een informatiesysteem begrijpelijke machinetaal die bepaalde kenniselementen en de relaties daartussen binnen een specifiek kennisgebied beschrijft. Een privacyontologie beschrijft de kennis over het kennisdomein gegevensbescherming op een niet-dubbelzinnige gestandaardi-seerde wijze met het doel uiteindelijk de privacywetgeving in een taal om te zetten die begrijpelijk is voor een informatiesysteem, zodat automatisch door dat -systeem de privacywetgeving op het verwerken van persoonsgegevens wordt toegepast en aldus onrechtmatige verwerking wordt voorkomen.

PRM

Privacy Rights Management is bescherming van persoonsgegevens door middel van een op een digitale technologie gebaseerde methode om auteursrechten vastgelegd op gegevensdragers te beschermen. De bedoeling is persoonsgegevens te voorzien van een onlosmakelijk digitaal label waarop de privacyvoorkeuren zijn vermeld.

QET

Quality Enhancing Technologies is een verzamelnaam voor technologieën, die de kwaliteit van de gegevensverwerking en de gegevens zelf verhogen.

Chipkaart

Een digitale gegevensdrager waarop een microprocessor met de capaciteit van een kleine computer is vastgelegd om voor vele doeleinden gebruikt te kunnen worden, onder andere betaalpas, identificatie en authenticatie (zie authenticatiemiddel), toegangsbeveiliging, verwijsindex voor medische gegevens, klantkaart, etc. Ook wel smartcard genoemd.

TTP

Een Trusted Third Party is een betrouwbare derde partij. Een TTP levert betrouwbaarheidsdiensten, zoals betrouwbare hosting-services of het uitgeven van digitale certificaten. (Tegenwoordig wordt de partij die digitale certificaten uitgeeft, aangeduid met de term CSP.)

VIR

In het Voorschrift Informatiebeveiliging Rijksdienst 1994 heeft de minister van Algemene Zaken een aantal basisregels voor de informatiebeveiliging vastgesteld. Het VIR is een doelstellende regeling, die veel overlaat aan de verantwoordelijke beheerders zelf. De regeling stelt minimumeisen aan het te ontwikkelen beveiligingsbeleid binnen een ministerie. Daarnaast stelt de regering eisen aan het stelsel van maatregelen dat dit beleid in de praktijk moet brengen. Daarvoor moet de beheerder twee 'instrumenten' opstellen: afhankelijkheids- en kwetsbaarheidsanalyses en informatiebeveiligingsplannen. (Bron: www.overheid.nl.)

Wbp

De Wet bescherming persoonsgegevens is sinds 1 september 2001 van kracht en na een overgangsjaar zijn sinds 1 september 2002 organisaties verplicht om de Wbp in zijn geheel na te leven. De Wbp is de implementatie van de Europese Richtlijn 95/46 en de vervanger van de Wet persoonsregistraties.

W3C

Het World Wide Web Consortium is een consortium dat zich bezighoudt met de ontwikkeling van interoperabele technieken (standaarden, software en hulpmiddelen) voor het internet. Het W3C heeft onder andere P3P (zie P3P) ontwikkeld en verbeterd. Het JRC (Joint Research Center van de EU in Ispra (Italië)) heeft een versie van P3P ontwikkeld die conform de EU Richtlijn voor de bescherming van persoonsgegevens (95/46/EC) is.

D Opgenomen casussen met PET-toepassing