Privacy: van organisatorisch beleid naar Privacy Enhancing Technologies

Drs. ing. R.F. Koorn CISA RE en drs. J. ter Hart

De privacybescherming is nog veelal een kwestie van juridische en organisatorische procedures. De Wet bescherming persoonsgegevens besteedt ook aandacht aan het toepassen van ICT-maatregelen om de betrouwbaarheid en efficiëntie van naleving van privacyvereisten te verbeteren. Dit artikel behandelt een aantal relevante ontwikkelingen op het gebied van privacy in het algemeen en de zogeheten Privacy Enhancing Technologies in het bijzonder, waarbij ook concrete voorbeelden worden behandeld.

Inleiding

Na een korte inleiding over de privacywetgeving wordt een aantal privacyontwikkelingen besproken. Hierbij wordt ingegaan op de organisatorische positionering, het privacybewustzijn en maatschappelijke en ICT-ontwikkelingen die de privacybeleving en -naleving beïnvloeden. Tevens wordt kort stilgestaan bij de overeenkomsten en verschillen van privacy en beveiliging. Vervolgens wordt ingegaan op de wijze waarop organisaties sinds de introductie van wetgeving op dit terrein privacy hebben aangepakt. Hierbij is een ontwikkeling naar het geleidelijk meer toepassen van technische maatregelen zichtbaar, uiteindelijk leidend tot vormen van Privacy Enhancing Technologies. Na behandeling van twee casussen wordt afgesloten met het belichten van de belangrijkste financiële en implementatieaspecten van deze technieken.

Drs. ing. R.F. Koorn CISA RE
is partner bij KPMG Information Risk Management te Utrecht. Hij heeft ruime ervaring op het terrein van privacy, informatiebeveiliging, elektronisch factureren, Identity Management, elektronische handtekeningen en de flexibiliteit van ICT-toepassingen. Hij heeft voor het Ministerie van BZK het *Witboek Privacy Enhancing Technologies* geschreven en heeft op privacygebied CBP, TRUSTe en AICPA ondersteund. Hij is twee jaar in San Francisco en Silicon Valley voor KPMG werkzaam geweest.

koorn.ronald@kpmg.nl

Drs. J. ter Hart
is consultant bij KPMG Information Risk Management te Amstelveen. Hij is gespecialiseerd in identiteitsmanagement, elektronische handtekeningen, mobiele beveiliging, elektronisch factureren en privacy. Hij heeft diverse advies- en auditopdrachten op deze gebieden uitgevoerd. Daarnaast is hij co-auteur van het *Witboek Privacy Enhancing Technologies*, dat in opdracht van het Ministerie van BZK is opgesteld.

terhart.joris@kpmg.nl

Ontwikkeling privacywetgeving

Privacybescherming en schendingen van privacy zijn van alle tijden. Zelfs in de middeleeuwen is op deelgebieden van privacy al wetgeving van kracht geworden, maar pas na de tweede wereldoorlog is de privacybescherming in een stroomversnelling gekomen. In de Universele Declaratie van de Rechten van de Mens uit 1948 is aangegeven dat territoriale en communicatieprivacy als primair recht gelden.

De introductie van informatie- en communicatietechnologie (ICT) in publieke en private organisaties en de privacyconsequenties van het gebruik en misbruik hiervan gaven een belangrijke impuls aan privacywetgeving. Na een eerste privacywet in de Duitse deelstaat Hessen (1970) volgde nationale wetgeving in Zweden (1973), de Verenigde Staten (1974), Duitsland (1977) en Frank-

rijk (1978). Dit legde de basis voor de Raad van Europa's *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (1980) en OECD's[1] *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*[2] (beide in 1981).

1) OECD: Organisation for Economic Cooperation and Development.
2) Bekend als de Fair Information Practices.

De Raad van Europa-conventie is geadopteerd door meer dan twintig landen; de OECD-richtlijnen zijn eveneens verwerkt in diverse nationale wetten. Nederland was één van die landen en introduceerde in 1988 de Wet persoonsregistraties (Wpr). Zoals bekend heeft de Europese Unie vanaf begin jaren negentig privacy prioriteit gegeven, wat in 1995 is uitgemond in de Data Protection Directive[3]. Deze privacyrichtlijn is in Nederland per 1 september 2001 als de Wet bescherming persoonsgegevens (Wbp) in werking getreden, enigszins later dan de deadline van oktober 1998. In [Koor01] en [EPIC03] is verdere achtergrond te vinden over de ontwikkeling van privacywetgeving. In het vervolg van dit artikel wordt uitsluitend ingegaan op informatie- en communicatieprivacy; lichamelijke en territoriale privacy blijven buiten beschouwing.

3) European Directive EC95/46, ook bekend als Europese privacyrichtlijn.

Verantwoordelijkheid en bewustzijn voor privacy

Wie binnen organisaties verantwoordelijk is voor privacy, verschilt aanzienlijk. Veelal betreft het een jurist op de afdeling Juridische Zaken, maar in andere gevallen is het de beveiligingsfunctionaris of zelfs de IT-auditor die privacy 'erbij doet'. Waar het voorheen een parttime functie was, is de laatste paar jaar een professionalisering gaande onder leiding van fulltime privacyverantwoordelijken. Ook de in de Wbp nieuw geïntroduceerde rol van Functionaris Gegevensverwerking (FG)[4] heeft hiertoe bijgedragen, ook al vergde die nieuwe functie in de startfase enig aanpassingsvermogen van de privacybetrokkenen vanwege de gewijzigde situatie qua privacygovernance. Privacy ressorteert nu veelal onder de juridische, compliance- of risicomanagementafdeling.

4) Voor een uitgebreide behandeling van de Functionaris Gegevensverwerking zie www.cbpweb.nl.

Minder dan 5% van de organisaties opereert geheel Wbp-proof.

Waar privacy organisatorisch goed is verankerd, heeft zij een sterke impact op de omgang met privacyvraagstukken. Dit varieert van een sterke juridische benadering met stringente reglementen en procedures tot aan een gebalanceerde benadering met aandacht voor organisatorische en ICT-facetten. Waar de privacyverantwoordelijke zich ook bevindt, de communicatie tussen juristen, eigenaren van processen/systemen/gegevens, projectleiders, ICT'ers en gebruikers blijft een grote hindernis voor de goede inrichting van de privacybescherming. Gebaseerd op onze praktijkervaring durven wij te stellen dat minder dan vijf procent van de organisaties geheel Wbp-proof opereert.

Bewustzijn

Het privacybewustzijn correleert wel enigermate met de wetgevingsgolven, maar niet geheel. Hoewel het onderzoek naar het bewustzijn van privacyregels en de naleving hiervan beperkt is, is uit enquêtes wel zichtbaar geworden dat het bewustzijn ook onderhevig is aan golfbewegingen. Rond de introductie van de Wpr was er niet alleen bij de overheid, maar ook in het bedrijfsleven aandacht voor privacy. Onder druk van deze wet hebben de meeste grote organisaties privacybeleid en -reglementen opgesteld en deze vervolgens – veelal ten dele – geïmplementeerd. Andere belangrijke impulsen die niet direct samenhingen met nieuwe wetgeving, maar eerder door ICT- en externe ontwikkelingen werden veroorzaakt, betroffen:

- *Toepassing van internet voor gegevensuitwisseling en transacties*. Door de on-line vergaarde persoonsgegevens en creditcardgegevens ontstond er bij gebruikers terughoudendheid vanwege onduidelijkheid over de privacybescherming en beveiliging van deze websites. Als reactie hierop werden onder andere privacy- en beveiligingsstatements op websites geplaatst en werd er via zelfreguleringsprogramma's vertrouwen gegeven aan derden (Thuiswinkel, WebTrust, TRUSTe, e.d.).
- *Outsourcing en off-shoring*. Deze activiteiten omvatten de overdracht van bedrijfsprocessen en ICT-systemen naar derde partijen, al dan niet zich bevindend in het buitenland en veelal buiten de Europese Unie (bijvoorbeeld Aziatische landen). Deze trend heeft het privacybewustzijn vergroot. In de praktijk blijkt zelfs dat er kritischer naar de privacybescherming bij deze service providers wordt gekeken dan naar die in de eigen organisatie. Dit heeft geleid tot verschillende bewerkersovereenkomsten en privacyclausules in contracten en service level agreements (SLA's).
- *Centrale informatiesystemen en shared service centers met HR- en klantgegevens*. Deze ontwikkeling deed en doet zich voornamelijk voor bij multinationals en de overheid en is te beschouwen als de organisatie-interne variant van het voorgaande punt. Het wereldwijd uitwisselen van persoonsgegevens, waaronder gevoelige gegevens, leidde bij veel organisaties tot aandacht voor privacyaspecten. Vooral in situaties waarin het centrale HR-systeem buiten de Europese Unie, bijvoorbeeld in de Verenigde Staten, staat opgesteld, bleken medewerkers, ondernemingsraad en toezichthouders aanvullende privacywaarborgen, zoals contracten, te eisen.
- *Audits door het College Bescherming Persoonsgegevens*. Het College heeft sinds 1996 in diverse sectoren privacyaudits uitgevoerd, deels op eigen initiatief en deels na klachten. Ook zijn boetes uitgedeeld. Dit heeft een ster-

ke bewustwordende functie gehad bij onder andere zorginstellingen, arbodienstverleners, handelsinformatiebureaus, financiële instellingen en gemeenten. Ook andere toezichthouders zoals DNB (De Nederlandsche Bank) en PVK (Pensioen- en Verzekeringskamer) tonen in hun controleonderzoeken toenemende interesse in privacy.

- *Fraude en misbruik van sociale voorzieningen*. Van een andere orde is de wettelijke verruiming van het koppelen van gegevensbestanden voor het bestrijden van fraude. Pas toen dit daadwerkelijk ging gebeuren, trad privacybewustzijn bij de betrokkenen op.
- *Dreiging van terrorisme*. De terroristische dreiging heeft ertoe geleid dat politie- en opsporingsdiensten ruimere bevoegdheden hebben gekregen, waarbij de privacy van verdachten kan worden aangetast. Enerzijds wordt dit geaccepteerd aangezien hiermee een hoger doel wordt gediend, anderzijds ontstaat het gevoel dat hiermee een 'big brother'-achtige situatie kan ontstaan. Dit onderwerp wordt veeleer beïnvloed door de politiek en de stemming over de nationale veiligheid, dan dat het een sterke privacycomponent kent.

Ontegenzeggelijk hebben privacyincidenten een zeer grote invloed gehad op het privacybewustzijn. Onder de noemer 'een hacker als wekker' zijn door privacy- en beveiligingsfouten uiterst gevoelige persoonsgegevens geopenbaard. Bekende gevallen betreffen:

- het lek in de Univé-website met het toegankelijk zijn van ziektekostenverzekerden;
- het onrechtmatig uitwisselen van persoonsgegevens tussen GAK en Centraal Beheer;
- het hacken van de universiteit van Berkeley (zie kader 1);
- het benaderen van klanten met een ongevraagd hypotheekaanbod door een Belgische bank na analyse van hun maandelijkse automatische afschrijving van hun bankrekening van de hypotheekrente die zij aan andere hypotheekverstrekkers betaalden;
- de problemen met Microsofts Hotmail en Passport;
- het op een website vermeld zijn van het gedrag van schoolkinderen in Almere;
- het stalken van leden van een vereniging van alleenstaande vrouwen;
- het filmen en vervolgens aanschrijven van bordeelbezoekers;
- het gebruik door de landsadvocaat van een handelsinformatiebureau dat op een illegale wijze persoonsgegevens verkreeg;
- de vele inbraken in websites met vervolgens diefstal van creditcardgegevens.

Het wederrechtelijk verkrijgen en misbruiken van identificerende persoonsgegevens, identiteitsdiefstal, is inmiddels uitgegroeid tot één van de grootste fraudeoorzaken in de Verenigde Staten met enkele honderdduizenden Amerikanen per jaar die hierdoor gedupeerd zijn, met een schadepost van vele miljarden dollars.

Hacker steelt persoonsgegevens van 1,4 miljoen Amerikanen (www.securityfocus.nl)

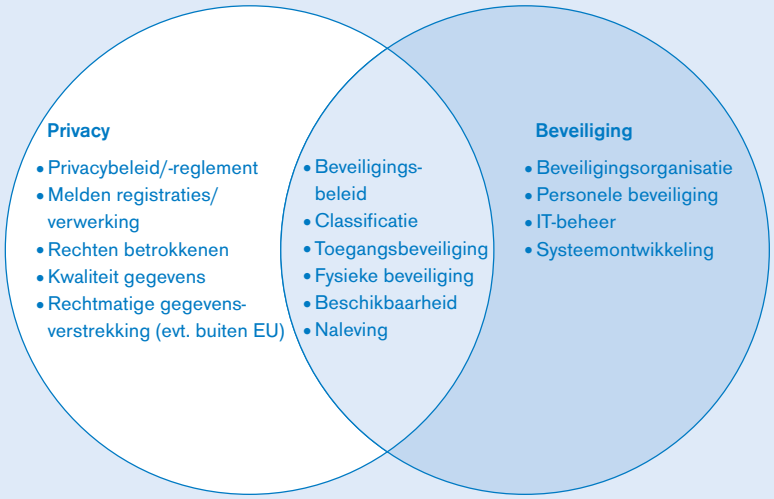
Een hacker heeft, naar nu blijkt, de persoonsgegevens van 1,4 miljoen Amerikanen gestolen uit een systeem van de Amerikaanse universiteit in Berkeley. De nog niet geïdentificeerde computerinbreker bemachtigde met zijn kraak de sofi-nummers, namen, thuisadressen, telefoonnummers en geboortedata van 1,4 miljoen oudere Amerikanen en zorgverleners. De gegevens waren met toestemming van de staat Californië, maar zonder toestemming van de burgers, opgeslagen bij de universiteit voor een onderzoek. De universiteit van Berkeley ontdekte de inbraak eind augustus 2004, maar stapte pas twee maanden later naar de politie om aangifte te doen. De FBI en de politie van de staat Californië onderzoeken de misdaad nog. Volgens een woordvoerder van de universiteit betreft het één van de grootste inbraken op een educatief computersysteem ooit in Amerika. De hacker maakte voor zijn inbraak gebruik van een onder technici algemeen bekend veiligheidsgat dat de universiteit niet tijdig had gerepareerd. Met de persoonsgegevens van de getroffen Amerikanen in handen kan de hacker talloze identiteiten aannemen en ook met de gestolen persoonsinformatie bankrekeningen openen en leningen aangaan.

Kader 1.

Beveiliging versus privacy

Een bekend misverstand – met name onder ICT'ers – is het als bijna synoniem zien van beveiliging en privacy: 'Als we de beveiligingsmaatregelen hebben getroffen volgens de Code voor Informatiebeveiliging, dan hebben we direct de privacybescherming geregeld'. Dit is echter een misvatting, aangezien beveiliging slechts één van de zeven privacyprincipes kan invullen (zie figuur 1).

Figuur 1. Overeenkomsten en verschillen tussen beveiliging en privacy.



Kader 2.

De juridische en procesmatige aspecten van privacy hebben weinig tot niets met beveiliging te maken. In figuur 1 is aangegeven op welke gezamenlijke aspecten en welke afzonderlijke aspecten het accent ligt. Zoals in dit artikel aangegeven, ligt voor de toepassing van Privacy Enhancing Technologies de uitdaging bij de privacyaspecten die niet louter door beveiligingsmaatregelen worden gerealiseerd.

Daarnaast kennen beide ook een andere insteek: het beveiligen richt zich op het bouwen van muren om een grote database met persoonsgegevens. Privacybescherming richt zich veeleer op het beperken van de geregistreerde en verwerkte persoonsgegevens en het zorgvuldig behandelen van deze gegevens in alle verwerkingsstappen.

Er zijn ook situaties waarin het verbeteren van de beveiliging de privacy juist kan aantasten. Hierbij valt te denken aan de toepassing van verdergaande identificatiegegevens, biometrie en gedetailleerde controles. Dit geldt evenzo voor antifraude- en antiterrorismemaatregelen. Hierdoor zal weer een nieuw evenwicht tussen beveiliging en privacy moeten worden gezocht.

Evolutie in de aanpak van privacy

De benadering van het privacyvraagstuk was na de introductie van de Wpr aanvankelijk sterk gericht op de beleidsmatige, procedurele en juridische aspecten en het treffen van traditionele beveiligingsmaatregelen. Dit omvatte dan de volgende generieke stappen:

- aanstellen van een privacyverantwoordelijke;
- ontwikkelen van een privacyreglement en soms een overkoepelend privacybeleid;
- inventariseren van registraties met persoonsgegevens; veelal werd dit verengd tot de geautomatiseerd vastgelegde persoonsgegevens. Vervolgens werden de doelstellingen en verwerkingen van deze registraties in kaart gebracht;
- aanmelden van registraties bij de Registratiekamer en na inwerkingtreding van de Wbp bij het College Bescherming Persoonsgegevens;
- opstellen en implementeren van richtlijnen en procedures voor onder andere verstrekkingen, verzoek om inzage en correctie, en dergelijke. Bijvoorbeeld in de 'scripts' voor toepassing in alle kanalen waarlangs interactie met klanten plaatsvindt (internet, callcenter, balie);
- opnemen van privacyspecifieke bepalingen in de contracten en SLA's met businesspartners en service providers;
- implementeren van traditionele beveiligingsmaatregelen zoals logische toegangsbeveiliging en het bouwen van 'dikke muren' ter bescherming van de persoonsgegevens.

Onderbelichte zaken betroffen onder meer het verhogen van het privacybewustzijn en de verdergaande organisatorische en technische implementatie van het privacybeleid. Geleidelijk aan heeft de privacyimplementatie zich verbreed en is de behoefte ontstaan om ook technische aspecten in te zetten voor het afdwingen van een betere naleving van het privacybeleid. De technische implementatie omvatte in die organisaties ook maatregelen voor de aangescherpte authenticatie (op basis van bezitskenmerk), gedifferentieerde afscherming met autorisatieprofielen, geprogrammeerde integriteitscontroles en het testen met gefingeerde gegevens. Tevens werden persoonsgegevens die werden verstuurd over openbare netwerken in toenemende mate versleuteld.

Huidige status privacymaatregelen

Zijn we er daarmee? Nee, aangezien een aantal privacyprincipes nog immer niet goed organisatorisch of technisch wordt gewaarborgd. Dit betreft zaken als:

- het niet bovenmatig verzamelen van persoonsgegevens;
- het uniek registreren van personen;
- het beveiligen van de persoonsgegevens, hetgeen met name van belang is bij het groeiend aantal koppelingen van gegevensbanken en informatiesystemen, keteninformatisering en het voornemen van de overheid om authentieke registraties in te richten;
- het rolgebaseerd of zelfs op dynamische basis en – sterker nog – 'business rule'-gebaseerd autoriseren van toegang tot gegevensgroepen en individuele velden met gevoelige persoonsgegevens;
- het verbeteren van de kwaliteit van de persoonsgegevens;
- het registreren welke medewerker welke persoonsgegevens heeft ingezien;
- het anoniem kunnen verwerken van persoonsgegevens;
- het handhaven van bewaartermijnen en de vernietigingsplicht van persoonsgegevens;
- het registreren van verstrekkingen aan derden in Nederland en andere EU-landen en aan derden daarbuiten.

Noodzaak tot Privacy Enhancing Technologies

Voor vrijwel alle bovenstaande onderwerpen kan de toepassing van technische maatregelen de afhankelijkheid van organisatorische procedures en het privacybewustzijn beperken en consistentie garanderen. De term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen. In de paragraaf 'PET-vormen' wordt in detail ingegaan op de PET-maatregelen die kunnen worden getroffen.

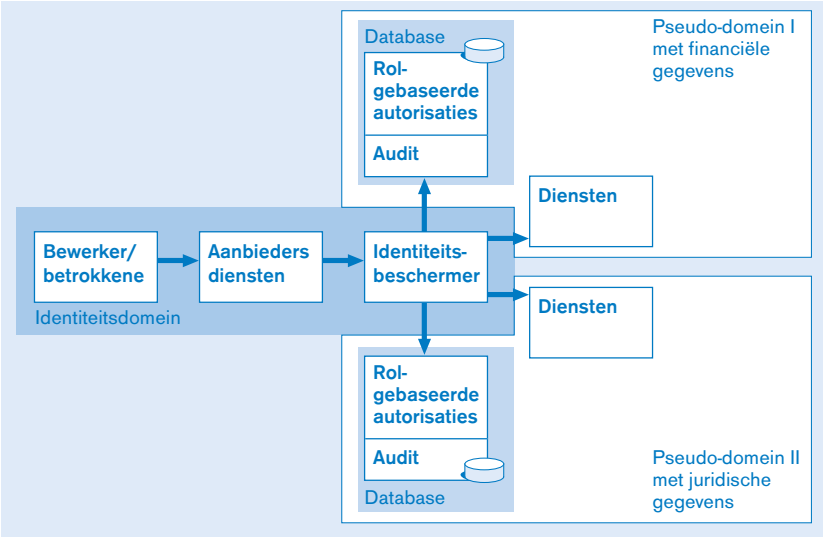
In de toepassing en ontwikkeling van PET is een trend te herkennen. Zoals in dit artikel is gesteld, werd de techniek in eerste instantie vooral ingezet ter bescherming van reeds geregistreerde persoonsgegevens. Vandaag de dag wordt PET echter ook al door een beperkt aantal organisaties ingezet om reeds aan de bron technische maatregelen te treffen en het aantal identificerende gegevens tot het absolute minimum te beperken. Daar waar het niet nodig is, wordt de identiteit niet vastgelegd of wordt de identiteit losgekoppeld van de overige persoonsgegevens. Een belangrijke stap die nog moet worden gezet, is dat alle gegevensverwerkende organisaties kritisch kijken welke gegevens nu echt noodzakelijk zijn voor de dienstverlening. Vaak worden uit gewoonte meer gegevens vastgelegd dan nodig is. Deze overtollige gegevens moeten worden beheerd en beschermd, terwijl ze geen nut dienen en dus alleen maar een risico en kostenpost vormen. De gemakkelijkste manier om dit 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. Een belangrijk aspect hierbij is dat moet worden vastgesteld of het verwerken van persoonsgegevens ([PKIO02]):

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

PET-vormen

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 autorisatiegegevens 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 (identiteitsbeschermer) 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. In figuur 2 is de scheiding van gegevens in meerdere domeinen grafisch weergegeven.

Een verdergaande integratie van gegevens en programmatuur wordt gevormd door een PET-vorm waarin de

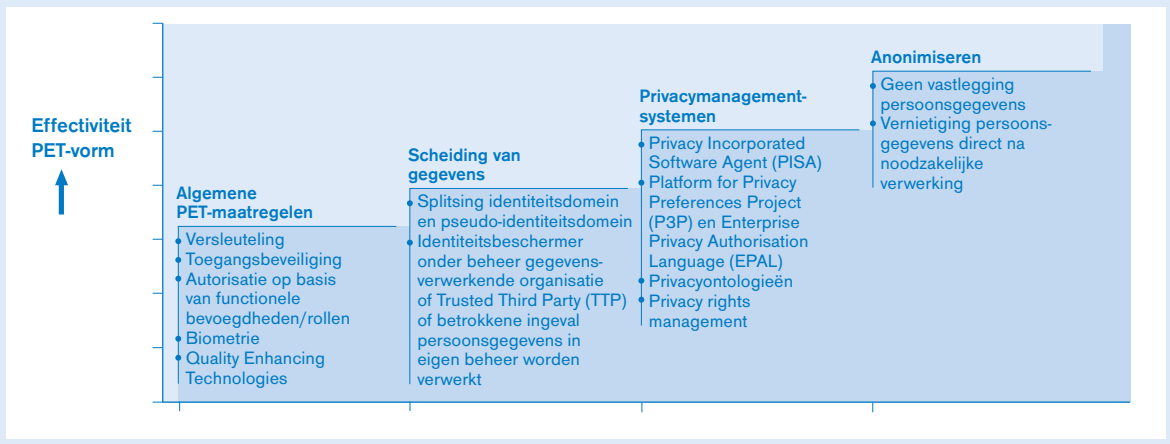


Figuur 2. Scheiding van gegevens in meerdere domeinen met identiteitsbeschermer.

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 privacyreglement. 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 figuur 3 is in de PET-trap aangegeven dat de effectiviteit van de bescherming van persoonsgegevens wordt bepaald door de toegepaste PET-vorm. 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 met name afhankelijk van het type informatiesysteem, het nagestreefde ambitieniveau en de gevoeligheid van de persoonsgegevens.

In het algemeen kan worden gesteld dat algemene PET-maatregelen op dit moment het meest worden toegepast, gevolgd door scheiding van gegevens en anonimisering. Het toepassen van privacymanagementsystemen staat in de kinderschoenen en vindt op beperkte schaal plaats.



Figuur 3. De PET-trap.

Nationaal Trauma Informatie Systeem (NTIS)

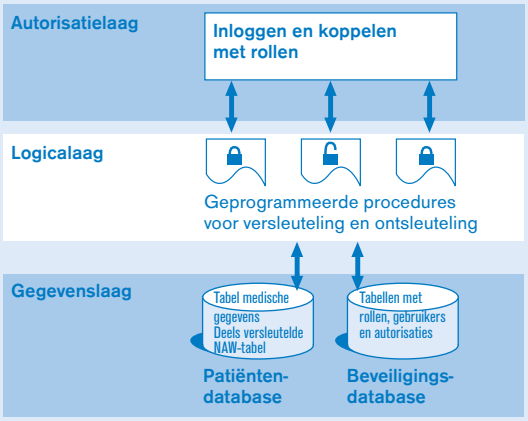
Het NTIS is een digitaal registratiesysteem voor traumapatiënten met zwaar acuut letsel die geholpen worden op de afdeling Spoed Eisende Hulp. Artsen, verpleegkundigen en assistenten hebben toegang tot dit systeem. Door de elektronische vastlegging en uitwisseling van medische gegevens kan een efficiëntere 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, waardoor 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 (RGF) 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.

In figuur 4 is weergegeven op welke wijze de scheiding van gegevensdomeinen is aangebracht.



Figuur 4. Globale structuur traumasysteem.

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 het regionale succes van dit systeem is een landelijke uitrol van het NTIS gaande.

In [Wijs04] is de toepassing van Privacy Enhancing Technologies voor het NTIS-systeem uitgebreider beschreven.

Kader 3.

PET-kosten

Is PET te duur voor uw 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. Om te onderzoeken of er voor uw organisatie een positieve business case bestaat voor de toepassing van PET, moeten drie kernvragen worden beantwoord. Deze vragen zijn:

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

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 geregistreerde burgers c.q. klanten zijn echter aanzienlijk. De kosten van PET-toepassing bedragen bij de meeste projecten gemiddeld slechts enkele procenten van het totaalbudget en laten zich derhalve snel terugverdienen.

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 natuurlijk hoger dan bij nieuwe systemen. De oorzaak hiervan is dat de meeste kostenposten van PET eenmalig zijn en de eenmalige activiteiten deel uitmaken van het gehele systeemontwikkelingstraject. 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.

PET-implementatie

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. Het later toevoegen van PET in een informatiesysteem is zeker mogelijk gezien enkele praktijkervaringen, maar kan soms dieper in het informatiesysteem ingrijpen. In het algemeen zijn hier meer tijd en meer kosten mee gemoeid. Overigens geldt dat met name voor de geavanceerde PET-vormen en -maatregelen.

In tabel 1 worden de verschillende fasen weergegeven die moeten worden doorlopen om tot een succesvolle PET-implementatie te komen. Per fase is aangegeven welke PET-specifieke vragen in de betreffende fase moeten worden beantwoord.

Toekomst

Onze verwachting is dat privacy en Privacy Enhancing Technologies een integraal deel zullen uitmaken van systeemontwikkeling. De burgers en consumenten verwachten van organisaties dat zij zorgvuldig en efficiënt met persoonsgegevens omgaan. Eenmalige registratie aan de bron en vertrouwelijke omgang in alle fasen van gegevensverwerking in het systeem en de keten behoren daartoe. Om deze verwachtingen te kunnen inlossen en om de kwaliteit van de gegevens te waarborgen zullen organisaties in toenemende mate dergelijke technologieën gaan toepassen. Wij verwachten dat in eerste instantie het merendeel van de overheidsorganisa-

'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 zevenenvijftig procent 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. Deze 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 zorg dragen 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 gebruikersinterfaces en het gebruik van technologie om het privacybeleid af te dwingen, maar ook over een identiteitssysteem gebaseerd op betekenisloze maar unieke nummers (MBUN's)[5]. 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.

Kader 4.

5) De MBUN's zijn niet gebaseerd op reeds bestaande identificerende nummers.

Projectfase	PET-specifieke afwegingen
Doelbinding en noodzaak	• Welke persoonsgegevens zijn noodzakelijk om de diensten te kunnen verlenen en waarom zijn deze persoonsgegevens noodzakelijk?
Gegevensanalyse en -classificatie	• Welk niveau van gegevensbescherming moet worden gerealiseerd gezien de risicoanalyse en de Wbp-classificatie? • Levert de toepassing van PET een bijdrage aan de te realiseren gegevensbescherming of wordt de bescherming reeds gewaarborgd en is PET niet noodzakelijk? • Welke PET-vorm(en) gaat (gaan) worden toegepast? • Wat zijn de kwantitatieve én kwalitatieve kosten en de baten?
Basisontwerp	• Hoe lopen de gegevensstromen in het informatiesysteem? • Welke koppelingen met andere systemen en instanties zijn in ketenverband aanwezig? • Wat is het gegevensmodel voor iedere gegevensstroom in het verwerkingsproces van verzamelen, opslaan, bewaren tot aan vernietigen?
Detailontwerp	• Hoe wordt het technisch ontwerp van de PET-vorm geïntegreerd in het volledige technisch ontwerp van het informatiesysteem?
Ontwikkeling	• Moet de gekozen PET-vorm zelf worden ontwikkeld of zijn er standaardoplossingen beschikbaar?
Testen	• Functioneert PET op een juiste wijze als onderdeel van het gehele informatiesysteem? • Voldoet de geïmplementeerde PET-vorm aan de eisen qua gebruikersvriendelijkheid?
Implementatie	• Verandert de werkwijze voor gebruikers door de toepassing van PET en hoe worden gebruikers hierover ingelicht? • Moeten beheerders en gebruikers getraind worden in de toepassing van PET? • Moeten er specifieke middelen, zoals bijvoorbeeld tokens, worden uitgegeven aan medewerkers?
Beheer en onderhoud	• Welke specifieke PET-beheeractiviteiten moeten worden uitgevoerd in aanvulling op de reguliere beheeractiviteiten?
Evaluatie	• Zijn de PET-maatregelen effectief? • Is een audit of een certificering van het informatiesysteem gewenst? • Wat zijn de gebruikers- en beheerderservaringen?

Tabel 1. PET-stappenplan.

ties een vorm van Privacy Enhancing Technologies gaat toepassen, gevolgd door bedrijven die gevoelige persoonsgegevens verwerken of moeten voldoen aan stringente wet- en regelgeving. Hiermee zullen vraag en aanbod van Privacy Enhancing Technology-oplossingen gelijke tred moeten houden.

Conclusie

Door technische maatregelen te treffen wordt niet alleen een effectievere en efficiëntere gegevensbescherming bereikt. De toepassing van technische maatregelen vraagt namelijk ook om kritisch na te denken over persoonsgegevens en over de noodzaak en de bescherming ervan. Deze aanpak verhoogt de integriteit en vertrouwelijkheid van de gegevens en maakt een efficiëntere verwerking van persoonsgegevens mogelijk. Met Privacy Enhancing Technologies behoeft in mindere mate te worden gesteund op de naleving van procedures, maar worden privacybepalingen direct in de applicatie of in de ICT-infrastructuur verankerd.

Derhalve willen we op een onorthodoxe wijze dit artikel besluiten.

PET is meer dan een manier om persoonsgegevens te beschermen:

- *Vraag naar PET*
  - 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 controlemogelijkheden over hun persoonsgegevens te geven.
  - De toepassing van PET geeft de organisatie een innovatief imago.
- *Noodzaak tot PET*
  - 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.
- *Mogelijkheden voor PET-toepassing*
  - PET is al vele malen succesvol geïmplementeerd (zie ook casussen in [BZK04]).
  - PET heeft slechts een beperkte invloed op de ontwikkelkosten van een nieuw informatiesysteem aangezien de technieken voorhanden zijn en de kosten voornamelijk samenhangen met het toepassen ervan. Het 'kost' met name denk- en ontwerpwerk.
  - Het opnemen van PET in de informatiearchitectuur biedt een basis om PET in verschillende informatiesystemen efficiënt toe te passen.

Literatuur

[BZK04] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Witboek Privacy Enhancing Technologies, een witboek voor beslissers*, december 2004.

[EPIC03] EPIC/Global Internet Liberty Campaign/ Privacy International, *Privacy and Human Rights: An international survey of privacy laws and practices*, 2003.

[Koor01] R.F. Koorn en M. Dontje, *Internationale privacyaspecten en de Wbp*, Compact 2001/4.

[PKIO02] PKIoverheid, *PET en de PKI voor de overheid*, november 2002.

[Wijs04] B. Wijskamp, J. ter Hart, L. Taal en R.F. Koorn, *Casusbeschrijving Nationaal Trauma Informatie Systeem, toepassing van Privacy Enhancing Technologie bij traumacentra*, oktober 2004.