Registratiekamer

G.W. van Blarkom
drs. J.J. Borking

VOORWOORD

Beveiliging van persoonsgegevens

Achtergrondstudies en Verkenningen 23

G.W. van Blarkom
drs. J.J. Borking

Beveiliging van persoonsgegevens

Achtergrondstudies en Verkenningen 23

Voorwoord

In de hedendaagse samenleving, waarin informatie een cruciale rol speelt in talloze processen en activiteiten, is het van groot belang dat gegevens worden beschermd. Dat geldt temeer als die gegevens over personen gaan.

De Wet bescherming persoonsgegevens die in de loop van 2001 in werking zal treden, gaat over persoonsgegevens zoals die op grote schaal worden verwerkt door overheid, bedrijven en andere organisaties. De wet stelt de normen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens. Een belangrijk element is dat passende technische en organisatorische maatregelen worden getroffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Dit rapport gaat over de uitwerking van die verplichting tot beveiliging.

Met welke risico's moet rekening worden gehouden? Met welke maatregelen kunnen we die risico's beperken? Welke maatregelen zijn in een bepaald geval passend? Kortom: aan welke eisen moet de beveiliging van persoonsgegevens voldoen? Bij wijze van handreiking aan de praktijk heeft de Registratiekamer in dit rapport een aantal eisen geformuleerd die een nadere invulling geven aan de wettelijke norm.

Een belangrijke bijdrage aan de totstandkoming van dit rapport is geleverd door een commissie van deskundigen op het gebied van informatiebeveiliging onder voorzitterschap van drs. J.J. Borking, plaatsvervangend voorzitter van de Registratiekamer. Bijzondere dank gaat uit naar vijf leden van die commissie die – op persoonlijke titel – hun professionele expertise hebben ingebracht: prof. M.E. van Biene-Hershey RE, ing. J.N.M. Koppes, prof. A.W. Neisingh RE RA., ing. J.H. Sneep en H. de Zwart RE RA RO.

Het rapport is ten dele een bewerking van het advies 'Beveiliging van persoonsregistraties' dat de Registratiekamer in 1994 uitbracht. Met de reacties op dit advies en de ervaringen die daarmee zijn opgedaan, is in het rapport zo goed mogelijk rekening gehouden.

De Registratiekamer beveelt het gebruik van dit rapport in de beveiligingspraktijk van harte aan en ziet ook nu weer met belangstelling uit naar de reacties.

mr. P.J. Hustinx
Voorzitter van de Registratiekamer

Publicaties in de serie Achtergrondstudies en Verkenningen zijn het resultaat van onderzoeken uitgevoerd door of in opdracht van de Registratiekamer. Met het uitbrengen van de publicaties beoogt de Registratiekamer de discussie en meningsvorming te stimuleren over ontwikkelingen in de samenleving waarin de persoonlijke levenssfeer van de burger in het geding is.

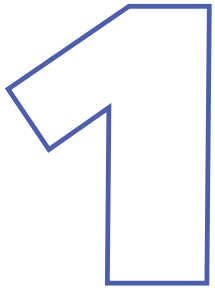
Beveiliging van persoonsgegevens
Registratiekamer, Den Haag, april 2001

ISBN 90 74087 27 2

Druk: Sdu Grafisch Bedrijf bv

Inhoud

Beveiliging van persoonsgegevens



1 Beveiliging van persoonsgegevens

Beveiliging van persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking

De ontwikkelingen die samenhangen met informatie- en communicatietechnologie (ICT) beïnvloeden in steeds sterkere mate onze samenleving. Naarmate het gegevensverkeer intensiever wordt, het aantal deelnemers daaraan toeneemt en de hoeveelheid gegevens die over personen wordt verwerkt groeit, moeten hogere eisen gesteld worden aan de bescherming van die gegevens.

De beveiliging van gegevens betreffende identificeerbare personen, *persoonsgegevens*, is een onderdeel van het recht op privacybescherming. Dit recht is verankerd in internationale verdragen, in Europese wetgeving, in de Grondwet en in nationale wetgeving. In Nederland vormt de Wet bescherming persoonsgegevens (WBP) het algemene kader.

De WBP heeft onder meer betrekking op de *verwerking van persoonsgegevens*. Onder het verwerken van persoonsgegevens worden alle handelingen verstaan die met persoonsgegevens kunnen worden verricht, van het *verzamelen* tot en met het *vernietigen* (artikel 1 onder b WBP). Paragraaf 2.1 gaat nader in op het begrippenkader van de WBP.

Het toezicht op de naleving van de WBP is opgedragen aan het College bescherming persoonsgegevens (CBP). De naleving van de WBP dient primair te zijn ingebed in de reguliere beheers- en verantwoordingprocessen. Het CBP heeft de bevoegdheid een onderzoek in te stellen naar de wijze waarop de wet wordt nageleefd. De *beveiliging van persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking* (verder genoemd de *beveiliging van persoonsgegevens*) is bij deze onderzoeken een bijzonder aandachtspunt.

Omdat het kader van de WBP breder is dan het aandachtsgebied van de informatie- en communicatietechnologie (ICT) hanteert de WBP een begrippenkader dat aanleiding kan geven tot onduidelijkheden in relatie tot de in de dagelijkse praktijk gehanteerde begrippenkaders, met name in de sfeer van de ICT.

In de dagelijkse praktijk zal er veelal sprake zijn van een interactie tussen het ICT domein en de toepassing van de WBP. Om te voorkomen dat misverstanden ontstaan omtrent de herkomst en betekenis van een begrip volgt hier een kort overzicht van de in deze studie gehanteerde begrippenkaders:

WBP artikel	WBP context	ICT context
1 onder a	persoonsgegevens	gegevens
1 onder b	verwerking van persoonsgegevens	gegevensverwerking
13	beveiliging van persoonsgegevens	'(informatie)beveiliging'

Deze studie bevat een uitwerking van de wettelijke verplichting tot het beveiligen van persoonsgegevens. De aanbevolen beveiligingsmaatregelen zijn in algemene termen geformuleerd en daardoor toepasbaar voor alle organisaties (privaat en publiek; groot en klein) die persoonsgegevens verwerken. De studie

sluit aan bij in de praktijk gehanteerde normen voor informatiebeveiliging, in het bijzonder bij de Code voor Informatiebeveiliging, die voornamelijk in het bedrijfsleven wordt gehanteerd en bij het Voorschrift Informatiebeveiliging Rijksdienst. De vertaling van de, in algemene termen geformuleerde, (informatie)beveiligingsmaatregelen in de praktijk vereist maatwerk dat is gebaseerd op een analyse. Bij deze analyse wordt rekening gehouden met de reeds aanwezige normatieve kaders.

Deze studie zal tevens als een van de uitgangspunten gelden voor het onderzoek (ex artikel 60 WBP) dat het CBP kan instellen in het kader van het toezicht op de naleving van de wet.

1.1 Kwaliteitsaspecten van beveiliging

De beveiliging van persoonsgegevens kent drie kwaliteitsaspecten:

1. **Exclusiviteit**
   Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.

2. **Integriteit**
   De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

3. **Continuïteit**
   De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.

Bij deze studie wordt ervan uitgegaan dat in de meeste organisaties en bedrijven, omwille van het bedrijfsbelang, de *integriteit* en *continuïteit* van de informatiesystemen voldoende zijn gewaarborgd. De bescherming van de privacy van de personen over wie persoonsgegevens worden verwerkt, vereist dat met name de *exclusiviteit* voldoende gewaarborgd wordt.

Deze studie bevat een normatief kader hoe met name die *exclusiviteit* van persoonsgegevens door middel van maatregelen en procedures kan worden gewaarborgd.

1.2 Leeswijzer

Hoofdstuk 2 beschrijft het juridisch kader voor de bescherming van persoonsgegevens. De Wet bescherming persoonsgegevens wordt kort uiteengezet, in het bijzonder de gevolgen van deze wet voor de beveiliging van persoonsgegevens.

Hoofdstuk 3 behandelt hoe het niveau van de te nemen beveiligingsmaatregelen bepaald wordt. De mate van beveiliging van persoonsgegevens die noodzakelijk is, wordt bepaald door de risicoklasse. Deze klasse wordt bepaald door de kans dat onzorgvuldig of onbevoegd gebruik zich voordoet en door de schade die daaruit voortvloeit. De uitkomst van een analyse bepaalt de risicoklasse en daarmee het vereiste niveau van maatregelen en procedures. Het CBP gaat daarbij uit van een indeling van persoonsgegevens in vier risicoklassen.

Hoofdstuk 4 bevat een beschrijving van de eisen waarmee rekening moet worden gehouden voor een afdoende beveiliging van persoonsgegevens. Deze eisen worden beschreven voor elke risicoklasse. De verantwoordelijke voor de verwerking van persoonsgegevens dient deze vervolgens uit te werken in een stelsel van concrete maatregelen en procedures.

Juridisch kader

2 Juridisch kader

2.1 Begrippenkader van de WBP

Deze studie is gebaseerd op de Wet bescherming persoonsgegevens. Deze wet roept voor de verantwoordelijke voor een verwerking van persoonsgegevens een aantal rechten en plichten in het leven. De reikwijdte van de WBP wordt in belangrijke mate bepaald door de definities die in de wet zijn opgenomen.

De definities van de belangrijkste begrippen worden hierna weergegeven (artikel 1 onder a tot en met g en onder l WBP):

a. Persoonsgegeven
elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

b. Verwerking van persoonsgegevens
elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in elk geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

c. Bestand
elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

d. Verantwoordelijke
de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

e. Bewerker
degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

f. Betrokkene
degene op wie een persoonsgegeven betrekking heeft.

g. Derde
ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

l. Functionaris
de functionaris voor de gegevensbescherming als bedoeld in artikel 62.

In artikel 62 tot en met 64 WBP, worden de taken en verantwoordelijkheden van de functionaris voor de gegevensbescherming nader geregeld:

> De functionaris voor de gegevensbescherming houdt binnen één of meerdere organisaties, onafhankelijk toezicht op de toepassing en naleving van de WBP. Tevens is hij een deskundig aanspreekpunt voor de verantwoordelijke, voor betrokkenen en voor het CBP.

Volgens artikel 2 WBP is deze wet van toepassing op geheel of gedeeltelijk geautomatiseerde, alsmede, in bepaalde gevallen, de niet geautomatiseerde verwerking van persoonsgegevens. Dit heeft tot gevolg dat persoonsgegevens, een verwerking van persoonsgegevens en een bestand (artikel 1 onder a tot en met c WBP) zich zowel binnen als buiten het ICT domein kunnen bevinden.

2.2 Relatie met bestaande beveiligingsmaatregelen

De invoering van de Wet bescherming persoonsgegevens (WBP) heeft gevolgen voor alle organisaties. De wet heeft betrekking op zowel geautomatiseerde als niet geautomatiseerde gegevensverwerkingen. Dit houdt in, dat de verantwoordelijke (artikel 1 onder d WBP) voor een verwerking van persoonsgegevens ervoor moeten zorgen, dat adequate invulling aan de WBP gegeven wordt. Dit vereist een doelgerichte aanpak van het creëren van de maatregelen en procedures die in het kader van deze wet getroffen moeten worden. Eerder genomen maatregelen en procedures met betrekking tot de (informatie)-beveiliging en de gegevensverwerking zullen moeten worden getoetst aan de doelstellingen van de WBP en kunnen aanleiding geven tot een heroverweging.

Om de eisen die in de WBP zijn geformuleerd op een doeltreffende manier te implementeren en daarmee de rechten van de betrokkene te ondersteunen, is het van belang om een adequaat stelsel van algemene maatregelen en procedures te realiseren. Die maatregelen en procedures zullen veelal op grond van de beheersing van bedrijfsprocessen reeds aanwezig zijn. Specifieke maatregelen en procedures voor de bescherming van de privacy van de burger en de daarmee samenhangende verwerking van persoonsgegevens moeten worden bezien. In relatie tot privacybescherming zal in de regel een aanvullend stelsel van maatregelen en procedures vereist zijn bovenop de normaliter al vereiste controle- en (informatie)beveiligingsmaatregelen die met betrekking tot de bedrijfsprocessen gelden. Om een evenwichtig beleid ten aanzien van de verwerking van persoonsgegevens samen te stellen, te implementeren en te onderhouden zal dat beleid een belangrijke plaats in de managementcyclus dienen in te nemen.

Basisniveau van privacybescherming

De basis voor de rechtmatige verwerking van persoonsgegevens wordt gevormd door een aantal in de WBP vastgelegde privacy eisen die van toepassing zijn op elke organisatie. Deze eisen zijn vertaald in concrete aandachtsgebieden en verder ontwikkeld in een samenwerkingsverband tussen beroepsorganisaties, marktpartijen en de Registratiekamer en vastgelegd in het door dit samenwerkingsverband ontwikkelde ‘Raamwerk Privacy Audit’.

Deze eisen, afgeleid uit de Wet bescherming persoonsgegevens, hebben betrekking op de volgende onderwerpen:

1. Voornemen en melden;
2. Transparantie;
3. Doelbinding;
4. Rechtmatige grondslag;
5. Kwaliteit;
6. Rechten van de betrokkenen;
7. Beveiliging;
8. Verwerking door een bewerker;
9. Gegevensverkeer met landen buiten de EU.

2.3 Juridisch kader voor privacybescherming

Eerbiediging van de persoonlijke levenssfeer is een van de grondslagen van onze rechtsorde. Het recht op eerbiediging van de persoonlijke levenssfeer is vastgelegd in artikel 10 van de Grondwet:

1. *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
2. *De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
3. *De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

Hoe kan dit artikel worden vertaald in een stelsel van concrete maatregelen en procedures? Sinds 1989 geldt de Wet persoonsregistraties (WPR), waaruit regels voortvloeien voor de rechtmatige en zorgvuldige omgang met persoonsgegevens. De WPR zal in de loop van 2001 worden vervangen door de Wet bescherming persoonsgegevens (WBP). Deze nieuwe wet verschilt op een aantal punten van de WPR. De wijzigingen weerspiegelen de sterk gegroeide en nog steeds groeiende mogelijkheden van informatie- en communicatietechnologie.

De WBP is op hoofdlijnen gelijk aan de Europese richtlijn 95/46/EG, die op 25 oktober 1995 werd aangenomen. Deze richtlijn beschrijft de wijze waarop in de lidstaten moet worden omgegaan met persoonsgegevens. Tevens wordt in deze richtlijn bepaald onder welke voorwaarden persoonsgegevens verstrekt mogen worden aan (organisaties in) landen buiten de Europese Unie.

2.4 Bescherming van persoonsgegevens

De WBP is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2, eerste lid WBP).

De WBP bevat onder meer regels die betrekking hebben op de toelaatbaarheid en de kwaliteit van de verwerking van persoonsgegevens (artikel 6 tot en met 11 WBP).

Persoonsgegevens moeten in overeenstemming met de wet op een behoorlijke en zorgvuldige wijze worden verwerkt (artikel 6 WBP). Het begrip ‘zorgvuldig’ sluit aan bij de zorgvuldigheidsnorm in het Burgerlijk Wetboek en het

zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur. Dit basisbegrip wordt verder uitgewerkt in diverse andere bepalingen van de WBP. Zo gelden voor de verwerking van persoonsgegevens op hoofdlijnen de volgende regels:

- persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (artikel 7 WBP);
- de omschrijving van het doel blijkt uit de melding van de verwerking bij het CBP of bij de functionaris voor de gegevensbescherming (artikel 28 WBP) of uit de doelstelling van één van de verwerkingen van persoonsgegevens genoemd in het Vrijstellingsbesluit (artikel 29 WBP);
- de persoonsgegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor deze zijn verkregen (artikel 9, eerste lid WBP).

Zoals aangegeven moet de verantwoordelijke een gerechtvaardigd belang hebben bij de verwerking van persoonsgegevens. Hierbij moet in alle stadia van de verwerking altijd minimaal één van de volgende voorwaarden van toepassing zijn (artikel 8 WBP):

Persoonsgegevens mogen slechts worden verwerkt indien:

- *de betrokkene voor de verwerking ondubbelzinnig toestemming heeft verleend;*
- *de verwerking van persoonsgegevens* (de wet spreekt hier over gegevensverwerking) *noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;*
- *de verwerking van persoonsgegevens noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;*
- *de verwerking van persoonsgegevens noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;*
- *de verwerking van persoonsgegevens noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan;*
- *de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.*

2.5 Wettelijke verplichting tot beveiliging

De wettelijke grondslag voor de maatregelen voor beveiliging van persoonsgegevens wordt gevormd door artikel 13 WBP. De beveiliging van persoonsgegevens valt onder de verantwoordelijkheid van de *verantwoordelijke*, zoals gedefinieerd in artikel 1 onder d WBP.

Artikel 13 WBP luidt:

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

Artikel 13 WBP vormt de grondslag van deze studie. Het artikel spreekt over *technische en organisatorische maatregelen:*

- *Technische* maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen (zoals toegangscontroles, vastlegging van gebruik en back-up). Onder technische maatregelen worden tevens verstaan de voorzieningen die bekend staan onder de verzamelnaam **Privacy-Enhancing Technologies** (PET)[1].
- *Organisatorische* maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens (zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen).

Voor elke verwerking van persoonsgegevens afzonderlijk, moet bepaald worden welke technische en organisatorische maatregelen dienen te worden genomen om een *passend beveiligingsniveau* voor de verwerking van persoonsgegevens te bereiken. Technische en organisatorische maatregelen behoren altijd een onderling samenhangend en afgestemd stelsel te vormen, afgeleid uit een (informatie)beveiligingsbeleid, (informatie)beveiligingsplan en terug te vinden in een stelsel van algemene maatregelen en procedures.

Het vereiste niveau van beveiliging van persoonsgegevens zal afhangen van de risicoklasse. De bepaling van deze risicoklasse komt in hoofdstuk 3 aan de orde. Wanneer de risico's van de verwerking zijn geschat, komen andere aspecten aan de orde, namelijk de in artikel 13 WBP vermelde stand der techniek en de kosten van de ten uitvoerlegging van de maatregelen (paragraaf 2.6: Wat zijn passende maatregelen?). Deze risico's zijn van invloed op de mate waarin maatregelen en procedures moeten worden getroffen.
Waar richt de beveiliging van persoonsgegevens zich nu op? Artikel 13 WBP spreekt over *maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking*. Er wordt dus enerzijds beveiliging tegen 'verlies' voorgeschreven, anderzijds beveiliging tegen 'enige vorm van onrechtmatige verwerking'. De verwerking van persoonsgegevens is in de WBP zeer ruim omschreven. Het omvat alle stadia waarin persoonsgegevens zich in een organisatie kunnen bevinden. Artikel 13 WBP geeft aan dat de maatregelen gericht moeten zijn op de beveiliging van persoonsgegevens tegen onrechtmatige verwerking in elk van deze stadia. Dit betekent dat de maatregelen ingezet moeten worden om te voorkomen dat er in strijd met de overige artikelen van de WBP wordt gehandeld.

Ook legt artikel 13 WBP op dat er maatregelen worden genomen om *onnodige verzameling en verdere verwerking van persoonsgegevens* te voorkomen. Dit betekent dat er niet meer persoonsgegevens mogen worden verzameld dan strikt noodzakelijk is voor het van tevoren gespecificeerde doel. Wanneer persoonsgegevens eenmaal zijn verzameld, moet worden voorkomen dat deze alsnog op onrechtmatige wijze verder worden verwerkt. Het voorkomen van dergelijke verdere verwerking kan door het treffen van organisatorische maatregelen. Een betere beveiliging van persoonsgegevens kan worden bereikt door het gebruik van Privacy-Enhancing Technologies (PET), technisch verankerde maatregelen ter bescherming van de privacy.

[1] Achtergrondstudies en Verkenningen nr. 11: Privacy-Enhancing Technologies – The path to anonymity

Het schema (zie hierna) geeft de reikwijdte van artikel 13 WBP aan. Uitgaande van de mogelijke handelingen met betrekking tot het verwerken persoonsgegevens, zoals in artikel 1 onder b WBP genoemd, wordt aangegeven hoe de

risico's moeten worden beperkt.
Het vervolg van deze studie beschrijft veertien aandachtsgebieden (zie hoofdstuk 4) van dergelijke (informatie)beveiligingsmaatregelen die van toepassing zijn op zowel een geautomatiseerde als op een niet geautomatiseerde omgeving. In het schema worden de maatregelen benoemd die de onderkende risico's kunnen beperken. Deze maatregelen kunnen technisch of organisatorisch van karakter zijn. Voor een aantal vormen van beveiliging is PET de geadviseerde weg.

Schematische voorstelling van de reikwijdte van artikel 13, Wet bescherming persoonsgegevens

Toelichting:

In de tabel is de tekst van artikel 13 WBP opgenomen in kolom 1. In kolom 2 is weergegeven op welk onderdeel uit artikel 1 onder b dit betrekking heeft. Daarna is in de kolom 'object' aangegeven via welk(e) object(en) de maatregelen voor de beveiliging van persoonsgegevens kunnen worden ingevuld.
Bij elk van de objecten in de tabel is een verwijzing opgenomen naar andere artikelen uit de WBP die een raakvlak hebben met artikel 13 (de kolom Ander artikel WBP) en / of met deze studie (een paragraaf in hoofdstuk 4).

De passende maatregelen kunnen slechts na een analyse door de verantwoordelijke worden bepaald (paragraaf 2.6: Wat zijn passende maatregelen?). Deze analyse maakt gebruik van de drie criteria:
1. stand van de techniek;
2. kosten van de tenuitvoerlegging;
3. de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Bij elk van de maatregelen is aangegeven waarmee deze correspondeert met betrekking tot de kwaliteitsaspecten (paragraaf 1.1):

- E Exclusiviteit
- I Integriteit
- C Continuïteit

Deze eerste tabel geeft een schematische voorstelling van de zin uit artikel 13: *Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die*

Factoren bij het bepalen van de maatregelen:	**Risico's komen voort uit:**	**Randvoorwaarden:**
Risico's	verwerking aard en omvang van de te beschermen persoonsgegevens	stand der techniek kosten

Maatregelen:

Onderdeel artikel 13	*Onderdeel artikel 1 onder b*	*Object*	*Ander artikel WBP*	*Paragraaf*	*Kwaliteits-aspect*
• Beveiliging tegen verlies		back-up procedure		4.11	C
		fysieke beveiliging persoonsgegevens		4.11	C
		netwerken en externe verbindingen		4.8	E, I
		continuïteitsplan		4.13	C
• Beveiliging tegen onrechtmatige verwerking	algemeen	beveiligingsbeleid / plan		4.1	C, E, I
		beveiligingsbewustzijn in de organisatie	12	4.3	C, E, I
		administratieve organisatie		4.2	C, E, I
		eisen ten aanzien van personeel, geheimhouding	9.4	4.4	E
		beheer en classificatie ICT infrastructuur		4.6	E
• Beveiliging tegen onrechtmatig:	verzamelen / vastleggen	doel bepaling en omschrijving	7		C, E, I
		toetsing van de aard van de persoons-gegevens (bijzondere)	16		I
		toestemming vragen van betrokkene	8a		I
		toetsing overige rechtmatigheidsgronden	8b-f, 16-23		I
		toetsing verzamelen persoonsnummers	24		I
		toets toereikend / ter zake / niet bovenmatig	11.1		I
		toets juist / volledig	11.2		I
		informatieverstrekking betrokkene	33 (34)		E, I
		vastlegging herkomst persoonsgegevens	34		I
	bewaren	bewaartermijn respecteren	10.1		E, I
		procedure voor vernietigen		4.12	E, I
		anonimiseren; PET	10.1		E, I
		recht op correctie / verwijderen / verzet	35, 36, 40, 41		E, I
	wijzigen	logisch toegangsbeheer en controle		4.7, 4.10	E
		gebruik van (goedgekeurde) software		4.9	E, I
	opvragen/ raadplegen	inrichten van de werkplek		4.5	E
		logisch toegangsbeheer		4.7, 4.10	E
		netwerken en externe verbindingen		4.8	E, I
	verstrekken / verspreiden	PET: voorkomen / vastleggen verstrekkingen		2.6	E, I

Maatregelen:

Onderdeel artikel 13 vervolg	*Onderdeel artikel 1 onder b*	*Object*	*Ander artikel WBP*	*Paragraaf*	*Kwaliteits-aspect*
	samenbrengen / in verband brengen	PET: voorkomen koppelingen		2.6	I
	afschermen	recht op inzage betrokkene	35		E
		medewerking aan controle	61		E
	uitwissen / vernietigen	procedure vernietigen persoonsgegevens		4.12	E
		logisch toegangsbeheer en controle		4.7	E
• Voorkomen:	onnodige verzameling	toets toereikend / ter zake / niet bovenmatig	11.1		I
		toets juist / volledig	11.2		I
	onnodige verdere verwerking	toets verenigbaar gebruik	9		I
		informatie verstrekken betrokkenen	34		E
		recht op correctie / verwijderen / verzet	35, 36, 40, 41		E, I
		PET: voorkomen onverenigbaar gebruik		2.6	E

de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
Artikel 14 WBP is van toepassing op omgevingen waar de verantwoordelijke de verwerking van persoonsgegevens, of gedeelten daarvan, heeft uitbesteed aan

Maatregelen:

Artikel 14	*Object*	*Paragraaf*	*Kwaliteits-aspect*
• Bewerker	de maatregelen gelden mutatis mutandis voor de bewerker	4.14	C, E, I

een ander.

2.6 Wat zijn passende maatregelen?

Artikel 13 WBP noemt drie criteria die bij de keuze van de te nemen technische en organisatorische maatregelen gebruikt moeten worden:

1. de stand der techniek
   - hierbij wordt allereerst vastgesteld welke technische maatregelen op dat moment beschikbaar zijn;
   - ten aanzien van de aanwezige voorzieningen geldt dat achterhaalde technieken niet langer als passend geclassificeerd kunnen worden;
   - dit betekent dat een verantwoordelijke bij het bepalen van de te nemen technische maatregelen een afstemming moet vinden tussen de technische faciliteiten die in gebruik zijn bij de verwerking en die in gebruik zijn bij de beveiliging van persoonsgegevens;
   - de verantwoordelijke moet deze analyse periodiek herhalen.
2. de kosten van de tenuitvoerlegging
   hier moet de verantwoordelijke een keuze maken tussen de mogelijke technische en organisatorische maatregelen: in alle redelijkheid moet worden afgewogen of er een evenredigheid bestaat tussen de kosten van de beveiliging en het effect daarvan voor de beveiliging van persoonsgegevens;

3. de risico's die de verwerking met zich meebrengen
   hier wordt vastgesteld welk risico de betrokkene c.q. de verantwoordelijke lopen bij verlies of onrechtmatige verwerking van persoonsgegevens: naarmate het risico toeneemt zullen de maatregelen evenredig verzwaard moeten worden.

Bij de schriftelijke behandeling van de WBP in de Eerste Kamer werd door de minister van Justitie het volgende antwoord gegeven op de vraag welke maatregelen nu als passend kunnen worden beschouwd:

'Er kunnen geen algemene uitspraken worden gedaan over wat als een «passende beveiligingsmaatregel» kan worden beschouwd. Dit is namelijk afhankelijk van een aantal factoren. Het begrip «passend» duidt er op dat de maatregelen in overeenstemming dienen te zijn met de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Met andere woorden de te nemen maatregelen moeten worden afgestemd op de risico's van onrechtmatige verwerking die zich in de betrokken organisatie voordoen, waarbij tevens rekening dient te worden gehouden met de stand van de techniek en de kosten om de betrokken maatregelen ten uitvoer te brengen. Dit criterium moet in het licht van de concrete omstandigheden worden ingevuld en is voor een deel dynamisch. Het vereiste niveau van bescherming is hoger naarmate er meer mogelijkheden voorhanden zijn om dat niveau te waarborgen. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico voor de persoonlijke levenssfeer van betrokkenen inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd deze als «passend» moeten worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist. Met zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt.'

Bij het maken van de keuzes dient de verantwoordelijke te zoeken naar een balans tussen de benoemde criteria. Indien er met inachtneming daarvan een gemotiveerde keuze is gemaakt, is er sprake van een stelsel van passende technische en organisatorische maatregelen. Bij twijfel dient de vastgestelde risicoklasse sturend te zijn.

2.7 Privacy-Enhancing Technologies

Bij de behandeling van de Wet bescherming persoonsgegevens in de Tweede Kamer is kamerbreed de motie Nicolaï[2] aangenomen. Hierin wordt de regering opgeroepen in haar eigen systemen voor de verwerking van persoonsgegevens PET toe te passen.

Definitie

Privacy-Enhancing Technologies (PET) zijn een samenhangend geheel van ICT maatregelen dat de persoonlijke levenssfeer (conform de richtlijn 95/46/EG en de WBP) beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem.

[2] Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31

Wettelijke basis

Artikel 13 WBP vormt de grondslag van de inzet van Privacy-Enhancing Technologies.

Dit artikel schrijft voor, dat degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen:

- tegen verlies;
- tegen enige vorm van onrechtmatige verwerking.

PET biedt niet alleen de mogelijkheid om passende technische maatregelen te nemen, maar ook een structurele oplossing voor het juist toepassen van de WBP.

Bovendien geldt voor persoonsgegevens, conform dit artikel, dat de maatregelen dienen te voorkomen de:

- onnodige verzameling;
- onnodige verdere verwerking.

Deze maatregelen worden gewogen aan de hand van de criteria:

- stand der techniek;
- kosten;
- risico's zowel van de verwerking, als ook van de aard[3] en de omvang[4] van de persoonsgegevens.

Daar waar technische maatregelen niet voldoende of niet haalbaar zijn, kunnen organisatorische maatregelen genomen worden of kunnen organisatorische maatregelen de technische ondersteunen in een samenhangend stelsel van maatregelen.
Wanneer als onderdeel van een evenwichtig verwerkingsbeleid, de keuze bestaat tussen een organisatorische en een technische voorziening, geeft de toezichthouder de voorkeur aan de laatste. Technische maatregelen zijn doeltreffender omdat het moeilijker is aan het effect ervan te ontkomen.

Bij de schriftelijke behandeling[5] van de WBP in de Eerste Kamer antwoordde de minister van Justitie:

'dat de tegenwoordige informatietechnologische mogelijkheden om persoonsgegevens te misbruiken, noodzaken om te zien naar aanvullende mogelijkheden om een behoorlijke en zorgvuldige omgang met persoonsgegevens te waarborgen. Hierbij kan gedacht worden aan gedeeltelijke of algehele anonimisering, bijvoorbeeld door persoonsgegevens te ontdoen van identificerende kenmerken of door deze af te schermen voor bepaalde toepassingen of gebruikers of om het gebruik tot bepaalde doeleinden te beperken.
In deze lijn is bij amendement 22 van de Tweede Kamer artikel 13 van het wetsvoorstel aangevuld in die zin dat de voorgeschreven beveiligingsmaatregelen er mede op moeten zijn gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
Daarmee is de wettelijke basis gegeven voor de toepassing van Privacy-Enhancing Technologies (PET). Dit soort regels sluiten aan bij de zich ontwikkelende informatietechnologie.'

[3] Onder het begrip 'aard' wordt begrepen de verscheidenheid aan attributen en het aantal bronnen van die attributen die per betrokkene verwerkt worden.
[4] Onder het begrip 'omvang' wordt begrepen het aantal betrokkenen waarover persoonsgegevens worden verwerkt.
[5] Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 92c.

Gezien de wettelijke verplichting tot het toepassen van Privacy-Enhancing Technologies publiceert de Registratiekamer naast het rapport 'Privacy-Enhancing Technologies - The path to anonymity', een brochure 'Mag het een bitje minder zijn?'.

2.8 Toezicht

Het CBP kan de verantwoordelijke en de bewerker aanspreken op het niveau van de maatregelen voor de beveiliging van de verwerking van persoonsgegevens en de wijze waarop het stelsel van deze 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).

Het CBP heeft het recht om inlichtingen in te winnen en te vorderen bij de verantwoordelijke en de eventuele bewerker(s). Voorts kan het zich toegang verschaffen tot plaatsen waar persoonsgegevens worden verwerkt. Op grond van een dergelijk onderzoek heeft het CBP de mogelijkheid om uiteindelijk dwingende maatregelen te treffen.

2.9 Juridische status

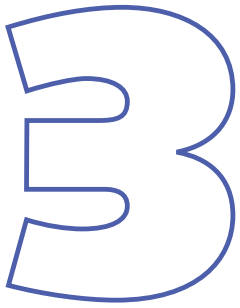
Deze Achtergrondstudie en Verkenning 'Beveiliging van persoonsgegevens' van de Registratiekamer geeft een normatief kader voor de concrete invulling van maatregelen en procedures ten aanzien van de beveiliging van persoonsgegevens tegen verlies of tegen onrechtmatige verwerking (privacy eis 7: Beveiliging, uit het Raamwerk Privacy Audit).

Deze studie is gebaseerd op het bepaalde in artikel 13 WBP en geeft richting aan hoe de verantwoordelijke met de beveiliging van persoonsgegevens dient om te gaan.

Deze studie is tevens een uitgangspositie voor de privacy auditor voor het bepalen in hoeverre de beveiliging adequaat is ingevuld.

Vanuit het Raamwerk Privacy Audit wordt naar deze studie verwezen.

Niveaus voor de beveiliging van persoonsgegevens



3 Niveaus voor de beveiliging van persoonsgegevens

In artikel 13 WBP staat dat persoonsgegevens moeten worden beveiligd tegen verlies of tegen enige vorm van onrechtmatige verwerking. Een ontoereikende beveiliging van persoonsgegevens kan leiden tot ongewenste gevolgen voor de persoonlijke levenssfeer van één of meer betrokkenen. De verantwoordelijke en de bewerker van de persoonsgegevens kunnen aansprakelijk worden gesteld voor de door de betrokkene(n) geleden schade.

Een adequaat niveau van beveiliging van persoonsgegevens kan worden bereikt door het treffen van een stelsel van technische en organisatorische maatregelen. Bij de beveiliging van persoonsgegevens is het belangrijk dat de te treffen maatregelen worden afgestemd op bedreigingen die realistisch zijn gezien de aard van de persoonsgegevens in relatie tot de omvang en de verwerkingen daarvan. Hierdoor kan het risico van verlies of onrechtmatige verwerking tot een aanvaardbaar niveau worden beperkt. Het risico kan worden gezien als het product van de kans op ongewenste gevolgen en de schade die het intreden van die gevolgen kan veroorzaken voor de betrokkene, de verantwoordelijke of de bewerker.

Wanneer het risico van ongewenste gevolgen en de schade die daaruit voortvloeit groot is, zullen hogere eisen worden gesteld aan de kwaliteit van het stelsel van algemene maatregelen en van de andere beveiligingseisen die vanuit de Wet bescherming persoonsgegevens worden gesteld dan bij een klein risico. De invulling van het beveiligingsniveau is dan ook afhankelijk van diverse aspecten die deels worden bepaald door de organisatie zelf en deels door de aard, het doel, het gebruik en de omvang van de persoonsgegevens, de invloed daarvan op de maatschappelijke positie van de betrokkene en de schade die de organisatie leidt door een onrechtmatige verwerking van persoons-gegevens. In de paragraaf 3.1 zullen deze aspecten nader worden toegelicht. De aanbevolen methode voor het bepalen van het beveiligingsniveau is beschreven in paragraaf 3.2. Toepassing van deze methode leidt tot een indeling van de te beoordelen verwerking van persoonsgegevens in een risicoklasse. De indeling in klassen bepaalt het niveau van de normen weergegeven per risicoklasse die de verantwoordelijke of de bewerker (in opdracht van de verantwoordelijke) moet hanteren voor de beveiliging van persoonsgegevens. De beschrijving van de klassen is gegeven in paragraaf 3.3. De eisen voor de beveiliging van persoonsgegevens in elk van de klassen zijn weergegeven in hoofdstuk 4. Het is aan te raden om een methode toe te passen waarbij de *risicoklasse* wordt vastgesteld en waar over besluiten ten aanzien van maatregelen verantwoording kan worden afgelegd, en dit in relatie tot de hier gedefinieerde risicoklasse en het daarbij passende stelsel van maatregelen en procedures.

Deze methode wordt ook gebruikt bij het uitvoeren van de onderzoeken ex artikel 60 WBP (zie paragraaf 2.7).

3.1 Aspecten die het niveau van beveiliging beïnvloeden

Verwerking van persoonsgegevens vindt plaats binnen verschillende sectoren, markten, culturen en landen. De maatregelen die moeten worden getroffen voor de vereiste beveiliging van persoonsgegevens zullen dus sterk variëren. In dit hoofdstuk is een beschrijving opgenomen van een aantal belangrijke aspecten dat het beveiligingsniveau beïnvloedt:

- de betekenis van de te verwerken persoonsgegevens binnen het maatschappelijk verkeer;
- het bewustzijn binnen een organisatie ten aanzien van (informatie)beveiliging van persoonsgegevens en privacybescherming;
- de ICT infrastructuur waarin de persoonsgegevens worden verwerkt.

Uiteraard dient een organisatie attent te zijn op de zich wijzigende normen binnen het maatschappelijk verkeer en daarop tijdig in te spelen met adequate beveiligingsmaatregelen.

Betekenis van de te verwerken persoonsgegevens binnen het maatschappelijk verkeer

De invloed die de aard van de persoonsgegevens in combinatie met de omvang, het doel, het gebruik en de verwerking kan hebben op de positie van een betrokkene in de maatschappij, bepaalt mede welke eisen aan de beveiliging van persoonsgegevens dienen te worden gesteld. In artikel 16 WBP wordt een aantal soorten persoonsgegevens aangeduid als zogenaamde 'bijzondere persoonsgegevens':

> *De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.*

Deze persoonsgegevens genieten een bijzondere rechtsbescherming (artikel 17 tot en met 23 WBP) en vereisen daardoor een hoger niveau van beveiliging dan de overige persoonsgegevens.

Naast deze via de WBP aangewezen bijzondere persoonsgegevens kunnen ook de overige persoonsgegevens in combinatie met de omvang, het doel en het gebruik een verhoogde gevoeligheidsgraad hebben. Voor veel mensen is het immers onwenselijk dat gegevens omtrent hun financiële positie, erfrechtelijke aspecten of arbeidsprestaties bekend raken bij anderen. Naarmate de gevoeligheid toeneemt zal ook de beveiliging van de overige persoonsgegevens op een hoger niveau gerealiseerd moeten worden.

Bewustzijn binnen een organisatie

De mate waarin de organisatie doordrongen is van de noodzaak van beveiliging in het algemeen en van de noodzaak om zorgvuldig met persoonsgegevens om te gaan in het bijzonder, bepaalt mede de effectiviteit van het getroffen stelsel van maatregelen en procedures.

Als dat bewustzijn niet of nauwelijks aanwezig is of in stand wordt gehouden zullen de genomen technische en organisatorische maatregelen veelal slechts ten dele effectief zijn.

ICT infrastructuur waarin de persoonsgegevens worden verwerkt

Nagenoeg alle persoonsgegevens worden tegenwoordig geautomatiseerd verwerkt. De gebruikte informatie- en communicatietechnologie (ICT) verschilt echter qua gebruik, complexiteit, mogelijkheden en zal ook met de stand der techniek variëren. Onderstaande punten moeten in relatie tot het bepalen van de risicoklasse in beschouwing worden genomen bij het definiëren van het toereikend niveau van de te nemen beveiligingsmaatregelen:

- de eigenschappen en organisatorische plaats van de computerapparatuur: personal of netwerk computer, client-server architectuur, mainframe, toepassingssoftware, etc;
- de netwerken waarover wordt gecommuniceerd: intranet, extranet, internet etc. en de wijze waarop de verbindingen tussen de werkstations en de (externe) netwerken zijn gerealiseerd;
- de database en data retrieval technologieën die worden gebruikt voor de verwerking van persoonsgegevens;
- de media waarop persoonsgegevens of toegangscodes tot die persoons-gegevens worden opgeslagen;
- de samenhang / architectuur van de geautomatiseerde verwerking van persoonsgegevens en de daarvoor in te richten processen.

Van invloed op het bepalen van de risicoklasse is ook de informatiewaarde van de te verwerken persoonsgegevens. De informatiewaarde wordt bepaald door de aard van de gegevens in combinatie met de omvang en het gebruik, maar tevens door de complexiteit van de verwerking van persoonsgegevens.

De complexiteit kan worden afgemeten aan het aantal persoonsgegevens dat over één persoon bekend is, of aan het aantal personen waarover gegevens zijn vastgelegd.

Ingeval er veel gegevens over een persoon bekend zijn, bijvoorbeeld via een verzameling van persoonsgegevens uit diverse niet samenhangende systemen, zal het beeld over die persoon gedetailleerder zijn. Het risico voor de betrokkene bestaat er dan uit dat veel persoonsgegevens over hem of haar bekend kunnen worden bij van onrechtmatige verwerkingen.

Als het aantal personen in een verwerking van persoonsgegevens groot is, bestaat het risico vooral uit het aantal personen dat kan worden geschaad indien de persoonsgegevens onzorgvuldig of onrechtmatig worden verwerkt.

3.2 Bepaling van de risicoklasse van persoonsgegevens

Aan de bepaling van de risicoklasse van persoonsgegevens hoort een analyse vooraf te gaan waarin de verantwoordelijke bepaalt welk risico aan de verwerking van persoonsgegevens is verbonden.

In de beschrijving van deze analyse wordt aangenomen dat er al eerder is vastgesteld dat er sprake is van een rechtmatige verwerking van persoonsgegevens.

Een dergelijke analyse kent een aantal stappen:

1. het inventariseren van de processen waarin persoonsgegevens worden verwerkt (artikel 1 onder b WBP);
2. het vaststellen van de aard van de persoonsgegevens in combinatie met de omvang en het gebruik. De evaluatie dient mede aan de hand van de WBP plaats te vinden: gegevens die in de WBP als bijzondere persoonsgegevens worden aangemerkt, leveren een hoger risico op (artikel 16 WBP; zie paragraaf 3.1);
3. het inventariseren van de mogelijke vormen van onbevoegde of onzorgvuldige verwerking van de gegevens, zoals: verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking (zie schema in paragraaf 2.5);
4. het bepalen van de risicoklasse. Dit is het product van de kans op ongewenste gevolgen van de kans op ongewenste gevolgen en de schade die dit kan veroorzaken voor de betrokkene, de verantwoordelijke of de bewerker. Hierbij moet worden uitgegaan van situaties die redelijkerwijs te verwachten zijn.

De laatste stap van deze analyse, toegepast op persoonsgegevens, levert een risico op. De gevonden factor bepaalt de mate van risico van de gegevens. Er worden verschillende risicoklassen onderscheiden. Elke klasse kent een bijbehorend niveau van beveiliging.

3.3 Risicoklassen

In de vorige paragraaf kwam de risicobepaling aan de orde. In deze paragraaf wordt deze analyse gebruikt om de verwerking van persoonsgegevens in te delen in een zogenaamde risicoklasse. Verwerkingen van persoonsgegevens met een vergelijkbaar risico worden in dezelfde klasse ingedeeld. De in deze studie, voor een klasse gedefinieerde normen voor beveiliging gelden als een (minimaal) uitgangspunt voor de te nemen maatregelen. De feitelijk te bepalen specifieke maatregelen moeten worden afgeleid uit de voor die klasse gedefinieerde eisen voor beveiligingsmaatregelen. Gezien het accent dat in deze studie wordt gelegd op het kwaliteitsaspect *exclusiviteit,* hebben de beschreven maatregelen primair op dit aspect betrekking. De andere kwaliteitsaspecten zijn min of meer vanzelfsprekend omdat er vanuit wordt gegaan dat deze in het kader van goed huisvaderschap noodzakelijk zijn.

Er wordt uitgegaan van vier ‘risicoklassen’. De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij die hogere risicoklasse:

- risicoklasse 0 publiek niveau;
- risicoklasse I basis niveau;
- risicoklasse II verhoogd risico;
- risicoklasse III hoog risico.

De verantwoordelijke komt tot een afweging in welke risicoklasse de gegevens vallen. In alle gevallen moet de verantwoordelijke op grond van een grondige analyse kiezen voor een bepaalde risicoklasse en het daarbij behorende beveiligingsniveau. Deze analyse moet toetsbaar zijn en hierover moet verantwoording kunnen worden afgelegd.

Vrijstellingsbesluit

Artikel 27 WBP verplicht de verantwoordelijke elke verwerking van persoonsgegevens bij het CBP te melden. Op grond van artikel 29 WBP is er een Vrijstellingsbesluit waarin is bepaald welke verwerking van persoonsgegevens vrijgesteld zijn van deze melding. Een verantwoordelijke kan een beroep doen op dit artikel en daarmee hoeft die verwerking van persoonsgegevens niet bij het CBP gemeld te worden.

Het niet hoeven melden van een verwerking van persoonsgegevens betekent niet dat die verwerking van persoonsgegevens niet onder de reikwijdte van de WBP valt. Artikel 13 WBP blijft van toepassing en dus ook het vaststellen van de risicoklasse als basis voor de te nemen beveiligingsmaatregelen.

Indien een beroep gedaan wordt op de genoemde vrijstelling tot melden geeft het Vrijstellingsbesluit nadere wettelijke eisen voor de betrokken verwerking van persoonsgegevens.

Risicoklasse 0: Publiek niveau

Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. De persoonsgegevens behoeven ten aanzien van de exclusiviteit van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Als gevolg van de Wet bescherming persoonsgegevens worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld dan welke al noodzakelijk zijn voor een zorgvuldige bedrijfsvoering.

In deze studie zijn voor deze risicoklasse dan ook geen specifieke maatregelen opgenomen.

Risicoklasse I: Basis niveau

De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.

Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer.

Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan dient de beveiliging van persoonsgegevens tenminste te worden ondergebracht in risicoklasse II.

Risicoklasse II: Verhoogd risico

De uitkomst van de analyse toont aan dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De te nemen (informatie)beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basis niveau.

In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkene);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.

Soms moet de verwerking van bijzondere gegevens vanwege een hoge gevoeligheidsgraad in het maatschappelijk verkeer, bijvoorbeeld wanneer het gegevens over levensbedreigende ziektes betreft, ondergebracht worden in risicoklasse III.

Risicoklasse III: Hoog risico

Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren dat het gerechtvaardigd is deze verwerking van persoonsgegevens in risicoklasse III te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen.

De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt. Bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse.

Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse. Deze geheimhoudingsplicht kan zowel wettelijk of anderszins formeel zijn geregeld door de overheid of door een private organisatie zijn ingevoerd voor haar medewerkers.

In relatie tot de indeling van persoonsgegevens in risicoklassen, wordt ook in het kader van een bewuste omgang met die persoonsgegevens, gebruik gemaakt van markering. Markering is het aangeven van de risicoklasse die van toepassing is op de persoonsgegevens die op deze gegevensdrager zijn vastgelegd. De gegevensdrager wordt dus, indien technisch mogelijk, voorzien van een redelijkerwijs zichtbaar kenmerk dat aangeeft hoe de persoonsgegevens

op die drager behandeld dienen te worden. Gegevensdragers zijn alle media waarin of waarop de persoonsgegevens kunnen worden vastgelegd, zoals papier, CD-ROM's, diskettes en tapes, schijven en intern geheugen.

De functie van markering is dat de risicoklasse van de persoonsgegevens direct zichtbaar is. Hierop dienen de maatregelen voor het bewaren en gebruik van de gegevensdragers te worden afgestemd.

Markering van persoonsgegevens tot en met risicoklasse II is optioneel. Markering van de persoonsgegevens behorende bij risicoklasse III is noodzakelijk.

Schema voor het bepalen van de risicoklasse

De onderlinge relatie tussen de risicoklassen is in onderstaand schema weergegeven.

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	*Aard van de verwerking*		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**	

Dit model illustreert de gegeven tekst voor het bepalen van de risicoklasse die van toepassing is op een verwerking van persoonsgegevens.

Beveiliging van persoonsgegevens in de praktijk

4 Beveiliging van persoonsgegevens in de praktijk

In dit hoofdstuk worden de eisen die gesteld worden aan de beveiliging van persoonsgegevens weergegeven. Deze zijn gerelateerd aan de risicoklasse die aan de betreffende verwerking van persoonsgegevens is toegekend op basis van de uitgevoerde analyse (hoofdstuk 3).

Er wordt verondersteld dat voor alle klassen al toereikende maatregelen met betrekking tot de kwaliteitsaspecten *integriteit* en *continuïteit* zijn genomen.

Verder wordt opgemerkt dat in deze studie slechts beperkt aandacht wordt besteed aan het stelsel van maatregelen en procedures met betrekking tot fysieke beveiliging. Laat het duidelijk zijn dat het op zijn plaats hebben van voldoende maatregelen op het terrein van fysieke beveiliging, de verantwoordelijke niet ontslaat van de verplichting tot het nemen van de noodzakelijke maatregelen in het kader van logische beveiliging. Voor het overige wordt verwezen naar de veelvuldig in de vaklitteratuur voorkomende checklists rond het onderwerp van de fysieke beveiliging.

In het voorgaande hoofdstuk zijn vier risicoklassen onderscheiden. In dit hoofdstuk worden de beveiligingseisen per klasse weergegeven. Voor risicoklasse 0, het publiek niveau, zijn geen bijzondere maatregelen noodzakelijk omdat de gegevens in beginsel voor iedereen toegankelijk zijn. Risicoklasse I, het basis niveau, bevat de eisen waaraan de beveiliging van persoonsgegevens die niet in risicoklasse 0 vallen, moet voldoen. Voor zover van toepassing, zijn onder risicoklasse II en risicoklasse III de *cumulatieve* eisen ten opzichte van risicoklasse I respectievelijk risicoklasse II geformuleerd waaraan de beveiliging moet voldoen. De eisen in de risicoklassen zijn zodanig geformuleerd dat de te treffen maatregelen afgestemd kunnen worden op de specifieke omstandigheden in de betreffende organisatie.

De verantwoordelijke dient er voor te zorgen dat het niveau van de beveiliging van de persoonsgegevens overeenkomt met de eisen die in dit hoofdstuk worden gepresenteerd. Als er sprake is van een bewerker in de zin van de wet (artikel 14 WBP; zie hoofdstuk 2), dient de verantwoordelijke die bewerker te instrueren over de wijze waarop de persoonsgegevens moeten worden beveiligd. Bij de uiteindelijke keuze van het stelsel van algemene maatregelen kunnen de ‘state of the art’, de kosten van de maatregelen en de continuïteit van bepaalde voorzieningen een grote rol spelen. De verantwoordelijke dient een evenwichtige afweging te maken tussen deze factoren en het belang van de beveiliging van de persoonsgegevens en hij dient deze afweging te documenteren. Het uit deze afweging voortvloeiende beveiligingsstelsel behoort permanent een evenwichtig stelsel van zowel technische als organisatorische maatregelen te zijn.

4.1 Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. Daarvoor moet het management een beleid vaststellen dat aangeeft welke eisen er worden gesteld aan de informatiebeveiliging in het algemeen en aan de beveiliging van persoonsgegevens in het bijzonder. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid. Ook moet worden vastgesteld of de maatregelen door de medewerkers worden nageleefd. Gegeven zowel de veranderende maatschappelijke relevantie als de technisch organisatorische bedreigingen en mogelijke beveiligingsmaatregelen, is het nodig dat het management regelmatig het beleid evalueert en zonodig herziet. Bovendien is het van groot belang dat het management zich duidelijk achter dit beleid opstelt, een voorbeeldfunctie vervult en de medewerkers informeert en motiveert om het beleid actief gestalte te geven.

In principe moet voor informatiebeveiliging een lange termijn beleid worden ontwikkeld, moet er een implementatieplan voor de middellange termijn en een stelsel van maatregelen en procedures voor de dagelijkse praktijk zijn. De beveiliging van persoonsgegevens moet onderdeel uitmaken van dit beleid. Voor kleinere organisaties zal deze opzet wellicht te uitvoerig zijn en zal een andere vorm worden gekozen. Het belangrijkste is dat daarbij de uitgangspunten en de praktische uitvoering duidelijk worden vastgelegd en regelmatig worden bezien op de actualiteit. De naleving van beleidsuitgangspunten moet regelmatig worden gecontroleerd. Er moeten duidelijke afspraken worden gemaakt over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures.

Risicoklasse I

Beleid

Het management van een organisatie stelt het informatiebeveiligingsbeleid inclusief dat terzake van de beveiliging van persoonsgegevens vast en draagt dit beleid uit binnen de organisatie.

In het informatiebeveiligingsbeleid worden de volgende onderwerpen opgenomen:

- een definitie van de term informatiebeveiliging, de doelstellingen en het belang van de informatiebeveiliging als een instrument voor het realiseren van de zorgvuldige en effectieve maatregelen met betrekking tot een betrouwbare, continue en exclusieve verwerking van persoonsgegevens;
- de organisatie van de informatiebeveiligingsfunctie, waaronder de verantwoordelijkheden, taken en bevoegdheden voor alle aspecten van informatiebeveiliging en de verantwoordelijkheid ervoor bij het management;
- een verplichting voor het management om de implementatie van de procedures en maatregelen in de organisatie te realiseren en te beheren;
- de wijze waarop het beveiligingsbewustzijn vanuit het management wordt overgedragen aan de organisatie en het instandhouden ervan;

- de onafhankelijke beoordeling van de toereikendheid van het beleid, alsmede de tactische en operationele uitvoering daarvan;
- het nakomen van wettelijke en contractuele verplichtingen.

Medewerkers worden expliciet geïnformeerd over de aanwezigheid en het gebruik van persoonsgegevens die worden gegenereerd in het kader van de uitvoering van en de controle op de naleving van de maatregelen voor informatiebeveiliging (bewustzijn). Vertrouwelijke informatie omtrent de naleving en handhaving van de beveiligingsmaatregelen mag niet in handen komen van een niet-geautoriseerde ontvanger[6].

Regelmatig rapporteert de daarvoor aangewezen persoon aan de hoogste autoriteit (de verantwoordelijke in de termen van de WBP) in de organisatie over de naleving van het beleid van de beveiliging van persoonsgegevens en de invulling daarvan binnen de organisatie.

Implementatie

De verantwoordelijke zorgt er voor dat invulling wordt gegeven aan het beleid voor de beveiliging van persoonsgegevens. Het te schrijven beveiligingsplan bevat de hieronder aangegeven punten. Daarna dient een implementatieplan te worden opgesteld. Hierbij kan onderscheid worden gemaakt tussen een plan voor informatiebeveiliging en, indien de gewijzigde omstandigheden daartoe aanleiding geven, een plan voor een bepaalde planperiode.

Kleinere organisaties kunnen wellicht volstaan met een vereenvoudigde vorm van een dergelijk plan.

Bij het opstellen van een beveiligingsplan wordt aandacht besteed aan:

- het verankeren van de activiteiten voor beveiliging van persoonsgegevens in de dagelijkse werkzaamheden van de medewerkers van de organisatie;
- de methoden en technieken waarmee wordt vastgesteld dat de ingevoerde maatregelen en procedures voor beveiliging voldoen aan het beveiligingsbeleid van de organisatie;
- de frequentie waarmee de controles op handhaving en naleving plaatsvinden;
- het aangeven van gebieden waarop specialistisch advies binnen de organisatie noodzakelijk is en de wijze waarop dit specialistisch advies wordt georganiseerd;
- de zorg voor een voldoende kennisniveau van het personeel;
- de wijze waarop het beleid, het plan en de te nemen maatregelen ten aanzien van de beveiliging van persoonsgegevens, worden gecommuniceerd naar de medewerkers in de organisatie, de klanten, de leveranciers en overige derden;
- de wijze waarop incidenten en inbreuken op de beveiliging van persoonsgegevens worden gemeld en afgehandeld.

[6] Artikel 1 onder h WBP; ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

Bij het opstellen van een plan voor een bepaalde periode wordt aandacht besteed aan:

- het uitvoeren van een analyse voor elke verwerking van persoonsgegevens om te bepalen in welke risicoklasse de persoonsgegevens moeten worden opgenomen;
- het tijdspad waarbinnen het plan moet worden uitgevoerd;
- het definiëren van de functies en verantwoordelijkheden voor de uitvoering van het plan.

Stelsel van maatregelen en procedures

De manager onder wiens gedelegeerde verantwoordelijkheid het dagelijkse beheer van de verwerking van persoonsgegevens plaatsvindt, legt de benodigde maatregelen en procedures voor beveiliging van persoonsgegevens vast, implementeert deze en draagt deze uit. Het handhaven respectievelijk naleven van de maatregelen en procedures wordt volgens een van tevoren vastgesteld schema gecontroleerd.

De taken van de verantwoordelijke manager omvatten ten minste:

- het beschrijven van de maatregelen en procedures voor het beveiligen van de verwerking van persoonsgegevens conform het beveiligingsbeleid en -plan;
- het schriftelijk vastleggen van de maatregelen en procedures voor het beveiligen van persoonsgegevens;
- het actualiseren van de verantwoordelijkheden, bevoegdheden en taken van de betrokken medewerkers;
- een programma ter stimulering van het privacybewustzijn rond het verwerken van persoonsgegevens;
- het toezicht houden op de handhaving en naleving van de maatregelen en procedures.

Risicoklasse II

Het te voeren beleid houdt rekening met de bijzondere eisen die voortvloeien uit deze klassen. Het beleid heeft een sterk preventief karakter en draagt zorg voor tijdig handelen bij het detecteren en voorkomen van echte bedreigingen alsmede het treffen van corrigerende maatregelen gericht op:

- het aanpassen van beleid, implementatie en het stelsel van maatregelen en procedures;
- het herstel van fouten.

Risicoklasse III

Hier worden geen extra maatregelen of procedures vereist.

4.2 Administratieve organisatie

Onder administratieve organisatie wordt verstaan: het geheel van maatregelen met betrekking tot het systematisch verwerken van gegevens gericht op het verstrekken van informatie ten behoeve van het besturen en doen functioneren van de organisatie, alsmede ten behoeve van de verantwoording die daarover moet worden afgelegd.

Voor een effectieve informatiebeveiliging is het nodig dat de maatregelen en procedures op een gestructureerde manier worden beschreven. Ook is het belangrijk dat deze worden herzien als gewijzigde omstandigheden daartoe aanleiding geven. Hierbij wordt steeds gecontroleerd of de procedures en maatregelen nog goed aansluiten bij de dagelijkse praktijk. Een ander belangrijk aspect van de administratieve organisatie is het vastleggen van de verantwoordelijkheden voor de informatiebeveiliging en gegevens-verwerking.

Risicoklasse I

De richtlijnen met betrekking tot de administratieve organisatie betreffende het beheer van de verwerking van persoonsgegevens worden expliciet vastgelegd.

Bij wijzigingen van het stelsel van maatregelen en procedures voor de beveiliging van persoonsgegevens, wordt de beschreven administratieve organisatie overeenkomstig aangepast.

De inrichting van de technische maatregelen sluit aan op de organisatorische maatregelen voor de beveiliging van de persoonsgegevens zoals die in het beveiligingsplan zijn weergegeven.

De verantwoordelijkheid voor het onderhouden van de beschrijving van de administratieve organisatie wordt expliciet toegewezen.

Risicoklasse II

Alle taken, bevoegdheden en verantwoordelijkheden binnen de organisatie voor het beheer van de persoonsgegevens worden expliciet vastgelegd.

Nadrukkelijk dient er voor gewaakt te worden dat taken betrokken bij de uitvoering en bij de controle daarop, niet door dezelfde medewerker worden uitgevoerd (functiescheiding).

Binnen de organisatie is er een beveiligingsfunctionaris die regelmatig aan de verantwoordelijke rapporteert.

Risicoklasse III

De inrichting van de organisatie voorziet in procedures om snel te kunnen reageren op ontwikkelingen die nieuwe maatregelen vereisen.

4.3 Beveiligingsbewustzijn

Het bewustzijn van medewerkers op elk niveau binnen de organisatie over de noodzaak van beveiliging en van de zorgvuldige verwerking van persoonsgegevens, is de belangrijkste voorwaarde om een stelsel van algemene maatregelen en procedures voor beveiliging effectief te laten functioneren. De mens vormt immers vaak de zwakste schakel in de beveiligingsketen. Het goed bedoeld helpen van een collega door het uitlenen van een toegangscode, het vergeten om afgedrukte stukken op te halen, het onbeheerd achterlaten van opengeslagen documenten of computersystemen waarop is ingelogd, zijn voorbeelden hiervan. Deze voorbeelden geven aan hoe de *exclusiviteit* van de persoonsgegevens kan worden aangetast.

Beveiliging van persoonsgegevens heeft geen effect als deze alleen maar op papier bestaat. De beveiligingsmaatregelen zullen daadwerkelijk door de medewerkers moeten worden uitgevoerd en alle medewerkers moeten hun bijdrage daaraan leveren. Om dit te bereiken moet aandacht worden besteed aan het vergroten of op peil houden van het beveiligingsbewustzijn. Dit moet continu gebeuren en er zijn verschillende manieren om dit te doen. Uiteraard moeten alle medewerkers regelmatig op de hoogte worden gehouden van de afgesproken maatregelen en procedures voor de beveiliging van persoonsgegevens. Dat kan schriftelijk, maar ook door middel van instructies, voorlichting of door het onderwerp aan de orde te brengen in periodiek werkoverleg, bij werkevaluaties of beoordelingsgesprekken. Het moet daarbij duidelijk zijn dat beveiliging van persoonsgegevens niet vrijblijvend is. Controle op de handhaving en de naleving is belangrijk. Er moeten sancties staan op het niet naleven van deze regels en dat moet aan alle medewerkers duidelijk gemaakt worden.

Risicoklasse I

Alle werknemers, inclusief de tijdelijke werknemers, worden geïnstrueerd over het informatiebeleid inzake het beveiligen van persoonsgegevens. Het beleid en de daarbij behorende maatregelen en procedures worden schriftelijk verstrekt of on-line beschikbaar gesteld.

De gebruikers nemen kennis van het stelsel van beveiligingsmaatregelen en -procedures op het gebied van de beveiliging van persoonsgegevens en leren op correcte wijze om te gaan met onderdelen van de ICT infrastructuur waarmee zij in aanraking komen.

Bij trainingen voor informatiesystemen en beveiligingsmaatregelen op het gebied van de beveiliging van persoonsgegevens worden uitsluitend gegevens van niet bestaande personen gebruikt.

Passende disciplinaire maatregelen worden genomen bij het doorbreken van de geheimhoudingsplicht of het niet correct uitvoeren van de maatregelen en procedures.

Gedurende functioneringsgesprekken en beoordelingen komt het onderwerp beveiliging van persoonsgegevens aan de orde.

Risicoklasse II

De verantwoordelijkheden van de medewerkers voor het beveiligen van persoonsgegevens worden expliciet in de functieomschrijving of het arbeidscontract opgenomen.

De verantwoordelijke medewerkers rapporteren de opgetreden beveiligingsincidenten direct aan hun manager en aan de voor de beveiliging van persoonsgegevens verantwoordelijke functionaris, indien deze laatste is benoemd.

Regelmatig worden de medewerkers geïnstrueerd over beveiligingseisen en zij worden opgeleid of bijgeschoold om de maatregelen en procedures correct te kunnen uitvoeren.

Risicoklasse III

Regelmatig informeren de verantwoordelijke medewerkers hun manager en de functionaris die verantwoordelijk is voor de beveiliging (indien die is benoemd), over het niveau van beveiligingsbewustzijn van de medewerkers.

Bij het in dienst treden dient expliciet een geheimhoudingsverklaring getekend te worden.

4.4 Eisen te stellen aan personeel

Er is altijd een risico dat persoonsgegevens op een onzorgvuldige manier worden verwerkt. Het risico komt ook van buiten de organisatie, maar de grootste risico's bevinden zich binnen de organisatie. Het is mogelijk dat een medewerker, al dan niet met opzet, onzorgvuldig met persoonsgegevens omgaat. Om dit risico te beperken is het belangrijk dat hiermee al bij de werving en selectie van personeel rekening wordt gehouden. Beveiliging van persoonsgegevens moet worden besproken bij het aannemen van medewerkers die bij het uitoefenen van hun werkzaamheden met persoonsgegevens omgaan. Vaak zal het ook nodig zijn om inlichtingen in te winnen over de nieuwe medewerkers. Waar nodig en waar mogelijk zal een verklaring omtrent het gedrag worden vereist. In andere gevallen is een antecedentenonderzoek verplicht.

In functieomschrijvingen moet de verantwoordelijkheid voor de beveiliging van persoonsgegevens worden opgenomen. Bij de functieomschrijvingen moet er ook op worden gelet dat een medewerker niet twee taken vervult die onverenigbaar zijn als het gaat om de beveiliging (functiescheiding). In veel gevallen zal een medewerker een geheimhoudingsverklaring moeten tekenen voordat deze toegang krijgt tot persoonsgegevens. Deze plicht tot geheimhouding kan ook in de arbeidsvoorwaarden opgenomen zijn. Voor tijdelijke medewerkers dienen vergelijkbare maatregelen te worden getroffen.

Risicoklasse I

Bij de aanstelling tekenen alle medewerkers die met persoonsgegevens zullen gaan werken een geheimhoudingsverklaring. Dit geldt ook voor tijdelijke medewerkers, bijvoorbeeld via hun contract met het uitzendbureau.
Bij aanstelling van personeelsleden komen de volgende punten aan bod:

- de controle op de juistheid van het curriculum vitae van de sollicitant door het vragen naar bewijsstukken zoals diploma's en getuigschriften;
- de controle van de identiteit door middel van een legitimatiebewijs. Dit is overigens een algemene verplichting ingevolge de Wet op de identificatieplicht.

Risicoklasse II

Tijdelijke medewerkers krijgen onder strikte, schriftelijk overeengekomen, voorwaarden toegang tot verwerkingen van persoonsgegevens.

Risicoklasse III

Nieuwe personeelsleden die persoonsgegevens verwerken moeten een verklaring omtrent het gedrag overleggen.

Bij het inwinnen van referenties komt het gedrag van de sollicitant met betrekking tot het omgaan met persoonsgegevens aan de orde.

Bij organisaties die daarvoor in aanmerking komen op basis van een wettelijke grondslag of ministeriële regeling, maakt ook een betrouwbaarheids- of veiligheidsonderzoek deel uit van de selectieprocedure.
Tijdelijke medewerkers verkrijgen geen toegang tot verwerkingen van persoonsgegevens.

4.5 Inrichting van de werkplek

Informatiebeveiliging betekent vooral het voorkomen dat gegevens (in het algemeen) in handen komen van onbevoegde personen. Dit aspect van beveiliging begint op de werkplek. Met, vaak eenvoudige, maatregelen kan de kans dat onbevoegden toegang krijgen tot persoonsgegevens worden verkleind. Het afsluiten van kasten, kamers en het leeg achterlaten van bureaus zijn voorbeelden van dergelijke maatregelen. Ook is het van belang dat de toegang tot PC's en draagbare computers, waarop persoonsgegevens worden verwerkt, adequaat beveiligd is. Hierbij kan gedacht worden aan de login-procedures met wachtwoordbeveiliging of aan het automatisch uitloggen na een bepaalde periode. Ook moet er op gelet worden dat randapparatuur, zoals printers, niet voor onbevoegden toegankelijk is.

Bijzondere aandacht verdient het werken van medewerkers buiten hun kantoor, bijvoorbeeld het thuiswerken. Verschillende regels, zoals hoe elders omgaan met persoonsgegevens, moeten hier eveneens worden nageleefd. Vooral de beveiliging van netwerkverbindingen is erg belangrijk, zie daartoe paragraaf 4.8 over netwerken en externe verbindingen.

Persoonsgegevens worden getransporteerd via draagbare media. Het is noodzakelijk dat PC's en gegevensdragers (vaak papier, tapes, diskettes, etc.) niet in handen van onbevoegden kunnen komen. Een maatregel hiervoor is het aanbrengen van duidelijke markeringen op de gegevensdragers met persoonsgegevens, waaruit blijkt tot welke risicoklasse de te verwerken persoonsgegevens horen. Voor persoonsgegevens van de hoogste risicoklasse is dit vereist.

Risicoklasse I

De verantwoordelijke stelt maatregelen en procedures vast voor het verwerken van persoonsgegevens. Deze moeten schriftelijk worden vastgelegd en bij alle medewerkers bekend zijn. Hierin wordt minimaal het volgende opgenomen:

- de randapparatuur wordt zodanig opgesteld dat deze onder toezicht staat. Voorkomen moet worden dat de apparatuur wordt gebruikt door onbevoegden, dat de uitvoer van de apparatuur door onbevoegden kan worden gelezen of dat anderszins onbevoegd inzage in persoonsgegevens kan worden verkregen;
- de gegevensdragers mogen niet onbeheerd op een niet veilige plaats achter blijven (clean desk policy);
- de beeldschermen zijn voorzien van een screensaver met wachtwoord waarbij automatisch wordt uitgelogd indien de apparatuur een bepaalde tijd niet gebruikt is.

Risicoklasse II

Bij gebruik van (draagbare) apparatuur inclusief apparatuur die zich buiten de fysiek gecontroleerde omgeving bevindt, bestaat er zekerheid dat de in- en uitvoer van persoonsgegevens alleen door de daartoe geautoriseerde ontvanger kan worden geraadpleegd en gewijzigd.

Mobiele apparatuur is voorzien van een betrouwbare toegangscontrole en de persoonsgegevens op die apparatuur worden versleuteld opgeslagen.

Risicoklasse III

Uitsluitend met door de daarvoor verantwoordelijke goedgekeurde apparatuur worden persoonsgegevens verwerkt.

Het kopiëren van documenten met persoonsgegevens wordt door of onder toezicht van de opdrachtgever uitgevoerd. De overbodige en foutieve kopieën worden direct vernietigd. De gedistribueerde kopieën zijn traceerbaar.

Alle gegevensdragers met persoonsgegevens van deze risicoklasse zijn voorzien van een markering waaruit de risicoklasse blijkt.

4.6 Beheer en classificatie van de ICT infrastructuur

Voor de bedrijfsvoering is het belangrijk dat een organisatie de actuele stand bijhoudt van de voorzieningen waarover deze beschikt. Ook voor de beveiliging van persoonsgegevens is een degelijk beheer van de ICT infrastructuur nodig.

Onder de ICT infrastructuur wordt verstaan: computersystemen (mainframe, servers, (PC)clients), computernetwerk, systeemsoftware, toepassingssoftware, gegevensverzamelingen, mensen, documentatie en procedures van toepassing op de verwerking van persoonsgegevens.

Risicoklasse I

In het ontwikkelingstraject van informatiesystemen worden de maatregelen en procedures voor de beveiliging van persoonsgegevens en de controle daarop geïnventariseerd zodat kan worden nagegaan of voldaan wordt aan het informatiebeveiligingsbeleid met betrekking tot de beveiliging van persoonsgegevens. De maatregelen die voortvloeien uit deze inventarisatie moeten bij de ontwikkeling van de software worden geïmplementeerd (ondermeer door het toepassen van PET).

Bij de ontwikkeling en het onderhoud van informatiesystemen worden toereikende procedures voor change management en versiebeheer gevolgd. De beslissingsbevoegdheid in deze procedures ligt bij de verantwoordelijke voor de persoonsgegevens waarvoor de informatiesystemen worden ontwikkeld, onderhouden of geëxploiteerd.

Aan documentatie behorende bij de verwerking van persoonsgegevens worden de volgende eisen gesteld:

- de verwerking van persoonsgegevens, indien niet daarvan vrijgesteld, wordt aangemeld bij het CBP of de functionaris voor de gegevensbescherming (artikel 27 tot en met 30, artikel 62 tot en met 64 WBP);
- de volgende onderwerpen worden tenminste gedocumenteerd: datamodellen, software, datacommunicatieprotocollen, alsmede de onderdelen waaruit het proces van de verwerking van de persoonsgegevens bestaat;
- de toegekende (tijdelijke) bevoegdheden in de organisatie worden in een overzicht bijgehouden .

Voor het ondervangen van calamiteiten, incidenten of problemen met betrekking tot de verwerking van persoonsgegevens (binnen het ICT domein) moeten door of namens de verantwoordelijke goedgekeurde procedures zijn opgesteld. Bij toepassing van deze procedures moeten alle door de gebruiker ondernomen acties worden vastgelegd. Deze vastlegging gebeurt zodanig dat manipulatie van de gegevens niet mogelijk is.

Voor het kunnen ondervangen van incidenten met een verwerking van persoonsgegevens, waarbij de ICT infrastructuur de mogelijke oorzaak kan zijn, is inzicht in het configuration management systeem noodzakelijk.

Risicoklasse II

Bij onderhoud aan apparatuur door derden moet de vertrouwelijke omgang met persoonsgegevens in het contract zijn vastgelegd. De toegankelijkheid van de persoonsgegevens door derden moet zo veel mogelijk beperkt zijn.

Voor het testen van informatiesystemen met persoonsgegevens mogen uitsluitend gegevens van fictieve personen gebruikt worden.

Risicoklasse III

Alle gegevensdragers met persoonsgegevens van deze risicoklasse zijn voorzien van een markering waaruit de risicoklasse blijkt.

4.7 Toegangsbeheer en -controle

Het is vereist dat de organisatie maatregelen en procedures heeft gedefinieerd om te voorkomen dat onbevoegden toegang krijgen tot locaties en informatiesystemen met persoonsgegevens. Wanneer iemand immers met weinig moeite een gebouw kan binnenkomen waar zich persoonsgegevens bevinden, zal het risico op onrechtmatige verwerking sterk toenemen. Fysieke toegangsbeveiliging is daarom noodzakelijk. Dit houdt in dat maatregelen moeten worden getroffen om ruimtes te kunnen afsluiten en om te beheersen wie tot welke ruimtes toegang heeft. Daarnaast moet worden voorkomen dat onbevoegde personen toegang krijgen tot informatiesystemen. De apparatuur en de systemen moeten voorzien zijn van een logische toegangsbeveiliging. Voor de beveiliging van PC's moet op zijn minst gebruik gemaakt worden van wachtwoorden. Vermeden moet worden dat deze wachtwoordbeveiliging eenvoudig omzeild kan worden. Hiervoor bestaan verschillende regels, bijvoorbeeld over de lengte van wachtwoorden, en over de regelmaat waarmee deze moeten worden gewijzigd.

Ook is het van belang dat de autorisaties binnen de organisatie zijn vastgelegd en dat deze worden gecontroleerd: welke medewerker mag toegang krijgen tot welke persoonsgegevens en wat mag hij/zij daarmee doen? De toegekende bevoegdheden moeten nauwkeurig worden bijgehouden. Wanneer iemand bijvoorbeeld van functie wijzigt of bij ontslag de organisatie verlaat, moet direct de autorisatie worden aangepast. Bij gegevens die een hoge graad van beveiliging eisen, is het van belang dat wordt bijgehouden wie, waarom tot welke persoonsgegevens toegang heeft gehad, op welke tijden en op grond van welke bevoegdheid.

Risicoklasse I

De verantwoordelijke geeft aan welke functionarissen toegang tot de persoonsgegevens mogen hebben en welke functie(s) mogen worden uitgevoerd. Tevens geeft de verantwoordelijke aan, wie in de organisatie bevoegdheden voor het verwerken van persoonsgegevens mag toedelen. De verantwoordelijke dient hiertoe een procedure vast te stellen.
Gewaarborgd is, zowel in de organisatie als in de ICT infrastructuur, dat de toegekende bevoegdheden volledig en juist in het toegangscontrolesysteem zijn geïmplementeerd.
Voor de toegang tot persoonsgegevens worden slechts specifieke toegangsbevoegdheden afgegeven. Een bevoegdheidsprofiel wordt nauwkeurig samengesteld en mag slechts op een zo klein mogelijke verzameling van bevoegdheden betrekking hebben.

Aangegeven wordt welke handelingen met welke persoonsgegevens door een functionaris mogen worden uitgevoerd.
Bij ontslag, vertrek, wijziging van functie of bij verlies van bevoegdheid om andere redenen, worden de bevoegdheden van de betrokken functionaris hem/haar met onmiddellijke ingang ontnomen.

Voor extern personeel wordt voor het definiëren en toekennen van bevoegdheden een overeenkomstige procedure als voor het eigen personeel toegepast. Deze regel geldt tevens voor opsporingsambtenaren, indien zij in het kader van een justitieel onderzoek toegang verkrijgen tot een verwerking van persoonsgegevens.

De opzet van een logische toegangscontrole op informatiesystemen is zodanig dat alleen een functionaliteit kan worden gebruikt waarvoor uitdrukkelijk een bevoegdheid is verleend.

Bij de logische toegangscontrole wordt de identiteit en de authenticiteit van gebruikers vastgesteld door tenminste een gebruikersnaam en een wachtwoord.

Een wachtwoord is slechts gedurende een van tevoren vastgestelde periode geldig. Bij wijziging van het wachtwoord wordt gecontroleerd of het oude en nieuwe wachtwoord niet gelijk zijn. Voor de hand liggende wachtwoorden zijn niet toegestaan. Tevens moeten er regels opgesteld zijn waarin is vastgelegd aan welke eisen een goed gekozen wachtwoord moet voldoen. Het systeem voor toegangscontrole moet hierop ook controleren.

Het wachtwoord wordt nergens in leesbare vorm vastgelegd. In het systeem voor toegangscontrole worden de wachtwoorden voldoende beveiligd, bijvoorbeeld door een one-way-hashing encryptie algoritme.

Het aantal keren dat een foutief wachtwoord kan worden ingevoerd, moet worden beperkt tot maximaal 3. Bij overschrijding hiervan wordt de toegang tot het systeem onder de betreffende identificatie volledig geblokkeerd. Slechts een hiertoe geautoriseerde functionaris is gerechtigd de geblokkeerde identificatie weer vrij te geven. Dit gebeurt conform een vastgestelde procedure nadat de afwijkingen zijn onderzocht.

Risicoklasse II

Bij het verkrijgen van toegang tot persoonsgegevens via een computernetwerk wordt de gebruiker nauwkeurig geïdentificeerd. Het bevoegd gebruik van de persoonsgegevens is afhankelijk van meer dan alleen de toegangscontrole door gebruikersnaam en wachtwoord in te voeren, maar bijvoorbeeld ook van het tijdstip en de apparatuur die gebruikt wordt om toegang te krijgen.

Bij het overschrijden van het toegestane aantal pogingen om toegang te krijgen wordt de verantwoordelijke terstond geïnformeerd, zodat deze actie kan ondernemen.

Elke poging (geslaagd of niet) om toegang te krijgen tot een informatiesysteem met persoonsgegevens wordt vastgelegd in een logbestand. Dit logbestand heeft een voldoende lange bewaartijd, zodat een analyse van bijzonderheden kan worden gemaakt en hierover kan worden gerapporteerd.

Bij het overdragen van bevoegdheden moet de rechtmatigheid ervan achteraf vastgesteld kunnen worden.

Risicoklasse III

Het overdragen van bevoegdheden is verboden. Bevoegdheden worden pas actief nadat een tweede daarvoor verantwoordelijke vaststelt dat de bevoegdheden voor die gebruiker juist zijn vastgelegd.

Het gebruik van controle op fysieke kenmerken als middel voor authenticatie van gebruikers dient te worden overwogen door middel van een kosten / baten analyse, daarbij rekening houdend met de ‘state of the art’.

4.8 Netwerken en externe verbindingen

Voor het transporteren van gegevens wordt in bijna alle organisaties gebruik gemaakt van netwerken. Deze datacommunicatie kan binnen de organisatie plaatsvinden, al dan niet binnen één locatie, maar ook met andere organisaties in de buitenwereld.

Wanneer persoonsgegevens over netwerken worden getransporteerd, ontstaat een belangrijk beveiligingsrisico. Het is mogelijk dat de gegevens tijdens het transport in handen komen van onbevoegden of dat gegevens gewijzigd worden. Bovendien kan bij netwerken die gekoppeld zijn met externe netwerken, denk aan internet, een extra risico ontstaan. De koppeling tussen de netwerken vergroot de kans om van buitenaf het informatiesysteem binnen te dringen en het verhoogt het risico voor het ongeautoriseerd benaderen van de persoonsgegevens die zich daarin bevinden. Het beveiligen van deze koppeling is dan ook van groot belang. Dit kan door middel van beveiligde apparatuur en bijvoorbeeld het gebruik van firewalls bij koppeling met het internet. Ook zijn er procedures nodig die ervoor zorgen dat de juiste identiteit van de zendende en ontvangende netwerkapparatuur verzekerd is.

Bij dit onderwerp wordt een onderscheid gemaakt tussen communicatie via netwerken die volledig onder toezicht van de verantwoordelijke vallen en netwerken die geheel of gedeeltelijk als publiek netwerk kunnen worden aangemerkt. Aangezien de verantwoordelijke, bij gebruik van publieke netwerken, slechts in beperkte mate kennis kan nemen van en invloed heeft op de beveiliging daarvan, dient hij/zij zelf zoveel mogelijk maatregelen te treffen om de inhoud van de persoonsgegevens te beschermen.

Een sterk aanbevolen maatregel voor het beveiligen van de data-communicatie van persoonsgegevens is het versleutelen van berichten (encryptie). Hierdoor kan in ieder geval worden voorkomen dat berichten met persoonsgegevens zonder expliciet, bewust handelen ongeoorloofd worden gelezen door onbevoegde personen.

Risicoklasse I

De verantwoordelijke legt vast op welke wijze de datacommunicatie plaats behoort te vinden.

Er wordt gebruik gemaakt van de beveiligingsopties die de aanwezige netwerkapparatuur en software bieden.

Toegang tot en vanuit publiek toegankelijke netwerken zoals internet wordt uitsluitend gemaakt via algemeen erkende beveiligingsmaatregelen, zoals firewalls.

Bijzondere aandacht wordt gegeven aan het voorkomen van onbevoegde toegang tot persoonsgegevens via netwerkverbindingen (inbelpunten, modems etc.).

Netwerkfaciliteiten, waarmee toegang kan worden verkregen tot persoons-gegevens, moeten verder worden afgeschermd door middel van een logische toegangsbeveiliging.

Risicoklasse II

Bij de keuze en aanschaf van netwerkapparatuur en -software wordt expliciet aandacht geschonken aan de eisen voor de beveiliging van persoonsgegevens. De netwerkleverancier of de ICT afdeling heeft de vereiste maatregelen conform de gemaakte afspraken geïmplementeerd.

De verantwoordelijke zorgt voor een adequate fysieke beveiliging tegen verlies of onrechtmatige verwerking van persoonsgegevens.

De zend- en ontvangstpunten bij datacommunicatie verzekeren zich van elkaars juiste identiteit (terugbelsystemen, terminal identificatie, digitale certificaten). Deze authenticatie is niet door onbevoegden te onderscheppen.

Draadloze datacommunicatie geschiedt uitsluitend indien de persoonsgegevens versleuteld worden verzonden.

Voor datacommunicatie via publieke netwerken, zoals internet, worden de persoonsgegevens op applicatieniveau, met algemeen erkende cryptografische methoden, versleuteld alvorens deze te verzenden. De gebruikte methoden en de sleutelprocedures dienen het risico van onbevoegde ontsleuteling uit te sluiten.

Risicoklasse III

De verantwoordelijke past uitsluitend datacommunicatie toe over netwerken buiten het toezicht van zijn eigen organisatie, indien hij expliciete waarborgen (zekerheden) heeft over de kwaliteit van de geïmplementeerde beveiligingsmaatregelen.

De verzender legt het berichtenverkeer zodanig vast dat achteraf vastgesteld kan worden wanneer en aan wie een bericht met persoonsgegevens is verzonden en treft voorzieningen voor een vergelijkbare functionaliteit voor de ontvangen berichten.

De verzender van een bericht (systeem of gebruiker) vergewist zich ervan dat een getransporteerd bericht ongewijzigd is overgebracht.

4.9 Gebruik van software van derden

Voor het verwerken van persoonsgegevens wordt sterk uiteenlopende software gebruikt. Software is niet in alle gevallen foutvrij waardoor persoonsgegevens onbedoeld gewijzigd zouden kunnen worden of verloren gaan. Ook is het mogelijk dat, in de software ingebouwde, toegangsbeveiligingen omzeild kunnen worden. Om deze risico's uit te sluiten mag geen illegale of niet goedgekeurde software van derden gebruikt worden. Regelmatige controle op de naleving van dit uitgangspunt is belangrijk.

Een zorgvuldig beheer van de aanwezige software is noodzakelijk. Dit betekent dat alle aanwezige software gedocumenteerd moet worden. Ook moeten er procedures zijn die beschrijven hoe het vervangen of wijzigen van software moet plaatsvinden. Als regel geldt dat wijzigingen in software altijd moeten worden gedocumenteerd en opgenomen in een systeem voor problem en change management.

Risicoklasse I

Voor het verwerken van persoonsgegevens wordt gebruik gemaakt van door de verantwoordelijke goedgekeurde software.

Bij aanschaf van software voor de verwerking van persoonsgegevens wordt rekening gehouden met de beveiligingseisen.

Er moet een adequate administratie van het versiebeheer van de software worden gevoerd en dit moet worden gedocumenteerd. De procedures voor het onderhoud worden schriftelijk vastgelegd. De wijzigingen worden door de verantwoordelijke goedgekeurd.

Risicoklasse II

De software die wordt gebruikt voor het verwerken van persoonsgegevens moet door de verantwoordelijke schriftelijk goedgekeurd worden.

Voor de continuïteit van de verwerking van persoonsgegevens dient de software van derden gedeponeerd te worden onder het regime van een ESCROW overeenkomst. Dit is een overeenkomst waarbij, bij een derde buiten de macht van de software ontwikkelaar, de broncode wordt gedeponeerd. De broncode kan in geval van niet-nakoming van contractuele verplichtingen van de software ontwikkelaar of bij calamiteiten, binnen de contractstermen toegankelijk worden gemaakt voor de verantwoordelijke.

Risicoklasse III

Toepassingssoftware in gebruik bij een verwerking van persoonsgegevens in deze risicoklasse dient onderwerp van onderzoek te zijn geweest in een 'code review'. Hierbij wordt door een onafhankelijke deskundige beoordeeld of de gebruikte software, met een redelijke mate van zekerheid, voldoet aan de gestelde eisen met betrekking tot informatiebeveiliging.

4.10 Bulkverwerking van persoonsgegevens

Veel processen waarin persoonsgegevens worden verwerkt, die van toepassing zijn op meerdere betrokkenen, zijn gedeeltelijk of volledig geautomatiseerd. Geautomatiseerde, al dan niet geïntegreerde, bulkverwerkingen worden opgestart en verder zonder onderbrekingen automatisch uitgevoerd.

Risicoklasse I

Het verwerken van persoonsgegevens is alleen toegestaan met een door de verantwoordelijke schriftelijk geautoriseerde versie van de gebruikte software.

Voor de verwerking van persoonsgegevens moet aangegeven zijn welke persoonsgegevens het betreft, met welke software wordt gewerkt, welke bestanden nodig zijn en welke verwerkingen worden uitgevoerd.

Voor de afhandeling van calamiteiten tijdens de geautomatiseerde bulkverwerking van persoonsgegevens moeten procedures aanwezig zijn. In voorkomende gevallen worden de oorzaak, de gevolgen en de getroffen maatregelen schriftelijk vastgelegd.

De instructies voor de uit te voeren handelingen zijn van tevoren expliciet vastgelegd en goedgekeurd door of namens de verantwoordelijke. Om persoonsgegevens te mogen verwerken moet het personeel daartoe zijn opgeleid.

De productieverslagen (logbestanden) van de gegevensverwerkende processen met persoonsgegevens moeten voldoende lang worden bewaard voor bewijs- en analysedoeleinden.

Uitsluitend bevoegde personen hebben toegang tot de productieverslagen van persoonsgegevensverwerkende processen.

Risicoklasse II

Hier worden geen extra maatregelen of procedures vereist.

Risicoklasse III

Hier worden geen extra maatregelen of procedures vereist.

4.11 Bewaren van persoonsgegevens

Persoonsgegevens kunnen op verschillende soorten media worden bewaard. Dergelijke media worden hier gegevensdragers genoemd. Gegevensdragers kunnen zijn papier(en dossiers) maar ook elektromagnetische media, zoals magneetbanden, diskettes, harddisks, of optische media zoals CD-ROM's of intern geheugen.

Het opslaan van gegevensdragers is van belang voor de beveiliging van persoonsgegevens. Regelmatig moeten, op vaste tijdstippen, back-ups gemaakt worden van systemen. De gevoeligheid voor storingen en calamiteiten wordt hierdoor beperkt. Het maken van back-ups met persoonsgegevens moet in duidelijke procedures zijn vastgelegd, waarvan de naleving wordt gecontroleerd. Voor het waarborgen van de continuïteit van de verwerking van persoonsgegevens is het belangrijk dat deze back-ups op een veilige plaats worden bewaard, zo mogelijk op een plek buiten de gebouwen van de organisatie.

Een andere functie van gegevensdragers is het transport van gegevens. Gegevensdragers met persoonsgegevens moeten zorgvuldig worden bewaard en getransporteerd, zodat onbevoegde personen deze niet kunnen meenemen of de gegevens inzien. Gegevensdragers die persoonsgegevens uit risicoklassen II of III bevatten moeten in ruimtes worden bewaard die afgesloten kunnen worden en voorzien zijn van inbraakbeveiliging, ook indien de gegevens versleuteld zijn.

Risicoklasse I

De gegevensdragers met persoonsgegevens moeten op een zodanige wijze worden bewaard en behandeld dat alleen bevoegde personen er over kunnen beschikken.

Er mogen geen gegevensdragers met persoonsgegevens onbeheerd worden achter gelaten op algemeen toegankelijke plaatsen.

Risicoklasse II

De gegevensdragers met persoonsgegevens worden in een afgesloten ruimte, voorzien van een inbraakdetectie, bewaard.

Risicoklasse III

De (eventueel gemarkeerde) gegevensdragers worden in een inbraakwerende ruimte (kluis) bewaard, ook indien de persoonsgegevens versleuteld zijn. Deze ruimte, of de omgeving waarin die zich bevindt, is voorzien van een inbraak-detectie. De persoonsgegevens op de gegevensdragers zijn niet zonder meer leesbaar voor onbevoegden.

4.12 Vernietiging van persoonsgegevens

Wanneer persoonsgegevens niet meer gebruikt worden, moeten deze zorgvuldig worden vernietigd. Dit dient te gebeuren na de (al dan niet wettelijke) bewaartermijn. Wanneer persoonsgegevens niet tijdig worden vernietigd, bestaat immers alsnog de mogelijkheid voor onbevoegden om de gegevens te lezen. Daarom moeten in veel gevallen de gegevensdragers fysiek vernietigd worden. De vernietiging kan ook apparatuur betreffen waarbinnen de persoonsgegevens zijn opgeslagen, zoals een PC met daarin een vaste schijf. Het is daarbij belangrijk dat de verantwoordelijkheden voor deze vernietiging duidelijk zijn en bekend bij de medewerkers.

Risicoklasse I

Het vernietigen van persoonsgegevens nadat de bewaartermijn is verlopen moet zorgvuldig gebeuren. Afdoende maatregelen worden genomen om te voorkomen dat de persoonsgegevens fysiek aanwezig blijven op elektromagnetische gegevensdragers en op eenvoudige wijze weer beschikbaar kan worden gemaakt. Persoonsgegevens die op een ander medium zijn vastgelegd (CD-ROM, microfilm etc.) worden zorgvuldig vernietigd.

Voor het vernietigen van persoonsgegevens is de toestemming van de verantwoordelijke nodig. De vernietigingsprocedure voor originelen, kopieën, back-ups en andere bestanden dient inzichtelijk te zijn voor de verantwoordelijke. De verantwoordelijke zorgt ervoor dat de procedure en het protocol voor de vernietiging van persoonsgegevens schriftelijk zijn vastgelegd.

Aandacht wordt ook besteed aan de vernietiging van tussen- en testresultaten behorende bij de verwerking van persoonsgegevens.

Risicoklasse II

Er wordt een administratie gevoerd van de vernietigde persoonsgegevens waarin is vermeld welke functionaris, op welk tijdstip, de gegevens heeft vernietigd en wie daartoe opdracht heeft gegeven.

De leverancier van gegevensdragers of de onderhoudsfirma ondertekent een geheimhoudingsverklaring waarin ook de verplichting tot vernietiging van de persoonsgegevens bij vervanging van gegevensdragers is vastgelegd.

Afgewerkte, afgedankte of niet meer functionerende gegevensdragers verlaten de organisatie alleen als de persoonsgegevens die erop zijn vastgelegd zijn vernietigd. Eventueel kan onder toezicht van de verantwoordelijke de vernietiging van de persoonsgegevens elders plaatsvinden.

Risicoklasse III

Hier worden geen extra maatregelen of procedures vereist.

4.13 Calamiteitenplan

Elke organisatie kan te maken krijgen met onvoorziene calamiteiten, zoals brand, waterschade of ernstige computerstoringen. Dergelijke calamiteiten kunnen er voor zorgen dat de bedrijfsvoering moet worden onderbroken. In het ernstigste geval komt de continuïteit van een organisatie in gevaar. Ook voor de aanwezige persoonsgegevens kan een calamiteit ernstige gevolgen hebben, bijvoorbeeld het in onbevoegde handen raken door chaotische toestanden of door het buiten het gebouw brengen van persoonsgegevens.

Als regel moet iedere organisatie een continuïteitsplan hebben waarin precies beschreven staat hoe moet worden opgetreden bij calamiteiten. Het plan heeft echter alleen zin als het bij de medewerkers bekend is en ook regelmatig met hen geoefend wordt. Bij het plan hoort ook een procedure waarin staat hoe na een calamiteit de gegevensverwerking weer op gang kan worden gebracht.

Risicoklasse I

Van elk bestand met persoonsgegevens worden een of meerdere back-ups gemaakt. Een exemplaar van de back-up wordt op een andere locatie bewaard dan waar de originele persoonsgegevens zich bevinden.

Voor elke back-up met persoonsgegevens wordt een bewaartermijn vastgesteld.

Risicoklasse II

De bewaarlocatie van back-ups bevindt zich buiten de locatie waar de verwerking van persoonsgegevens plaatsvindt.

Risicoklasse III

Back-ups met persoonsgegevens worden voorzien van een markering die de risicoklasse aangegeven.

4.14 Uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens

In een aantal gevallen zal een organisatie niet alle verwerkingen van persoonsgegevens zelf uitvoeren maar geheel of gedeeltelijk uitbesteden aan een bewerker (artikel 14 WBP).

Voor de beveiliging van persoonsgegevens geldt dat de bewerker hetzelfde niveau van beveiliging moet garanderen als de verantwoordelijke organisatie. In de contracten met bewerkers moet de beveiliging van de persoonsgegevens opgenomen worden. Ook is het wenselijk dat de bewerker een geheimhoudingsverklaring tekent. Wanneer de bewerker persoonsgegevens uit de hoogste risicoklasse verwerkt, zal er toezicht moeten worden gehouden op de beveiligingsmaatregelen die deze neemt, bijvoorbeeld in de vorm van periodieke controles.

Risicoklasse I

In het kader van de controle van de verantwoordelijke op de bewerker kan deze gebruikmaken van een Third Party Mededeling. Dit is een onafhankelijk oordeel over de kwaliteit van de door de bewerker getroffen maatregelen van de beveiliging van persoonsgegevens.

In een contract tussen de verantwoordelijke en de bewerker wordt vastgelegd dat beide zich aan de, op de risicoklasse betrekking hebbende, eisen zullen houden. Hierbij wordt onder meer het volgende vastgelegd:

- procedures rond autorisaties;
- het bijhouden van logbestanden;
- de opslag van gegevensdragers met persoonsgegevens;
- het verstrekken van persoonsgegevens aan derden.

Het fysieke en logische beveiligingsniveau bij de bewerker moet toereikend zijn voor de risicoklasse van de te verwerken persoonsgegevens.

De verantwoordelijke dient zich op de hoogte te stellen van het beveiligingsniveau voor de persoonsgegevens bij de bewerker. De verantwoordelijke moet een geheimhoudingsartikel in het contract opnemen.

Risicoklasse II

De verantwoordelijke moet het niveau van het beleid voor de beveiliging van persoonsgegevens bij de bewerker (laten) controleren. De controle en rapportage geschieden jaarlijks. De verantwoordelijke voert hierop steekproefsgewijs een controle bij de bewerker uit.

Risicoklasse III

Persoonsgegevens worden alleen opgeslagen of bewerkt door een bewerker indien de verantwoordelijke zich er, middels een overeenkomst en afspraken over controle, van heeft verzekerd dat vereiste beveiligingsmaatregelen zijn getroffen.

Bijlage

Bij **Bijlage**

Leden van de commissie beveiliging

drs. J.J. Borking
plv. voorzitter Registratiekamer, voorzitter van de commissie

G.W. van Blarkom
Privacy Auditor, Registratiekamer, secretaris van de commissie

prof. M.E. van Biene-Hershey RE
Vrije Universiteit Amsterdam

ing. J.N.M. Koppes
Pink Roccade N.V.

prof. A.W. Neisingh RE RA
KPMG Information Risk Management

ing. J.H. Sneep

H. de Zwart RE RA RO
Claassen, Moolenbeek & Partners

Dank is eveneens verschuldigd aan de oud-medewerker van de Registratiekamer dr. R. Hes

Achtergrondstudies en Verkenningen

In de serie Achtergrondstudies en Verkenningen zijn verschenen:

Versmissen, J.A.G., *Sleutels van vertrouwen, TTP's, digitale certificaten en privacy*, A&V-22. Registratiekamer, 2001

Terstegge, J.H.J., *Goed werken in netwerken, regels voor controle op e-mail en internetgebruik van werknemers*, A&V-21. Registratiekamer, 2000.

Buitenhuis, R., Campen, N.G.M. van, Helden, W.J. van, Vries, H.H. de, *Bankverzekeraars en privacy, gegevensverwerking in financiële conglomeraten*, A&V-20. Registratiekamer, 2000.

Helden, *W.J. van, Herkomst van de klant, privacyregels voor etnomarketing.* A&V-19, Registratiekamer, 2000.

Wishaw, R.W.A. *De gewaardeerde klant, privacyregels voor credit scoring.* A&V-18, Registratiekamer, 2000.

Artz, M. en Eijk, M.M.M. van, *Klant in het web. Privacywaarborgen voor internettoegang.* A&V-17, Registratiekamer, 2000.

Zeeuw, J. de. *Informatieverstrekking. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving.* A&V-16, Registratiekamer, 1999.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. *At face value. On biometrical identification and privacy.* A&V-15, Registratiekamer, 1999.

Artz, M.J.T. *Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden.* A&V-14, Registratiekamer,1999.

Borking, J.J., e.a., *Intelligent software agents and privacy*. A&V-13, Registratiekamer 1999.

Hooghiemstra, T.F.M., *Privacy & Managed care.* A&V-12, Registratiekamer 1998.

Hes, R. en Borking, J.J. *Privacy-Enhancing Technologies: the path to anonymity, revised edition.* A&V-11, Registratiekamer 1998.

Almelo, L. van, e.a., *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy.* A&V-10, Registratiekamer 1998.

Zandee, C., *Doelbewust volgen. Privacy-aspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling.* A&V-9, Registratiekamer 1998.

Zeeuw, J. de, *Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken.* A&V-8, Registratiekamer 1998.

P.C. Ippel, Gegeven: de Genen. *Morele en juridische aspecten van het gebruik van genetische gegevens.* A&V-7, Registratiekamer 1996.

Gardeniers, H.J.M., *Chipcards en privacy. Regels voor een nieuw kaartspel.* A&V-6, Registratiekamer, 1995.

Rossum, H. van e.a., *Privacy-Enhancing Technologies: the path to anonymity, volume I and II.* A&V-5, Registratiekamer, 1995 (uitverkocht).

Rommelse, A.F., *Zwarte lijsten. Belangen en effecten van waarschuwingssystemen.* A&V-4, Registratiekamer 1995.

Rommelse, A.F., *Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer.* A&V-3, Registratiekamer, 1995.

Casteren, J.P.M. van, *Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden.* A&V-2, Registratiekamer, 1995 (uitverkocht).

Publicaties van de Registratiekamer kunt u gratis inzien en downloaden van de website www.registratiekamer.nl. Voor toezenden van gedrukte publicaties kunnen verzend- en handlingkosten in rekening worden gebracht.

Registratiekamer

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
Telefoon 070 - 381 13 00
Fax 070 - 381 13 01
mail@registratiekamer.nl
Internet: www.registratiekamer.nl
ISBN 90 74087 27 2
april 2001