Wet bescherming persoonsgegevens

Samenwerkingsverband Audit Aanpak / Werkgroep Privacy Audit

Raamwerk Privacy Audit

Disclaimer

Dit product 'Raamwerk Privacy Audit' is met de grootste zorg ontwikkeld door het 'Samenwerkingsverband Audit Aanpak', waarbij de wettelijke regels gesteld bij of krachtens de Wet bescherming persoonsgegevens zo goed mogelijk in acht zijn genomen.

Mede omdat de exacte betekenis van deze regels steeds afhankelijk is van omstandigheden waarmee bij de ontwikkeling van dit product 'Privacy Audit Raamwerk' geen rekening kon worden gehouden, geschiedt het gebruik van dit product 'Privacy Audit Raamwerk' steeds geheel voor risico van de gebruiker.

Raamwerk Privacy Audit

Reacties

Het Samenwerkingsverband Audit Aanpak houdt zich aanbevolen voor reacties op dit document. U kunt uw reacties schriftelijk kenbaar maken aan:

College bescherming persoonsgegevens
t.a.v. Samenwerkingsverband Audit Aanpak
Postbus 93374
2509 AJ Den Haag

of e-mail: auditaanpak@cbpweb.nl

Inhoudsopgave

Voorwoord

De bescherming van gegevens over personen raakt ons allemaal. De mate waarin voorzieningen moeten worden getroffen om die persoonsgegevens te beschermen tegen misbruik of oneigenlijk gebruik verschilt door onder meer de inhoud van de gegevens, de hoeveelheid gegevens, de doelstelling van het gebruik, de wijze van verwerking en de verwerkingsomgeving. Daarnaast spelen factoren een rol als technologische ontwikkelingen en de maatschappelijke en persoonlijke visie. Kortom, een complex geheel van factoren dat invloed heeft op de wijze van implementatie van de Wet bescherming persoonsgegevens (WBP) in organisaties en in het bijzonder in de ICT-voorzieningen.

De complexiteit van de WBP noodzaakt voor veel facetten tot interpretatie en vertaling naar de praktijk van alle dag. Een dergelijke vertaling is ook nodig voor het toezicht op de manier waarop verwerkers (degenen die gegevens over personen onder hun beheer hebben) persoonsgegevens behandelen en gebruiken. Om die vertaling zo goed mogelijk op de praktijk af te stemmen is door het College bescherming persoonsgegevens (CBP) een samenwerkingsverband in het leven geroepen. Dit samenwerkingsverband heeft een productenset samengesteld waarmee organisaties, met verschillende niveaus van diepgang, primair zelf kunnen nagaan hoe hun eigen situatie zich verhoudt tot de WBP. De inhoud en betekenis van deze producten zijn in hoofdstuk III nader uitgewerkt.
De meest uitgebreide aanpak (de Privacy Audit) kan leiden tot een certificaat. Wanneer de onderzochte organisatie aan de gedefinieerde eisen voldoet kan een privacycertificaat worden afgegeven.

Vaststellen

Voordat is overgegaan tot het vaststellen van het Raamwerk Privacy Audit is het product bij een aantal organisaties getest op inhoud en bruikbaarheid.

Dit document is vastgesteld in de vergadering van de Stuurgroep van het 'Samenwerkingsverband Audit Aanpak' d.d. 19-12-2000.

Deelnemers in het Samenwerkingsverband

De volgende marktpartijen hebben een bijdrage geleverd aan het Samenwerkingsverband:

- BDO Camps Obers Accountants & Adviseurs;
- BESTUUR & MANAGEMENT CONSULTANTS (BMC);
- Continuity Planning Associates;
- Deloitte & Touche;
- EDP AUDIT POOL;
- Ernst & Young;
- IQUIP Informatica B.V.;
- KPMG Information Risk Management;
- Mazars Paardekooper Hoffman;
- PricewaterhouseCoopers;
- Roccade Public;
- Singewald Consultants Group.

Gebruikers en afnemers van de audit producten zijn via de volgende koepelorganisaties bij het ontwikkel- en testproces betrokken:

- Consumentenbond;
- Information Systems Audit and Control Association Nederland (ISACA-NL-Chapter);
- Koninklijk Nederlands Instituut van Registeraccountants (NIVRA);
- Nederlandse Orde van Register EDP-auditors (NOREA);
- Nederlandse Orde van Accountant-Administratieconsulenten (NOvAA);
- VNO-NCW;
- FNV;
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
- Ministerie van Justitie.

Het Samenwerkingsverband onderhoudt de productenset, die door het CBP mede wordt gehanteerd bij het uitoefenen van haar toezichthoudende taak.

Inleiding

Het Raamwerk Privacy Audit is opgesteld voor het uitvoeren van Privacy Audits bij organisaties waar persoonsgegevens worden verwerkt. Het uitvoeren van een Privacy Audit dient weloverwogen plaats te vinden: niet elke organisatie is op voorhand klaar om een Privacy Audit te ondergaan. Een gedegen analyse of een Privacy Audit meerwaarde heeft voor een organisatie dient daarom altijd vooraf plaats te vinden. Hiermee wordt voorkomen dat achteraf teleurstelling ontstaat bij de opdrachtgever over de resultaten van de Privacy Audit. Als uit bovengenoemde analyse blijkt dat een Privacy Audit op dit moment onvoldoende toegevoegde waarde voor de organisatie oplevert, dient de organisatie eerst adequate maatregelen te treffen. Hiervoor kan bijvoorbeeld de WBP Zelfevaluatie gebruikt worden. De auditor kan een organisatie bij het verbetertraject behulpzaam zijn via het geven van adviezen.

Voor het laten uitvoeren van een Privacy Audit kan een organisatie verschillende motieven hebben. Het is belangrijk dat de auditor op de hoogte is van de motieven van de opdrachtgever. Globaal kunnen twee belangrijke motieven worden onderkend:

1 economisch motief (hoofdzakelijk intern gericht);
2 maatschappelijk motief (hoofdzakelijk extern gericht).

Economisch motief

Organisaties hebben de plicht de wettelijke eisen voor de bescherming van persoonsgegevens na te leven. Daartoe dienen organisaties de bepalingen van de WBP, binnen de gestelde overgangstermijnen, in hun organisatie te vertalen naar een toereikend stelsel van maatregelen en procedures. Tevens hebben organisaties er belang bij om eventuele sancties en negatieve berichtgeving die kunnen voortvloeien uit het niet naleven van de wet, te voorkomen. Om deze redenen kan het management van een organisatie een auditor opdracht geven om een Privacy Audit uit te voeren, waarmee het management zekerheid verkrijgt over de implementatie en naleving van de wet.

Vanuit het College bescherming persoonsgegevens wordt zelfregulering door organisaties en via branche- en koepelorganisaties aangemoedigd. In dat kader past een actieve houding van het management om de wettelijke bepalingen binnen de eigen organisatie adequaat in te vullen.

Maatschappelijk motief

Het correct naleven van de eisen van de WBP kan voor organisaties een publicitair voordeel opleveren ten opzichte van bijvoorbeeld concurrenten. Een zorgvuldige verwerking van persoonsgegevens kan het imago van een organisatie in positieve zin beïnvloeden en heeft daardoor commerciële waarde. Op deze wijze kan een organisatie zich met privacy in positieve zin profileren naar afnemers, leveranciers, werknemers, publiek, etc. In deze gevallen is te overwegen de Privacy Audit te laten uitvoeren om een privacycertificaat te verkrijgen. Overigens kunnen ook andere vormen van rapportage over de Privacy Audit in maatschappelijke zin worden gebruikt.

Doelgroep en toepassing

Het Raamwerk is geschreven voor auditors die belast zijn met de uitvoering van een Privacy Audit. Voor een juist gebruik van dit Raamwerk is voldoende kennis en vaardigheid van audits in het algemeen en IT-audits in het bijzonder noodzakelijk. Tevens dient de auditor toereikende kennis te hebben van de Wet bescherming persoonsgegevens. Mocht de auditor de juridische kennis ontberen dan dient deze in teamverband met een gespecialiseerd jurist de audit op te zetten en uit te voeren.

Het Raamwerk biedt een handvat voor het opstellen van een auditplan. Het gebruik van een auditplan dat op de specifieke situatie van de organisatie is toegesneden, is essentieel voor een effectieve en efficiënte uitvoering van de Privacy Audit. Het toepassen van dit Raamwerk vraagt van de auditor op verschillende momenten een gedegen en weloverwogen oordeel. Het Raamwerk biedt namelijk geen kant en klare oplossing. Vanuit het Raamwerk worden vervolgens de werkprogramma's ontwikkeld.

Normering en reikwijdte

In het Raamwerk is geen normering aangegeven voor de criteria die de wet stelt aan organisaties als het gaat om de bescherming van persoonsgegevens. De wet laat namelijk ruimte voor organisaties om een toereikende invulling van bepaalde wettelijke eisen te realiseren. Dit kan afgeleid worden uit artikel 13 WBP, dat stelt dat 'passende technische en organisatorische maatregelen getroffen moeten worden om persoonsgegevens te beveiligen tegen verlies of tegen onrechtmatige verwerking'. Wat in een specifieke situatie als passend kan worden aangemerkt is niet op voorhand aan te geven. Criteria die meegenomen moeten worden bij de overweging of er sprake is van passende maatregelen zijn:

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

De auditor definieert vanuit de wettelijke bepalingen de specifieke toetsingsnormen, gegeven de gewenste reikwijdte en diepgang en in aanmerking nemende de technische ICT-infrastructuur en de betekenis van de privacybeschermingsmaatregelen. Vervolgens vindt afstemming plaats met de auditee, waarna besluitvorming ten aanzien van de toetsingsnormen (normenkader) plaatsvindt. Het raadplegen van collega-auditors en WBP juristen kan in dit traject zeer nuttig zijn.

De auditor draagt uiteraard de eindverantwoordelijkheid voor de opdrachtformulering. Voor zover de Privacy Audit wordt uitgevoerd met het oogmerk een certificaat te verkrijgen, dienen in het kader van de opdrachtformulering de reikwijdte en diepgang vastgesteld te worden in overeenstemming met de eisen van het certificeringschema (zie paragraaf III.8 Certificaat privacybescherming).

Introductie Raamwerk Privacy Audit

III . 1 Inleiding

De invoering van de Wet bescherming persoonsgegevens heeft gevolgen voor alle organisaties die persoonsgegevens verwerken. De wet heeft betrekking op zowel geautomatiseerde als niet-geautomatiseerde verwerking van persoonsgegevens. Het management moet ervoor zorgen dat binnen de organisatie adequate invulling aan de WBP wordt gegeven. Dit vereist een doelgerichte implementatie van de voorzieningen die in het kader van deze wet getroffen moeten worden. Het stelsel van reeds getroffen maatregelen en procedures voor het beheer, de beveiliging en de verwerking zullen expliciet getoetst moeten worden aan de doelstelling van de WBP en zo nodig moeten worden heroverwogen.

In het vervolg van dit hoofdstuk wordt uiteengezet dat het implementeren van de WBP primair een organisatievraagstuk is en derhalve ook tot de primaire verantwoordelijkheid van het management van een organisatie behoort. De auditor dient zich hiervan in de communicatie naar zijn opdrachtgever altijd bewust te zijn.

Het proces om tot een goede privacybescherming te komen gaat niet van vandaag op morgen. Een organisatie heeft tijd nodig om het bewustwordingsproces op gang te brengen. Het proces vraagt ook om begeleiding. De auditor kan vanuit zijn natuurlijke adviesfunctie hierin voorzien. Daarnaast is het voor het management dat belast is met de implementatie van de WBP raadzaam één of meerdere contactpersonen aan te stellen die verantwoordelijk zijn voor onder meer de coördinatie van de te treffen voorzieningen en de evaluatie van de getroffen voorzieningen. Hierbij kan onder meer gedacht worden aan de functionaris voor de gegevensbescherming of de security-officer.

III . 2 Positionering Privacy Audit

De WBP stelt eisen aan de verwerking van persoonsgegevens en heeft gevolgen voor de procedures en maatregelen die een organisatie heeft genomen om haar gegevensverwerking goed te beveiligen en beheersen. Het kwaliteitsspectrum voor de bescherming van persoonsgegevens (zie paragraaf III.7.2) is overigens enger dan het kwaliteitsspectrum van de gegevensverwerking in brede zin (betrouwbaar, efficiënt, effectief, exclusief, integer, continu en controleerbaar).

Het Samenwerkingsverband Audit Aanpak heeft drie producten ontwikkeld om organisaties behulpzaam te zijn bij het analyseren van de feitelijke situatie van de bescherming van persoonsgegevens en het implementeren van de gewenste situatie. Deze producten zijn: Quickscan, WBP Zelfevaluatie (eventueel met review) en Raamwerk Privacy Audit.

Via de Quickscan kunnen functionarissen binnen een organisatie op snelle wijze inzicht verkrijgen in de mate van bewustzijn van de bescherming van persoonsgegevens. De reikwijdte van de Quickscan gaat niet verder dan het creëren van bewustwording binnen de organisatie en is te beschouwen als een globale checklist. Een uitspraak over de mate waarin voldaan wordt aan de bepalingen van de wet wordt dan ook niet gedaan.

De WBP Zelfevaluatie is een meer omvangrijk product dat door functionarissen die bij de privacybescherming betrokken zijn, uitgevoerd moet worden. De WBP Zelfevaluatie is een systematische methode om zelfstandig de kwaliteit van een organisatie voor wat betreft de privacybescherming te beoordelen. De uitkomsten van de WBP Zelfevaluatie geven een duidelijk beeld over de huidige situatie en de noodzakelijke verbeterpunten. Desgewenst kan een organisatie de intern uitgevoerde WBP Zelfevaluatie laten reviewen door een interne of externe auditor (bijvoorbeeld een accountant of IT-auditor).

De Privacy Audit vormt het sluitstuk van de productenset. De Privacy Audit dient door een deskundige auditor/jurist of team van deskundigen uitgevoerd te worden. Het is een full scope audit naar de wijze waarop en de mate waarin de organisatie voldoet aan de eisen die de wet heeft gesteld aan de bescherming van persoonsgegevens.

Daarnaast heeft de Registratiekamer, rechtsvoorganger van het College bescherming persoonsgegevens, Achtergrondstudie & Verkenning, nummer 23 'Beveiliging van persoonsgegevens' uitgegeven. Deze uitgave beschrijft de noodzakelijke beveiligingsmaatregelen die aan de verwerking van persoonsgegevens, in verschillende situaties, worden gesteld. Deze A&V studie is te bestellen bij het CBP.

De onderlinge verhouding tussen de drie ontwikkelde producten en de A&V studie Beveiliging van persoonsgegevens is in het hierna volgende schema weergegeven.

Overzicht diepgang productenset

Behoefte/diepgang	
Globale indruk	Quickscan
Interne meting	WBP Zelfevaluatie
Interne meting + beoordeling	WBP Zelfevaluatie + review
Onafhankelijk onderzoek + certificaat	Privacy Audit

Dit document bevat het Raamwerk Privacy Audit. Uit het schema blijkt, dat uitvoering van een Privacy Audit de grootste diepgang heeft van alle genoemde producten en derhalve het meest omvattende onderzoek is.

III . 3 Hoofdlijnen WBP

Met het in werking treden van de WBP in 2001 voldoet Nederland aan de eis van de EG privacy richtlijn om de nationale wetgeving in overeenstemming met deze richtlijn te brengen. De WBP vervangt de Wet persoonsregistraties (WPR) uit 1989 en geeft algemene wettelijke regels ter bescherming van de privacy van burgers.

Belangrijk verschil met de WPR is gelegen in de uitbreiding van het object. De WPR regelde met name de eisen ten aanzien van persoonsregistraties. De WBP stelt eisen aan de hele verwerkingsketen, waaronder onder meer wordt verstaan het verzamelen, vastleggen, bewaren, wijzigen, koppelen en raadplegen van persoonsgegevens, alsmede het verstrekken van persoonsgegevens aan een derde en het vernietigen van persoonsgegevens.

De wet biedt burgers waarborgen voor de zorgvuldige en doelgebonden verwerking van persoonsgegevens en geeft hen mogelijkheden tot correctie van verwerkte persoonsgegevens. Ook kunnen betrokkenen desgewenst bezwaar aantekenen tegen de verwerking van hun persoonsgegevens. Dat betekent overigens niet dat vormen van verwerking van persoonsgegevens verboden worden, maar de wet verbindt hieraan wel duidelijke voorwaarden.

De WBP kan vanuit twee invalshoeken kort worden samengevat:

Op juridische wijze

De verzameling van persoonsgegevens vindt plaats volgens welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, bijvoorbeeld met toestemming van de betrokkene of op basis van een wettelijke verplichting, waarbij de verdere verwerking van de persoonsgegevens verenigbaar moet zijn met het doel, ter zake, niet bovenmatig, juist en nauwkeurig.

Op algemene wijze

De verwerking van persoonsgegevens biedt waarborgen dat de juiste persoonsgegevens, voor het juiste doel, op de juiste gronden, voor de juiste mensen op het juiste tijdstip beschikbaar zijn.

De wet onderscheidt categorieën persoonsgegevens waarvoor strikte voorwaarden voor gebruik gelden. Daarbij gaat het om de zogenoemde 'bijzondere gegevens', bijvoorbeeld over ras, politieke gezindheid, gezondheid en seksuele leven. Deze persoonsgegevens mogen alleen worden verwerkt door bij wet bepaalde instanties of in de wet omschreven situaties dan wel met uitdrukkelijke toestemming van de betrokkene. De WBP maakt geen onderscheid tussen verwerkingen van persoonsgegevens door overheden of door het bedrijfsleven.

De WBP stelt een College bescherming persoonsgegevens (CBP) in dat toezicht houdt op het naleven van deze privacywetgeving. Het CBP heeft de bevoegdheid (ex art. 60 WBP) een onderzoek in te stellen naar de wijze waarop in de aanwezige verwerking van persoonsgegevens invulling wordt gegeven aan de geldende privacywetgeving. Bij het meest diepgaande onderzoek, een Privacy Audit, zal het College het Raamwerk Privacy Audit daarvoor als uitgangspunt hanteren.

III . 4 Privacybescherming als onderdeel managementcyclus

De in de WBP geformuleerde eisen dienen op een doeltreffende manier in de organisatie te worden geïmplementeerd om de rechten van de burger op adequate wijze tewaarborgen. Het is daarom van belang een adequaat stelsel van algemene verwerkingsmaatregelen en -procedures te realiseren rekening houdende met de specifieke beschermingsmaatregelen die voor de verwerking van persoonsgegevens noodzakelijk zijn. Zo zal privacybescherming in de regel tot een aanvullend stelsel van maatregelen en procedures leiden, bovenop de normaliter al vereiste verwerkings- en beveiligingsmaatregelen. Wil men tot een evenwichtig verwerkingsbeleid voor persoonsgegevens komen en dit adequaat implementeren en onderhouden dan zal dat een belangrijke plaats in de managementcyclus moeten innemen. Het voeren van beleid gericht op privacybescherming past ook in het streven van het management naar totale kwaliteit en maatschappelijk verantwoord ondernemen.

Het realiseren van bedrijfsdoelstellingen, via de managementcyclus, verloopt in het algemeen via de volgende drie fasen: de organisatie van de processen (inclusief de beleidsvoering), de processen zelf en een evaluatie en bijsturing van de processen. In paragraaf III.5 wordt deze fasering nader uitgewerkt. De aanpak en werkwijze die aan de ontwikkeling van dit Raamwerk Privacy Audit ten grondslag hebben gelegen, sluit hierop aan.

III . 5 Vaststellen, implementeren en evalueren privacybeleid

In voorgaande paragrafen is het belang van privacybeleid als verantwoordelijkheid van het management en als onderdeel van de managementcyclus uiteengezet. Voor het definiëren van een verwerkingsbeleid en vervolgens het implementeren en onderhouden daarvan dient men systematisch een aantal fasen te doorlopen. In de praktijk is dit proces meestal niet zo gestileerd. Dit mag voor het management echter geen argument zijn om het proces niet op enigerlei (gestructureerde) wijze aan te pakken.

Het is op deze plaats niet de bedoeling een uiteenzetting te geven over de beste wijze waarop men tot een verwerkingsbeleid kan komen en de daaraan gekoppelde implementatie en onderhoud van maatregelen en procedures. Als handreiking is onderstaand een uitwerking gegeven toegespitst op de implementatie van de WBP in een organisatie.

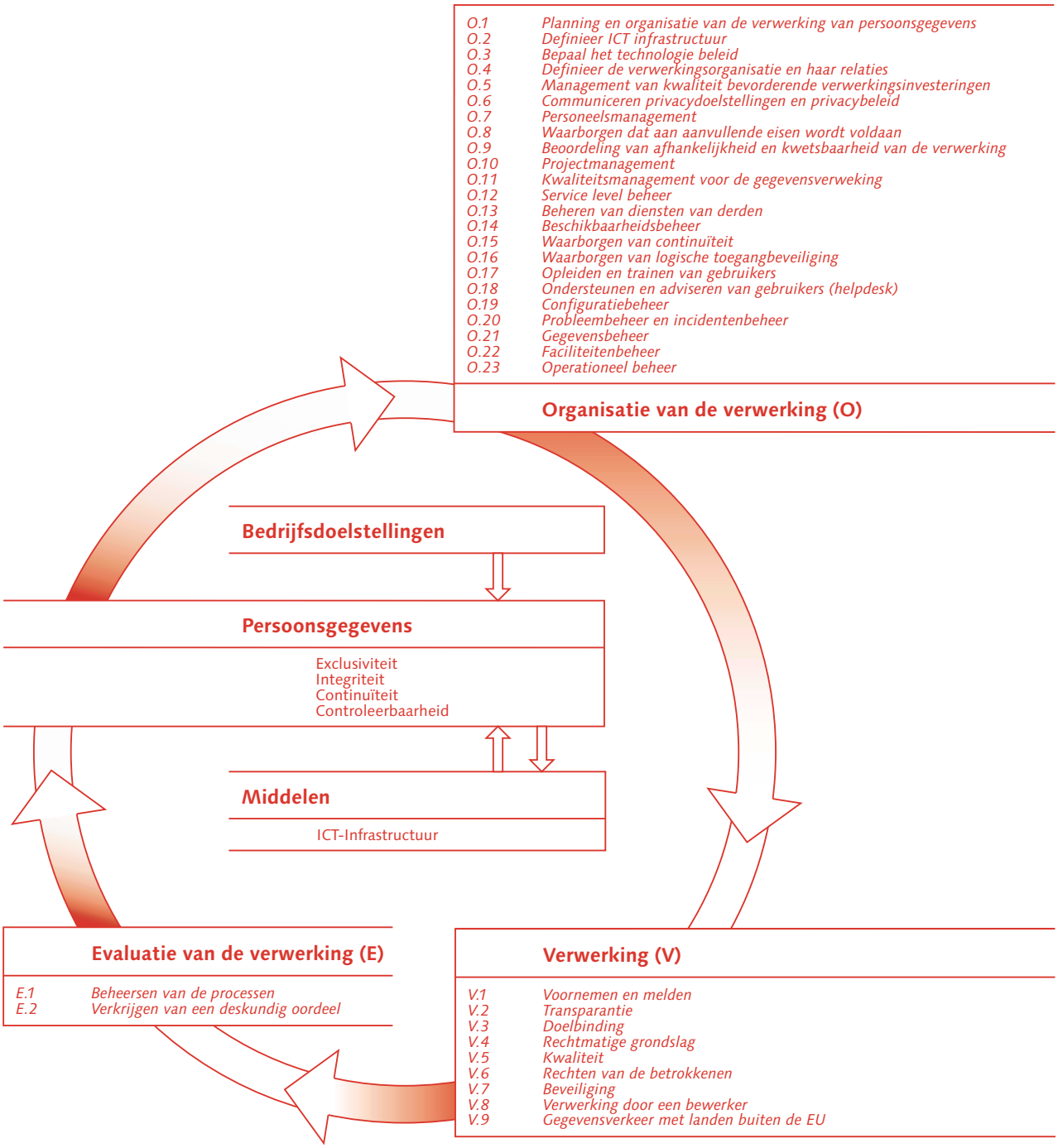
Fase 1 Beleid en Organisatie

Uitgangspunt is om vanuit de doelstelling van de organisatie een privacybeleid te ontwikkelen, op basis waarvan een beleid voor de verwerking van persoonsgegevens kan worden geformuleerd. Aanvullend zal het bestaande privacybeleid worden geëvalueerd en verschillen ten opzichte van de implementatie van de WBP-eisen in kaart worden gebracht.

Fase 2 Verwerking (in termen van de WBP)

Het geformuleerde beleid dient geconcretiseerd te worden naar specifieke maatregelen en procedures voor de verwerkingscyclus van persoonsgegevens. Het definiëren van concrete maatregelen en procedures vindt plaats na een grondige risicoanalyse, waarin bedreigingen worden geïnventariseerd waaraan de verwerking van persoonsgegevens blootstaat. In dit verband worden de sterke en zwakke

Managementcyclus



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

Fase 3

Beheersing en Evaluatie (van fase 1 en 2)

Met behulp van een systeem van monitoring dient het management na te gaan in hoeverre de getroffen voorzieningen de doelstelling van het geformuleerde privacybeleid realiseren. Het management moet aangeven op welke wijze en met welke intensiteit zij de monitorgegevens wil ontvangen. De resultaten van de uitgevoerde monitoring vormen de basis voor eventuele correctieve acties, aanpassing van getroffen maatregelen en procedures dan wel bijstelling van het geformuleerde beleid.

De drie fasen uit de managementcyclus zijn hierna schematisch weergegeven. De specifieke invulling van de verschillende elementen van het schema is als volgt in het Raamwerk verwerkt:

- de eisen gesteld aan de verwerking van persoonsgegevens (V.1 tot en met V.9) zijn beschreven in hoofdstuk V;
- een normatief kader voor de te treffen maatregelen en procedures (de voorzieningen) is weergegeven in bijlage 2 en 3 en vastgelegd in de eerder genoemde A&V studie nr. 23.

III . 6 Opzet Raamwerk Privacy Audit

Kern van de in dit Raamwerk beschreven aanpak is, dat bij het uitvoeren van een Privacy Audit wordt nagegaan waar en op welke wijze de eisen voortvloeiende uit de WBP reeds in de operationele organisatie worden geborgd en welke aanvullende voorzieningen eventueel nog moeten worden getroffen teneinde een toereikende bescherming van persoonsgegevens te verzekeren.

Leeswijzer

Het Raamwerk bevat daarvoor in hoofdstuk V (V-deel) een analyse van de aandachtspunten die op grond van de WBP noodzakelijk in ogenschouw te nemen zijn. De doelmatigheid vereist dat wordt nagegaan waar, op grond van het realiseren van de bedrijfsdoelstellingen, reeds voorzieningen in de organisatie zijn getroffen die mede invulling geven aan de bescherming van persoonsgegevens. Om deze analyse te ondersteunen is in de bijlagen van dit Raamwerk aangegeven waar de raakvlakken met de privacybescherming in de organisatie kunnen worden gevonden.

Zo geeft bijlage 2 Organisatie van de verwerking (hierna te noemen het O-deel) een toelichting op de categoriëen van maatregelen en procedures waaraan binnen de organisatie van de verwerking van persoonsgegevens in het algemeen aandacht besteed dient te worden. Als handreiking aan de auditor is ervoor gekozen een vrij gedetailleerde uiteenzetting van de mogelijk te treffen maatregelen en procedures te geven. De keuze en daadwerkelijke implementatie van maatregelen en procedures in een specifieke situatie binnen een organisatie is sterk afhankelijk van de vigerende omstandigheden binnen die organisatie en de criteria genoemd in de paragraaf 'Normering en reikwijdte' in hoofdstuk II. In A&V studie nr. 23 'Beveiliging van persoonsgegevens' is een normatief kader geschetst voor de concrete invulling van maatregelen en procedures ten aanzien van de beveiliging van persoonsgegevens. Deze methodiek gaat uit van een risicoanalyse die verschillende risicoklassen van persoonsgegevens onderkent.

Bijlage 3 Evaluatie van de verwerking (hierna te noemen het E-deel) beschrijft de mogelijke maatregelen en procedures om het verwerkingsproces (zie bijlage 2, respectievelijk A&V studie nr. 23) te beheersen. In bijlage 4 tenslotte, is een handreiking opgenomen die de relatie weergeeft tussen de maatregelen en procedures uit bijlagen 2 en 3 en de eisen die de wet stelt aan de verwerking van persoonsgegevens (zie hiervoor hoofdstuk V).

Daarnaast is in bijlage 1 een overzicht opgenomen waarin de relatie tussen de wetsartikelen en de negen aandachtsgebieden is aangegeven. Bijlage 5 tenslotte geeft een handreiking voor de invulling van het contract tussen de verantwoordelijke en een bewerker en is een uitwerking van aandachtsgebied V.8.

Opzet Privacy Audit

In hoofdstuk V van het Raamwerk zijn de uit de wet af te leiden eisen geclusterd naar negen aandachtsgebieden. In dat hoofdstuk worden de implicaties van de wettelijke bepalingen voor de verwerking van persoonsgegevens uitgewerkt. Elk aandachtsgebied in hoofdstuk V (V-deel) heeft implicaties voor de inrichting van de administratieve organisatie en de maatregelen van interne controle en beveiliging. De beoordeling van de vraag of een aandachtsgebied relevant is en zo ja, in welke mate hier bij de Privacy Audit aandacht aan moet worden besteed, is afhankelijk van de concrete situatie. Dit wordt onder meer bepaald door de typologie, aard en omvang van de desbetreffende organisatie en de aard en omvang van de verwerking van persoonsgegevens binnen die organisatie.

De wettelijke bepalingen zijn zo geformuleerd dat deze voor alle organisaties en voor alle vormen van verwerkingen toepasbaar zijn. Er is derhalve geen specifieke invulling gegeven naar typologie en omvang van de organisatie of naar aard en omvang van de verwerking van persoonsgegevens. Dit betekent dat organisaties de wettelijke bepalingen specifiek voor hun eigen situatie moeten invullen. Vervolgens dienen zij passende technische en organisatorische maatregelen te treffen die voorzien in de beveiliging tegen verlies of onrechtmatige verwerking van persoonsgegevens (art. 13 WBP) en maatregelen en procedures die de overige wettelijke bepalingen moeten waarborgen.

Bij de uitvoering van de Privacy Audit toetst de auditor primair of de organisatie adequaat is ingericht om in voldoende mate tegemoet te komen aan de wettelijke bepalingen (de opzet). Vervolgens zal de auditor de door de organisatie getroffen maatregelen en procedures qua bestaan beoordelen die in de borging van de wettelijke eisen moeten voorzien. Tot slot zal hij aandacht besteden aan de toetsing van de werking van de betreffende maatregelen over een vooraf te bepalen periode.

Het management van een organisatie kan naar eigen keuze invulling geven aan de technische en organisatorische maatregelen ter borging van de bescherming van de persoonsgegevens. Daarbij zal zij aansluiting zoeken bij de reeds binnen de organisatie gekozen opzet en invulling van de administratief-organisatorische en technische maatregelen en procedures ter waarborging van de (geautomatiseerde) gegevensverwerking. Vanuit het bestaande beheersingsinstrumentarium kan het management zo op effectieve en efficiënte wijze invulling geven aan de WBP-

vereisten. De wet legt organisaties geen dwingende inrichting van deze technische en organisatorische maatregelen voor.

Dat het management deze maatregelen moet treffen om te voldoen aan de eisen van de WBP staat vast. Ter illustratie is daarvoor in de bijlagen 2 en 3 van het Raamwerk Privacy Audit vanuit de methodiek van CobiT[1] een vertaling gemaakt naar de wijze waarop de organisatie haar (geautomatiseerde) gegevensverwerking kan inrichten en beheersen. Via deze methode zijn de eisen die uit de WBP (V-deel) zijn af te leiden, vertaald naar concrete technische en organisatorische (O-deel) en beheersmatige (E-deel) maatregelen en procedures. In A&V studie nr. 23 'Beveiliging van persoonsgegevens' is een vertaling van de wettelijke eisen naar maatregelen gegeven gebaseerd op een indeling van persoonsgegevens naar risicoklassen. Elke keuze, anders dan in het Raamwerk als handreiking en voorbeeld is uitgewerkt, voor de inbedding van de WBP-eisen in de organisatie is toegestaan.

Raamwerk

Eerder is gesteld dat aard en omvang van persoonsgegevens, de doelstellingen van de verwerking en wijze waarop dat geschiedt, per organisatie verschilt. Dit product heeft daarom het begrip 'Raamwerk' als kenmerk meegekregen. Hiermee wordt aangeduid dat de uitwerking, zoals die is gegeven in dit document, is gebaseerd op de meest gangbare, algemene uitgangspunten van de organisatieleer. Aan de hand van die uitgangspunten zal per verwerking moeten worden nagegaan in hoeverre de toepassing van dit Raamwerk aanvullende werkzaamheden vraagt of meer specifieke invulling noodzakelijk maakt in relatie tot het object van onderzoek.

III . 7 Uitvoering Privacy Audit

Fasering

De Privacy Audit dient als elke andere audit op een gestructureerde wijze opgezet en uitgevoerd te worden. Dit waarborgt een effectieve en efficiënte uitvoering van het onderzoek. In het algemeen zal een Privacy Audit uit de volgende stappen bestaan:

- vaststelling van de onderzoeksopdracht;
- voorbereiding van het onderzoek;
- uitvoering van het onderzoek;
- evaluatie en rapportering van bevindingen.

Vaststelling van de onderzoeksopdracht

Auditor en opdrachtgever dienen overeenstemming te bereiken over doel en reikwijdte van de opdracht. De minimale reikwijdte van het onderzoek ligt verankerd in de wet. Tevens dienen afspraken gemaakt te worden over de verantwoordelijkheden van beide partijen, de uitvoering en de wijze van rapportering. Het is aan te bevelen de onderzoeksopdracht, voor aanvang van het onderzoek, schriftelijk vast te leggen in een opdrachtbevestiging.

[1] *Control Objectives for Information and related Technology, 2nd edition, 1998, Information Systems Audit and Control Foundation.*

In het kader van de Privacy Audit zijn de volgende kwaliteitsaspecten relevant voor de borging van de door de WBP gestelde eisen en de controle daarop:

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 daarover gemaakte afspraken en de wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van de gegevensverwerking.

4 Controleerbaarheid
De controleerbaarheid is de mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat het kwaliteitsaspect controleerbaarheid de mate waarin het mogelijk is vast te stellen dat de verwerking van persoonsgegevens in overeenstemming met de eisen ten aanzien van de hiervoor genoemde kwaliteitsaspecten is uitgevoerd.

De mate waarin deze aspecten in een concrete situatie gehanteerd moeten worden, is mede afhankelijk van de door de auditor uitgevoerde risicoanalyse. De keuze voor de kwaliteitseisen per onderzoeksobject dient in het auditplan gemotiveerd weergegeven te worden. In welke mate de genoemde kwaliteitsaspecten relevant zijn voor het verkrijgen van een certificaat wordt uitgewerkt in het certificeringschema.

Het is mogelijk om in een opdrachtbevestiging voor een Privacy Audit een bredere reikwijdte te hanteren dan zoals in dit Raamwerk is aangegeven. Zo kan een opdrachtgever er belang bij hebben dat de auditor ook de efficiency van de getroffen maatregelen en procedures beoordeelt. Een dergelijke uitbreiding van de reikwijdte tast het fundament van de audit niet aan. Het beperken van de reikwijdte van het onderzoek is niet toegestaan.

Voorbereiding van het onderzoek

Onderzoek organisatie en controleomgeving

Voor een doeltreffende en efficiënte uitvoering van het onderzoek dient de auditor inzicht te hebben in de organisatie en de controleomgeving. Deze activiteit vormt het fundament voor het in deze fase te ontwikkelen auditplan. Dit onderzoek omvat in ieder geval een beoordeling van de volgende elementen:

- organisatie (kennis van de bedrijfsactiviteiten, concernstructuur, organisatieschema, informatiebeleid, privacybeleid, aanwezigheid functionaris voor de gegevensbescherming);
- leiding van de organisatie (integriteit, houding ten opzichte van privacybescherming en gegevensverwerking in het algemeen, gebruik beheersingsinstrumenten);
- overige relevante wetgevingsvereisten (specifieke sectorale of

horizontale wetgeving, gedragscodes);
- aard en omvang van de persoonsgegevens (soorten persoonsgegevens, verwerking van bijzondere gegevens, impact maatschappelijke schade voor betrokkenen bij onrechtmatige verwerking);
- inrichting van de verwerkingsomgeving (gegevensstromen, inrichting ICT-infrastructuur, inrichting fysieke verwerkingsomgeving, administratief-organisatorische procedures en maatregelen).

Het is wenselijk vooraf overleg te voeren met de bij de bescherming van de persoonsgegevens betrokken functionarissen binnen de organisatie. Daarbij 2valt onder meer te denken aan: de hoogste leiding, de verantwoordelijke functionarissen voor de verwerking, de bewerker en de functionaris voor de gegevensbescherming (ex art. 62 WBP).

Risicoanalyse

Voor een effectieve en efficiënte opzet van een Privacy Audit is het noodzakelijk een gedegen risicoanalyse uit te voeren. De uitkomst van deze analyse bepaalt in belangrijke mate de soort en omvang van de controlewerkzaamheden op het intern getroffen stelsel van technische en organisatorische maatregelen ter beveiliging van de verwerking van persoonsgegevens. Verwacht mag worden dat de leiding van de organisatie deze maatregelen heeft afgestemd op de bedreigingen die gezien de aard van de persoonsgegevens, de omvang van de verwerking en de invloed daarvan op de maatschappelijk positie van de betrokkenen bij een onrechtmatige verwerking verwacht mogen worden. Het College bescherming persoonsgegevens adviseert organisaties om het stelsel van technische en organisatorische maatregelen af te stemmen op de in de A&V studie 'Beveiliging van persoonsgegevens' gedefinieerde risicoklassen. Het schema voor het bepalen van de risicoklasse is hieronder opgenomen. Voor een toelichting op het schema wordt verwezen naar A&V studie nr. 23 'Beveiliging van persoonsgegevens'.

Schema voor het bepalen van de risicoklasse

Hoeveelheid persoonsgegevens	*Aard van de verwerking (complexiteit)*	*Aard van de persoonsgegevens*		
		Algemeen	*Bijzonder art. 16 WBP*	*Financieel/economisch*
Weinig	Laag	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Veel	Hoog	Risicoklasse I	Risicoklasse III	

De risicoanalyse in het kader van de Privacy Audit omvat naast bovengenoemde analyse tevens een beoordeling van de overige in de paragraaf 'Onderzoek organisatie en controleomgeving' genoemde elementen.

Gebruik bevindingen (andersoortige) audits

De Privacy Audit is te kenschetsen als een reguliere vorm van auditing met een eigen specifieke onderzoeksscope. De Privacy Audit kan daarom worden ingepast in bestaande kaders die gelden voor de audit van (financiële) verantwoordingen en IT-audits. Bij de uitvoering van de controle kan de auditor, waar mogelijk, gebruik

maken van de bevindingen van eerder uitgevoerde audits. Een externe auditor kan bij zijn controle ook gebruik maken van door interne auditors uitgevoerde onderzoeken, waaronder Privacy Audits.

Bij gebruik maken van eerdere onderzoeken kan gedacht worden aan IT-audits op rekencentra of andere verwerkingsomgevingen waarbinnen de te onderzoeken verwerking van persoonsgegevens plaatsvindt, alsmede system audits op applicaties waarmee persoonsgegevens worden verwerkt. Het is aan de auditor om op basis van het auditplan en de geconstateerde bevindingen van deze audits vast te stellen, voor welke onderzoeksobjecten en kwaliteitsaspecten en in welke mate de auditor hiervan gebruik kan maken bij de uitvoering van de Privacy Audit.

De voorbereiding van het onderzoek mondt uit in een op de te controleren organisatie en verwerking van persoonsgegevens toegespitst auditplan en daarop aansluitend werkprogramma.

Uitvoering van het onderzoek

De kernactiviteit van de Privacy Audit is het onderzoeken of de verwerking van persoonsgegevens in een organisatie voldoet aan de WBP. De auditor dient vast te stellen dat alle, voor de organisatie, relevante aandachtsgebieden uit het V-deel door de onderzochte organisatie toereikend zijn ingevuld. Het eventueel niet relevant zijn van een of meerdere aandachtsgebieden moet expliciet en gemotiveerd door de organisatie of auditor worden vastgelegd zodat zo nodig achteraf de juistheid en volledigheid van deze motivatie kan worden beoordeeld. Vervolgens dient de auditor de door de organisatie getroffen maatregelen te beoordelen op toereikendheid. Dit vraagt om een weloverwogen professionele oordeelsvorming door de auditor, waar nodig in samenwerking met specifieke juridische ondersteuning.

Hieronder is een inventarisatie opgenomen van de aspecten waaraan de auditor aandacht moet schenken in het kader van de beoordeling van de technische en organisatorische maatregelen ter waarborging van een geoorloofde verwerking in het kader van de WBP.

Als eerste dient de auditor te inventariseren hoeveel verwerkingen van persoonsgegevens binnen de organisatie plaatsvinden. In hoofdstuk 2, paragraaf 1 en 2 van de WBP wordt de verwerking van persoonsgegevens geregeld. De organisatie zal moeten definiëren welke vormen van verwerking er zijn. Aandachtspunten hierbij zijn onder meer:

- van wie de gegevens worden verkregen;
- aan wie welke soorten van (bijzondere) gegevens worden verstrekt;
- waarvoor de gegevens worden gebruikt;
- de structuur van de organisatie en interne en externe relaties;
- welke informatiesystemen en soorten gebruikers worden onderkend;
- binnen welke ICT-infrastructuur de verwerking plaatsvindt;
- welke instanties en informatiesystemen gegevens aanleveren of ontvangen en de wijze waarop dit gebeurt.

Vervolgens dient de auditor per verwerking een analyse te maken waarbij aandacht wordt geschonken aan de volgende aspecten:

- of er een meldingsplicht is;
- of er nadere eisen voor verwerkingen van bijzondere persoonsgegevens zijn;
- wie de verantwoordelijke is en wie de bewerker(s) is (zijn);
- wie de interne beheerder(s) is (zijn);
- welke categorieën betrokkenen er zijn;
- welke soorten van gegevens verwerkt worden of zullen worden;
- wat de herkomst van gegevens is;
- wat de gronden voor verwerking zijn;
- welke categorieën derden er zijn;
- welke personen en instanties bij de verwerking verplicht zijn tot het melden van de verwerking van persoonsgegevens;
- de vaststelling van het doel van het verzamelen;
- wie met de controle belast is (intern verbijzonderd of onafhankelijke auditor);
- wie persoonsgegevens ontvangen.

Er zullen voor de verwerking van persoonsgegevens maatregelen en procedures zijn beschreven respectievelijk moeten worden ontwikkeld. Hieraan liggen ten grondslag de artikelen 6 en 13 WBP. De auditor dient de toereikendheid van deze maatregelen en procedures te beoordelen, waaronder:

- de bewustwording van de personen die persoonsgegevens verwerken;
- de meldingsplicht bij het College bescherming persoonsgegevens (CBP) of de functionaris voor de gegevensbescherming (art. 62 WBP);
- de rechtmatigheid van de verwerking;
- het behoorlijk en zorgvuldig verwerken van persoonsgegevens;
- de transparantie van de verwerking van persoonsgegevens;
- het inzage-, correctie- en verzetsrecht van betrokkenen;
- de bewaking van de actualiteit van de maatregelen;
- het vaststellen van het handhaven en naleven van de WBP (verantwoordingsrecht en controlerecht/-plicht).

Evaluatie en rapportering van bevindingen

Voor het afgeven van een oordeel over de mate waarin de organisatie de wettelijke bepalingen voor de bescherming van persoonsgegevens naleeft, dient de auditor een deugdelijke grondslag te verkrijgen. Hiervoor dient de auditor toereikende controle-informatie te verzamelen en vast te leggen in het onderzoeksdossier. Hierin dienen tevens de overwegingen vastgelegd te worden die hebben geleid tot het oordeel. Het oordeel van de auditor dient altijd helder geformuleerd te zijn.

Tijdens de Privacy Audit kan blijken dat in de organisatie reeds aanwezige specifieke maatregelen moeten worden bijgesteld of dat nieuwe maatregelen moeten worden getroffen om ervoor te zorgen dat in de betreffende omgeving aan de eisen van de WBP wordt voldaan. Via advies aan het verantwoordelijk management kan hieraan invulling worden gegeven.

III . 8 Certificaat privacybescherming

Door technologische ontwikkelingen kunnen organisaties in toenemende mate omvangrijke hoeveelheden gegevens over de persoonlijke levenssfeer van individuen op eenvoudige wijze verzamelen, registreren, verwerken en aanwenden voor verschillende doeleinden. De toenemende technische mogelijkheden om op relatief eenvoudige wijze koppelingen tussen geautomatiseerde gegevensbestanden te realiseren, verdient in dit verband zeker speciale aandacht. Door koppeling van gegevensbestanden wordt de herkomst en het gebruik van gegevens nog moeilijker te traceren. Op deze wijze kunnen de persoonsgegevens die op het eerste oog relatief onschuldig zijn, een andere betekenis krijgen. Deze ontwikkelingen worden maatschappelijk gezien slechts geaccepteerd binnen bepaalde grenzen. Die grenzen heeft de wetgever in de WBP vastgelegd.

Het belang van de bescherming van persoonsgegevens verschilt per organisatie en is afhankelijk van een groot aantal elkaar beïnvloedende factoren. Voorbeelden van dergelijke factoren zijn: de omvang van de organisatie, de aard en de omvang van de verwerkte persoonsgegevens, de (commerciële) organisatiedoelstelling, het gebruik van persoonsgegevens om die doelstelling te realiseren, de maatschappelijke gevolgen van oneigenlijk gebruik van persoonsgegevens.
In het algemeen kan worden gesteld dat, naarmate het belang van de hiervoor genoemde factoren toeneemt, de behoefte aan bescherming van de persoonlijke levenssfeer bij klanten, afnemers, medewerkers etc. groter wordt. Door middel van een privacycertificaat kan een organisatie naar betrokkenen aantonen dat zij op zorgvuldige wijze omgaat met de bescherming van hun persoonsgegevens.

Het realiseren van een privacybescherming die op de specifieke situatie van een organisatie is toegesneden, is geen sinecure. Vaak wordt verondersteld dat een certificaat per definitie uitsluitend bestemd is voor grootschalige gegevensverzamelingen en grote organisaties. Ook in kleinschaliger situaties waarin sprake is van het verwerken van persoonsgegevens met een hoog risiconiveau, kan een certificaat echter wenselijk zijn. Het management van een organisatie zal zelf een gemotiveerde keuze moeten maken. Interne en externe adviseurs kunnen aan het maken van die keuze een zinvolle bijdrage leveren. Daarnaast kunnen belangengroepen bij de leiding van een organisatie aandringen op het verkrijgen van een privacycertificaat.

De strekking van een privacycertificaat dient voor de maatschappelijke acceptatie helder en eenduidig geformuleerd te zijn. De wereld die achter een certificaat schuil gaat, is omvangrijk en complex. Het is daarom noodzakelijk eisen te formuleren over de betekenis en inhoud van het certificaat en eisen te formuleren over de deskundigheid van degene die het certificaat afgeeft.

Het Raamwerk Privacy Audit vormt de basis voor het afgeven van een certificaat door een erkende, onafhankelijke auditor. De eisen waaraan de verwerking van persoonsgegevens moet voldoen, zijn verder uitgewerkt in een certificeringschema. De eisen die worden gesteld aan de auditor en de wijze waarop de Privacy Audit moet worden uitgevoerd, zijn opgenomen in het accreditatieschema. Beide schema's zullen zodra deze gereed zijn, worden opgenomen op de website van het CBP (www.cbpweb.nl).

Juridisch kader voor privacybescherming

IV . 1 Grondwet

Eerbiediging van de persoonlijke levenssfeer is één van de grondrechten van onze rechtsorde. Het recht op eerbiediging van de persoonlijke levenssfeer in vastgelegd in artikel 10 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.*

Waarin vertalen zich nu deze beginselen? Sinds 1989 wordt hieraan uitvoering gegeven door de Wet persoonsregistraties (WPR), waaruit regels voortvloeien voor de rechtmatige en zorgvuldige omgang met persoonsgegevens. De WPR is in 2001 vervangen door de Wet bescherming persoonsgegevens (WBP). Deze nieuwe wet verschilt op een aantal belangrijke punten van de WPR. De wijzigingen weerspiegelen de sterk gegroeide en nog steeds groeiende mogelijkheden van informatie- en communicatietechnologie (ICT). De WBP is op hoofdlijnen gelijk aan de Europese richtlijn 95/46/EG, die op 25 oktober 1995 werd aangenomen. Deze richtlijn schrijft voor hoe lidstaten moeten omgaan met de verwerking van persoonsgegevens.

IV . 2 Begrippenkader van de WBP

De WBP roept een aantal rechten en plichten in het leven. De reikwijdte van de in de WBP opgenomen bepalingen wordt in belangrijke mate bepaald door de definities die in de wet zijn opgenomen. De belangrijkste begrippen worden hieronder weergegeven (art. 1 onder a tot en met g 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.

De Wet bescherming persoonsgegevens hanteert een begrippenkader dat aanleiding kan geven tot onduidelijkheden in relatie tot de in de dagelijkse praktijk gehanteerde begrippen, met name in de sfeer van de informatie- en communicatietechnologie (ICT). Dit betreft met name de term 'verwerking' die in relatie tot persoonsgegevens wordt gehanteerd. Ook het deelbegrip 'gegevens' in persoonsgegevens dient duidelijk onderscheiden te worden van de term 'gegevens' zoals dat in ICT-jargon gebruikt wordt.

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 de betekenis van een begrip zijn in dit document de volgende begrippenkaders gehanteerd:

WBP artikel	WBP context	ICT context
1 onder a	*Persoonsgegevens*	*Gegevens*
1 onder b	*Verwerking van persoonsgegevens*	*Gegevensverwerking*
13	*Beveiliging van persoonsgegevens*	*(Informatie)beveiliging*

Volledige teksten

Op de website van het College bescherming persoonsgegevens zijn de integrale teksten opgenomen van:

- de Wet bescherming persoonsgegevens;
- het Vrijstellingsbesluit;
- het Meldingsbesluit;
- de procedure voor het melden van een verwerking van persoonsgegevens.

Het ministerie van Justitie heeft een Handleiding Wet bescherming persoonsgegevens opgesteld ten behoeve van organisaties. Deze handleiding geeft in begrijpelijke taal een uitleg van de wettelijke bepalingen en bevat nuttige tips en handreikingen die organisaties helpen bij het implementeren van de wettelijke eisen. De handleiding is te vinden op www.minjust.nl.

Verwerkingseisen voor persoonsgegevens

(artikel 1, 2, 3, 4)

Reikwijdte van de wet

Artikel 2, eerste lid Wet bescherming persoonsgegevens luidt:

Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Dit artikel houdt in dat een verwerking van persoonsgegevens zich niet per definitie volledig binnen het ICT-domein hoeft te bevinden. Ook (delen van) verwerkingen van persoonsgegevens die vastgelegd worden op andere media zoals papier, audio of video vallen onder de reikwijdte van de Wet bescherming persoonsgegevens en zijn derhalve object van onderzoek tijdens een Privacy Audit.

Uitgangspunt Raamwerk

Uitgangspunt van het Raamwerk is dat is vastgesteld dat er sprake is van een verwerking van persoonsgegevens en dat deze verwerking valt onder de reikwijdte van de wet (art. 1 tot en met 4 WBP).

Inleiding

(artikel 25, 26, 29)

De Wet bescherming persoonsgegevens biedt het normatief kader van waaruit de specifieke technische en organisatorische maatregelen voor voor een organisatie moeten worden afgeleid. Naast deze wet waarin de algemene privacybescherming wordt geregeld, is er mogelijk nog andere wet- en regelgeving waaruit normen voor de organisatie gehaald moeten worden. In de Privacy Audit wordt de toepassing van alle relevante wetgeving in de beoordeling betrokken.

Vrijstellingsbesluit
Indien een verwerking van persoonsgegevens wordt vrijgesteld van melden dan geeft het Vrijstellingsbesluit extra bepalingen die van toepassing zijn op de noodzakelijke maatregelen zoals die voor organisaties uit de WBP volgen.

Sectorale wetgeving
Hierbij worden de wetten bedoeld die speciaal voor een sector zijn ontwikkeld en waarin privacy een onderdeel is van de regelgeving. Voorbeelden van sectorale wetgeving zijn: Wgba, Wgbo, Wpolr, Wmk en Osv.

Andere wet- en regelgeving
Hierbij wordt regelgeving bedoeld die een horizontale werking heeft.
Als voorbeeld geldt hier de Telecommunicatiewet.

Gedragscodes
Er zijn bedrijfssectoren die een gedragscode (art. 25 WBP) hebben ontwikkeld. Dergelijke gedragscodes, goedgekeurd door het CBP, bevatten regels die bij een Privacy Audit in die sector als norm gebruikt moeten worden.

Algemene maatregel van bestuur
Er kunnen sectoren zijn waarvoor bij Algemene maatregel van bestuur nadere regels worden gesteld voor de artikelen 6 tot en met 11 en 13 (art. 26 WBP). Dergelijke maatregelen bevatten eveneens regels die bij een Privacy Audit in die sector als norm gebruikt moeten worden.

Voornemen en melden

(artikel 24, 27, 28, 29, 30, 31, 32, 43)

Binnen de organisatie worden persoonsgegevens verwerkt waarop de Wet bescherming persoonsgegevens van toepassing is. Dit feit moet gemeld worden bij het College bescherming persoonsgegevens of bij de functionaris voor de gegevensbescherming.

Tijdens het uitvoeren van de Privacy Audit zal een oordeel gegeven moeten worden over één van de volgende twee punten:

1 Als er een beroep gedaan is op het Vrijstellingsbesluit, zal vastgesteld moeten worden of dit op de juiste gronden is gedaan.

2 Als de verwerking van persoonsgegevens bij het College bescherming persoonsgegevens of bij de functionaris voor de gegevensbescherming is gemeld, zal vastgesteld moeten worden dat de gemelde informatie overeenstemt met de feitelijke situatie in de organisatie.

1 Vaststellen van de aard van de verwerking en de verplichting tot melden

De eerste stap die genomen wordt, is het typeren van de verwerking. Deze stap is noodzakelijk om te kunnen beoordelen of de verwerking mogelijk is vrijgesteld van de verplichting tot melden bij het CBP of de functionaris voor de gegevensbescherming (art. 62 en vervolgens art. 27 WBP).

Stel vast:

- de aard van de verwerking;
- of de gegevensverwerking voorkomt in het Vrijstellingsbesluit;
- of de verwerking overeenkomt met de beschrijving daarvan in het toepasselijke artikel van het Vrijstellingsbesluit;
- voorlichtingsmateriaal van het CBP (bijvoorbeeld meldingsdiskette of website) geeft na correcte invulling uitsluitsel of er gemeld moet worden of niet. De middelen die het CBP ter beschikking stelt voor het doen van de melding bevat een overzicht van de van melding vrijgestelde verwerkingen;
- dat de verwerking is vrijgesteld van de verplichting tot melden bij het CBP of de functionaris voor de gegevensbescherming;
- dat de verwerking is gemeld bij het CBP of bij de functionaris voor de gegevensbescherming;
- dat actie wordt ondernomen om de melding bij het CBP of de functionaris voor de gegevensbescherming te realiseren.

2 Melding

Voor de melding van de verwerking die niet is vrijgesteld van de verplichting tot aanmelding, is het noodzakelijk dat een aantal zaken bekend is voordat de aanmelding plaatsvindt. Een vrijstelling tot melding ontslaat de organisatie niet van de naleving van de overige bepalingen van de WBP.
De auditor dient vast te stellen dat alle wettelijk vereiste informatie in de melding is opgenomen, te weten:

- de naam en het adres van de verantwoordelijke;
- het doel of de doeleinden van de verwerking;
- een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben;

- een beschrijving van de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;
- een mededeling over voorgenomen doorgifte(n) van gegevens naar landen buiten de Europese Unie;
- een algemene beschrijving van de technische en organisatorische maatregelen die de beveiliging van persoonsgegevens waarborgen;
- een beschrijving van het doel of de doeleinden waarvoor de gegevens of categorieën van gegevens zijn of worden verzameld.

3 Voorafgaand onderzoek door het CBP

In bepaalde gevallen gaat aan het melden van de verwerking een onderzoek door het CBP vooraf. Dit is het geval indien:

- het voornemen bestaat om een nummer ter identificatie van personen te verwerken voor een ander doel dan waarvoor het nummer specifiek bestemd is of bij wet of algemene maatregel van bestuur uitdrukkelijk is toegelaten, teneinde gegevens in verband te kunnen brengen met gegevens die worden verwerkt door een andere verantwoordelijke;
  Hierbij geldt de volgende uitzondering: indien het gebruik van het nummer geschiedt voor de doeleinden van de wet waarin het gebruik van het nummer is voorgeschreven;
- het voornemen bestaat om gegevens vast te leggen op grond van eigen waarneming zonder de betrokkene te informeren;
- het voornemen bestaat om anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken voor derden.

Vastgesteld wordt om welke van de bovengenoemde gevallen het gaat.
Daarvan wordt vastgelegd:

- de melding bij het CBP;
- de opschorting van de verwerking;
- het moment waarop het resultaat van het onderzoek van het CBP vaststaat.

4 Bijhouden van een centraal register

In de organisatie wordt op een centraal punt, bijvoorbeeld bij de functionaris voor de gegevensbescherming een overzicht bijgehouden van de gemelde verwerkingen van persoonsgegevens. Het overzicht bevat ten minste de inlichtingen die voor een melding zijn voorgeschreven en voor zover relevant ook de ontvangstbevestigingen van de meldingen bij het CBP. Het overzicht kan door iedereen kosteloos worden geraadpleegd.

5 Periodieke beoordeling (vrijgestelde) meldingen

Periodiek of bij gelegenheid van wijzigingen in het verwerkingsproces wordt beoordeeld of een verwerking nog steeds aan de voorwaarde voor vrijstelling voldoet en dat een melding nog steeds juist is.

Vastgelegd wordt:

- een verwerking die afwijkt van de melding. Dit gegeven wordt ten minste drie jaar bewaard;
- of de afwijkende verwerking meer dan van incidentele aard is en of de melding bij het CBP of de functionaris voor de gegevensbescherming moet worden aangevuld en moet worden gemeld.

6 **Verstrekken van inlichtingen over de verwerking**

Aan iedereen die daarom verzoekt worden inlichtingen verstrekt over de verwerking zoals deze is gemeld bij het CBP of de functionaris voor de gegevensbescherming of over de vrijgestelde verwerkingen. Vastgelegd wordt:

- de wijze waarop inlichtingen over het verwerken van persoonsgegevens worden gegeven.

In de situatie waarin niet aan deze verzoeken wordt voldaan, wordt vastgelegd of dit noodzakelijk is in het belang van:

- de veiligheid van de staat;
- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Transparantie

(artikel 33, 34, 41, 43, 44)

Iedereen moet op de hoogte zijn van wat er met zijn persoonsgegevens wordt gedaan.
De betrokkene moet hierover worden geïnformeerd.

1 Informatieverstrekking aan de betrokkene

De betrokkene moet worden geïnformeerd over de gegevensverwerking. Hij heeft het recht op de hoogte te zijn van de verwerking van zijn persoonsgegevens. Hierbij zijn twee situaties te onderscheiden:

De persoonsgegevens worden van de betrokkene zelf verkregen.

Stel vast:

a dat vóór het moment van de verkrijging, het volgende aan de betrokkene wordt medegedeeld:
- de identiteit van de verantwoordelijke;
- de doeleinden van de verwerking waarvoor de persoonsgegevens bestemd zijn.

b of nadere informatie verstrekt moet worden om een behoorlijke en zorgvuldige verwerking te waarborgen. Let daarbij op:
- de aard van de persoonsgegevens;
- de omstandigheden waaronder deze zijn verkregen;
- het gebruik dat ervan wordt gemaakt.

De persoonsgegevens worden op andere wijze verkregen.

Stel vast dat uiterlijk op het moment van vastlegging van de persoonsgegevens of bij verstrekking aan een derde op het moment van de eerste verwerking:

a de betrokkene wordt geïnformeerd over:
- de identiteit van de verantwoordelijke;
- de doeleinden van de verwerking waarvoor de persoonsgegevens bestemd zijn.

b nadere informatie wordt verstrekt om een behoorlijke en zorgvuldige verwerking te waarborgen. Let daarbij op:
- de aard van de persoonsgegevens;
- de omstandigheden waaronder deze zijn verkregen;
- het gebruik dat ervan wordt gemaakt.

Stel vast dat als de betrokkene niet wordt geïnformeerd:

a de betrokkene al op de hoogte is van de verwerking;

b de mededeling van de informatie aan de betrokkene onmogelijk is of een oneven-redige inspanning kost
- leg dan de herkomst van de gegevens vast.

c vastlegging of verstrekking geschiedt bij of krachtens de wet
- verzamel informatie over het betreffende wettelijke voorschrift.

d dit noodzakelijk is in het belang van:
- de veiligheid van de staat;
- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen;

- de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

2 Bijzonderheden bij informatieverstrekking aan betrokkene

Stel vast:

- dat als de organisatie een instelling of dienst is voor wetenschappelijk onderzoek of statistiek er voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor wetenschappelijke en statistische doeleinden kunnen worden gebruikt. De betrokkene hoeft in dat geval niet te worden geïnformeerd;
- of het gaat om persoonsgegevens die deel uitmaken van archiefbescheiden die ingevolge de artikelen 12 of 13 Archiefwet 1995 zijn overgebracht naar een archiefbewaarplaats. De betrokkene hoeft in dat geval evenmin te worden geïnformeerd.

3 Informeren bij werving voor commerciële of charitatieve doelen

Stel vast of persoonsgegevens worden verwerkt in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen. Er dient geregeld te zijn dat:

- er rechtstreeks een boodschap aan de betrokkene wordt gezonden en dat deze daarbij telkens wordt gewezen op de mogelijkheid tot het doen van verzet;
- bij het voornemen om persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken aan betrokkene de mogelijkheden bekend worden gemaakt tot het doen van verzet. De bekendmaking vindt plaats via één of meer dag-, nieuws- of huis-aan-huisbladen of op een andere geschikte wijze;
- als persoonsgegevens regelmatig aan derden worden verstrekt of persoonsgegevens voor rekening van derden worden gebruikt dat de bekendmaking ten minste eenmaal per jaar plaatsvindt.

Doelbinding

(artikel 7, 9, 10)

Persoonsgegevens worden slechts voor een vooraf bepaald doel verzameld. Deze kunnen voor dat doel worden verwerkt en onder voorwaarden voor andere doelen.

1 Doelbinding

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld. Stel vast voor welk doel de gegevens van de onderzochte verwerking zijn verzameld. De hier gevraagde informatie is terug te vinden bij onderdeel V.1. Bepaal of het doel van de verzameling voldoende concreet is omschreven.

2 Verenigbaarheid van de gegevensverwerking

Persoonsgegevens worden verwerkt op een wijze die verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Bepaal voor de onderzochte verwerking of er sprake is van verenigbaarheid met het doel. Bij deze beoordeling dient rekening te worden gehouden met:

- de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens;
- de gevolgen van de beoogde verwerking voor de betrokkene;
- de wijze waarop de gegevens zijn verkregen en de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Als het verwerken niet verenigbaar is met het doel wordt gemotiveerd aangegeven of dit gebeurt op grond van één of meer van de volgende uitzonderingen:

- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen,
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- de veiligheid van de staat;
- de verwerking van de gegevens vindt plaats voor historische, statistische of wetenschappelijke doeleinden. Hierbij wordt vermeld welke voorzieningen zijn getroffen om te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

3 Bewaren van persoonsgegevens

Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Persoonsgegevens mogen langer worden bewaard dan bepaald voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de nodige voorzieningen zijn getroffen om te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

De bewaartermijn kan in bepaalde gevallen ook worden bepaald door een wettelijke regeling, bijvoorbeeld de Algemene wet inzake rijksbelastingen of de Wet geneeskundige behandelovereenkomst:

- stel vast of er een, al dan niet wettelijke, bewaartermijn is vastgesteld.
- bepaal of de persoonsgegevens worden bewaard in overeenstemming met de vastgestelde,
  of, bij het ontbreken van een vastgestelde bewaartermijn
  of de gehanteerde bewaartermijnen acceptabel zijn met het oog op de hiervoor genoemde doeleinden.

4 Geheimhoudingsverplichting

Persoonsgegevens worden niet verwerkt als een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat. Bepaal voor de onderzochte verwerking of er sprake is van een geheimhoudingsplicht en stel vast dat er geen verwerking (buiten de geheimhoudingsvoorschriften) plaatsvindt.

Rechtmatige grondslag

(artikel 6, 8, 16, 17, 18, 19, 20, 21, 22, 23)

Persoonsgegevens mogen alleen worden verzameld en verwerkt wanneer de grondslag daarvoor in de WBP kan worden gevonden. Voor bijzondere persoonsgegevens gelden specifieke regels.

1 Grondslag voor de verwerking van persoonsgegevens

Persoonsgegevens worden slechts verwerkt in één of meer van de volgende gevallen:

- de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die maatregelen zijn noodzakelijk voor het sluiten van een overeenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- de gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
- de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt,
- de gegevensverwerking is noodzakelijk 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 van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Bepaal op welke van de hiervoor genoemde grondslagen in welke gevallen de vastgelegde persoonsgegevens worden verwerkt. De informatie verkregen in onderdeel V.1 is hierbij leidraad.

2 Verwerking van bijzondere gegevens

Bijzondere gegevens worden niet verwerkt tenzij de wet daarvoor een mogelijkheid biedt. Bijzondere gegevens zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (art. 16 WBP).

Bepaal of één van de hierboven genoemde soorten van gegevens worden verwerkt. Is dat het geval, onderzoek dan of dit in overeenstemming is met de situaties genoemd in de artikelen 17 tot en met 23 WBP.

Kwaliteit

(artikel 6, 10, 11)

De verwerking van persoonsgegevens moet voldoen aan kwaliteitseisen. Kwaliteit betekent dat de persoonsgegevens toereikend, terzake dienend, niet bovenmatig, juist en nauwkeurig zijn gelet op de doeleinden waarvoor ze worden verzameld of vervolgens verwerkt.

1 Kwaliteit van de gegevensverwerking

Stel vast dat bij de gegevensverwerking op adequate wijze rekening wordt gehouden met:

- bewaartermijnen (zie ook V.3);
- maatregelen voor de verwerking van bijzondere tekens (diacrieten);
- periodieke opschoning;
- informeren over het verstrekken van gecorrigeerde gegevens aan derden aan wie die gegevens eerder zijn verstrekt;
- eindcontrole bij geautomatiseerde beslissingen;
- juistheid-, volledigheid- en autorisatiecontroles bij ingevoerde gegevens (o.a. ingevoerde gegevens worden zo dicht mogelijk bij de bron gevalideerd en bewerkt).

2 Fouten in de gegevensverwerking

Bij het werken met gegevens worden fouten gemaakt. Stel vast dat er ter beperking van fouten in de gegevensverwerking:

- maatregelen zijn genomen waardoor het maken van fouten wordt geminimaliseerd of gegevensinvoer achterwege wordt gelaten (o.a. integriteit van gegevensverwerking);
- een procedure is voor afhandeling van geconstateerde fouten (juist, volledig en tijdig) en voor het controleren van onregelmatigheden tijdens het opstellen van basisdocumenten, inclusief melding;
- maatregelen zijn genomen waardoor fouten (juist en volledig) tijdens gegevensinvoer worden ontdekt en gemeld;
- een herstelprocedure is voor correctie van onjuiste invoer van gegevens;
- afhandeling plaatsvindt van foutmeldingen door betrokkenen.

Rechten van de betrokkenen

(artikel 5, 35, 36, 37, 38, 39, 40, 41, 42)

Personen over wie gegevens worden verzameld hebben een aantal rechten waaronder het recht op inzage, correctie, verwijdering, afscherming en verzet.

1 Effectueren van het recht op inzage

De betrokkene heeft het recht om inzage in zijn persoonsgegevens teverkrijgen. Geregeld wordt:

- hoe en waar het verzoek moet worden ingediend;
- dat de betrokkene binnen vier weken schriftelijk wordt meegedeeld of over hem persoonsgegevens worden verwerkt;
- dat, indien dit zo is tegelijkertijd een volledig overzicht in begrijpelijke vorm wordt verstrekt van de relevante persoonsgegevens, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft, de ontvangers of categorieën van ontvangers en de beschikbare informatie over de herkomst van de gegevens;
- dat, indien een derde naar verwachting bedenkingen zal hebben, die derde in de gelegenheid wordt gesteld zijn zienswijze naar voren te brengen, tenzij gemotiveerd wordt waarom dit onmogelijk is of een onevenredige inspanning kost;
- dat, indien de betrokkene daarom verzoekt, mededelingen worden gedaan over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de betreffende gegevens;
- dat, indien de logica niet wordt meegedeeld, de motivering wordt gegeven waarom op grond van één of meer van de volgende gevallen een beroep is gedaan op het noodzakelijke belang van:
  - de voorkoming, opsporing en vervolging van strafbare feiten;
  - gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
  - het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen;
  - de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
  - de veiligheid van de staat.

Er kunnen zich bijzonderheden voordoen bij verzoeken om inzage. Zijn er maatregelen getroffen opdat:

- indien een gewichtig belang van de verzoeker dit eist, aan een andere dan schriftelijke vorm die aan dat belang is aangepast, aan het verzoek wordt voldaan;
- het verzoek ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt en ten aanzien van een onder curatele gestelde gedaan wordt door hun wettelijke vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijke vertegenwoordigers;
- de identiteit van de verzoeker deugdelijk wordt vastgesteld.

2 Verbeteren, aanvullen, verwijderen of afschermen

Een verzoek om inzage kan worden gevolgd door een verzoek de persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig

of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. In dat geval wordt aandacht besteed aan de volgende onderwerpen:

- of het verzoek de aan te brengen wijzigingen bevat;
- of de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk wordt bericht of dan wel in hoeverre aan het verzoek wordt voldaan;
- of een weigering op het verzoek met redenen is omkleed;
- of een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd;
- of, indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, de gebruiker van de gegevens wordt geïnformeerd over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming;
- of het verzoek ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt en ten aanzien van een onder curatele gestelde gedaan wordt door hun wettelijke vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijke vertegenwoordigers;
- of, indien er persoonsgegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd, de derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis te geven van de verbetering, aanvulling, verwijdering of afscherming, tenzij gemotiveerd is dit dat dit onmogelijk blijkt of een onevenredige inspanning kost;
- of, indien de betrokkene dit verzoekt, opgave wordt gedaan van degenen aan wie de mededeling is gedaan;
- of de vergoeding wordt teruggegeven als er op het verzoek, op aanbeveling van het CBP of op bevel van de rechter tot verbetering, aanvulling, verwijdering of afscherming is overgegaan.

Uitzondering: er kan sprake zijn van bij de wet ingestelde openbare registers, waarvoor in die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is opgenomen.

3 Verzet

Onder verzet wordt verstaan het aantekenen van bezwaar tegen de verwerking van persoonsgegevens.

Relatief verzet

Tegen specifieke verwerking van gegevens kan de betrokkene bij de verantwoordelijke te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

Dit kan in de volgende gevallen:

- de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt;

- de gegevensverwerking is noodzakelijk 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 van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Voor het verzet dient geregeld te zijn dat:

- binnen vier weken na ontvangst van het verzoek wordt beoordeeld of het verzet gerechtvaardigd is;
- indien het verzet gerechtvaardigd is, de verwerking terstond wordt beëindigd;
- voor het in behandeling nemen van het verzet de gevraagde vergoeding van kosten niet hoger is dan een bij of krachtens algemene maatregel van bestuur vastgesteld bedrag;
- de vergoeding teruggegeven wordt in geval het verzet gegrond wordt bevonden.

Het voorgaande is niet van toepassing op openbare registers die bij wet zijn ingesteld.

Absoluut verzet (verzet tegen verwerking voor commerciële of charitatieve doelen)

Als er persoonsgegevens worden verwerkt in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen, heeft de betrokkene het recht zich tegen deze verwerking te verzetten.

Aan een dergelijk verzoek moet altijd gehoor worden gegeven. Stel vast of is geregeld dat:

- de betrokkene te allen tijde kosteloos verzet kan aantekenen;
- indien rechtstreeks een boodschap aan de betrokkene wordt toegezonden, deze daarbij telkens wordt gewezen op de mogelijkheid tot het doen van verzet;
- maatregelen worden getroffen om deze vorm van verwerking terstond te beëindigen;
- indien het voornemen aanwezig is om persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken passende maatregelen worden genomen om de betrokkenen de mogelijkheden bekend te maken tot het doen van verzet;
- de bekendmaking plaats vindt via één of meer dag-, nieuws- of huis-aan-huisbladen of op een andere aan te geven geschikte wijze;
- bij regelmatige verstrekking aan derden of gebruik voor rekening van derden, de bekendmaking jaarlijks plaatsvindt.

4 Geautomatiseerde beslissingen over iemands persoonlijkheid

Niemand kan worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van

persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid. Indien dit wel gebeurt moet worden vastgesteld waarom dit gebeurt. Stel vast of:

- het besluit wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst en:
  - aan het verzoek van de betrokkene is voldaan;
  - de betrokkene in de gelegenheid is gesteld omtrent het besluit zijn zienswijze naar voren te brengen;
- de grondslag te vinden is in een wet waarin maatregelen zijn vastgelegd die strekken tot bescherming van het gerechtvaardigde belang van de betrokkene;
- de betrokkene de logica wordt meegedeeld die ten grondslag ligt aan de geautomatiseerde verwerking van gegevens over hem.

Beveiliging

(artikel 6, 12, 13)

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

Het CBP heeft een apart document ontwikkeld waarin een normatief kader is uitgewerkt dat volgt uit artikel 13 WBP. Dit is A&V studie nr. 23 'Beveiliging van persoonsgegevens'. In deze studie zijn de te nemen maatregelen, afhankelijk van de onderkende risicoklassen van persoonsgegevens, gegroepeerd in de volgende 14 categoriëen:

1 Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van procedures en maatregelen
2 Administratieve organisatie
3 Beveiligingsbewustzijn
4 Eisen te stellen aan personeel
5 Inrichting van de werkplek
6 Beheer en classificatie van de ICT infrastructuur
7 Toegangsbeheer en -controle
8 Netwerken en externe verbindingen
9 Gebruik van software
10 Bulkverwerking van gegevens
11 Bewaren van gegevens
12 Vernietiging van gegevens
13 Continuïteitsplan
14 Uitbesteding van verwerking van persoonsgegevens

Het CBP stimuleert het gebruik van technische maatregelen (Privacy-Enhancing Technologies - PET). Indien er een keuze bestaat tussen een technische en een organisatorische maatregel heeft de minister van Justitie de voorkeur uitgesproken voor een technische (PET) maatregel. De achtergrond hiervan is dat een technische maatregel doeltreffender is omdat het moeilijker is aan het effect ervan te ontkomen.

Beoordeel de toereikendheid van de getroffen maatregelen en stel vast dat deze passend zijn gelet op:

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

Beoordeel de afweging tussen organisatorische en technische maatregelen door de verantwoordelijke gelet op de uitspraken van de minister van Justitie zoals hierboven verwoord.

Verwerking door een bewerker

(artikel 14)

Niet de verantwoordelijke zelf verwerkt de persoonsgegevens, maar dit is (deels) uitbesteed aan een bewerker. Dit is vastgelegd in een overeenkomst of een andere rechtshandeling zodat er een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

Bepaal of er sprake is van uitbesteding van de verwerking aan een bewerker. Indien hiervan sprake is stel vast dat er een overeenkomst tussen verantwoordelijke en bewerker is en dat daarin wordt geregeld dat:

- iedereen die handelt onder het gezag van de bewerker, alsook de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, deze slechts in opdracht van de verantwoordelijke verwerken, behoudens afwijkende wettelijke verplichtingen;
- de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten voor het ten uitvoer leggen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiliging tegen verlies of tegen enige vorm van onrechtmatige verwerking. Het betreft hier de in hoofdstuk V.9 beschreven maatregelen en procedures;
- indien de bewerker is gevestigd in een ander land van de Europese Unie dat de bewerker de WBP en het specifieke recht van dat land met betrekking tot algemene beveiligingseisen naleeft;
- met het oog op het bewaren van het bewijs de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens alsmede de bedoelde beveiligingsmaatregelen, schriftelijk of in een andere, gelijkwaardige vorm worden vastgelegd;
- de verantwoordelijke de naleving van de overeenkomst en wettelijke bepalingen die op de verwerking van toepassing zijn, periodiek controleert. De controle kan namens de verantwoordelijke worden uitgevoerd door een (externe) onafhankelijke auditor. De bewerker kan ook periodiek een controle laten uitvoeren door een externe onafhankelijke auditor. Van de uitgevoerde controle krijgt de verantwoordelijke een rapport.

Gegevensverkeer met landen buiten de Europese Unie

(artikel 76, 77)

Voor persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt in een land buiten de Europese Unie, gelden, onverminderd de naleving van de wet, aanvullende regels. Dit gegevensverkeer is aan regels gebonden.

Bepaal of er sprake is van gegevensverkeer met landen buiten de Europese Unie.

Indien daarvan sprake is wordt in het onderzoek gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevens van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doel of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.

Beoordeel bij gegevensverkeer buiten de EU dat:

- het betreffende land een passend beschermingsniveau waarborgt, of
- als het betreffende land geen passend beschermingsniveau waarborgt, dat aan één of meer van de volgende voorwaarden is voldaan:
  - de betrokkene heeft daarvoor zijn ondubbelzinnige toestemming gegeven;
  - de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
  - de doorgifte is noodzakelijk voor de sluiting of uitvoering van een overeenkomst die in het belang van de betrokkene tussen de verantwoordelijke en een derde is gesloten of zal worden gesloten;
  - de doorgifte is noodzakelijk vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht;
  - de doorgifte is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
  - de doorgifte geschiedt vanuit een register dat bij wettelijk voorschrift is ingesteld en dat door een ieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, voor zover in het betrokken geval is voldaan aan de wettelijke voorwaarden voor raadpleging;
- de minister van Justitie heeft, gehoord het CBP, een vergunning gegeven voor een doorgifte of een categorie doorgiften van persoonsgegevens. De doorgifte vindt plaats conform de voorschriften die aan de vergunning zijn verbonden.

Bijlagen

Relatie tussen de artikelen van de WBP en de verwerkingseisen

Deze bijlage geeft aan in welke wetsartikelen de basis wordt gevonden voor de in dit Raamwerk geïdentificeerde aandachtsgebieden van verwerking (V.I, V.1 tot en met V.9).

Verwerkingseisen volgens Raamwerk	V.I	V.1	V.2	V.3	V.4	V.5	V.6	V.7	V.8	V.9
Artikelen										
Algemene bepalingen										
1										
2										
3										
4										
5							●			
Rechtmatigheid										
6					●	●		●		
7				●						
8					●					
9				●						
10				●		●				
11						●				
12								●		
13								●		
14									●	
15										
Bijzondere gegevens										
16					●					
17					●					
18					●					
19					●					
20					●					
21					●					
22					●					
23					●					
24		●								
Gedragscodes										
25	●									
26	●									

Verwerkingseisen volgens Raamwerk

	V.I	V.1	V.2	V.3	V.4	V.5	V.6	V.7	V.8	V.9
Artikelen										
Melden en voorafgaand onderzoek										
27		●								
28		●								
29	●	●								
30		●								
31		●								
32		●								
Informatieverstrekking										
33			●							
34			●							
Rechten van de betrokkene										
35							●			
36							●			
37							●			
38							●			
39							●			
40							●			
41			●				●			
42							●			
Uitzondering en beperkingen										
43		●	●							
44			●							
Gegevensverkeer buiten de EU										
76										●
77										●

Organisatie van de verwerking

Deze bijlage geeft een toelichting op de onderwerpen waaraan binnen de organisatie van de verwerking invulling gegeven dient te worden. Hierbij wordt uitgegaan van de managementcyclus. Deze bijlage is te beschouwen als een handreiking waarbij op basis van de methodiek van CobiT (2nd edition, 1998) een uitwerking is gegeven van mogelijke maatregelen en procedures die bijdragen aan de realisering van de wettelijke eisen.

De managementcyclus start met het formuleren van beleid alvorens de verwerkingsorganisatie in te richten. Deze bijlage, Organisatie van de verwerking, bevat de onderwerpen die hiervoor relevant zijn, zoals het bepalen van het algemene informatiebeveiligingsbeleid, het privacybeleid, privacyplanning, en het bepalen van het privacyplan. Van belang zijn hierbij onder meer het definiëren van de informatiearchitectuur en het inventariseren van privacyrisico's in relatie tot die architectuur.

Voor de organisatie van de verwerking worden de volgende 23 aandachtsgebieden onderkend. In het vervolg van deze bijlage zullen per aandachtsgebied de belangrijkste aspecten benoemd en kort toegelicht worden.

O.1	Planning en organisatie van de verwerking van persoonsgegevens
O.2	Definieer de ICT-infrastructuur
O.3	Bepaal het technologiebeleid
O.4	Definieer de verwerkingsorganisatie en haar relaties
O.5	Management van kwaliteit bevorderende verwerkingsinvesteringen
O.6	Communiceren van privacydoelstellingen en privacybeleid
O.7	Personeelsmanagement
O.8	Waarborgen dat aan aanvullende eisen wordt voldaan
O.9	Beoordelen van afhankelijkheid en kwetsbaarheid van de gegevensverwerking
O.10	Projectmanagement
O.11	Kwaliteitsmanagement voor de gegevensverwerking
O.12	Service level beheer
O.13	Beheren van diensten van derden
O.14	Beschikbaarheidsbeheer
O.15	Waarborgen van continuïteit
O.16	Waarborgen van logische toegangsbeveiliging
O.17	Opleiden en trainen van gebruikers
O.18	Ondersteunen en adviseren van gebruikers (helpdesk)
O.19	Configuratiebeheer
O.20	Probleembeheer en incidentenbeheer
O.21	Gegevensbeheer
O.22	Faciliteitenbeheer
O.23	Operationeel beheer

O.1 Planning en organisatie van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens is het van belang dat het management in het organisatieplan ook aandacht besteedt aan privacy. Het management vertaalt de WBP privacyaspecten (zie hoofdstuk V, Verwerkingseisen voor persoonsgegevens) in een privacybeleid dat in relatie staat tot de aard, de omvang en het gebruik van de persoonsgegevens die binnen de organisatie worden verwerkt.

Dit beleid vertaalt het management vervolgens in richtlijnen en procedures, waarbij aandacht is voor de volgende zaken:

1 **Definieer een strategisch WBP plan**

Definieer een strategisch plan voor de verwerking van persoonsgegevens. Het management is verantwoordelijk voor de ontwikkeling en invoering van lange en korte termijn organisatieplannen waarmee de organisatie haar verantwoordelijkheid waarmaakt om de persoonsgegevens behoorlijk en zorgvuldig te verwerken.

2 **Lange termijn WBP plan**

Het management van de verwerkingsfunctie is verantwoordelijk voor het periodiek ontwikkelen van lange termijn verwerkingsplannen die het behalen van de missie en doelstellingen van de organisatie ondersteunen. Het management dient dus een lange termijn planningsproces te implementeren, een gestructureerde aanpak te hanteren en een standaardstructuur voor plannen op te stellen.

3 **Lange termijn WBP planning; aanpak en structuur**

Het management van de verwerkingsfunctie dient een gestructureerde aanpak op te stellen en in te voeren voor het lange termijn planningsproces. Dit moet resulteren in een plan van hoge kwaliteit, dat de basisvragen 'hoe, wat en wie' beantwoordt.

4 **Lange termijn WBP planning; wijzigingen**

Het management van de verwerkingfunctie dient te zorgen voor een proces dat tijdig en volledig het lange termijn verwerkingsplan aanpast om de wijzigingen in het lange termijn organisatieplan en wijzigingen in de verwerkingsomgeving zijn weerslag te laten vinden in het lange termijn verwerkingsplan.

5 **Korte termijn planning voor de ICT-functie**

Het management van de verwerkingsfunctie dient er zorg voor te dragen dat het lange termijn verwerkingsplan periodiek vertaald wordt in korte termijn verwerkingsplannen. Dergelijke korte termijn plannen moeten ervoor zorgen dat de juiste verwerkingsmiddelen gebruikt worden, in overeenstemming met de lange termijn verwerkingsplannen. Korte termijn verwerkingsplannen dienen periodiek heroverwogen te worden en, indien nodig, aangepast te worden aan de veranderende bedrijfs- en verwerkingsomgeving. De tijdige uitvoering van haalbaarheidsstudies moeten ervoor zorgen dat de uitvoering van korte termijn verwerkingsplannen adequaat wordt gestart.

6 **Periodieke afstemming bestaande situatie**

Stelsel van beheersmaatregelen en - procedures die waarboren dat persoonsgegevens conform de regels van de WBP worden verwerkt.

O.2 Definieer de ICT infrastructuur

De ICT infrastructuur omvat de bedrijfsbrede omgeving waarin persoonsgegevens verwerkt worden.

Binnen deze infrastructuur worden onderkend: mainframecomputers, servers, pc-clients, netwerken, datacommunicatie, systeemsoftware, toepassingssoftware, gegevensverzamelingen, documentatie, procedures en de hierbij betrokken personeelsleden.

Van belang is dat de verwerking van de persoonsgegevens in overeenstemming is met de eisen die de WBP stelt. Het management richt de verwerkingsarchitectuur zodanig in dat de medewerkers in staat zijn hun verantwoordelijkheden efficiënt uit te voeren. De verwerkingsarchitectuur wordt consistent gehouden met de organisatie- en verwerkingsplannen op lange termijn.

Het management vertaalt dit in de navolgende overzichten:

1 **Overzicht van de ICT infrastructuur**

De verwerking van persoonsgegevens moet in overeenstemming worden gehouden met bepalingen in de WBP. Management en medewerkers moeten in staat worden gesteld hun verantwoordelijkheden tijdig en effectief uit te voeren. Hiertoe dient de verantwoordelijke de verwerkingsarchitectuur op te stellen en deze, indien nodig, aan te passen. De ICT infrastructuur dient het bedrijfsbrede gegevensmodel en de bijbehorende informatiesystemen te bevatten. De ICT infrastructuur dient consistent te worden gehouden met het lange termijn verwerkingsplan.

2 **Data dictionary en reken- en verwerkingsregels**

De verwerkingsfunctie dient te waarborgen dat een bedrijfsbrede data dictionary gemaakt en onderhouden wordt. In de data dictionary dienen de reken- en verwerkingsregels van de gegevens (van de organisatie) te zijn opgenomen.

3 **Schema voor gegevensclassificatie (risicoanalyse)**

Er dient een algemeen classificatiekader te worden gemaakt waarmee gegevens in risicoklassen kunnen worden geplaatst (bijv. beveiligingsniveaus) en waarmee het eigenaarschap (van gegevens) kan worden toegekend. De toegangsrechten tot de verschillende categorieën dienen adequaat te worden gedefinieerd.

4 **Beveiligingsniveaus (risicoklassen)**

Het management dient beveiligingsniveaus te definiëren, te implementeren en in stand te houden voor elke gegevensclassificatie boven het niveau van "geen beveiliging benodigd". Deze beveiligingsniveaus moeten een toereikende set van (minimale) beveiliging- en controlemaatregelen voor elke gegevensclassificatie bevatten.

O.3 Bepaal het technologiebeleid

Het technologiebeleid maakt onderdeel uit van het informatieplan van de organisatie. Het voor het technologiebeleid verantwoordelijke management ontwikkelt een technologisch infrastructuurplan en actualiseert dit regelmatig. Dit plan is in overeenstemming met het korte- en lange termijn verwerkingsplan en bevat elementen als: systeemarchitectuur, ICT infrastructuur en migratietrajecten. In het technologiebeleid geeft het management onder andere aan welke technologische ontwikkelingen relevant zijn voor de bedrijfsvoering.

Het management vertaalt dit in:

1 **Technisch infrastructuurplan**
De verantwoordelijke moet een technisch infrastructuurplan ontwikkelen en deze regelmatig actualiseren. Het plan moet in overeenstemming zijn met het korte en lange termijn verwerkingsplan en dient aspecten als systeemarchitectuur, technologiebeleid en migratietrajecten te bevatten.

2 **Toezicht houden op toekomstige trends en regelgeving**
De verantwoordelijke moet waarborgen dat voortdurend wordt gelet op toekomstige ontwikkelingen in de privacywetgeving, Privacy-Enhancing Technologies, verwerkingsbeleid en verwerkingsrichtlijnen. Deze factoren dienen in overweging te worden genomen bij de ontwikkeling en het onderhoud van het technisch infrastructuurplan.

3 **Continuïteitsaspecten in het technisch infrastructuurplan**
Het technisch infrastructuurplan moet systematisch worden onderzocht op continuïteitsdeelaspecten (zoals redundantie, robuustheid, geschiktheid en groeimogelijkheden van de technische infrastructuur).

4 **Hard- en software aanschafplanning**
Het management van de ICT functie moet waarborgen dat plannen voor de aanschaf van hard- en software worden opgesteld en dat deze voorzien in de behoeften die in het technisch infrastructuurplan zijn vastgelegd.

O.4 Definieer de verwerkingsorganisatie en haar relaties

Bij de verwerking van persoonsgegevens is van belang dat het management de organisatie van de verwerking van persoonsgegevens definieert. Duidelijk moet zijn hoe en waar persoonsgegevens worden verwerkt binnen de organisatie. Het management wijst een planning- of stuurgroep aan voor het aansturen van de verwerkingsfunctie en haar activiteiten. De groep is samengesteld uit leden van het topmanagement, management van de gebruikersorganisatie en leden van de Informatisering en Automatisering (I&A) functie. De groep vergadert regelmatig en rapporteert aan het topmanagement.

Aandachtspunten bij het definiëren van de verwerkingsorganisatie en haar relaties zijn:

1 **Verwerkingsplanning- of stuurgroep verwerking**

Het management moet een plannings- of stuurgroep aanwijzen voor het aansturen van de verwerkingsfunctie en haar activiteiten. Deze groep moet bestaan uit leden van het topmanagement, management van de gebruikersorganisatie en leden van de I&A functie. De groep moet regelmatig vergaderen en rapporteren aan het topmanagement.

2 **Organisatorisch plaatsen van de verwerkingsfunctie**

Het management dient de verwerkingsfunctie zodanig in de algemene organisatiestructuur te plaatsen dat voldoende autoriteit en onafhankelijkheid van de gebruikersorganisatie wordt gewaarborgd om effectieve verwerkingsoplossingen en voldoende voortgang in de implementatie ervan te kunnen garanderen. De verwerkingsfunctie dient een hechte relatie met het topmanagement op te zetten met als doel het bewustzijn, het begrip en de vaardigheden in de identificatie en oplossing van verwerkingsproblemen te bevorderen.

3 **Beoordelen van organisatorische prestaties**

Er moet een mechanisme zijn die periodiek de organisatiestructuur beoordeeld. Dit om te blijven voldoen aan doelstellingen en veranderende omstandigheden.

4 **Rollen en verantwoordelijkheden**

Het management moet waarborgen dat al het personeel binnen de organisatie op de hoogte is van zijn of haar rol en verantwoordelijkheid in relatie tot verwerkingssystemen. Al het personeel moet voldoende bevoegdheden hebben om de hem/haar toegewezen rol naar behoren uit te (kunnen) voeren. Iedereen moet er zich bewust van worden gemaakt dat hij/zij voor een deel verantwoordelijk is voor de interne controle en beveiliging. Hieruit volgend moeten indien nodig periodiek campagnes worden georganiseerd ter bevordering van bewustzijn en discipline.

5 Verantwoordelijkheid voor kwaliteitsborging

Het management moet de verantwoordelijkheid voor het uitvoeren van kwaliteitsborging toewijzen aan leden van de verwerkingsfunctie. Tevens moet zij waarborgen dat voldoende kennis van kwaliteitsborging, systemen, controle en communicatie aanwezig is binnen deze kwaliteitsfunctie binnen de verwerkingsfunctie. De organisatorische plaats, de verantwoordelijkheden en de omvang van de kwaliteitsfunctie moeten zijn afgestemd op de eisen van de organisatie.

6 Verantwoordelijkheid voor logische en fysieke beveiliging

Het management moet de verantwoordelijkheid voor waarborging van de logische en fysieke informatiebeveiliging formeel toewijzen aan een informatiebeveiligingsbeheerder die rapporteert aan het management. Minimaal dient er bedrijfsbreed een verantwoordelijkheid te worden belegd voor algemene beveiligingskwesties. Indien nodig dienen additionele beveiligingsverantwoordelijkheden te worden toegewezen voor specifieke systemen ter behandeling van de desbetreffende beveiligingskwesties.

7 Eigendom en beheer van persoonsgegevens

Het management moet een structuur opstellen waarbinnen gegevenseigenaren en -gebruikers formeel worden aangewezen. Hun rollen en verantwoordelijkheden moeten duidelijk worden gedefinieerd.

8 Eigendom van persoonsgegevens en verwerkingssystemen

Het management moet waarborgen dat alle persoonsgegevens die in bezit zijn van de organisatie, een aangewezen eigenaar heeft, die beslissingsrecht heeft over gegevensclassificatie en toegangsrechten. Systeemeigenaren delegeren veelal het dagelijks beheer aan systeembeheer en delegeren veelal de beveiliging aan de beveiligingsbeheerder. De eigenaren blijven echter verantwoordelijk voor het toepassen van afdoende beveiligingsmaatregelen.

9 Supervisie

Het management moet goede supervisieactiviteiten in de verwerkingsfunctie implementeren die waarborgen dat taken en verantwoordelijkheden goed worden uitgevoerd, dat onderzoekt of al het personeel de juiste autoriteit en middelen bezit voor het uitvoeren van hun taken en verantwoordelijkheden en dat een globale beoordeling van de prestatie-indicatoren wordt uitgevoerd.

10 Functiescheiding

Het management moet een adequate functiescheiding waarborgen die de mogelijkheid uitsluit dat één persoon een kritisch proces kan beïnvloeden. Het management dient te waarborgen dat medewerkers uitsluitend werkzaamheden verrichten die passen bij de toegewezen functie of positie. Minimaal dient een scheiding te worden aangebracht tussen de systeemontwikkelingfunctie, de gegevensverwerkende functie en de gebruikers van het systeem. De beveiligingsverantwoordelijkheid dient duidelijk gescheiden te zijn van de gegevensverwerkende functie.

11 Personeel

De vereiste samenstelling van personeel voor de verwerkingsfunctie moet periodiek worden geëvalueerd om te waarborgen dat de verwerkingsfunctie voldoende geschikt personeel heeft. De personeelsbehoefte dient minimaal één maal per jaar of bij grote wijzigingen binnen de bedrijfs- of verwerkingsomgeving (verwerkingsorganisatie) te worden geëvalueerd. Op de uitkomst hiervan moet meteen worden gereageerd zodat een goede personeelsvoorziening is gegarandeerd voor nu en de toekomst.

12 Functiebeschrijvingen voor verwerkingspersoneel

De beschrijvingen van de functies binnen de verwerkingsfunctie moeten worden opgesteld en regelmatig worden geactualiseerd. Zij moeten inzicht geven in de autoriteit en verantwoordelijkheid en moeten een definitie bevatten van de vaardigheden en ervaring die benodigd zijn voor de verschillende functies.
De functiebeschrijvingen moeten te gebruiken zijn als prestatie-indicator bij beoordelingsgesprekken.

13 Sleutelposities

Het management dient sleutelposities binnen de verwerkingsfunctie te definiëren en te identificeren.

14 Procedures voor tijdelijk personeel

Het management moet procedures opstellen voor het beheersen van activiteiten voor de verwerkingsfunctie, uitgevoerd door adviseurs en/of ander tijdelijk personeel, ter waarborging van de informatiebeveiliging.

15 Relaties

Het management van de verwerkingsfunctie moet zorg dragen voor een optimale coördinatie-, communicatie- en overlegstructuur tussen de verwerkingsfunctie en de verschillende andere partijen binnen en buiten de verwerkingsfunctie (bijv. gebruikers, leveranciers, beveiliging- en risicobeheerders).

O.5 Management van kwaliteit-bevorderende verwerkingsinvesteringen

Het management implementeert een budgetteringsproces ter waarborging van het jaarlijks opstellen en accorderen van een budget voor de verwerkingsfunctie. Het budget is in overeenstemming met zowel de korte en lange termijn organisatieplannen als de verwerkingsplannen.

Het management stelt een procedure op voor het budgetteringsproces.

1 Jaarlijks verwerkingsbudget

Het management moet een budgetteringsproces implementeren om het jaarlijks opstellen en accorderen van een budget voor de verwerkingsfunctie te waarborgen. Het budget dient in overeenstemming te zijn met zowel de korte en lange termijn organisatieplannen als de verwerkingsplannen.

O.6 Communiceren van privacydoelstellingen en privacybeleid

Het management stelt een raamwerk en een bewustwordingsprogramma op om een kwalitatieve beheersomgeving voor de gegevensverwerking binnen de gehele organisatie te bevorderen. Hierbij moet worden gedacht aan aspecten als integriteit; ethische waarden en vaardigheden van mensen; managementstijl en ook verantwoording, aandacht en sturing door de directie.

Deze uitgangspunten vertaalt het management in:

1 **Kwalitatieve beheersomgeving**

Het management moet een raamwerk en een bewustwordingsprogramma opzetten ter bevordering van de kwaliteit van de beheersomgeving voor de gegevensverwerking binnen de gehele organisatie. Hierbij moet worden gedacht aan aspecten als integriteit, ethische waarden en vaardigheden van mensen, managementstijl en ook verantwoording, aandacht en sturing door de directie.

2 **Managementverantwoordelijkheid voor beleid**

Het management moet de volledige verantwoordelijkheid op zich nemen voor het formuleren, ontwikkelen, documenteren, het openbaar maken en beheersen van een beleid dat aansluit bij de doelstellingen in de verwerkingsorganisatie. Periodiek dient te worden beoordeeld of het beleid voldoet. De complexiteit van geschreven beleid en procedures moet aansluiten bij de omvang van de organisatie en de managementstijl.

3 **Bekend maken van organisatiebeleid**

Het management moet waarborgen dat het organisatiebeleid naar iedereen binnen de organisatie wordt gecommuniceerd en door iedereen (op alle niveaus) wordt begrepen.

4 **Middelen voor de invoering van beleid**

Na bekendmaking van het beleid moet het management afdoende middelen toewijzen voor het implementeren van zijn beleid. Het management dient toezicht te houden op de tijdige invoering van het beleid.

5 **Onderhouden van beleid**

Het beleid moet periodiek worden aangepast aan de veranderende omstandigheden. Het beleid moet worden geëvalueerd, op z'n minst jaarlijks of na belangrijke veranderingen in de verwerkingsomgeving, om te onderzoeken of het beleid nog toereikend is. Indien nodig moet het beleid worden geactualiseerd.
Het management moet zorgen voor een raamwerk en een beheersproces dat het periodieke beoordelen en accorderen van standaarden, beleid, richtlijnen en procedures waarborgt.

6 **Overeenstemming procedures met beleid**

Het management moet waarborgen dat er adequate procedures aanwezig zijn voor het vaststellen van de mate waarin het personeel het geïmplementeerde beleid en procedures heeft begrepen en opgevolgd. Procedures voor overeen-

stemming met ethische, beveiliging- en interne controle standaarden moeten worden ontworpen en gestimuleerd door het management (goed voorbeeld doet goed volgen).

7 Beleid voor beveiliging en interne controle

Het management is vanzelfsprekend verantwoordelijk voor het ontwikkelen van een beleid dat de algemene aanpak van de organisatie voor beveiliging en interne controle ondersteunt. Het beleid moet afgeleid zijn uit de algemene bedrijfsdoelstellingen en moet zijn gericht op minimalisatie van risico's door preventieve maatregelen, tijdige identificatie van onregelmatigheden, beperking van verliezen en gericht op tijdig herstel. Aan de keuze van maatregelen zal een kosten-/baten-analyses voorafgaan. Tevens dient het management duidelijke prioriteiten te stellen. Daarnaast dient het management te waarborgen dat het beveiligings- en interne controlebeleid op hoog niveau de volgende elementen specificeert:

1. het doel;
2. de managementstructuur;
3. de omvang binnen de organisatie;
4. de toewijzing van verantwoordelijkheden voor implementeren;
5. de definitie van straffende en disciplinaire maatregelen als gevolg van het niet opvolgen van beveiligings- en interne controle-maatregelen.

8 Specifiek beleid

Maatregelen moeten worden genomen om te waarborgen dat specifiek beleid wordt gemaakt voor het documenteren van managementbeslissingen die betrekking hebben op specifieke activiteiten, informatiesystemen of technologie.

O.7 Personeelsmanagement

Het management van de ICT functie stelt periodiek vast of het personeel voldoende gekwalificeerd is op basis van een geschikte opleiding, vereiste training en/of ervaring. Het management houdt rekening met aanvullende opleidingsbehoeften van het ICT personeel zodat het ICT personeel voldoende gekwalificeerd is voor ontwikkelingen in de ICT.

Aandachtspunten zijn:

1 **Kwalificatie van personeel**
Het management moet periodiek vaststellen of het personeel (dat specifieke taken uitvoert) voldoende gekwalificeerd is op basis van een geschikte opleiding, vereiste training en/of ervaring.

2 **Training van personeel**
Het management moet waarborgen dat personeel wordt voorzien van voortdurende training voor het up to date houden van kennis, vaardigheden, mogelijkheden en beveiligingsbewustzijn tot het vereiste niveau om te (kunnen) werken.

3 **Screenen van (nieuw) personeel**
Het management moet waarborgen dat nieuw personeel wordt gescreend voor aanname of in geval van overstap naar een andere afdeling, afhankelijk van de gevoeligheid van de aard van de verwerking waarbij zij zijn betrokken. Een werknemer die niet gescreend is bij binnenkomst, moet bij promotie naar een gevoelige functie alsnog gescreend worden.

4 **Beoordelingsgesprek**
Het management moet zorgen voor het implementeren van een proces waarin de medewerker wordt beoordeeld op privacybewustzijn en moet zich ervan verzekeren dat de beoordeling periodiek geschiedt op basis van vastgestelde standaarden en specifieke functieverantwoordelijkheden.

5 **Verandering en beëindiging van functie**
Management moet waarborgen dat gepaste en tijdige acties worden ondernomen bij functieveranderingen en -beëindigingen, zodat deze acties geen gevolg hebben voor de kwaliteit van de interne controle en beveiliging.

O.8 Waarborgen dat aan aanvullende eisen wordt voldaan

De organisatie stelt procedures op en onderhoudt deze voor het beoordelen van externe eisen en voor het coördineren van deze activiteiten. Continu onderzoek moet aangeven welke externe eisen gelden voor de organisatie. Het verantwoordelijk management toetst de toepasselijkheid en naleving van wettelijke, overheids- en andere externe eisen, die samenhangen met uitvoering en beheersing van de gegevensverwerking. Het management onderzoekt wat de impact is van alle externe relaties, op de algemene informatiebehoefte van de organisatie, inclusief het vaststellen van de mate waarin de strategie van de verwerkingsfunctie aan moet sluiten en/of ondersteunend moet zijn aan de vereisten van derden.

Aandachtspunten zijn:

1 **Beoordeling van externe eisen**

De organisatie dient procedures op te stellen en te onderhouden voor de beoordeling van externe eisen en voor de coördinatie van deze activiteiten. Continu onderzoek moet aangeven welke externe eisen gelden voor de organisatie. Wettelijke en andere externe eisen, die samenhangen met uitvoering en beheersing van de gegevensverwerking, moeten worden beoordeeld op hun consequenties. Het management moet onderzoeken wat de impact is van alle externe relaties op de algemene informatiebehoefte van de organisatie, inclusief het vaststellen van de mate waarin de strategie van de verwerkingsfunctie aan moet sluiten en/of ondersteunend moet zijn aan de vereisten van derden.

2 **Acties en procedures om te voldoen aan externe eisen**

De organisatie moet waarborgen dat tijdig de benodigde acties worden ondernomen om te garanderen dat aan externe eisen wordt voldaan. Goede procedures ter waarborging van de continue overeenstemming met externe eisen moeten worden opgesteld en onderhouden.

3 **Elektronische handel (e-commerce, e-handel)**

Het management moet waarborgen dat formele contracten worden opgesteld om overeenstemming te bereiken tussen externe relaties over datacommunicatieprocessen en over standaarden voor transactieboodschappen, beveiliging en gegevensopslag (integriteit gegevensverwerking).

O.9 Beoordelen van afhankelijkheid en kwetsbaarheid gegevensverwerking

Het management zorgt ervoor dat de afhankelijkheid en de kwetsbaarheid van de gegevensverwerking binnen de organisatie duidelijk wordt gemaakt met behulp van een risicoanalyse. Hierbij maakt het management gebruik van een algemeen aanvaarde methode voor de uitvoering van een risicoanalyse. Zo'n methode dient een periodieke beoordeling van de relevante risico's voor het realiseren van WBP eisen en normen te bevatten.

Aandachtspunten zijn:

1 Beoordeling van het verwerkingsrisico

Het management moet zorgen voor een algemeen aanvaarde methode voor de uitvoering van een risicoanalyse. Zo'n methode moet een periodieke beoordeling van de relevante risico's t.a.v. het behalen van WBP doelen te bevatten.

2 Aanpak risicoanalyse

Het management moet zorgen voor een algemene risicoanalyse aanpak, die het bereik en de grenzen, de te gebruiken methodiek, de verantwoordelijkheid en de benodigde vaardigheden definieert. De kwaliteit van de risicoanalyse moet worden gewaarborgd door een gestructureerde methodiek en ervaren risicoanalisten.

3 Identificeren van risico's

De aanpak van de risicoanalyse moet zich richten op het vaststellen van essentiële elementen van een risico, zoals bezittingen, bedreigingen, zwakheden, beveiligingen, consequenties en de waarschijnlijkheid van de bedreigingen.

4 Meting van risico

De risicoanalysemethodiek moet waarborgen dat de informatie uit de risicoanalyse resulteert in een kwantitatieve en/of kwalitatieve meting van het risico waaraan het desbetreffende object onderhevig is. De mate waarin de organisatie het risico kan/wil aanvaarden, moet ook worden onderzocht.

5 Risicoactieplan

De risicoanalysemethodiek moet voorzien in het definiëren van een risicoactieplan om te waarborgen dat kosteneffectieve maatregelen en beveiligingen het blootstaan aan en de gevolgen van risico's continu verminderen.

6 Risico aanvaarding

De risicoanalysemethodiek moet leiden tot een formele aanvaarding van het uiteindelijke (overgebleven) risico op basis van:

1. de risico-identificatie en de meting;
2. het organisatiebeleid;
3. onzekerheden in de risicoanalyse methodiek zelf;
4. de kosten-/batenanalyse van beveiligingen en beheersmaatregelen.

O.10 Projectmanagement

In geval van complexe veranderingen in de architectuur respectievelijk doeleinden van de gegevensverwerking draagt het management zorg voor de realisatie van projectmanagement. Het management beschrijft het bereik en de grenzen van projectmanagement, alsmede de projectmanagement methodiek die wordt toegepast. De gekozen methodiek besteedt, minimaal, aandacht aan het toekennen van verantwoordelijkheden, taakverdeling, budgettering van zowel tijd als middelen, de kwaliteit van de mijlpaalproducten, controlepunten en goedkeuringsmomenten.

Deze uitgangspunten legt het management vast in een document waarin de volgende aandachtspunten zijn opgenomen:

1 **Projectmanagement methodiek**
Bij complexe veranderingen in de architectuur respectievelijk doeleinden van de verwerking moet het management zorgdragen voor de realisatie van projectmanagementaanpak dat het bereik en de grenzen van projectmanagement beschrijft en voor de projectmanagementmethodiek die moet worden toegepast. De methodiek moet, minimaal, aandacht besteden aan het toekennen van verantwoordelijkheden, taakverdeling, budgettering van zowel tijd als middelen, de kwaliteit van de mijlpaalproducten, controlepunten en goedkeuringsmomenten.

2 **Participatie van gebruikersorganisatie bij de start van een project**
Het projectmanagement moet de mogelijkheid bieden voor de participatie van het management van de betrokken gebruikersorganisatie bij de definitie en goedkeuring van een ontwikkel-, implementatie- of aanpassingsproject.

3 **Projectteamleden en hun verantwoordelijkheden**
Het projectmanagement moet voorzien in toekennen van personeel aan het project en het definiëren van verantwoordelijkheden en bevoegdheden aan projectteamleden.

4 **Projectdefinitie**
Het projectmanagement moet een eenduidige omschrijving van de aard en omvang van ieder implementatieproject opstellen, alvorens het werk wordt gestart.

5 **Goedkeuring van het project**
Het projectmanagement moet voorzien in een beoordeling van de relevante haalbaarheidsonderzoeken, als basis voor de beslissing om door te gaan met het project.

6 **Goedkeuring van projectfase**
Het projectmanagement moet managers van zowel de verwerking als de I&A functie aanwijzen. Deze managers geven hun goedkeuring aan het afgeronde werk in elke fase, voordat met de volgende fase kan worden aangevangen.

7 **Plan van aanpak**

Het projectmanagement moet waarborgen dat voor ieder goedgekeurd project een plan van aanpak wordt geschreven dat voldoende is om het project tijdens de uitvoering ervan te beheersen.

8 **Systeemkwaliteitsborgingsplan**

Het management moet waarborgen dat bij de implementatie van een nieuw of aangepast verwerkingssysteem een kwaliteitsplan wordt geschreven dat wordt opgenomen in het plan van aanpak en formeel wordt beoordeeld door en overeengekomen met alle betrokken partijen.

9 **Planning van kwaliteitsborgingsmethodieken**

Kwaliteitsborgingsactiviteiten moeten tijdens de planningsfase van het projectmanagement worden geïdentificeerd. Kwaliteitsborgingsactiviteiten dienen de goedkeuring van nieuwe of aangepaste systemen te ondersteunen en dienen te waarborgen dat interne controles en beveiligingskenmerken aan de gestelde eisen voldoen.

10 **Testplan**

Het projectmanagement moet eisen dat een testplan wordt geschreven voor elk ontwikkel-, implementatie- of aanpassingsproject.

11 **Opleidingsplan**

Het projectmanagement moet een opleidingsplan definiëren ten behoeve van elk ontwikkelings-, implementatie- en aanpassingsproject.

O.11 Kwaliteitsmanagement voor de gegevensverwerking

Het management ontwikkelt een algemeen kwaliteitsstatuut, gebaseerd op de lange termijn organisatie- en verwerkingsplannen van de organisatie. Dit statuut draagt de continue verbeteringsfilosofie van de organisatie uit en geeft antwoord op de basisvragen wat, wie en hoe dit kwaliteitsmanagement in de organisatie behaald kan worden.

Het kwaliteitsstatuut bevat:

1 **Algemeen kwaliteitsstatuut**
Het management moet een algemeen kwaliteitsstatuut, gebaseerd op de lange termijn organisatie- en verwerkingsplannen van de organisatie, ontwikkelen en onderhouden. Dit statuut moet de verbeteringsfilosofie uitdragen en antwoord geven op de basisvragen 'wat, wie en hoe'.

2 **Aanpak van kwaliteitsborging**
Het management moet voorzien in een standaardaanpak voor kwaliteitsborging waarin activiteiten voor kwaliteitsborging worden behandeld. De aanpak moet de verschillende kwaliteitsborgingsactiviteiten (beoordeling, audits, inspecties, enz.) beschrijven die nodig zijn om aan de maatregelen uit het algemeen kwaliteitsstatuut te voldoen. Tevens dient een specifieke kwaliteitsborgingsbeoordeling te zijn beschreven.

3 **Planning kwaliteitsborging**
Het management moet een proces voor de planning van kwaliteitsborging initiëren om zodoende het bereik en timing van de kwaliteitsborgingsactiviteiten te bepalen.

4 **De kwaliteitsborgingsbeoordeling op het volgen van procedures en standaarden van de verwerkingsfunctie**
Het management moet waarborgen dat in de verantwoordelijkheden van het personeel dat bij kwaliteitsborging betrokken is, een beoordeling op het volgen van de procedures en standaarden van de verwerkingsfunctie beschreven staat.

5 **Systeemontwikkelingmethodiek**
Het management moet normen en standaarden voor de ontwikkeling van informatiesystemen definiëren en implementeren en een systeemontwikkelingmethodiek kiezen die de processen van ontwikkeling, aanschaf, implementatie en onderhoud van geautomatiseerde informatiesystemen en de daaraan gerelateerde technologie beschrijft.

6 **Systeemontwikkelingmethodiek voor grote wijzigingen in bestaande techniek**
Bij omvangrijke wijzigingen in de bestaande technologie moet het management waarborgen dat de systeemontwikkelingmethodiek wordt gebruikt, net als bij de aanschaf van nieuwe technologie.

7 **Herzien van de systeemontwikkelingmethodiek**

Het management moet periodiek de systeemontwikkelingmethodiek beoordelen om zodoende te waarborgen dat de voorzieningen in de methodiek de actuele, algemeen geaccepteerde technieken en procedures weergeven.

8 **Coördinatie en communicatie**

Het management moet een proces initiëren dat nauwe coördinatie en communicatie tussen klanten van de verwerkingsfunctie en de implementeerders van het systeem waarborgt. Dit proces moet gestructureerde methodes gebruiken, gebaseerd op de systeemontwikkelingmethodiek, om te waarborgen dat kwalitatief goede ICT oplossingen worden opgeleverd, die aan de wensen van de bedrijfsomgeving voldoen. Het management moet dus een organisatie stimuleren die wordt gekarakteriseerd door nauwe samenwerking en communicatie binnen de gehele levenscyclus van systeemontwikkeling.

9 **Raamwerk voor aanschaf en onderhoud van de technische infrastructuur**

Er dient een algemeen raamwerk te zijn voor de aanschaf en het onderhoud van de technologische infrastructuur. De verschillende stappen die moeten worden gevolgd met betrekking tot de technologische infrastructuur (zoals aanschaffen, programmeren, documenteren en testen, parameters bepalen, onderhouden en aanbrengen van wijzigingen) moeten worden bestuurd door en voortkomen uit het raamwerk voor de aanschaf en onderhoud van de technologische infrastructuur.

10 **Relaties met derden**

Het management moet voorzien in een proces dat een goede werkverhouding met implementeerders van derden waarborgt. Zo'n proces moet erin voorzien dat de verantwoordelijke en de externe implementeerders overeenstemming bereiken over acceptatiecriteria, behandeling van wijzigingen, problemen tijdens de ontwikkeling, taken vande verantwoordelijke, faciliteiten, tools, programmatuur, standaarden en procedures.

11 **Standaarden voor systeemdocumentatie**

De systeemontwikkelingmethodiek moet normen en standaarden bevatten voor systeemdocumentatie die zijn gecommuniceerd met en zijn bekrachtigd door bij de systeemontwikkeling betrokken personeel. De methodiek moet waarborgen dat de documentatie die tijdens een systeemontwikkelings- of systeemaanpassingsproject wordt geschreven voldoet aan deze normen en standaarden.

12 **Standaarden voor systeemtests**

De systeemontwikkelingmethodiek moet voorzien in normen en standaarden omvattende testeisen, verificatie, documentatie en ruimte voor het testen van individuele programmatuur dat wordt ontwikkeld als onderdeel van elke ontwikkelings- of aanpassingsproject van een informatiesysteem.

13 **Standaarden voor integrale systeemtests**

De systeemontwikkelingmethodiek moet normen en standaarden omvatten voor testeisen, verificatie, documentatie en ruimte voor het testen van een integraal systeem dat wordt ontwikkeld als onderdeel van elke ontwikkelings- of aanpassingsproject van een informatiesysteem.

14 **Parallel/Pilot testen**

De systeemontwikkelingmethodiek van de organisatie moet de omstandigheden beschrijven waaronder parallel of pilot testen van nieuwe en/of bestaande systemen kan worden uitgevoerd.

15 **Systeemtestdocumentatie**

De systeemontwikkelingmethodiek moet erin voorzien dat, als onderdeel van ieder systeemontwikkelings-, implementatie- of aanpassingsproject, de gedocumenteerde resultaten van de systeemtest worden bewaard.

16 **De kwaliteitsborgingsevaluatie van het volgen van ontwikkelingsstandaarden**

De aanpak voor kwaliteitsborging moet erin voorzien dat een beoordeling van een operationeel informatiesysteem voorafgaand aan implementatie vaststelt of het projectteam zich heeft gehouden aan de voorwaarden van de systeemontwikkelingmethodiek.

17 **De kwaliteitsborgingsbeoordeling van het bereikte resultaat**

De aanpak voor kwaliteitsborging moet een beoordeling bevatten van de mate waarin de systeemontwikkelingsactiviteiten de doelstellingen van de verwerkingsfunctie hebben bereikt.

18 **Rapportages van kwaliteitsborgingsbeoordelingen**

De rapportages van kwaliteitsborgingsbeoordelingen moeten worden opgesteld en worden voorgelegd aan het management van de desbetreffende gebruikersafdeling(en) en de ICT-functie.

O.12 Service level beheer

Voor het waarborgen van de betrouwbaarheid en continuïteit van de gegevensverwerking is het van belang dat er een Service Level Agreement (SLA) is afgesloten. Het management van de verwerkingsorganisatie stelt een Service Level Agreement op waarbij aan de volgende aspecten aandacht wordt gegeven: continuïteit, betrouwbaarheid, niveaus van gebruikersondersteuning, ramp- en herstelplan, beveiliging, minimum acceptatieniveau van voldoen aan geleverde systeemfunctionaliteit, restricties, en wijzigingsprocedures. De verantwoordelijke en de verwerkingsfunctie ondertekenen een overeenkomst waarin het service niveau (kwaliteit en kwantiteit) en de verantwoordelijkheden van beide partijen zijn beschreven.

Hierbij zijn de volgende aandachtspunten relevant:

1 **Opstellen Service Level Agreement**

Het management van de verwerkingsorganisatie stelt in overleg met de verantwoordelijke een Service Level Agreement op. Hierbij dienen tenminste de volgende aspecten aan de orde te komen: beschikbaarheid, betrouwbaarheid, niveaus van gebruikersondersteuning, rampen- en herstelplan, beveiliging, minimum acceptatieniveau van voldoen aan geleverde systeemfunctionaliteit, restricties en wijzigingsprocedures. De ICT-functie moet voldoen aan de overeengekomen kwaliteit en kwantiteit van de service en de verantwoordelijke moeten zich in zijn verzoeken aan de ICT-functie houden aan de overeengekomen afspraken.

2 **Aspecten van een Service Level Agreement**

Er moet overeenstemming worden bereikt over de inhoud van de Service Level Agreement. Hierbij dienen tenminste de volgende aspecten aan de orde te komen: beschikbaarheid, betrouwbaarheid, niveaus van gebruikersondersteuning, rampen- en herstelplan, beveiliging, minimum acceptatieniveau van voldoen aan geleverde systeemfunctionaliteit en wijzigingsprocedures.

3 **Prestatieprocedures**

Procedures moeten waarborgen dat de wijze waarop en de verantwoordelijkheden voor de beheersing van de overeengekomen prestaties juist is belegd bij de betrokken partijen. De verantwoordelijkheden moeten worden bekendgemaakt bij alle partijen en moeten worden gecoördineerd, onderhouden en gecommuniceerd.

4 **Toezicht houden en rapporteren**

Het management moet een service level beheerder aanstellen die verantwoordelijk is voor het toezicht houden op en rapporteren over de criteria van het Service Level Agreement en alle voorkomende problemen die zich tijdens de verwerking hebben voorgedaan. De verzamelde (toezicht)gegevens dienen periodiek te worden geanalyseerd. Correctieve acties moeten worden ondernomen en fouten moeten worden hersteld.

5 **Review van Service Level Agreements en contracten**

Het management moet waarborgen dat de Service Level Agreements en de onderliggende contracten regelmatig worden geëvalueerd en worden onderhouden.

O.13 Beheren van diensten van derden

Het management van de verwerkingsfunctie definieert en beschrijft alle door derden te leveren diensten helder en zorgt ervoor dat de technische en organisatorische raakvlakken met leveranciers zijn gedocumenteerd.

Aandachtspunten zijn:

1 **Raakvlak met leverancier**
Het management van de verwerkingsfunctie moet waarborgen dat alle diensten van derden helder zijn gedefinieerd en dat de technische en organisatorische raakvlakken met leveranciers zijn gedocumenteerd. De invloed op de eigen maatregelen van interne controle en beveiliging dient onderkend te worden.

2 **Relatiebeheerder**
Het management dient een contactpersoon aan te wijzen die verantwoordelijk is voor het behoud van de kwaliteit van de relatie met derden.

3 **Contracten met derden**
Het management moet specifieke procedures definiëren om te waarborgen dat voor elke relatie met een externe dienstverlener een formeel contract is gedefinieerd en overeengekomen.

5 **Contracten voor outsourcing**
Specifieke organisatorische procedures moeten worden gedefinieerd om te waarborgen dat het contract tussen de leverancier van de faciliteiten (bewerker) en de organisatie is gebaseerd op de vereiste gegevensverwerkingsniveaus, beveiliging, monitoring, continuïteitseisen en waar nodig andere voorwaarden.

6 **Continuïteit van de diensten**
In het kader van de continuïteit van de dienstverlening (door derden) dient het management de bedrijfsrisico's ten aanzien van de derde partij af te wegen in termen van juridische onzekerheden en het going concern concept.

7 **Beveiligingsovereenkomsten**
In het kader van de relaties met externe leveranciers van diensten moet het management waarborgen dat beveiligingsovereenkomsten (vertrouwelijkheid) worden geïdentificeerd, expliciet worden beschreven en worden geaccordeerd in overeenstemming met de juridische en reguliere vereisten, inclusief aansprakelijkheid.

8 **Toezicht houden**
Een continu proces van toezicht houden op de dienstverlening van de externe dienstverlener moet worden opgezet door het management om vast te stellen dat de afspraken in het contract worden nageleefd.

O.14 Beschikbaarheidsbeheer

Het management definieert een beheersproces dat erin voorziet dat de bedrijfsbehoeften ten aanzien van de beschikbaarheid van ICT-diensten zijn geïdentificeerd en dat deze zijn weergegeven in termen van beschikbaarheids- en prestatie-eisen.

Aandachtspunten bij het definiëren van beschikbaarheids- en prestatie-eisen zijn:

1 **Beschikbaarheids- en prestatie-eisen**

Het beheersproces moet erin voorzien dat bedrijfsbehoeften m.b.t. beschikbaarheid van ICT-diensten zijn geïdentificeerd en dat deze zijn vertaald in termen van beschikbaarheids- en prestatie-eisen.

2 **Beschikbaarheidplan**

Het management dient te waarborgen dat een beschikbaarheidplan wordt opgesteld waarmee de beschikbaarheid van de ICT-diensten kan worden beheerst.

3 **Toezicht houden en rapporteren**

Er dient een beoordelingsproces te worden ingericht waarin het toezicht op de prestaties van de ICT-middelen is geregeld en waarbij uitzonderingen op een tijdige en adequate wijze worden gerapporteerd.

4 **Tool voor modelleren**

Er moeten tools zijn om een model te creëren van bestaande systemen wat is ingesteld op de actuele werkdruk. Deze tools moeten worden gebruikt bij het voorspellen van de betrouwbaarheid van de configuratie en de beschikbaarheidseisen. De hardware moet diepgaand worden onderzocht en dit technisch onderzoek moet een voorspelling over technologische ontwikkelingen bevatten.

5 **Pro-actief prestatiebeheer**

Het beheersproces moet waarborgen dat het mogelijk is om problemen te voorzien en te corrigeren voordat deze invloed krijgen op de prestaties van het systeem. Deze analyse richt zich op systeemfouten en onregelmatigheden in frequentie, mate van impact en omvang schade.

O.15 Waarborgen van continuïteit

Het management van de ICT-functie stelt een raamwerk voor calamiteitenopvang op waarin de verantwoordelijkheden en taken, de gehanteerde methodiek, regels en structuur voor het documenteren van het plan, alsmede de goedkeuring ervan, worden beschreven.

Dit is gedefinieerd in:

1 Calamiteitenopvangplan

Het management van de ICT-functie moet een calamiteitenopvangplan opstellen waarin verantwoordelijkheden en taken, de gehanteerde methodiek, regels en structuur voor het documenteren van het plan en de goedkeuring ervan, worden beschreven.

2 Continuïteitsplan

Het management van de ICT-functie moet waarborgen dat een plan wordt ontwikkeld en onderhouden in overeenstemming met het calamiteitenopvangplan om de kritieke functionaliteit te herstellen bij grote verstoringen (calamiteiten). Het plan moet de nadelige gevolgen van een calamiteit minimaliseren.

3 Strategie en filosofie van het calamiteitenopvangplan

Het management moet waarborgen dat het calamiteitenopvangplan is gebaseerd op het lange termijn verwerkingsplan en aansluit op het algemene (bedrijfsbrede) continuïteitsplan om zo de consistentie te waarborgen.

4 Onderhouden en testen van continuïteitsplan

Het management moet waarborgen dat de ICT-functie adequaat en effectief omgaat met het calamiteitenopvangplan. Het plan moet op reguliere basis worden beoordeeld, getest en onderhouden. Het onderhoud van dit plan moet worden ingepast in de beheersprocessen en geïntegreerd worden in de procedures van wijzigingsbeheer.

5 Alternatieve procedures voor gebruikersorganisatie

Het calamiteitenopvangplan moet zorgdragen dat de gebruikersafdelingen alternatieve verwerkingsprocedures samenstellen die kunnen worden gebruikt om de tijd te overbruggen die de ICT-functie nodig heeft om de dienstverlening te herstellen nadat een calamiteit zich heeft voorgedaan.

6 Trainingsplan voor herstel na calamiteiten/onvoorziene gebeurtenissen

Het beheersproces moet waarborgen dat alle betrokken partijen periodiek een training krijgen in de te volgen procedures ingeval van een calamiteit.

7 Kritieke informatiesystemen

Het calamiteitenopvangplan moet de meest kritieke informatiesystemen identificeren evenals besturingssystemen, benodigd personeel, toepassingen, gegevensbestanden en tijdschema's nodig voor het herstel na een calamiteit. Prioriteiten moeten zijn toegekend aan het herstarten van specifiek kritieke en gevoelige informatiesystemen.

8 **Uitwijklocaties en hardware**

Het calamiteitenopvangplan dient een identificatie van alternatieve uitwijklocatie en hardware te bevatten. Een formeel contract voor deze diensten moet worden opgesteld.

9 **Minimaliseren van herstelinspanningen**

De ICT-functie moet maatregelen en procedures opstellen die erin voorzien dat herstelinspanningen voor de back-up van programma's en gegevensbestanden na calamiteiten worden geminimaliseerd.

10 **Inhoud van calamiteitenopvangplan**

De ICT-functie dient ervoor zorg te dragen dat het calamiteitenopvangplan de volgende zaken bevat:

- verschillende procedures en tijdschema's voor calamiteiten-scenario's met verschillende gevolgen om te waarborgen dat op de juiste wijze op calamiteiten wordt gereageerd;
- planning en procedures die de reconstructie van informatie na calamiteiten beschrijft.

12 **Beveiligingsprocedures voor alle medewerkers**

Procedures voor het herstellen van de telecommunicatie- en netwerkdiensten die worden gebruikt door de organisatie dienen aanwezig te zijn. Het is verstandig als meer dan één bron voor het verkrijgen van goederen voor het herstellen van de ICT dienstverlening na een calamiteit is.

O.16 Waarborgen van logische toegangsbeveiliging

Het management definieert een beleid voor de informatiebeveiliging. In dit beleid legt het management vast welke eisen worden gesteld om de continuïteit van de verwerking van gegevens te kunnen waarborgen. Het voor de informatiebeveiliging verantwoordelijke management vertaalt dit beleid in richtlijnen en maatregelen die moeten worden getroffen.

In deze richtlijnen en maatregelen wordt aandacht besteed aan de volgende aspecten:

1 **Manage security measures**
Er dient beleid opgesteld te worden voor het toekennen en uitgeven van bevoegdheden en het gebruik van superbevoegdheden.

2 **Authenticatie en toegang**
De toegang tot en het gebruik van de geautomatiseerde middelen moet bij implementatie worden geregeld door het definiëren van een adequaat authenticatiemechanisme aangevuld met toegangsregels. Zo'n mechanisme beschermt tegen niet-geautoriseerd personeel, onrechtmatige externe (netwerk) toegang en minimaliseert meervoudige inlog procedures voor wel geautoriseerd personeel. Maatregelen moeten de effectiviteit van het authenticatie- en toegangsmechanisme bewaken.

3 **Beveiliging van directe toegang tot gegevens**
Het management van de gebruikersorganisatie moet procedures, in lijn met het beveiligingsbeleid, implementeren zodat de toegang per gebruiker is gebaseerd op basis van "need to know" (lezen, toevoegen, aanpassen of verwijderen van gegevens) voor de desbetreffende functie.

4 **Beheer van user accounts**
Het management moet procedures definiëren met betrekking tot verzoeken voor, tot stand brengen van, bekendmaken van en afsluiten van user accounts. Een formele toestemmingsprocedure voor de toekenning van gebruikersrechten dient opgenomen te worden.

5 **Beoordeling van user accounts**
De verantwoordelijke moet een beheersproces hebben ingericht met betrekking tot het periodiek beoordelen en bevestigen van toegangsrechten.

6 **Classificatie van gegevens**
De verantwoordelijke moet procedures definiëren opdat wordt gewaarborgd dat alle gegevens worden geclassificeerd in termen van gevoeligheid, formeel en expliciet vastgesteld door de eigenaar van de informatie, volgens het schema voor gegevensclassificatie. Ook voor gegevens die geen beveiliging behoeven moet dit officieel worden vastgesteld.

7 **Beheersing van centrale identificatie en toegangsrechten**

De identificatie van gebruikers, de vastlegging van toegangsrechten en de identificatie van het eigendom van systemen en gegevens moet op een unieke en centrale manier worden vastgelegd en beheerst. Dit in verband met de consistentie en efficiency van de algemene toegangscontrole.

8 **Rapportage van overtredingen en beveiligingsactiviteiten**

De ICT-functie moet overtredingen en beveiligingsactiviteiten bijhouden, vastleggen, beoordelen en op de juiste manier en reguliere basis behandelen zodat incidenten met betrekking tot ongeautoriseerde activiteiten worden opgemerkt. De informatie over de toegang tot geautomatiseerde middelen (beveiliging- en andere logs) moet beschikbaar zijn op basis van het 'need to know' principe.

9 **Incidentbehandeling**

Het management moet de capaciteit voor incidentbehandeling (van beveiligingsincidenten) bewerkstelligen door het aanbieden van een centraal platform met voldoende expertise en voorzien van snelle en veilige communicatiemiddelen. Verantwoordelijkheden en procedures voor incidentbehandeling moeten een optimale, effectieve en ordelijke reactie op beveiligingsincidenten verzekeren.

10 **Herkeuring**

Het management moet waarborgen dat herkeuring van de beveiliging periodiek wordt uitgevoerd om het formeel goedgekeurde beveiligingsniveau en de acceptatie van het resterend risico actueel te houden.

11 **Cryptografie**

Het bedrijfsbeleid moet er voor zorgen dat, indien de behoefte daarvoor bestaat, ontvangst- of transactiebevestigingen kunnen worden geïmplementeerd. De twee partijen die hierbij betrokken zijn, moeten werken met een gemeenschappelijke sleutel en elke partij zijn geheime sleutel. Dit systeem gebruikt men indien er geen andere mogelijkheid bestaat om de betrouwbaarheid van de andere partij te verzekeren.

12 **Beveiliging van cryptografiemodules**

De cryptografiemodules moeten worden beveiligd tegen misbruik om het geheime algoritme van de cryptografie te beschermen tegen bekendmaking ervan.

13 **Beheer van de cryptografiesleutels**

Het management moet procedures definiëren en implementeren evenals een protocol definiëren voor het genereren, distribueren, bewaren, gebruiken en archiveren van cryptografiesleutels om te waarborgen dat de sleutels tegen wijziging en ongeautoriseerd gebruik zijn beschermd.

14 **Bescherming en detectie van virussen**

Het management moet richtlijnen geven met betrekking tot adequate preventieve en detectieve beheersmaatregelen tegen computervirussen.

O.17 Opleiden en trainen van gebruikers

Afgeleid uit de lange termijn beleidsdoelstellingen stelt het management procedures op en onderhoudt deze procedures voor het identificeren en documenteren van de trainingsbehoeften van al het personeel dat gebruik maakt van de ICT-diensten. De trainingsbehoeften worden opgenomen in een trainings-overzicht per functiegroep.

Bij de invulling van de trainingsbehoeften zijn de volgende aandachtspunten van belang:

1 Identificatie van de behoefte aan training

Afgeleid uit de lange termijn beleidsdoelstellingen zal het management procedures moeten opstellen en onderhouden voor het identificeren en documenteren van de trainingsbehoeften van al het personeel dat gebruik maakt van de ICT-diensten. Een trainingsoverzicht moet worden gemaakt voor iedere groep van werknemers.

2 Organisatie van de training

Gebaseerd op de geïdentificeerde behoeften zal het management de doelgroepen moeten definiëren, trainers moeten regelen en moeten zorgdragen voor tijdige trainingssessies. Alternatieve trainingsmogelijkheden dienen ook in overweging genomen te worden (interne of externe locatie, eigen medewerkers als trainer, ingehuurd trainingspersoneel enz.).

3 Training beveiligingsbeginselen en bewustwording

Al het personeel moet worden getraind en opgeleid in beveiligingsprincipes. Het management moet voorzien in een trainingsprogramma dat het volgende inhoudt:

- ethische behandeling van de ICT functie;
- beveiligingsaspecten ter bescherming tegen storingen die de beschikbaarheid raken;
- vertrouwelijkheid, integriteit en uitvoering van taken op een veilige wijze.

O.18 Ondersteunen en adviseren van gebruikers (helpdesk)

Het management richt ter ondersteuning van medewerkers een helpdesk in.
De medewerkers van de helpdesk en van het probleem- en incidentenbeheer overleggen regelmatig.

In dit overleg komen de volgende punten op de agenda:

1 **Helpdesk**
Ter ondersteuning van gebruikers moet een helpdesk worden gecreëerd. Tussen de personen van de helpdesk en probleem- en incidentenbeheer moet regulier overleg zijn.

2 **Registratie van gebruikersvragen**
De helpdesk dient de vragen van gebruikers adequaat te registreren, zodat effectieve afhandeling en evaluatie mogelijk zijn.

3 **Escalatie van gebruikersvragen**
Helpdeskprocedures voorzien erin dat de vragen van gebruikers die niet direct kunnen worden opgelost, worden doorgegeven aan de juiste personen binnen de ICT functie.

4 **Toezicht houden op de afhandeling**
Het management moet voorzien in procedures gericht op het tijdig afhandelen van vragen van gebruikers. Lang uitstaande vragen moeten worden onderzocht en afgehandeld.

5 **Trendanalyse en rapporteren**
Adequate verslaggeving dient plaats te vinden van gebruikersvragen en oplossingen, responsetijden en waargenomen trends. De rapporten moeten worden geanalyseerd en afgehandeld.

O.19 Configuratiebeheer

Het management stelt eisen aan het configuratiebeheer, als basis voor de aanschaf van computer- en randapparatuur. Het verantwoordelijke management waarborgt wordt dat wijzigingen in de configuratie (nieuwe elementen, statuswijzigingen) centraal worden bijgehouden. Logging en beheer moeten een geïntegreerd geheel zijn van het configuratiebeheersysteem.

Voor het configuratiebeheer wordt aandacht besteed aan de documentatie van:

1 **Configuratieadministratie**
Gewaarborgd moet worden dat alleen geautoriseerde en te identificeren onderdelen na aanschaf worden opgenomen in de inventaris. Er moeten procedures zijn om de wijzigingen in de configuratie (nieuwe configuratieelementen, statuswijzigingen) bij te houden. Logging en beheer moeten een geïntegreerd geheel zijn van het configuratiebeheersysteem.

2 **Basisconfiguratie**
Het management van de ICT-functie moet er zeker van zijn dat een basis van configuratieonderdelen wordt aangehouden, zodat deze basis kan worden gebruikt als een controlepunt (basis) bij het terugdraaien van wijzigingen.

3 **Weergave van de status**
Het management van de ICT-functie moet waarborgen dat de configuratieregistratie de actuele status van alle configuratieonderdelen, inclusief de veranderingen in de tijd, weergeven.

4 **Configuratiebeheersing**
Het bestaan en de consistentie van het registratieproces van de I&A componenten periodiek wordt gecontroleerd.

5 **Niet geautoriseerde (illegale) software**
Het management van de ICT-functie moet periodiek de PC's binnen de organisatie controleren op niet geautoriseerde (illegale) software.

6 **Opslag van software**
Een plaats waar bestanden worden opgeslagen, moet worden gedefinieerd voor alle geldige softwareonderdelen in de overeenkomstige fasen van de levenscyclus van systeemontwikkeling. Deze plaatsen moeten van elkaar en van de plaatsen van ontwikkelings- , test- en productiebestandsopslag worden gescheiden.

O.20 Probleembeheer en incidentenbeheer

Het management van de ICT-functie moet een probleembeheersingssysteem definiëren en implementeren bedoeld om te waarborgen dat alle operationele gebeurtenissen welke geen onderdeel vormen van de standaardwerking (incidenten, problemen en fouten) worden vastgelegd, geanalyseerd en tijdig opgelost. Incidentrapportages moeten worden opgesteld indien zich (ernstige) problemen voordoen.

Aandachtspunten zijn:

1 **Probleembeheersingssysteem**

Het management van de ICT-functie moet een probleembeheersingssysteem definiëren en implementeren bedoeld om te waarborgen dat alle operationele gebeurtenissen die geen onderdeel vormen van de standaardwerking (incidenten, problemen en fouten) worden vastgelegd, geanalyseerd en tijdig opgelost. Incidentrapportages moeten worden aangemaakt indien zich (ernstige) problemen voordoen.

2 **Probleemescalatie**

Het management moet procedures opstellen die escalatie van problemen voorkomen zodat problemen efficiënt en tijdig worden opgelost (prioriteiten stellen).

3 **Opsporen van problemen en audit trail**

Het probleembeheersingssysteem moet voorzien in een audit trail die het mogelijk maakt om de achterliggende oorzaak van problemen te achterhalen. Dit moet nauw samenhangen met het wijzigingsbeheer, beschikbaarheids- en prestatiebeheer en configuratiebeheer.

O.21 Gegevensbeheer

Door het management wordt voorzien in procedures voor gegevensverwerking ten behoeve van de gebruikersorganisatie. Het ontwerp van invoerformulieren kan zekerheden bieden dat fouten en het achterwege laten van (delen van de) invoer wordt geminimaliseerd. Door gebruik te maken van foutenafhandelingprocedures wordt gewaarborgd dat fouten en dergelijke worden ontdekt, gemeld en gecorrigeerd.

Voor gegevensbeheer zijn de volgende aandachtspunten van belang:

1 **Gegevensvoorbereiding**
Het management moet voorzien in procedures voor gegevensvoorbereiding door de gebruikersorganisatie. Het ontwerp van invoerformulieren kan zekerheden bieden dat fouten en het achterwege laten van (delen van de) invoer wordt geminimaliseerd. Foutafhandelingsprocedures tijdens gegevensinvoer moeten waarborgen dat fouten e.d. worden ontdekt, gemeld en gecorrigeerd.

2 **Procedures voor autorisatie van basisdocumenten**
Het management moet zorgen dat brondocumenten worden gemaakt door geautoriseerd personeel. Er moet voldoende functiescheiding zijn voor de oorsprong en goedkeuring van een brondocument.

3 **Gegevens verzamelen voor basisdocumenten**
De procedures moeten waarborgen dat alle geautoriseerde brondocumenten tijdig, volledig, accuraat en juist worden verantwoord en verwerkt.

4 **Foutbehandeling basisdocumenten**
Foutbehandelingsprocedures tijdens het opstellen van gegevens moeten waarborgen dat fouten en onregelmatigheden worden ontdekt, gemeld en gecorrigeerd.

5 **Bewaren van brondocumenten**
Procedures zijn nodig om te waarborgen dat originele brondocumenten in bezit blijven van of binnen een acceptabele termijn reproduceerbaar zijn door de organisatie, indien reconstructie of herstel van gegevens nodig is en om te voldoen aan de wettelijke eisen.

6 **Autorisatieprocedures gegevensinvoer**
De organisatie moet afdoende procedures opstellen die erin voorzien dat gegevensinvoer alleen door geautoriseerde personeelsleden wordt uitgevoerd.

7 **Juistheid-, volledigheid- en autorisatiecontroles**
Transactiegegevens, ingevoerd voor verwerking moeten worden gecontroleerd op juistheid, volledigheid en autorisatie. Tevens moeten procedures erin voorzien dat de ingevoerde gegevens zo dicht mogelijk bij de bron worden gevalideerd en bewerkt.

8 **Herstelprocedure gegevensinvoer**
De organisatie moet herstelprocedures voor correctie van onjuiste invoer van gegevens opstellen.

9 **Integriteit van gegevensverwerking**
De organisatie moet procedures voor gegevensverwerking opstellen die functiescheiding en het routinematig controleren van het werk waarborgen. Deze procedures moeten adequate maatregelen waarborgen zoals verbandstotalen en mutatiecontroles.

10 **Validatie van gegevensverwerking en bewerking**
De organisatie moet procedures opstellen die voorzien in validatie van de gegevensverwerking en regelen dat authenticatie en bewerking zo dicht mogelijk bij de plaats van ontstaan plaatsvinden.

11 **Foutafhandeling bij gegevensverwerking**
De organisatie moet procedures opstellen voor de afhandeling van fouten die het mogelijk maken om onjuiste transacties te identificeren zonder dat ze verwerkt worden of dat andere juiste transacties vervallen of worden onderbroken.

12 **Behandelen en behouden van uitvoer**
De organisatie moet procedures opstellen voor het behandelen en behouden van uitvoer uit de informatiesystemen.

13 **Verspreiden uitvoer**
De organisatie moet procedures opstellen en communiceren voor het verspreiden van computeruitvoer.

14 **Vergelijken en herstellen uitvoer**
De organisatie moet procedures opstellen die erin voorzien dat de uitvoer automatisch wordt vergeleken met relevante controletotalen. Audit trails moeten ter beschikking worden gesteld voor het traceren van verwerkte gegevens en herstellen van verminkte gegevens.

15 **Beoordelen van uitvoer**
De organisatie moet procedures opstellen die erin voorzien dat de juistheid van de uitvoerverslagen wordt gecontroleerd door de verstrekker en de relevante gebruikers. Deze procedures zijn ook noodzakelijk voor het voorkomen van fouten in de uitvoer.

16 **Beveiliging van uitvoer**
De organisatie moet procedures opstellen die de beveiliging van reeds gedistribueerde verslagen en nog te distribueren verslagen waarborgen.

17 **Bescherming van gevoelige informatie**
Het management moet een adequate beveiliging tegen ongeautoriseerde toegang en wijzigingen van gevoelige informatie tijdens transmissie en transport waarborgen.

18 **Bescherming van te vernietigen gevoelige informatie**

Het management moet procedures ontwikkelen die voorzien in de exclusiviteit van de gegevensverwerking. Persoonsgegevens die ter vernietiging worden aangeboden moeten, ter voorkoming van misbruik door anderen worden beoordeeld en volgens de procedure worden afgehandeld.

19 **Opslagbeheer**

Er moeten procedures worden ontwikkeld voor gegevensopslag, rekening houdend met de gewenste beschikbaarheid en de effectiviteit van de kosten.

20 **Bewaarperioden en opslagvoorwaarden**

Bewaarperioden en opslagvoorwaarden moeten worden gedefinieerd voor documenten, gegevens, programma's en verslagen.

21 **Library beheer**

De ICT-functie moet procedures invoeren die erop gericht zijn dat de inhoud van de gegevens, opgeslagen in de bibliothek, systematisch worden geïnventariseerd en dat maatregelen worden genomen voor het instandhouden van de integriteit van de media bewaard in de bibliotheek.

22 **Verantwoordelijkheden van library beheer**

Huishoudelijke maatregelen voor de beveiliging van de inhoud van een mediabibliotheek moet worden opgesteld door het management van de ICT-functie. Standaarden moeten worden gedefinieerd voor de externe identificatie van opslagmedia en de beheersing van hun fysieke verplaatsing en opslag om de betrouwbaarheid te ondersteunen. Verantwoordelijkheid voor de gegevensbibliotheek moet worden toegewezen aan specifieke personeelsleden van de ICT-functie.

23 **Back-up en herstel**

Het management moet maatrgelen implementeren voor back-up en herstel om te waarbij aandacht wordt besteed aan: het beoordelen van de organisatie-eisen, de ontwikkeling, de implementatie, het testen en het documenteren van het herstelplan (restore). Procedures moeten worden opgezet die erin voorzien dat back-ups voldoen aan bovengenoemde eisen.

24 **Back-up**

Er moeten procedures zijn gericht op het maken van back-ups volgens de back-up procedures en dat de mogelijkheid van het gebruik van de back-ups regelmatig wordt gecontroleerd.

25 **Opslag van back-up**

Back-up procedures met betrekking tot ICT-media moeten aandacht besteden aan het vastleggen van gegevensbestanden en software. Back-ups moeten beveiligd worden opgeslagen en de plaats van opslag moet periodiek worden gecontroleerd op fysieke toegangsbeveiliging.

O.22 Faciliteitenbeheer

Het management stelt in overeenstemming met het algemene beveiligingsbeleid geschikte fysieke beveiligings- en controlemaatregelen vast voor toegang tot de faciliteiten van systeembeheer. Toegang is voorbehouden aan individuen die autorisatie hebben ontvangen.

Aandachtspunten bij faciliteitenbeheer zijn:

1 **Fysieke beveiliging**
Geschikte fysieke beveiligings- en toegangscontrolemaatregelen moeten worden ontwikkeld waarin geregeld is wie toegang heben tot de faciliteiten van systeembeheer, in overeenstemming met het algemeen beveiligingsbeleid. Toegang is voorbehouden aan individuen die een autorisatie hebben ontvangen.

2 **Low profile van locatie van gegevensverwerking**
Het management van de ICT-functie moet waarborgen dat een low profile wordt gehanteerd en fysieke identificatie van de locatie van gegevensverwerking wordt beperkt.

3 **Begeleiden van bezoekers**
Geschikte procedures zijn nodig om te identificeren dat andere functionarissen dan van systeembeheer worden begeleid bij het betreden van de computerruimte. Een bezoekerslog moet worden bijgehouden en regelmatig worden beoordeeld.

4 **Gezondheid- en beveiligingsregels**
Gezondheids- en beveiligingsregels moeten worden gebruikt volgens internationale, nationale en lokale wetten en eisen.

5 **Beveiliging tegen invloeden van buitenaf**
Het management van de verwerkingsfunctie moet waarborgen dat voldoende maatregelen worden getroffen ter bescherming tegen invloeden uit de omgeving (brand, stof, stroomonderbreking, hitte en vocht). Gespecialiseerde apparatuur om toezicht te houden (en bij te stellen) op de omgeving moeten worden opgesteld.

6 **Ononderbroken stroomvoorziening**
Het management moet regelmatig de behoefte aan ononderbroken stroom (batterijen, generatoren en accu's) voor belangrijke verwerkingscomponenten beoordelen, ter bescherming tegen stroomstoringen en -schommelingen.

O.23 Operationeel beheer

Het management van de ICT-functie draagt er zorg voor dat er standaardprocedures worden ontwikkeld voor operationele activiteiten (incl. netwerkbeheer). Van de operationele activiteiten wordt een documentatie bijgehouden. Het management stelt richtlijnen op voor alle technische oplossingen en systemen die binnen de organisatie worden gebruikt.
Het verantwoordelijke management controleert periodiek of er volgens deze procedures wordt gewerkt.

De volgende documenten worden opgesteld:

1 **Procedure- en instructiehandboek voor operationeel beheer**
De ICT-functie moet een standaardprocedure ontwikkelen en documenteren voor de operationele activiteiten (incl. netwerkbeheer). Alle technische oplossingen en systemen moeten worden gebruikt volgens deze procedures die periodiek moeten worden beoordeeld om de effectiviteit en de naleving te waarborgen.

2 **Documentatie voor het opstartproces en andere taken**
Het management van de I&A functie moet waarborgen dat de gebruikers voldoende vertrouwd en zeker zijn met de opstartprocedures en andere operationele taken door deze te documenteren, periodiek te testen en indien nodig aan te passen.

3 **Operatie log**
Beheersmaatregelen moeten garanderen dat voldoende chronologische informatie wordt opgeslagen in operatie logs om reconstructie, tijdig beoordelen en onderzoek naar opeenvolging van processen in de tijd en andere activiteiten rondom en ondersteunend aan het proces, mogelijk te maken.

4 **Operatie op afstand**
Voor verbindingen tussen qua afstand van elkaar gelegen locaties moeten specifieke procedures worden ontwikkeld en geïmplementeerd om te waarborgen dat verbindingen en afsluiting van de verbinding naar de op afstand gelegen locatie zijn gedefinieerd en geïmplementeerd.

Evaluatie van de verwerking

Deze bijlage beschrijft de maatregelen voor de evaluatie en zonodig bijsturing van de technische en organisatorische maatregelen van de verwerkingsorganisatie (bijlage 2).

Voor de evaluatie van de verwerking worden de volgende 2 aandachtsgebieden onderkend. In het vervolg van deze bijlage zullen per aandachtsgebied de belangrijkste aspecten benoemd en kort toegelicht worden.

E.1	Beheersen van processen
E.2	Verkrijgen van deskundig oordeel

E.1 Beheersen van de processen

1 Verzamelen van beheersgegevens

Het management zorgt voor het definiëren van relevante prestatie-indicatoren voor de beheersing en interne controle van de verwerking van persoonsgegevens. De gegevens worden voor het maken van managementinformatie en uitzonderingsrapportages verzameld.

2 Managementrapportage

Managementverslagen worden verstrekt aan het senior management ter beoordeling en bewaking van de behoorlijke en zorgvuldige verwerking van persoonsgegevens. Volgend op de beoordeling onderneemt en beheerst het management de juiste acties.

3 Toezicht houden op het beheer

Het management zorgt voor het ontwerpen van toezichthoudende maatregelen die een betrouwbare, tijdige en bruikbare terugkoppeling waarborgen en bevestiging van de beheersgegevens door (andere) bronnen van binnen en/of buiten de organisatie.

4 Tijdig uitvoeren van beheersmaatregelen

Kunnen vertrouwen op interne controlemaatregelen houdt in dat controles meteen fouten en inconsistenties aan het licht brengen en dat deze vervolgens worden gecorrigeerd voordat ze invloed hebben op de verwerking van persoonsgegevens. Informatie hierover wordt systematisch bewaard en ter beschikking gesteld aan het management.

5 Rapportage over niveau van beheer

Het management verstrekt informatie over het niveau en de bevindingen van interne controle aan de belanghebbende partijen om de effectiviteit van het interne controlesysteem te verzekeren. Acties worden ondernomen om vast te stellen welke informatie nodig is voor het nemen van beslissingen op verschillende niveaus.

6 Zekerheid over operationele beheer inzake beveiliging van persoonsgegevens

Operationele beveiliging van persoonsgegevens en zekerheid over de interne controle worden verkregen door interne en/of onafhankelijke audits. Hierbij wordt onderzocht of de beveiliging en interne controle wel of niet werkt zoals is gewenst en/of vereist door de beveiligings- en interne controlemaatregelen. Voortdurende uitvoering van beheers- en controlemaatregelen door het management zijn gericht op het ontdekken van kwetsbaarheden in de verwerking en beveiliging van persoonsgegevens.

7 Periodiek bijstellen

Het management richt een stelsel in van beheersmaatregelen en -procedures die waarboren dat periodiek wordt afgestemd dat persoonsgegevens conform de regels van het privacybeleid en het privacyplan worden verwerkt.

8 **Overeenstemmen met beleid, procedures en standaarden**

Het management waarborgt dat er afdoende procedures aanwezig zijn voor het vaststellen van de mate waarin het personeel het geïmplementeerde beleid en de procedures heeft begrepen en opgevolgd. Procedures voor overeenstemming met ethische, beveiliging en interne controle standaarden worden ontworpen en gestimuleerd door het management (goed voorbeeld doet goed volgen).

E.2 Verkrijgen van deskundig oordeel

1 **Auditbeleid**

Het management zorgt voor een auditbeleid zodat men verzekerd is van regelmatige en onafhankelijke beoordeling van de zorgvuldige en behoorlijke verwerking van persoonsgegevens. In dit beleid geeft het management aan welke prioriteiten zij stelt voor de te verkrijgen onafhankelijke zekerheid.

2 **Uitvoeren van het auditwerk**

Verplichte professionele zorg bestaat in alle aspecten van het auditwerk, inclusief het gebruik van geschikte auditstandaarden. Audits worden gepland en onder deskundig toezicht van de interne auditfunctie of ingeschakelde externe auditor uitgevoerd om het bereiken van de controledoelstellingen te waarborgen.
De auditor voorziet zich van voldoende bewijsmateriaal ter ondersteuning van de gerapporteerde bevindingen en conclusies.

3 **Technische deskundigheid van auditors**

Het management verzekert zich ervan dat de auditors die verantwoordelijk zijn voor de beoordeling van de activiteiten van het verwerkingssysteem van de organisatie technisch en juridisch competent zijn en collectief in het bezit zijn van de kennis en vaardigheden benodigd voor het effectief, efficiënt en economisch uitvoeren van de beoordeling.

4 **Auditrapportage**

De auditfunctie of externe auditor zorgt voor schriftelijke rapportage aan het betrokken management voor het afronden van elke beoordeling. Het auditrapport bevat de gestelde doelen en binnen welke randvoorwaarden de audit is uitgevoerd. Tevens bevat het rapport de bevindingen, de conclusies en de aanbevelingen, evenals voorbehouden en kwalificaties die de auditor heeft ten aanzien van de audit.

5 **Follow-up activiteiten**

Oplossing en voortgangsbewaking van de auditbevindingen is een taak van het management. De auditor adviseert het management vanuit zijn natuurlijke adviesfunctie over noodzakelijke vervolgacties. De auditor neemt kennis van de vervolgacties die het management heeft genomen.

Handreiking relatie verwerkingseisen en getroffen maatregelen/procedures

Navolgende matrix toont de relaties aan tussen de uit het V-deel van het Raamwerk af te leiden eisen en de technische en organisatorische maatregelen die in het O-deel en E-deel zijn opgenomen. Tevens is een beschrijvende toelichting opgenomen om de genoemde relaties te verduidelijken.
Zoals in het Raamwerk reeds is gesteld, is de keuze van de organisatie ter invulling van de technische en organisatorische maatregelen door de wet niet dwingend voorgeschreven. Slechts is gesteld dat passende maatregelen getroffen moeten worden. Deze bijlage geeft de gebruiker van het Raamwerk een handreiking voor de invulling hiervan. Bij gebruik van een ander dan in het Raamwerk gekozen model kan op analoge wijze een matrix worden opgesteld waarin de verbanden tussen de uit de wet af te leiden eisen en de door de organisatie te treffen maatregelen expliciet worden gemaakt.
Het is mogelijk dat één of meer aandachtsgebieden uit het V-deel niet van toepassing zijn voor de onderzochte organisatie. Dit kan met name het geval zijn voor V.8 (Verwerking door een bewerker) en V.9 (Gegevensverkeer met landen buiten de Europese Unie).

De toelichting op de matrix is opgesplitst in een algemeen deel en een specifiek deel. De algemene toelichting beschrijft waarom de individuele deelgebieden van het Raamwerk (V, O, en E) een relatie hebben met de overige deelgebieden. De specifieke toelichting geeft voor een aantal van de te onderkennen kruisverbanden een nadere uitleg. Vanuit de toelichting die in het specifieke deel is opgenomen, wordt geen weging toegekend aan de aanwezige verbanden tussen V en O en tussen V en E. Slechts een gedegen organisatiespecifieke afweging door de auditor kan tot een bepaalde weging aanleiding geven. Dit dient gemotiveerd in het onderzoeksdossier te worden vastgelegd.

Algemene toelichting

Er is een aantal algemene relaties te onderkennen tussen het V-deel en het O- en E-deel van het Raamwerk. De meest in het oog springende relaties zijn, vanuit V geredeneerd:

V.5 Kwaliteit

kwaliteit van de gegevensverwerking is een aspect dat in alle stappen van de managementcyclus verankerd dient te zijn. De organisatie moet zich bewust zijn van de noodzaak van het waarborgen van een kwalitatief betrouwbare verwerking van persoonsgegevens in de gehele organisatie.

V.7 Beveiliging

Het management van een organisatie moet zich voortdurend bewust zijn van de risico's die bij de verwerking van persoonsgegevens worden gelopen. Derhalve dient in de gehele managementcyclus voldoende aandacht aan de beveiligingsaspecten te worden besteed.

Vanuit O geredeneerd kunnen de volgende algemene relaties naar V worden gelegd:

O.1 Planning en organisatie van de verwerking van persoonsgegevens
bij de planning dient aandacht besteed te worden aan alle relevante aandachtsgebieden uit V.

O.4 Definieer de verwerkingsorganisatie en haar relaties
Reeds bij de inrichting van de verwerkingsorganisatie dient aandacht besteed te worden aan de realisering van de eisen die uit V voortvloeien.

O.6 Communiceren van privacydoelstellingen en -beleid
Het management dient alle functionarissen betrokken bij de verwerking van persoonsgegevens te informeren over de doelstellingen en het beleid inzake privacy. Via communicatie creëert de leiding zowel betrokkenheid als bewustwording bij de verantwoordelijke functionarissen.

O.8 Waarborgen dat aan aanvullende eisen wordt voldaan
De organisatie gaat periodiek na of nog steeds voldaan wordt aan de gestelde eisen op het gebied van de privacy en of er aanvullende eisen nodig zijn. Dit aspect strekt zich uit over de gehele verwerkingscyclus.

O.21 Gegevensbeheer
Dit betreft de feitelijke uitvoering van de gegevensverwerking. Hierin dienen alle relevante aandachtsgebieden van V op adequate wijze geborgd te zijn.

Vanuit E geredeneerd, kunnen de volgende relaties naar V worden gelegd:

E.1 Beheersing van de processen
Zonder toezicht op de daadwerkelijke verwerkingsprocessen heeft het management onvoldoende zekerheid over de realisering van de doelstellingen die hem vanuit de wet zijn afgeleid. Het beheersingsinstrumentarium dient derhalve op alle relevante aandachtsgebieden van V toegepast te worden.

E.2 Verkrijgen van deskundig oordeel
Indien een deskundig oordeel wenselijk dan wel nodig is, dienen alle relevante V-gebieden in het onderzoek te worden meegenomen.

Matrix Relaties

	I	V.1	V.2	V.3	V.4	V.5	V.6	V.7	V.8	V.9
O.1	○	○	○	●	○	○	○	○	○	○
O.2		○			●	○		○		
O.3					●	○		○		
O.4		○	●	○	○	○	○	○	○	○
O.5						●		○		
O.6	○	○	○	○	○	○	○	○	○	○
O.7				○		○		○		
O.8	○	○	○	○	○	○	○	○	○	●
O.9						○		○	○	○
O.10						○		○		
O.11						○		○	○	
O.12						○		○	●	
O.13						○		○	●	
O.14						○		○	○	
O.15						○		○	○	
O.16						○		●	○	
O.17				○		○		○	○	
O.18		○	○			○	●	○	○	
O.19						○		○	○	
O.20						○		○	○	
O.21		●	○	○	○	●	○	●	○	○
O.22						○		○	○	
O.23						○		○	○	
E.1	○	○	○	○	○	○	○	○	○	○
E.2	○	○	○	○	○	○	○	○	○	○

● *Zie specifieke toelichting op de volgende bladzijden*

I	*Inleiding*	*O.1*	*Planning en organisatie van de verwerking*	*O.11*	*Kwaliteitsmanagement voor de gegevensverwerking*
V.1	*Voornemen en melding*	*O.2*	*Definieer de ICT infrastructuur*		
V.2	*Transparantie*	*O.3*	*Bepaal het technologiebeleid*	*O.12*	*Service niveau beheer*
V.3	*Doelbinding*	*O.4*	*Definieer de verwerkingsorganisatie en haar relaties*	*O.13*	*Beheren van diensten van derden*
V.4	*Rechtmatige grondslag*			*O.14*	*Beschikbaarheidsbeheer*
V.5	*Kwaliteit*	*O.5*	*Management van kwaliteitbevorderende verwerkingsinvesteringen*	*O.15*	*Waarborgen van continuïteit*
V.6	*Rechten*			*O.16*	*Waarborgen van logische toegangs-beveiliging*
V.7	*Beveiliging*	*O.6*	*Communiceren van privacydoelstellingen en -beleid*	*O.17*	*Opleiden en trainen van gebruikers*
V.8	*Verwerking door een bewerker*	*O.7*	*Personeelsmanagement*	*O.18*	*Ondersteunen en adviseren van gebruikers*
V.9	*Gegevensverkeer met landen buiten de EU*	*O.8*	*Waarborgen dat aan aanvullende eisen wordt voldaan*	*O.19*	*Configuratiebeheer*
				O.20	*Probleembeheer en incidentenbeheer*
E.1	*Beheersing van de processen*	*O.9*	*Beoordelen van afhankelijkheid en kwetsbaarheid van de gegevensverwerking*	*O.21*	*Gegevensbeheer*
E.2	*Verkrijgen van deskundig oordeel*			*O.22*	*Faciliteitenbeheer*
		O.10	*Projectmanagement*	*O.23*	*Operationeelbeheer*

Specifieke toelichting

V.1 <> O.21

Indien verzamelingen van persoonsgegevens zijn aangemeld bij het CBP of een interne functionaris dan zal hiervan een centraal register moeten worden bijgehouden (V.1). Als gevolg hiervan zal het management moeten voorzien in adequate procedures voor gegevensverwerking als onderdeel van zijn gegevensbeheerbeleid (O.21).

V.2 <> O.4

Vanuit het 'transparantie'-beginsel geldt een informatie plicht naar de betrokkene voor de verwerking van zijn persoonsgegevens (V.2). Om te voldoen aan deze informatieplicht zal het management duidelijk moeten aangeven waar en hoe persoonsgegevens binnen de organisatie worden verwerkt (O.4).

V.3 <> O.1

Vanuit het principe van 'doelbinding' mogen persoonsgegevens worden verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel (V.3). De borging kan worden gevonden in het strategisch WBP plan. Het management zal hier de aard, omvang en gebruik van de persoonsgegevens moeten vastleggen en deze relateren aan privacyaspecten.

V.4 <> O.2 / O.3

Vanuit het principe van 'rechtmatige grondslag' zal duidelijk moeten worden of persoonsgegevens al dan niet mogen worden verwerkt (V.4). In het O gedeelte zal moeten worden geborgd dat in de ICT infrastructuur een gegevensclassificatie-schema is vastgelegd (O.2) en zal het management in het technologisch beleid de ontwikkelingen op het gebied van 'Privacy-Enhancing Technologies' moeten aangeven.

V.5 <> O.5 / O.21

Vanuit het 'kwaliteit'-beginsel moet worden onderzocht of persoonsgegevens ter zake dienend, niet bovenmatig, juist en volledig worden verzameld en verwerkt (V.5). Dit kan gewaarborgd worden door jaarlijks een verwerkingsbudget op te stellen (O.5) en door concrete technische en organisatorische maatregelen en procedures (O.21).

V.6 <> O.18

Indien persoonsgegevens worden verzameld/verwerkt zal een aantal rechten (recht op inzage, verzet, wijziging etc) moeten worden gerealiseerd voor betrokkenen (V.6). Om de rechten te effectueren zal het management een organisatie moeten hebben ingericht die de betrokkenen op dit gebied ondersteunt en adviseert (O.18).

V.7 <> O.16 / O.21

Indien persoonsgegevens worden verzameld/verwerkt zullen hiervoor passende technische en organisatorische maatregelen moeten worden getroffen (V.7). Het management dient de informatiebeveiliging te waarborgen door hiervoor een beleid te definiëren en concrete maatregelen te treffen. Hierbij zijn maatregelen in de sfeer van logische toegangsbeveiliging en gegevensbeheer onvermijdelijk.

V.8 <> O.12 / O.13

Indien persoonsgegevens worden verwerkt door een bewerker zal hiervoor een aantal eisen aan deze bewerker worden gesteld (V.8). Het management zal de diensten die door derden geleverd worden, helder moeten documenteren (O.13) en zal de afspraken die met derden worden gemaakt, moeten vastleggen in Service Level Agreements (O.12).

V.9 <> O.8

Indien gegevensverkeer met landen buiten de EU plaatsvindt dan zullen aanvullende regels moeten worden nageleefd (V.9). De organisatie moet procedures opstellen en onderhouden voor de beoordeling van externe eisen en voor de coördinatie van deze activiteiten (O.8).

Aandachtspunten voor de relatie tussen verantwoordelijke en bewerker

In deze bijlage is een checklist opgenomen met aandachtspunten voor de afspraken tussen de verantwoordelijke voor de verwerking van persoonsgegevens en de interne verwerkingsorganisatie of de (externe) bewerker. De aandachtspunten zijn onderverdeeld naar bepalingen op contractniveau, systeemniveau en administratief-organisatorisch niveau. De inhoud van deze bijlage is ontleend aan NIVRA-geschrift 58, Privacybescherming; de gevolgen voor organisaties en de rol van de accountant en waar nodig aangepast.

Contractniveau

De basis voor de werkzaamheden, in welke vorm dan ook, wordt gevormd door een overeenkomst (een contract) tussen de verantwoordelijke en de verwerkingsorganisatie. Aandachtspunten zijn hierbij:

- opdrachtgever;
- opdrachtnemer(s);
- object (systeembeschrijving);
- te verrichten activiteiten voor het beheer, de productie, het onderhoud en de ontwikkeling;
- looptijd van de overeenkomst inclusief opzegtermijn en verlengingsmogelijkheden;
- procedure tussentijds wijzigen contract;
- ontbindende voorwaarden;
- overlegstructuren (ten aanzien van de aspecten ontwikkeling, onderhoud, productie en beheer);
- functioneren controlerend accountant/IT-auditor;
- eigendom ((systeem-)documentatie, programmatuur en gegevens);
- beschikbaarheid van het systeem (machines en personeel)
- verwijzing naar algemeen geldende afspraken;
- toegang tot programmatuur, documentatie en bestanden
- overmacht;
- plaats van uitvoering;
- toepasselijk recht.

Op verschillende onderdelen dient de overeenkomst de elementen te bevatten die bij de controle als basis kunnen dienen voor de beoordeling van zowel de opzet en het bestaan van de getroffen maatregelen op een bepaald moment alsook de werking van het stelsel van maatregelen gedurende een bepaalde periode.

Systeemniveau

In de systeemdocumentatie, die de verantwoordelijke (de opdrachtgever) moet goedkeuren, dient het volgende te worden ingevuld:

Controleerbaarheid

a Een beschrijving van alle in het geautomatiseerde systeem opgenomen controles (specifieke systeemtechnische en geprogrammeerde) en de daarbij behorende organisatorische maatregelen en procedures.

b Een beschrijving van de door de automatiseringsorganisatie te verrichten controles, gericht op het vaststellen van een juiste, volledige, geoorloofde en tijdige verwerking van de gegevens:

- controles van de invoer (papier, tape, on-line, decentrale verwerking/centrale verwerking);
- controles van de productie (stuurinformatie, acceptatietest);
- controles van de uitvoer (retourinformatie, papier, tape, distributie);
- controles van de programmatuur (blijvende juistheid, integriteit, acceptatie, versiebeheer);
- controles van de bestanden (blijvende juistheid, integriteit).

De uitvoering en de resultaten van de controles dienen zodanig te worden vastgelegd dat zij verifieerbaar zijn voor de opdrachtgever. De beschreven controles dienen aangevuld te worden met een controle die bij de opdrachtgevende organisatie (systeembeheer en gebruikers) uitgevoerd dient te worden.

Betrouwbaarheid toepassingssoftware

Nadere invulling van de afspraken van het accepteren van nieuwe en gewijzigde programmatuur:

a Kwaliteitseisen voor de door de IT-ontwikkelingsorganisatie op te leveren programmatuur en documentatie (oplevering op basis van een schone systeemtest).

b Procedures met betrekking tot het acceptatietesten door de gebruiker (opdrachtgever):

- wie voert uit;
- wie is verantwoordelijk (opdrachtgever);
- door de automatiseringsorganisatie ter beschikking te stellen faciliteiten (machinecapaciteit en overige technische hulpmiddelen);
- testomstandigheden (onder andere test- of productieomgeving);
- tijdigheid op te leveren testoutput;
- wijze van aanleveren van testoutput.

c Acceptatieprocedure programmatuur (testbegeleidingsbrief/relatie met programmatuur).

d Verantwoordelijkheden voor het onderhoud van het systeem en de verantwoordelijkheden voor het onderhouden van de testset/testbestanden door de gebruikersorganisatie.

Deze aspecten maken deel uit van de in breder verband vast te stellen methodiek voor systeemontwikkeling en systeemonderhoud.

Beveiliging

Nadere invulling van de afspraken en eisen voor de beveiliging van programma's, bestanden en documentatie:

a Wie is bevoegd tot opdrachtverstrekking respectievelijk acceptatie van de productie, ontwikkeling, onderhoud en vrijgeven gegevens, etc.

b Nadere invulling voor het verlenen van toegang tot bestanden, programma's met behulp van de beschikbare beveiligingsprogrammatuur:

- wijze en vorm van aanleveren van mutaties;
- wie is bevoegd;
- wijze van controle op de inbreng;
- wijze en tijdigheid terugmelding;
- invulling actief beheer, onder andere:
  - afwijkingen van de gestelde regels;
  - overtredingen (gebruikers, locaties, periodes, etc.);
  - reactiveringen;
- expliciete beschrijving van alle gebruikers die toegang hebben tot bestanden/programma's van het systeem (met de omschrijving van de toegestane mogelijkheden. Dit geldt zowel voor in- als externe gebruikers uit zowel opdrachtgevende- als automatiseringsorganisatie.

c Beveiligingsmaatregelen met betrekking tot de integriteit van de bestanden en gegevensdragers.

d Wijze en voorwaarden van vernietiging van gegevens(dragers).

e Eisen en voorwaarden ten aanzien van het gebruik van standaardprogrammatuur, utilities en subroutines ten behoeve van het systeem.

Calamiteiten

Nadere invulling van de afspraken voor:

a Uitwijkmogelijkheden.

b Faciliteiten datacommunicatie in uitwijksituatie.

c Beschikbaarheid van zowel data-entry als verwerkingscapaciteit.

d Bewaartermijnen bestanden/programma's (ten behoeve van zowel back-up, reconstructie als wettelijke verplichtingen).

e Bewaartermijnen van de overige bescheiden zoals productiegegevens, systeemdocumentatie, handboeken, etc.

f Reconstructie en loggingsfaciliteiten.

Administratief-organisatorisch niveau

Naast de afspraken die in de contractuele sfeer moeten worden geregeld (juridisch) en de elementen die in de systeemdocumentatie moeten worden ingevuld door de ontwikkelorganisatie, zal met de bewerker tot overeenstemming moeten worden gekomen over de wijze waarop men materieel invulling geeft (administratief/organisatorisch) aan de afspraken in het contract en de eisen die zijn geformuleerd. Veelal wordt dit vastgelegd in een bijlage die onderdeel uitmaakt van het contract. Een dergelijke bijlage bij het contract wordt hier 'Dossier Afspraken en Procedures' (DAP) genoemd.
Dit zijn in het algemeen afspraken op uitvoerend niveau waardoor niet bij elke wijziging in de afspraken een geheel nieuw contract moet worden opgesteld.

Het opstellen van een DAP moet bezien worden in relatie tot de complexiteit van de organisatie van de bewerker en de verwerkingen daarbinnen. Veelal kan ook volstaan worden met duidelijke contractbepalingen of een verkorte bijlage bij het contract. Hieronder volgt een voorbeeld van een aandachtspuntenlijst voor de elementen die in een DAP zouden moeten zijn geregeld, hoewel er strikt genomen elementen instaan die ook in een contract geregeld kunnen worden.

Aandachtspuntenlijst DAP	
1	**Algemeen**
1.1	Doelstelling van het DAP
1.2	Beperkingen die in het DAP worden aangebracht (bijvoorbeeld: met privacy wordt geen rekening gehouden
1.3	Activiteiten voor onderhoud, beheer, exploitatie:
	——— systeembeheer
	——— systeem evaluatie
	——— wijzigingen op basis van systeemevaluatie
1.4	Indeling DAP
	——— voorschrijvend deel
	——— verantwoordend deel
1.5	Beheer DAP
	——— wie beheert het DAP
	——— wie kan en mag het DAP veranderen
	——— wie keurt de wijzigingen goed?
	——— hoe is de goedkeuringsprocedure
	——— welke formulieren behoren daarbij?
1.6	Begripsbepalingen
	——— algemeen
	——— opdrachtverstrekker (verantwoordelijke)
	——— opdrachtnemer (bewerker)
	——— applicatiebeheerder
	——— systeembeheerder

Vervolg Aandachtspuntenlijst DAP

2	**Organisatie**
2.1	Algemeen
	——— functionarissen bij beheer, exploitatie en onderhoud
	——— verantwoordelijkheden
	——— organisatieschema van genoemde functionarissen
	——— taken, bevoegdheden
	——— overlegstructuren tussen de functionarissen
2.2	Systeembeheer opdrachtgever
	——— wie, welke afdelingen, verantwoordelijkheden
	——— uitzonderingen daarop
2.3	Systeembeheer opdrachtnemer
	——— functioneel beheer, wie
	——— technisch beheer, wie
	——— definitie van systeembeheer
	——— wie treedt op als intermediair tussen opdrachtnemer en opdrachtgever
	——— hoe is de fiattering geregeld tussen opdrachtnemer en opdrachtgever
2.4	Overlegstructuren
	——— algemeen: schematische weergave
	——— opdrachtgever/opdrachtnemer, werkgroepen, afstemmingsoverleg testgroepen:
	——— doelstelling
	——— deelnemers
	——— voorzitterschap
	——— taken en bevoegdheden
	——— frequentie
	——— rapportage
	——— bijzonderheden
3	**Opdrachtverstrekking en bevestiging**
3.1	Algemeen
	——— welke opdrachtensoorten:
	——— reguliere productie
	——— incidentele productie
	——— tabelwijzigingen
	——— systeemontwikkeling en -onderhoud
	——— onderzoek-/uitzoekopdrachten
	——— autorisatie computertoegang
	——— verstrekking van gegevens aan derden
	——— wijziging van outputgegevens (formulieren)
3.2	Opdrachtverstrekking
	——— bevoegdheid tot opdrachtverstrekking
	——— naam en toenaam van bevoegde personen
	——— handtekeningenlijst bevoegde personen
	——— speciale formulieren
	——— kostenramingen
	——— wanneer begint de opdrachtuitvoering
	——— kostendrempels inzake uit te voeren werkzaamheden
	——— wie tekent bij drempeloverschrijding

3.3 Afhandeling diverse soorten opdrachten
- reguliere productie:
  - planning en data op te stellen door opdrachtnemer
  - aangeven wanneer wat waar moet zijn om verwerking te garanderen
  - goedkeuringsprocedure planning
  - afwijkingen op jaarplanning; opdracht hiertoe etc.
- overige opdrachten:
  - kostenramingen opdrachtnemer
  - uitvoering na opdrachtverstrekking opdrachtgever

3.4 Opdrachtbevestiging
- wie is verantwoordelijk voor bevestigingsbeheer
- kopie opdrachtbevestiging
- facturen factuurnummers
- kosten
- informatie binnen en buiten afgesproken mens- en machinecapaciteit

3.5 Voortgangsrapportage
- frequentie van rapportage
- opdrachtnummer
- datum opdracht
- datum opdrachtbevestiging
- korte omschrijving opdracht
- status opdracht

3.6 Formulieren
- de te gebruiken formulieren en ingevulde voorbeelden in een bijlage

4 Systeemdocumentatie

4.1 Algemeen
- welke eisen zijn te stellen aan documentatie
- vaste inhoud dossiers?
- welke dossiers worden aangelegd
- welke dossiers worden verstrekt aan de opdrachtgever
- wie verzorgt verspreiding
- wie onderhoudt de documentatie
- wie beheert de documentatie

4.2 Wijzigingen
- wie initieert wijzigingen
- hoe ontstaan wijzigingen
- opdrachtverstrekking tot wijziging
- opdrachtbevestiging bij wijziging
- goedkeuring wijzigingen
- begeleidingsbrief
- welke dossierbladen betreft het
- datum
- nummer
- periode van reclame

Vervolg Aandachtspuntenlijst DAP

5	Gegevensbeheer	
5.1	Algemeen	
	———	doel van gegevensbeheer
	———	verantwoordelijkheid
	———	uitbesteding van beheer bij opdrachtnemer
	———	delegatie van verantwoordelijkheid
	———	wie moet beschermingsmaatregelen nemen
5.2	Bestandsbeheer	
	———	volgens welke regels gaat het bestandsbeheer
	———	werkopdrachten ter uitvoering
	———	productiedossier
	———	bestandsbeschrijvingen
	———	bewaarvoorwaarden
	———	hoe wordt integriteit bewaakt
	———	bestand controlegetallen
	———	toegangsbeveiligingspakket
	———	welke bestandsorganisatiemethode
	———	archiefwet
5.3	Toegangsbeveiliging gegevensverzamelingen	
	———	opdrachten voor toegang schriftelijk
	———	door wie gefiatteerd
	———	toegang aan gebruikersnamen of aan personen
	———	wie kan toegang verlenen aan personen
	———	wie kan toegang verlenen aan gebruikersnamen
	———	bevestiging aan opdrachtverstrekker
	———	datum van bevestiging
	———	datum tot wanneer toegang
	———	aanvragen tot verandering in autorisaties
	———	periodiek overzicht van geïmplementeerde autorisaties
	———	mag opdrachtnemer ook gebruikersnamen?
	———	hoe wordt dat dan geregeld
	———	mondelinge toestemming van autorisatie bij acute productieproblemen
	———	schriftelijke melding spoedeisende autorisatie
	———	bevestiging van toestemming door opdrachtverstrekker
5.4	Aanvullende bepalingen	
	———	gegevensverstrekking aan instanties na goedkeuring van opdrachtverstrekker
	———	periodieke verstrekking aan derden vastleggen in dossier
	———	procedures ten aanzien van de in- en uitvoer van gegevens (gegevensdragers, wijze van verpakken, verzending en aflevering)
	———	wat te doen bij uitbesteding van data-entry door opdrachtnemer (geheimhouding schriftelijk bevestigen)
	———	wat te doen bij uitbesteding van de verwerking zelf door opdrachtnemer
	———	retourzending van invoer-gegevensdragers

6	Testen
6.1	Algemeen
	——— doel
	——— wijzigingen op systemen op kopie
	——— wijze van overeenstemming met wijziging en voorgestelde specificatie
	——— controle daarop
	——— gefingeerde cijfers voor het testen
6.2	Systeemtest
	——— doel
	——— wie is verantwoordelijk
	——— acceptatieprocedure
6.3	Testgroep
	——— opdrachtgever stelt testgroep in
	——— beoordeling van de testgroep
	——— ondersteuning voor beheerder bij opdrachtgever
	——— rapportage
	——— testprotocol:
	——— samenstelling testgroep
	——— beschrijving invoer en te verwachten uitvoer
	——— bevindingen
	——— advies
6.4	Acceptatietest
	——— gebruikersgerichte test
	——— doel
	——— functioneel ontwerp
	——— verantwoordelijkheid
	——— testmogelijkheden aangeven:
	——— uitgebreid
	——— alleen wijzigingen
	——— controleren van de systeemtest
	——— zelf genereren van testgegevens
	——— gebruik van andere testgegevens
	——— welke mogelijkheid wordt gekozen
	——— beschikbare capaciteit
	——— schriftelijke bevestiging aan opdrachtnemer
	——— aanlevering van testgegevens
	——— proefgevallen
	——— tabelgegevens
	——— testbestanden
	——— beschikbaarstelling bestanden
	——— tijdstip van test
	——— verzending van uitvoer van test
	——— testbegeleidingsbrief
	——— testdatum
	——— cycle van ingang
	——— programmagegevens (programmanaam, versie, moment van ingang, programmacontrolegetal)

_____	retourzending binnen 14 dagen naar verantwoordelijke van test
_____	goedkeuringsprocedure na een nieuwe test
_____	bepaling van tijdstip waarop goedgekeurde programma moet worden overgezet naar productieomgeving
_____	beschrijving van overzetprocedure

7 Programmatuur beheer

_____	welke wijze van beheer biedt de opdrachtnemer
_____	hoe wordt integriteit bewaakt en gewaarborgd
_____	goedkeuring van gewijzigde programma's schriftelijk namens opdrachtgever
_____	testbegeleidingsbrief

8 Productieproblemen

8.1 Algemeen

_____	wat zijn productiefouten
_____	procedures, hulpmiddelen
_____	kunnen ontstaan als gevolg van
_____	fout op productieafdeling van opdrachtnemer
_____	foute invoer opgeleverd door opdrachtgever
_____	programmafouten
_____	fouten in systeemontwerp

8.2 Procedurele afhandeling productieproblemen

_____	wanneer mag opdrachtnemer welke problemen oplossen
_____	kosten
_____	procedure voor elke foutencategorie
_____	afhandeling van bijzondere gevallen

8.3 Technisch afhandelen productieproblemen

_____	spoedproblemen
_____	speciaal formulier
_____	schriftelijke bevestiging
_____	gekozen methode van foutherstel
_____	tijdstip
_____	altijd melding van fouten in een specifiek register
_____	uitstel van foutenherstel om moverende redenen
_____	procedure voor uitstel van foutherstel

9 Calamiteiten

9.1 Begrip calamiteit

_____	dienstverlening niet na een bepaald tijdstip

9.2 Noodprocedure

_____	wanneer
_____	beschrijving van noodprocedure
_____	inwerkingtreding
_____	initiëren van procedure
_____	testen van noodprocedure
_____	frequentie van testen

- ——— aard en omvang van testen
- ——— beheerder

9.3 Bewaartermijnen bestanden
- ——— reconstructiedoeleinden
- ——— standaardvoorwaarden of aanvullende eisen
- ——— accorderen van uitwijkvoorziening van opdrachtnemer
- ——— welk principe wordt gehanteerd

9.4 Overige bepalingen
- ——— pijplijneffecten
- ——— specifieke uitvoerapparatuur
- ——— welke systeemonderdelen

10 Controle

10.1 Algemeen
- ——— soorten controles
- ——— invoer
- ——— productie
- ——— uitvoer en distributie
  - ——— programma's
  - ——— bestanden
  - ——— toegangsbeveiliging

10.2 Controles ten aanzien van invoer
- ——— hoe wordt de technische integriteit bewaakt en juistheid van de invoergegevens
- ——— inleesverslagen

10.3 Controle ten aanzien van de productie
- ——— productiedocumentatie
- ——— ontwerpdossier
- ——— geoorloofdheid
- ——— integriteit van programma's, invoerbestanden, ontstane uitvoerbestanden
- ——— opdrachtnemer moet zichtbaar kunnen maken dat:
  - ——— de juiste invoerbestanden zijn meegegaan
  - ——— de juiste uitvoerbestanden zijn ontstaan
  - ——— de juiste programmaversies zijn gebruikt
  - ——— de gegevensverwerking tot een goed einde is gekomen
  - ——— de diverse bewerkingen in de juiste volgorde hebben plaatsgevonden
  - ——— de juiste execute-informatie is ontstaan

10.4. Controles ten aanzien van de distributie
- ——— goedgekeurde ontwerpdossiers
- ——— verstrekking aan instanties
- ——— zie nabewerkinginstructies

10.5 Controles ten aanzien van programma's
- ——— integriteitbepaling en het aantonen daarvan
- ——— procedures
- ——— wijze van aantonen van de integriteit

10.6 Controles ten aanzien van bestanden
- ——— methode van bewaken en aantonen van de integriteit

	———	hashtotals
	———	systeem van bestandscontrolegetallen
	———	vaststelling van hashtotals
10.7	Controles ten aanzien van toegangsbeveiliging	
	———	integriteit van de geïmplementeerde autorisaties moet vastgesteld kunnen worden
	———	overzichten van geïmplementeerde autorisaties ter verstrekking aan de opdrachtgever
10.8	Procedures in geval van geconstateerde afwijkingen	
	———	melding van afwijking aan wie
	———	schriftelijk
	———	voorstel tot oplossing van afwijking
	———	analyse van afwijking
11	**Personele invulling functies**	
11.1	Algemeen	
	———	doel: aangeven welke met name genoemde medewerkers taken en verantwoordelijkheden hebben
11.2	Opdrachtverstrekking	
	———	ontwikkeling van applicatie
	———	onderhoud
	———	overige opdrachten
11.3	Applicatiebeheer	
	———	opdrachtnemer
11.4	Systeembeheer	
	———	bij opdrachtgever en bij opdrachtnemer
11.5	Overlegstructuren	
11.6	Werkgroepen	
12	**Systematische inhoudsopgave**	
13	**Historische inhoudsopgave**	

Medewerkers

De volgende personen hebben hun medewerking verleend aan de totstandkoming van dit Raamwerk:

G.W. van Blarkom (Registratiekamer)
Drs. J.E. Everts RA (Mazars Paardekooper Hoffman)
Drs. G.S. Flinkert (PricewaterhouseCoopers)
Mr. H.J.M. Gardeniers (Net2Legal Consultants)
Drs. G.A. Goud RA (Deloitte & Touche Bakkenist)
Drs. M.E.G. ten Have RE RA (EDP Audit Pool)
Drs. ing. R.F. Koorn RE (KPMG Information Risk Management)
Ing. J.N.M. Koppes (PinkRoccade)
J.P.M.J. Leerentveld RA (Registratiekamer)
Drs. R Schreijnders (Registratiekamer)
Mr. H. van der Wel (Mazars Paardekooper Hoffman)
R. van Yperen CISA (zelfstandig)
H. de Zwart RE RA RO (Claassen, Moolenbeek & Partners)

Colofon

Samenstelling
Samenwerkingsverband Audit Aanpak
Werkgroep Privacy Audit

Redactie
G.W. van Blarkom
J.P.M.J. Leerentveld RA
drs. R. Schreijnders

Vormgeving
Total Design Den Haag

Druk
SDU Grafisch Bedrijf bv

Versie
April 2001, versie 1