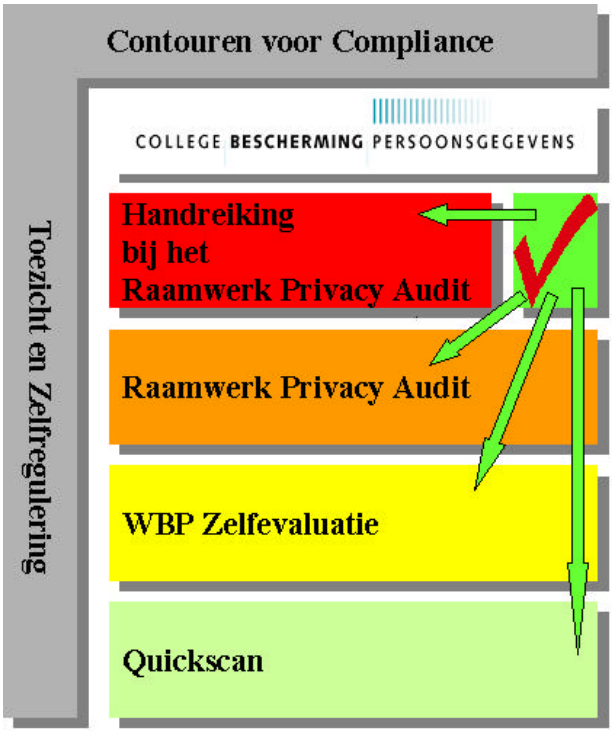
CONTOUREN
voor
COMPLIANCE

Handreiking
bij het
Raamwerk Privacy Audit



Samengesteld en gepubliceerd door:
College bescherming persoonsgegevens (CBP)
in samenwerking met:
Koninklijk Nederlands Instituut van Registeraccountants (NIVRA)
Nederlandse Orde van Register EDP-Auditors (NOREA)

Datum vaststelling:
24 mei 2005

0 Inhoudsopgave

1 Inleiding

De bescherming van persoonsgegevens is vanaf 1 september 2001 geregeld in de Wet bescherming persoonsgegevens (WBP). Deze wet stelt eisen aan de wijze waarop organisaties (zowel publiek als privaat) persoonsgegevens mogen verwerken. Vrijwel elke organisatie in Nederland verwerkt persoonsgegevens en heeft dus te maken met de WBP. Door middel van publicatie van Achtergrondstudies & Verkenningen, brochures en algemene (publieks)voorlichtingsmateriaal draagt het College bescherming persoonsgegevens (CBP) bij aan de bescherming van de persoonlijke levenssfeer in Nederland.

De verantwoordelijken voor het verwerken van persoonsgegevens, dienen deze bescherming als een vanzelfsprekendheid te ervaren en standaard in hun werkprocessen op te nemen. Bij de invoering van de WBP in de praktijk van alle dag spelen veel factoren een rol zoals technologische ontwikkelingen, de maatschappelijke en persoonlijke visie, hoeveelheid en de aard van de gegevens. Kortom, een complex geheel van factoren heeft invloed op de wijze van implementatie van de WBP in organisaties.

1.1 Randvoorwaarden

Alle werkzaamheden en beschrijvingen verbonden aan het beoordelen van een verwerking van persoonsgegevens nemen, naast dit document, de volgende drie documenten als uitgangspunt:

- Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen;
- Raamwerk Privacy Audit, uitgegeven door het Samenwerkingsverband Audit Aanpak;
- Achtergrondstudies & Verkenningen nummer 23, ‘Beveiliging van persoonsgegevens’ uitgegeven door de Registratiekamer.

Van de lezer wordt verwacht dat deze op de hoogte is van de inhoud van deze drie documenten.

1.2 Toezicht en zelfregulering

Het College bescherming persoonsgegevens (CBP) ziet toe op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. In het verlengde van het spraakgebruik wordt hier gesproken over ‘privacybescherming’, waarmee de bescherming van persoonsgegevens conform de Wet bescherming persoonsgegevens (WBP) wordt bedoeld.

Het CBP stimuleert zelfregulering door verantwoordelijken bij overheid en bedrijfsleven voor een adequate privacybescherming. Het CBP geeft daarmee aan zich te willen opstellen als tweedelijnsorganisatie. Die rol is alleen mogelijk indien de eerste lijn beschikt over kennis van zaken en zich bewust is van de eigen verantwoordelijkheid. De complexiteit van de WBP en de open normen noodzaakt tot interpretatie bij de vertaling naar de praktijk van alle dag.

Zelfregulering via gedragscodes en de mogelijkheden tot het aanstellen van een Functionaris voor de Gegevensbescherming (FG), die in de WBP een prominente plaats heeft gekregen, helpen hierbij.

Om zelfregulering nog meer te stimuleren is in samenwerking met marktpartijen (accountantsorganisaties, adviesbureaus en beroepsorganisaties) een viertal zelfreguleringproducten ontwikkeld waarmee overheid en bedrijfsleven, zelfstandig of met behulp van een (externe) adviseur, kunnen nagaan hoe zij er voorstaan bij de implementatie en naleving van de privacywet- en regelgeving.

1.3 Contouren voor Compliance[1]

De zelfreguleringproducten bevatten in beginsel dezelfde hoofdthema's. Tussen de verschillende producten zit een verschil in diepgang, zodat een goede afweging gemaakt moet worden bij de keuze tussen de producten. De toenemende diepgang van de vraagstelling en de wijze van verwerking van de antwoorden is productspecifiek. Onder de naam: Contouren voor Compliance zijn vier zelfreguleringproducten ontwikkeld.

1. Met 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.

2. De WBP Zelfevaluatie is een hulpmiddel voor functionarissen die bij de privacybescherming zijn betrokken. De WBP Zelfevaluatie is een systematische methode om zelfstandig de kwaliteit van een organisatie voor wat betreft de privacybescherming te beoordelen. Dit geeft een duidelijk beeld over de huidige situatie en de noodzakelijke verbeterpunten. Eventueel kan een organisatie de uitgevoerde zelfevaluatie laten reviewen door een externe deskundige.

De laatste twee producten zijn bedoeld als hulpmiddel bij de toetsing op het voldoen aan relevante wet- en regelgeving. Omdat de toepasselijkheid van wet- en regelgeving afhankelijk is van een veelheid van factoren kan geen eenduidig kader gegeven worden. In de praktijk betekent dit dat de toepasselijke wet- en regelgeving altijd kaderstellend is boven de zelfreguleringproducten. De professionele oordeelsvorming van de onderzoeker speelt, gezien de open wettelijke normen, bij de beoordeling een grote rol.

3. Het Raamwerk Privacy Audit wordt gebruikt door een deskundige of team van deskundigen als basis voor de uitvoering van een onderzoek naar de wijze waarop en de mate waarin de organisatie voldoet aan de eisen die de wet heeft gesteld aan de bescherming van persoonsgegevens. Een zogenaamde privacy-audit geeft de leiding van een organisatie met een hoge mate van zekerheid een onafhankelijk kwaliteitsoordeel over de naleving van de wettelijke bepalingen en daarmee ook inzicht in de sterke en zwakke punten rond de bescherming van persoonsgegevens. De resultaten van het onderzoek kunnen leiden tot het afgeven van een kwaliteitsoordeel, dat bestemd is voor het maatschappelijk verkeer.

In het Raamwerk Privacy Audit is geen normering aangegeven voor de criteria die de wet stelt aan organisaties als het gaat om de bescherming van persoonsgegevens.

[1] Compliance is een algemene Engelse term waarmee aangegeven wordt dat men voldoet aan de eisen gesteld in desbetreffende wet- en regelgeving.

4. Om richting te geven bij het gebruik van het raamwerk is het document Handreiking bij het Raamwerk Privacy Audit opgesteld. Deze handreiking is een hulpmiddel bij het concretiseren van de open norm, te gebruiken bij het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking. De handreiking is gebaseerd op het Raamwerk Privacy Audit. De handreiking is niet alleen bedoeld voor een onderzoeker die een privacy-audit uitvoert bij een verantwoordelijke, maar kan ook door medewerkers binnen de organisatie worden gebruikt, bijvoorbeeld door een Functionaris voor de Gegevensbescherming of een security officer.

1.4 Kwaliteitsoordeel

De roep om wat gemakshalve een privacy-audit heet, neemt toe. Privacy-audits worden niet alleen uitgevoerd ten behoeve van de verantwoordelijke zodat deze zijn interne processen kan bijstellen, maar er bestaat ook behoefte aan een kwaliteitsoordeel van een onafhankelijke partij, over de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking.

Wanneer dit kwaliteitsoordeel ten behoeve van het maatschappelijk verkeer wordt afgegeven is het volgende voor de opdrachtgever van belang. Een afgegeven kwaliteitsoordeel geeft zekerheid binnen het maatschappelijk verkeer wanneer aan de onderstaande aandachtspunten wordt voldaan.

Bij de uitvoering van het onderzoek door een onafhankelijke partij zijn de volgende vier documenten als uitgangspunt genomen:

- Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens;
- Achtergrondstudies & Verkenningen nummer 23, ‘Beveiliging van persoonsgegevens’;
- Raamwerk Privacy Audit;
- Handreiking bij het Raamwerk Privacy Audit.

De verantwoordelijke die een onderzoek wil laten instellen met als doel een kwaliteitsoordeel te krijgen, dient eisen te stellen aan de deskundigheid, onpartijdigheid, onafhankelijkheid en geheimhouding van de onderzoeker. De onderzoeker dient minimaal te beschikken over kennis op hbo-niveau van auditing in het algemeen, kennis over privacywet- en regelgeving, vertrouwd met informatie- en communicatietechnologie, inzicht in administratieve organisatie en een verplichting om op de hoogte te blijven van de ontwikkelingen op deze deskundigheidsgebieden. Voorts dient de onderzoeker te zijn onderworpen aan kwaliteitstoetsing en tuchtrecht.

Daarnaast dienen eisen te worden gesteld aan de organisatie van de onderzoeker en de organisatie van het beroep. Aan de organisatie worden eisen gesteld ten aanzien van interne kwaliteitstoetsing en kwaliteitsborging. Daarnaast zijn onpartijdigheid en onafhankelijkheid ten opzichte van de verantwoordelijke, onafhankelijkheid ten opzichte van de opdracht, geheimhouding, een onafhankelijke geschillen- of klachtenprocedure geregeld en mogelijk extern kwaliteitstoezicht.

Tevens is het raadzaam eisen te stellen aan een zorgvuldige opdrachtuitvoering (opdrachtformulering, uitvoering, oordeelsvorming, rapportage en dossieropbouw).

2 Begrippen

2.1 Privacy

Het begrip privacy wordt voor vier situaties gebruikt:

- Lichamelijke privacy
  Grondwet artikel 11:
  Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.
- Relationele privacy
  Grondwet artikel 13:
  1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
  2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.
- Ruimtelijke privacy
  Grondwet artikel 12:
  1. Het binnentreden in een woning tegen de wil van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.
  2. Voor het binnentreden overeenkomstig het voorgaande lid zijn voorafgaande legitimatie en mededeling van het doel van het binnentreden vereist, behoudens bij de wet gestelde uitzonderingen. Aan de bewoner wordt een schriftelijk verslag van het binnentreden verstrekt.
- Informationele privacy
  Grondwet artikel 10:
  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.

In het kader van compliance onderzoeken op het gebied van privacywet- en regelgeving wordt slechts gerefereerd aan de informationele privacy: de bescherming van persoonsgegevens.

2.2 Scope van het compliance onderzoek

Het object van onderzoek betreft één specifiek benoemde verwerking van persoonsgegevens.

Voor het verkrijgen van een kwaliteitsoordeel, bestemd voor het maatschappelijk verkeer, wordt de verwerking bij het CBP gemeld ook indien de verwerking ingevolge het Vrijstellingsbesluit WBP vrijgesteld is van melden of indien er voor de organisatie van de verantwoordelijke een Functionaris voor de Gegevensbescherming (art. 62 WBP) is benoemd, bij wie deze melding zou kunnen plaatsvinden.

De voordelen van deze melding bij het CBP zijn:

- de afbakening wordt door de verantwoordelijke zelf opgesteld, waarbij het aan de onderzoeker is om vast te stellen dat de aangetroffen verwerking van persoonsgegevens binnen die grenzen blijft;

- de belanghebbende bij het kwaliteitsoordeel kan in het openbare meldingenregister bij het CBP vaststellen welke verwerking van persoonsgegevens is beoordeeld.

Deze afbakening voorkomt dat een organisatie bijvoorbeeld zijn personeelsinformatie systeem laat onderzoeken en de aldus verkregen beoordeling, bijvoorbeeld in commerciële uitingen, betrekking laat hebben op verwerkingen van persoonsgegevens betreffende zijn klanten.

In de WBP wordt gesteld dat de wet van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. In de praktijk zal een verantwoordelijke een groot deel van de verwerking van persoonsgegevens inrichten binnen het IT domein. Delen van de verwerking bevinden zich echter buiten dit domein, zoals: postkamer, archief, papieren dossiers, vernietiging, handmatige verwerking. Bij het onderzoek dient de gehele verwerking te worden beoordeeld, dus ook die delen die zich buiten het IT domein bevinden.

Indien een verantwoordelijke meerdere verwerkingen van persoonsgegevens onder één melding bij het CBP heeft gemeld, zal het onderzoek op al deze verwerkingen betrekking moeten hebben.

2.3 Kwaliteitsaspecten

De onderstaande kwaliteitsaspecten met de op de WBP afgestemde definities zijn van toepassing op een compliance onderzoek op het gebied van privacywet- en regelgeving:

- Exclusiviteit
  Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens;
- Integriteit
  De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen;
- Continuïteit
  De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmering beschikbaar zijn overeenkomstig daarover gemaakte afspraken en wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van de gegevensverwerking;
- Controleerbaarheid
  De controleerbaarheid is de mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en de 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.

Deze vier kwaliteitsaspecten zijn gebaseerd op de standaard voor IT-audits. De open normen zoals die door de wetgever zijn opgesteld hebben geen één op één relatie met deze kwaliteitsaspecten. Wel is het zo dat de standaard als kapstok gebruikt kan worden voor het compliance onderzoek. Een standaard geeft houvast; een nieuw geïntroduceerd kwaliteitsaspect ‘privacy’ zou voor onnodige onduidelijkheid hebben gezorgd.

2.4 Risicokwalificatie

In het Raamwerk Privacy Audit wordt in hoofdstuk V onder verwerkingseis voor persoonsgegevens V.7 – 'Beveiliging' voor het normatief kader verwezen naar de 14 aandachtsgebieden die in het document Achtergrondstudies & Verkenningen nummer 23 worden onderkend. Hierin is, gerelateerd aan risicoklassen, een uitwerking opgenomen van eisen die moeten worden vertaald in concrete, op de specifieke situatie van de verwerking toegesneden, passende maatregelen. Deze risicoklassen zijn ook van toepassing op de andere acht verwerkingseisen voor persoonsgegevens en dus op het wegen van incidenten en deficiënties.

De uitgewerkte risicoclassificatie kan in hoofdlijnen als volgt kan worden samengevat:

- Risicoklasse 0
  publiek niveau
  In deze risicoklasse zijn gegevens opgenomen waarvan algemeen is aanvaard dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene (telefoonboeken, brochures, publieke internet sites, etc.).
  Naar verwachting zal voor de verwerking van dit type persoonsgegevens geen onderzoek worden aangevraagd. In de beoordeling per verwerkingseis is deze risicoklasse daarom buiten beschouwing gelaten.
- Risicoklasse I
  basisniveau
  In deze risicoklasse gaat het bij verwerking van persoonsgegevens meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantregistraties en overeenkomstige relaties tussen een betrokkene en een organisatie.
- Risicoklasse II
  verhoogd risico
  In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan één van de hieronder gegeven beschrijvingen:
  - de verwerking van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
  - de verwerking van gegevens in het bank- en verzekeringswezen over de persoonlijke of economische situatie van een betrokkene;
  - de verwerking van gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
  - de verwerking van, op zich onschuldige, gegevens die betrekking hebben op de gehele of grote delen van de bevolking;
  - alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.
- Risicoklasse III
  hoog risico
  Tot de verwerking van persoonsgegevens in deze risicoklasse worden gerekend de verwerkingen die betrekking hebben op:
  - opsporingsdiensten met bijzondere bevoegdheden;
  - gegevens waarop een bijzondere publieke of private geheimhoudingsplicht rust;
  - verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt (bijvoorbeeld DNA-databank).

Aard van de persoonsgegevens:		Persoons-gegevens	Bijzondere persoons-gegevens Conform artikel 16 WBP	Financieel en / of economische persoons-gegevens
Hoeveelheid persoons-gegevens	*Aard van de verwerking*			
Weinig persoons-gegevens	Lage complexiteit van de verwerking	**risicoklasse 0**	**risicoklasse II**	**risicoklasse II**
Veel persoons-gegevens	Hoge complexiteit van de verwerking	**risicoklasse I**	**risicoklasse III**	

Schema voor het bepalen van de risicoklasse

De risicoklasse is van invloed op het bepalen van het stelsel van maatregelen en procedures waarmee moet worden voldaan aan de norm (eisen). Daarmee bepaalt de risicoklasse het gewicht dat aan de afwijkingen van het stelsel wordt toegekend. De deficiënties en incidenten moeten integraal worden beoordeeld in relatie tot elke verwerking.

Voor de eisen in Achtergrondstudies & Verkenningen nummer 23 geldt daarbij dat die cumulatief van aard zijn, dat wil zeggen dat de omvang en / of het niveau van de eisen toeneemt naar mate er sprake is van een hogere risicoklasse. De verantwoordelijke moet daarom beschikken over een analyse waaruit blijkt:

- in welke risicoklasse de betreffende verwerking valt;
- wat de relatie is tussen het te hanteren niveau van de eisen en het getroffen passende stelsel van maatregelen en procedures, dat behoort bij de betreffende risicoklasse.

Het onderscheid tussen weinig en veel persoonsgegevens moet niet alleen worden bepaald aan de hand van het absolute aantal persoonsgegevens dat per betrokkene wordt verwerkt. Bij het vaststellen van de risicoklasse wordt hier tevens bedoeld na te gaan uit hoeveel verschillende soorten persoonsgegevens de verwerking is samengesteld. Bijvoorbeeld, alleen koopgedraggegevens (weinig) of koopgedrag- en betalingsmoraal- en gezinssamenstellingsgegevens (veel).

Het onderscheid tussen een lage en een hoge complexiteit van de verwerking van persoonsgegevens wordt bepaald door de wijze waarop deze verwerking is gerealiseerd. Een implementatie op een vrijstaande PC waarbij de papieren dossiers direct na verwerking worden vernietigd kan worden geclassificeerd als een verwerking met een lage complexiteit, een webapplicatie waarbij de papieren dossiers jarenlang in het archief worden bewaard als een met een hoge complexiteit.

In deze analyse moet rekening zijn gehouden met de beperking en / of aanvulling op grond van wetten en voorschriften als bedoeld in paragraaf 3.6 – V.I van de handreiking.

In hoofdstuk 3 van de handreiking is een concretisering van de wettelijke norm opgenomen. Deze zijn uitgewerkt op basis van de in Achtergrondstudies & Verkenningen nummer 23 gedefinieerde risicoklasse. Het niet voldoen aan die normen kan leiden tot non-conformiteiten, deficiënties en incidenten. Het gewicht dat, aan een afwijking ten opzichte van de norm, moet worden toegekend is gerelateerd aan de vastgestelde risicoklasse. Hierin is tevens het onderscheid tussen structurele en incidentele afwijkingen uitgewerkt.

2.5 Toleranties bij de beoordeling

Bij het beoordelen van een verwerking van persoonsgegevens zal de onderzoeker een vergelijking maken tussen de norm en de aangetroffen situatie. Indien geen verschil wordt vastgesteld, functioneert het (deel)object conform de norm.

Indien verschillen worden aangetroffen maakt het toetskader onderscheid in drie situaties:

- Non-conformiteit
  een structurele (stelselmatige), materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van de persoonsgegevens van een of meer betrokkene(n) in ernstige mate is of kan worden geschaad.
- Deficiëntie
  een structurele (stelselmatige), niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van persoonsgegevens van een of meer betrokkene(n) niet in ernstige mate is of kan worden geschaad.
- Incident
  een incidentele, niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscode waardoor de bescherming van persoonsgegevens van een of meer betrokkene(n) niet in ernstige mate is of kan worden geschaad.

De onderzoeker kan afhankelijk van de concrete aangetroffen situatie besluiten tot een op- of afwaardering van de ernst van de afwijking.

Het onderscheid tussen een materiële en een niet-materiële tekortkoming wordt bepaald door de mate waarin de betrokkene geschaad wordt in de bescherming van zijn persoonlijke levenssfeer. Dit is ter beoordeling van de onderzoeker.

3 Beoordeling

3.1 Verwerking van persoonsgegevens, is de WBP van toepassing?
(artikel 1, 2, 3, 4)

Bij dit onderdeel van het onderzoek wordt formeel vastgesteld dat er sprake is van een verwerking van persoonsgegevens en dat de WBP van toepassing is.

Uitgangspunt van het Raamwerk Privacy Audit is dat vastgesteld is dat er sprake is van een verwerking van persoonsgegevens en dat deze verwerking valt onder de reikwijdte van de wet.

Om vast te kunnen stellen of de WBP van toepassing is, worden de volgende vijf stappen uitgevoerd:

- stel vast dat er sprake is van een persoonsgegeven in de zin van de WBP (artikel 1 onder a);
- stel vast dat er sprake is van het verwerken van persoonsgegevens in de zin van de WBP (artikel 1 onder b);
- stel hiertoe vast dat deze persoonsgegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt (artikel 2 eerste lid);
  of
  stel vast dat bij een niet geautomatiseerde verwerking de persoonsgegevens in een bestand zijn of worden opgenomen (artikel 2 eerste lid);
- stel vast dat de verwerking van persoonsgegevens niet valt onder één van de in artikel 2 tweede en derde lid genoemde verwerkingen van persoonsgegevens;
- stel vast dat de verwerking van persoonsgegevens niet valt onder één van de in artikel 3 of 4 genoemde uitzonderingen.

3.2 Risicoklasse

Voor de beoordeling van de feitelijke constateringen rond de negen verwerkingseisen voor persoonsgegevens en de twee eisen voor de evaluatie van de verwerking, zoals gedefinieerd in het Raamwerk Privacy Audit, is het van belang dat allereerst de risicoklasse voor de verwerking van persoonsgegevens is vastgesteld.

De risicoklasse is oorspronkelijk door het CBP gedefinieerd voor het bepalen van het stelsel van maatregelen en procedures in het kader van de beveiliging van persoonsgegevens (artikel 13 WBP). Voor het compliance onderzoek is deze classificatie van toepassing verklaard op de gehele verwerking van persoonsgegevens.

De verantwoordelijke stelt vast welke risicoklasse van toepassing is op de te beoordelen verwerking van persoonsgegevens. Deze analyse dient door de verantwoordelijke schriftelijk te zijn gemotiveerd. In het rapport over het onderzoek wordt melding gemaakt van de wijze waarop de risicoklasse is vastgesteld.

Er dient vastgesteld te worden dat:

- de door de verantwoordelijke uitgevoerde risicoclassificatie aansluit op de (in de melding genoemde) verwerking;
- de analyse van de verantwoordelijke juist en volledig is;
- het in het kader van het onderzoek te beoordelen passende stelsel van maatregelen en procedures overeenkomt met minimale normen zoals die in dit document zijn geconcretiseerd;

- de aanvullingen op het Raamwerk Privacy Audit en Achtergrondstudies & Verkenningen nummer 23 op grond van aanvullende wetten en voorschriften volledig en juist (passend) zijn;
- de aanvulling van de non-conformiteiten, deficiënties en incidenten op grond van de uitkomsten van de analyse aansluiten op de uitwerking in hoofdstuk 3.6 van dit document.

Met het van toepassing verklaren van de risicoklasse op de gehele verwerking van persoonsgegevens, is er een relatie tussen de risicoklasse en elk van de negen verwerkingseisen zoals die in het raamwerk zijn gedefinieerd.

Er is gekozen voor een wegingsfactor voor elk van de verwerkingseisen vast te stellen. Dit heeft slechts te maken met het feit dat het daarmee mogelijk is, op termijn, één (reken)model op te stellen voor de uiteindelijke beoordeling van de gehele verwerking van persoonsgegevens. Dit definitieve rekenmodel zal na de evaluatie, nadat de nodige praktijk ervaring is opgedaan, in de Handreiking worden opgenomen.

3.3 Voorlopige rekenmodel

Bij de beoordeling van de verwerking van persoonsgegevens wordt gewerkt met een systeem van punten. Het aantal punten is afhankelijk van de vastgestelde risicoklasse en van de ernst van de afwijking. In deze voorlopige vorm is deze tabel een hulpmiddel bij de professionele oordeelsvorming door de onderzoeker.

Een non-conformiteit leidt voor elke risicoklasse tot een dusdanige situatie dat het kwaliteitsoordeel niet wordt afgegeven, niet wordt verlengd of waarvan de geldigheid wordt opgeschort.

Bij incidenten en deficiënties geldt het onderstaande schema.

Deficiëntie				**Incident**			
Punten per risicoklasse							
0	I	II	III	0	I	II	III
1	2	4	8	1	1	2	3

Deze tabel geeft aan dat elke deficiëntie in een verwerking van persoonsgegevens in risicoklasse II, leidt tot vier (straf)punten. Na afloop van het onderzoek worden alle punten opgeteld. Vervolgens is het aan de professionele oordeelsvorming van de onderzoeker om vast te stellen welke gevolgen dit totaal heeft op het afgeven, verlengen of (tijdelijk) opschorten van de geldigheid van het kwaliteitsoordeel.

3.4 Toelichting op het model Verwerkingseisen voor persoonsgegevens

In hoofdstuk 3.6 wordt het toetskader voor alle negen verwerkingseisen voor persoonsgegevens beschreven.

Elke verantwoordelijke heeft zijn eigen specifieke omgevingsvariabelen voor het inrichten van de verwerking van persoonsgegevens. Deze hebben betrekking op een groot aantal factoren, zoals:

- de aard en omvang van de persoonsgegevens;
- de complexiteit van de interne verwerking;
- de relaties met externe partijen;
- de van toepassing zijnde wettelijke verplichtingen en regelingen;
- de inleving van de menselijke factor met betrekking tot de persoonsgegevens;

- de bedrijfssector;
- de publieke sector of een private onderneming;
- een grote of kleine organisatie;
- een eenvoudige of complexe infrastructuur.

Dit maakt het onmogelijk een normenkader te schrijven waarbij voor elke situatie een kant en klaar recept wordt gegeven om het kwaliteitsoordeel vast te stellen. Dit betekent per definitie dat volledigheid in deze handreiking onmogelijk is. Ter illustratie van deze 'onvolledigheid' wordt elke lijst met mogelijke non-conformiteiten, deficiënties en incidenten afgesloten met een 'leeg aandachtspunt'.

Het volgende hoofdstuk beoogt de onderzoeker voor elke van de verwerkingseisen een aantal concrete handvatten te geven. Samen met de noodzakelijke deskundigheid van de onderzoeker om tot een professionele oordeelsvorming te komen, wordt de verwerking van persoonsgegevens met een zo groot mogelijke mate van zekerheid beoordeeld.

De opbouw van hoofdstuk 3.6 is gebaseerd op het Raamwerk Privacy Audit (V.I, V.1 tot en met V.9 met uitzondering van V.7) en Achtergrondstudies & Verkenningen nummer 23 (V.7).

3.5 Model verwerkingseisen voor persoonsgegevens

3.5.1 Leeswijzer

Per verwerkingseis wordt allereerst een aantal voorbeelden van mogelijke non-conformiteiten gegeven. De controle op het voorkomen van, in ieder geval, één van deze situaties zal tijdens een vooronderzoek aan het licht komen.

Tijdens het onderzoek kunnen dus alleen deficiënties en incidenten ontdekt worden. Bij elke verwerkingseis zijn hiervan een aantal voorbeelden gegeven.

Op basis van het de professionele oordeelsvorming kunnen deze afwijkingen van de norm worden op- of afgewaardeerd.

3.5.2 Gebruik van schuinschrift

In de volgende paragrafen van dit hoofdstuk wordt gebruik gemaakt van citaten uit het Raamwerk Privacy Audit en Achtergrondstudies & Verkenningen nummer 23. Voor deze citaten wordt gebruik gemaakt *'schuinschrift'*.

3.6 Beoordeling per verwerkingseis

Voor de paragraafindeling bij elk van de verwerkingseisen wordt de indeling in subnormen gebruikt zoals deze in het Raamwerk Privacy Audit is gedefinieerd.

V.I Inleiding
(artikel 25, 26, 29)

De Wet bescherming persoonsgegevens biedt het normatief kader van waaruit de specifieke technische en organisatorische maatregelen 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 WBP
Indien een verwerking van persoonsgegevens wordt vrijgesteld van melden dan geeft het Vrijstellingsbesluit WBP 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 sociale wetgeving.

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 compliance onderzoek 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 compliance onderzoek in die sector als norm gebruikt moeten worden.

Jurisprudentie
Vanaf de inwerkingtreding van de WBP zijn en worden er door de toezichthouder en de diverse rechtscolleges uitspraken gedaan waarbij de open norm geconcretiseerd wordt. Deze jurisprudentie vormt vanaf het moment van de uitspraak een onderdeel van het van toepassing zijnde normenkader.

V.1 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 WBP, 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.*

Non-conformiteiten

- De concrete verwerking van persoonsgegevens in de praktijk wijkt onaanvaardbaar af van de inhoud van de melding.
- De verantwoordelijke heeft de verwerking van persoonsgegevens bij het CBP gemeld. De procedure voor het verstrekken van inlichtingen door de verantwoordelijke omtrent de verwerking ontbreekt.
- De verantwoordelijke heeft, ondanks de verplichting daartoe, geen voorafgaand onderzoek bij het CBP aangevraagd, dan wel is voortijdig begonnen met deze verwerking van persoonsgegevens.
- De verwerking van persoonsgegevens is aangevangen voordat het CBP in het kader van een voorafgaand onderzoek een verklaring van rechtmatigheid heeft afgegeven.
- De melding heeft slechts betrekking op één of enkele van de handelingen met betrekking tot persoonsgegevens, in plaats van op de gehele verwerking.
-

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).

Dit onderdeel van de verwerkingseis is niet van toepassing omdat voor goedkeuring geldt dat de verantwoordelijke de verwerking van persoonsgegevens bij het CBP moet melden.

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.

Deficiënties en Incidenten

- De beschreven verwerking en de aangetroffen situatie wijken onderling af;
- De personalia op de melding zijn niet meer actueel;
- De gegevens omtrent de beveiliging van persoonsgegevens zijn niet meer actueel;

- De melding geeft ten onrechte aan dat er geen gegevens buiten de EU worden doorgegeven;
-

3. Voorafgaand onderzoek door het CBP

In bepaalde gevallen gaat aan het melden van de verwerking een onderzoek door het CBP vooraf.

Deficiënties en Incidenten

- De verantwoordelijke heeft nagelaten een voorafgaand onderzoek aan te vragen;
- De aanbevelingen van het CBP zijn niet opgevolgd;
-

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.

Dit onderdeel van de verwerkingseis is niet van toepassing omdat voor goedkeuring geldt dat de verantwoordelijke de verwerking van persoonsgegevens bij het CBP moet melden.

5. Periodieke beoordeling 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.

Deficiënties en Incidenten

- Wijzigingen in de verwerking van persoonsgegevens zijn niet verwerkt in de melding;
- Wijzigingen op de melding worden niet ten minste drie jaar bewaard;
-

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.

Deficiënties en Incidenten

- De procedure voor het verstrekken van inlichtingen omtrent de verwerking behorende bij de melding is niet volledig;
- Er is een tekortkoming in de informatieverschaffing over de melding;
-

V.2 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.

Non-conformiteiten

- De algemene informatieverstrekking aan de betrokkene is in het geheel niet in overeenstemming met de aangetroffen situatie. Deze informatie kan ondermeer betrekking hebben op een algemene folder of op een privacyverklaring op bestelformulier of website.
- Bij het verzamelen van de persoonsgegevens niet bij de betrokkene zelf, zijn er grove tekortkomingen in de informatieverschaffing aan de betrokkene. Dit betreft met name de identiteit van de verantwoordelijke, de doeleinden van de verwerking en de nadere informatie die moet worden verschaft om een behoorlijke en zorgvuldige verwerking te waarborgen (aard van de persoonsgegevens, nevengebruik en dergelijke).
- De verantwoordelijke maakt misbruik van de wettelijke uitzonderingsgronden op de informatieverplichting.
- De verantwoordelijke maakt onrechtmatig gebruik van niet openbare bronnen voor het verzamelen of verrijken van persoonsgegevens.
- De verantwoordelijke heeft geen stelsel van maatregelen en procedures getroffen om de herkomst van de verzamelde persoonsgegevens vast te leggen.
- De verantwoordelijke stelt de betrokkene niet in de gelegenheid verzet aan te tekenen tegen verwerking van persoonsgegevens voor commerciële of charitatieve doelen.
- De verantwoordelijke heeft geen maatregelen getroffen persoonsgegevens te beschermen (bijvoorbeeld door het anonimiseren) indien deze voor wetenschappelijke of statistische doeleinden worden gebruikt.
-

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:

1. *De persoonsgegevens worden van de betrokkene zelf verkregen.Hier geldt de informatieverplichting vóór het moment van verkrijging.*

   Deficiënties en Incidenten

   - De verantwoordelijke maakt vaker dan noodzakelijk gebruik van de wettelijke uitzonderingsgronden op de informatieverplichting;
   - De verantwoordelijke verzuimt de herkomst van de persoonsgegevens vast te leggen;
   -

2. *De persoonsgegevens worden op andere wijze verkregen. Hier geldt de informatieverplichting het moment van vastlegging of bij verstrekking aan een derde het moment van de eerste verwerking.*

   Deficiënties en Incidenten

- De verantwoordelijke maakt vaker dan noodzakelijk gebruik van de wettelijke uitzonderingsgronden op de informatieverplichting;
- De verantwoordelijke verzuimt de herkomst van de persoonsgegevens vast te leggen;
-

2. Bijzonderheden bij informatieverstrekking aan betrokkene

De plicht tot informatieverstrekking aan betrokkene vervalt indien de verwerking plaatsvindt in het kader van wetenschappelijk onderzoek of statistiek en er voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens alleen voor deze doeleinden worden gebruikt.

Deficiënties en Incidenten

- De verantwoordelijke heeft onvoldoende maatregelen genomen de persoonsgegevens te beschermen indien deze voor wetenschappelijk onderzoek of statistiek worden verwerkt;
-

3. Informeren bij werving voor commerciële of charitatieve doelen

De informatieplicht van de verantwoordelijke is in deze uitgebreid met het actief informeren van de betrokkene over het recht op verzet.

Deficiënties en Incidenten

- De verantwoordelijke biedt de betrokkene onvoldoende mogelijkheden verzet aan te tekenen tegen verwerking van persoonsgegevens voor commerciële of charitatieve doelen;
-

V.3 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.

Non-conformiteiten

- De doeleinden zoals die in de melding door de verantwoordelijke zijn gedaan, zijn niet specifiek.
- De verdere verwerking van persoonsgegevens is onverenigbaar met het doel waarvoor deze worden verzameld.
- De verantwoordelijke heeft geen bewaartermijnen vastgesteld voor de verzamelde persoonsgegevens.
- De door de verantwoordelijke vastgestelde bewaartermijn is langer dat de noodzakelijke termijn om het doel van de verwerking te bereiken.
- De verantwoordelijke, niet zijnde de geheimhoudingsplichtige, verwerkt persoonsgegevens waarop een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift rust.
-

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.

Deficiënties en Incidenten

- De persoonsgegevens die de verantwoordelijke verzamelt passen niet binnen het doeleinde zoals de verantwoordelijke die heeft gemeld;
-

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.

Deficiënties en Incidenten

- De verdere verwerking is onvoldoende verenigbaar met het doel waarvoor deze worden verzameld;
-

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.

Deficiënties en Incidenten

- De verantwoordelijke houdt zich niet aan de vastgestelde bewaartermijn;
-

---

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[2].

Non-conformiteit

De ernst van de overtreding is dusdanig dat er bij overtreding altijd sprake is van een non-conformiteit.

---

[2] Bij het onderzoek naar, de naast de WBP, van toepassing zijnde wet- en regelgeving (Raamwerk hoofdstuk V.I) zal de onderzoeker de hier bedoelde bepalingen aantreffen.

V.4 Rechtmatige grondslag

(artikel 6, 8, 16, 17, 18, 19, 20, 21, 22, 23, 24)

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

Non-conformiteiten

- De verantwoordelijke verwerkt persoonsgegevens zonder een wettelijke grondslag.
- De verantwoordelijke verwerkt bijzondere gegevens zonder dat daarvoor een ontheffing van het wettelijke verbod is.
- Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt door de verantwoordelijke verwerkt buiten de uitvoering van die wet dan wel buiten de doeleinden bij wet- of regelgeving bepaald.
-

1. Grondslag voor de verwerking van persoonsgegevens

Non-conformiteit

Indien er geen grondslag is voor de verwerking van persoonsgegevens is er in alle gevallen sprake van een non-conformiteit.

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).

Deficiënties en Incidenten

- De verantwoordelijke verzamelt regelmatig bijzondere gegevens zonder dat hij het oogmerk heeft deze verder te verwerken; [3]
- De verantwoordelijke verzamelt regelmatig wettelijk ingestelde persoonsnummers zonder dat hij daarbij het oogmerk heeft deze verder te verwerken;
-

[3] Hier wordt gedoeld op situaties waar een verantwoordelijke bedoelde persoonsgegevens, ongevraagd verstrekt krijgt. Verdere verwerking vindt niet plaats en vernietiging ervan is niet mogelijk omdat dan andere gegevens eveneens worde vernietigd. Deze voetnoot heeft betrekking op beide gegeven voorbeelden

V.5 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.

Non-conformiteiten

- De verantwoordelijke verzamelt meer persoonsgegevens dan die welke noodzakelijk zijn voor het doel van de verwerking van persoonsgegevens. Hierbij heeft de verantwoordelijke geen gerechtvaardigd belang voor de bovenmatige verzameling.
- De verantwoordelijke heeft geen maatregelen om de persoonsgegevens, voor zover dat binnen zijn bereik ligt, op juistheid te controleren.
- De verantwoordelijke heeft geen maatregelen voor het corrigeren van onjuiste invoer van gegevens.
- De verantwoordelijke heeft geen procedure voor het verstrekken van gecorrigeerde gegevens aan derden aan wie de gegevens eerder zijn verstrekt.
- De verantwoordelijke laat na juistheids- en, volledigheidscontroles uit te voeren op door hem verzamelde persoonsgegevens.
-

1. Kwaliteit van de gegevensverwerking

Deficiënties en Incidenten

- De maatregelen voor het controleren of corrigeren van de invoer van gegevens is niet toereikend;
-

2. Fouten in de gegevensverwerking

Deficiënties en Incidenten

- De verantwoordelijke heeft geen maatregelen genomen voor het corrigeren van foutieve invoer van gegevens;
- De verantwoordelijke gaat onzorgvuldig om met het afhandelen van foutmeldingen tijdens de verwerking van gegevens;
-

V.6 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.

Non-conformiteiten

- De verantwoordelijke heeft geen procedure op basis waarvan de betrokkene zijn rechten kan uitoefenen.
- De verantwoordelijke hanteert onjuiste gronden bij het de betrokkene weigeren van zijn rechten.
- De verantwoordelijke schermt ten onrechte gegevens af bij het effectueren van verzoeken tot inzage.
- De verantwoordelijke ten onrechte geeft geen gehoor aan het recht op verzet van een betrokkene.
- De verantwoordelijke laat een menselijke tussenkomst bij de eindcontrole na bij een geautomatiseerd voorbereide beslissing.
- De verantwoordelijke geeft geen inzage in de logica die ten grondslag ligt aan een geautomatiseerde beslissing.
-

1. Effectueren van het recht op inzage

De betrokkene heeft het recht om inzage in zijn persoonsgegevens te verkrijgen.

Deficiënties en Incidenten

- Het uitvoeren van de procedure voor het effectueren van het recht op inzage vertoont leemtes in de gehanteerde wettelijke termijn;
-

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.

Deficiënties en Incidenten

- Het uitvoeren van de procedure voor het verbeteren, aanvullen, verwijderen of afschermen van gegevens vertoont leemtes in de gehanteerde wettelijke termijn;
-

3. Verzet

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

3.a 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.

Deficiënties en Incidenten

- De verantwoordelijke geeft niet binnen de wettelijke termijn een reactie op het aangetekende verzet;
-

3.b Absoluut verzet

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.

Deficiënties en Incidenten

- De verantwoordelijke geeft geen gehoor aan het aangetekende verzet;
-

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.

Deficiënties en Incidenten

- De door de verantwoordelijke gegeven inzage in het geautomatiseerde verwerking is onvoldoende transparant;
-

V.7 Beveiliging
(artikel 6, 12, 13)

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

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. *Calamiteitenplan*
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.

Non-conformiteiten

- De verantwoordelijke heeft geen goedgekeurd lang termijn beveiligingsbeleid, dan wel in dit beleid is geen expliciete aandacht voor de bescherming van persoonsgegevens.
- De verantwoordelijke vertaalt het beveiligingsbeleid niet regelmatig in geactualiseerde beveiligingsplannen.
- De implementatie van het stelsel van procedures en maatregelen door de verantwoordelijke spoort niet met het beveiligingsplan.
- Door de verantwoordelijke is in onvoldoende mate de afweging gemaakt tussen het nemen van technische (Privacy-Enhancing Technologies) en organisatorische maatregelen.
- De verantwoordelijke heeft geen sluitende procedure voor het vernietigen van persoonsgegevens.
-

Deficiënties en Incidenten

- Er is niet voorzien in een duidelijke functiescheiding tussen de uitvoering van taken en de controle daarop.
- De werknemers zijn zich niet bewust van hun taak beveiligingsincidenten aan de verantwoordelijke te melden.
- Van nieuwe werknemers wordt onvoldoende vastgesteld of zij van onbesproken gedrag zijn.
-

1. Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van procedures en maatregelen

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

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

Deficiënties en Incidenten

- Het beleid zoals dat door de verantwoordelijke is vastgesteld bevat onjuistheden en tekortkomingen die in onvoldoende mate rekening houden met de vastgestelde risicoklasse;
- Het beveiligingsbeleid houdt in onvoldoende mate rekening met het feit dat een deel van de verwerking van persoonsgegevens zich buiten het ICT-domein bevindt;
-

2. Administratieve organisatie

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

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

Deficiënties en Incidenten

- In het geheel van maatregelen in het kader van de administratieve organisatie is onvoldoende rekening gehouden met het feit dat er persoonsgegevens worden verwerkt;
- Er is onvoldoende sprake van functiescheiding;
-

3. Beveiligingsbewustzijn

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

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

<u>Deficiënties en Incidenten</u>

- In het kader van de interne opleiding van personeel is onvoldoende aandacht voor het beveiligingsbewustzijn in het algemeen en voor de het privacybewustzijn in het bijzonder;
- De sancties, opgenomen in functiebeschrijving of arbeidscontract, bij het doorbreken van de geheimhoudingsplicht of bij het niet naleven van de beveiligingsmaatregelen zijn niet in overeenstemming met de vastgestelde risicoklasse;
- De kwaliteit van de melding van beveiligingsincidenten door medewerkers aan de verantwoordelijke is onvoldoende;
-

4. Eisen te stellen aan personeel

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

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

Deficiënties en Incidenten

- Tijdelijke medewerkers worden ingezet bij het verwerken van persoonsgegevens daar waar dat volgens de vastgestelde risicoklasse niet is toegestaan;
- Bij indiensttreding wordt geen expliciete geheimhoudingsverklaring ondertekend, een vergelijkbare verklaring wordt geëist voor tijdelijke medewerkers;
- Voor medewerkers van de afdelingen beveiliging en systeembeheer zijn geen strengere eisen gesteld;
-

5. Inrichting van de werkplek

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

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

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

Deficiënties en Incidenten

- Apparatuur die wordt gebruikt voor de verwerking van persoonsgegevens staat dusdanig opgesteld dat ook niet-geautoriseerde medewerkers inzage in persoonsgegevens kunnen krijgen;
- Er is in onvoldoende mate sprake van een clean desk policy;
- De werkplek apparatuur is niet uitgerust met een adequaat systeem van screensavers en autorisatie structuur;
- Mobiele apparatuur is onvoldoende beveiligd;
-

6. Beheer en classificatie van de ICT infrastructuur

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

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

Deficiënties en Incidenten

- Gegevensdragers zijn niet voorzien van een markering waaruit de risicoklasse blijkt;
- De verantwoordelijke heeft geen beheerssysteem voor de ICT-infrastructuur;
-

7. Toegangsbeheer en -controle

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

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

Deficiënties en Incidenten

- Het autorisatiesysteem houdt onvoldoende rekening met de functie van de werknemer;
- Het autorisatie systeem houdt in onvoldoende mate rekening met de mutaties in het personeelsbestand;
- Er is geen sprake van persoonsgebonden logische toegangscontrole;
- Het systeem van wachtwoorden (geldigheidsduur, samenstelling en herhaling van reeds gebruikte wachtwoorden) is niet in overeenstemming met de vastgestelde risicoklasse;
- Het ontbreken van voldoende toezicht op het naleven van de procedures voor het toegangsbeheer en de toegekende autorisaties;
- Het ontbreken van calamiteiten en continuïteitsplannen en –procedures;
-

8. Netwerken en externe verbindingen

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

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

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

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

Deficiënties en Incidenten

- Er zijn geen extra maatregelen voor het beschermen van persoonsgegevens indien deze via niet beveiligde externe verbindingen worden verwerkt;
- Er zijn geen maatregelen om de identiteit van een externe ontvanger van persoonsgegevens vast te stellen;
-

9. Gebruik van software

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

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

Deficiënties en Incidenten

- Voor de verwerking van persoonsgegevens wordt gebruikgemaakt van software die niet is voorzien van de noodzakelijke beveiligingsmaatregelen zoals logische toegangscontrole en logging;
- Er is onvoldoende versiebeheer van de in gebruik zijnde software;
-

10. Bulkverwerking van gegevens

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

Deficiënties en Incidenten

- Bulkverwerking van persoonsgegevens geschiedt zonder de uitdrukkelijke toestemming van een door de verantwoordelijke gemandateerde medewerker;
- Van bulkverwerking van persoonsgegevens wordt geen logboek bijgehouden, waardoor niet vastgesteld kan worden wie de opdrachtgever was;
-

11. Bewaren van gegevens

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

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

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

Dit onderdeel van de verwerkingseis is beoordeeld in verwerkingseis V.3.

12. Vernietigen van gegevens

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

Deficiënties en Incidenten

- Het vernietigen van persoonsgegevens vindt niet plaats onder toezicht van de verantwoordelijke[4];
- Het vernietigen van persoonsgegevens is niet onherroepelijk;
-

[4] Voor het vernietigen van persoonsgegevens wordt regelmatig een gespecialiseerd bedrijf ingeschakeld. Omdat vernietigen volgens artikel 1 onder b als handeling met persoonsgegevens wordt beschouwd, is er hier dus sprake van een bewerker, op wiens handelingen de verantwoordelijke toezicht houdt op passende waarborgen.

13. Calamiteitenplan

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

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

Deficiënties en Incidenten

- De back-up procedure is niet in overeenstemming met de vastgestelde risicoklasse;
- De back-up media worden niet op een andere locatie bewaard dan waar de verwerking plaatsvindt;
- De back-ups zijn niet voorzien van een markering die de vastgestelde risicoklasse aangeeft;
-

14. Uitbesteden van verwerking van persoonsgegevens

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

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

Dit onderdeel van de verwerkingseis is beoordeeld in verwerkingseis V.8.

V.8 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.

In het kader van zowel de vrijwillige certificering als ook voor het toezicht door het CBP wordt de organisatie van een bewerker beschouwd als een onlosmakelijk verbonden onderdeel van de organisatie van de verantwoordelijke. Indien de verantwoordelijke dus een of meer bewerkers heeft ingeschakeld voor de verwerking van persoonsgegevens dient het onderzoek zich uit te strekken tot en met de omgeving van die bewerker(s).

Indien een verantwoordelijke gebruikmaakt van bewerkers is niet alleen verwerkingseis V.8 van toepassing op het gehele onderzoek. Alle andere verwerkingseisen, in het bijzonder V.7, zijn eveneens van toepassing op de omgeving van de bewerker. De overeenkomst gaat dus in op alle van toepassing zijnde bepalingen van de relevante privacywet- en regelgeving.

Non-conformiteiten

- De verantwoordelijke heeft geen Service Level Agreement (Diensten Niveau Overeenkomst) afgesloten met de ingeschakelde bewerker.
- De verantwoordelijke ziet niet toe op de naleving van het Service Level Agreement.
- De bewerker heeft, buiten toestemming van de verantwoordelijke, zelf een verdere bewerker ingeschakeld.
- Indien de bewerker in een ander land van de EU is gevestigd, is onvoldoende geregeld dat de bewerker naast de eisen uit de WBP ook het specifieke recht van dat land naleeft.
-

Deficiënties en Incidenten

- Het toezicht op de naleving van de Service Level Agreement heeft in onvoldoende mate betrekking op de controle en beheersing van:
  - Procedures rond autorisaties;
  - Logbestanden;
  - Opslag van gegevensdragers met persoonsgegevens;
  - Verstrekken van persoonsgegevens;
  -
- De verantwoordelijke houdt geen archief bij van de rapportage omtrent het onderzoek op de naleving van de Service Level Agreement;
-

V.9 Gegevensverkeer met landen buiten de Europese Unie

(artikel 76, 77)

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

Non-conformiteit

- De verantwoordelijke voert gegevensverkeer met landen buiten de EU die geen passend beschermingsniveau kennen, zonder dat aan één of meer van de gestelde 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.

Deficiënties en Incidenten

De ernst van de overtreding is dusdanig dat er bij overtreding altijd sprake is van een non-conformiteit.

3.7 Evaluatie van de verwerking

Dit hoofdstuk beschrijft de maatregelen voor de evaluatie en zonodig bijsturing van de technische en organisatorische maatregelen van de verwerkingsorganisatie.

Voor de evaluatie van de verwerking worden de twee aandachtsgebieden onderkend. In het vervolg van dit hoofdstuk zullen per aandachtsgebied de belangrijkste aspecten benoemd en kort toegelicht worden.

Het beoordelen van de evaluatie van de verwerking is met name de controle van het stelsel van beheersmaatregelen dat de rechtmatigheid van de verwerking moet waarborgen ten opzichte van het kwaliteitsaspect ‘controleerbaarheid’.

E.1 Beheersen van 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 een 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 privacy-auditors* *Het management verzekert zich ervan dat de privacy-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 privacy 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 privacy 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.*

3.8 Samenvatting van de verwerkingseisen voor persoonsgegevens

Verwerkingseis voor persoonsgegevens				aantal	n.v.t.
V.1	**Voornemen en melden**			**6**	**2**
1		Vaststellen van de aard van de verwerking en de verplichting tot melden	n.v.t.		
2	1	Melding			
3	2	Voorafgaand onderzoek door het CBP			
4		Bijhouden van en centraal register	n.v.t.		
5	3	Periodieke beoordeling meldingen			
6	4	Verstrekken van inlichtingen over de verwerking			
V.2	**Transparantie**			**3**	**0**
1	5	Informatieverstrekking aan de betrokkene			
2	6	Bijzonderheden bij informatieverstrekking aan betrokkene			
3	7	Informeren bij werving voor commerciële of charitatieve doelen			
V.3	**Doelbinding**			**4**	**0**
1	8	Doelbinding			
2	9	Verenigbaarheid van de gegevensverwerking			
3	10	Bewaren van persoonsgegevens			
4	11	Geheimhoudingsverplichting			
V.4	**Rechtmatige grondslag**			**2**	**0**
1	12	Grondslag voor de verwerking van persoonsgegevens			
2	13	Verwerking van bijzondere gegevens			
V.5	**Kwaliteit**			**2**	**0**
1	14	Kwaliteit van de gegevensverwerking			
2	15	Fouten in de gegevensverwerking			
V.6	**Rechten van de betrokkenen**			**4**	**0**
1	16	Effectueren van het inzagerecht			
2	17	Verbeteren, aanvullen, verwijderen of afschermen			
3	18	Verzet			
4	19	Geautomatiseerde beslissingen over iemands persoonlijkheid			
V.7	**Beveiliging**			**14**	**2**
1	20	Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures			
2	21	Administratieve organisatie			
3	22	Beveiligingsbewustzijn			
4	23	Eisen te stellen aan personeel			
5	24	Inrichting van de werkplek			
6	25	Beheer en classificatie van de ICT infrastructuur			
7	26	Toegangsbeheer en –controle			
8	27	Netwerken en externe verbindingen			
9	28	Gebruik van software			
10	29	Bulkverwerking van gegevens			
11		Bewaren van gegevens	Zie V.3 (3)		
12	30	Vernietigen van gegevens			
13	31	Calamiteitenplan			
14		Uitbesteden van verwerking van persoonsgegevens	Zie V.8		
V.8	**Verwerking door een bewerker**			**1**	**0**
1	32	Verwerking door een bewerker			
V.9	**Gegevensverkeer met landen buiten de EU**			**1**	**0**
1	33	Gegevensverkeer met landen buiten de EU			
		Totaal aantal aandachtsgebieden		**33**	

Totaal V	Vooronder-zoek Potentiële bevinding	Compliance onderzoek Feitelijke bevinding							
	Non-confor-miteit	Non-confor miteit	Deficiëntie per risicoklasse				Incident per risicoklasse			
			0	I	II	III	0	I	II	III
Aantal deficiënties / incidenten V.1										
Aantal deficiënties / incidenten V.2										
Aantal deficiënties / incidenten V.3										
Aantal deficiënties / incidenten V.4										
Aantal deficiënties / incidenten V.5										
Aantal deficiënties / incidenten V.6										
Aantal deficiënties / incidenten V.7										
Aantal deficiënties / incidenten V.8										
Aantal deficiënties / incidenten V.9										
Totaal:										
Gewicht deficiëntie / incident			**1**	**2**	**4**	**8**	**1**	**1**	**2**	**3**
aantal x gewicht:										
• Op basis van het aantal van 33 aandachtsgebieden bij de negen verwerkingseisen voor persoonsgegevens bedraagt het maximale aantal '(straf)punten':			**33**	**66**	**132**	**264**	**33**	**33**	**66**	**99**

Totaal E	Vooronder-zoek Potentiële bevinding	Compliance onderzoek Feitelijke bevinding							
	Non-confor-miteit	Non-conform iteit	Deficiëntie per risicoklasse				Incident per risicoklasse			
			0	I	II	III	0	I	II	III
Aantal deficiënties / incidenten E.1										
Aantal deficiënties / incidenten E.2										
Totaal:										
Gewicht deficiëntie / incident			**1**	**2**	**4**	**8**	**1**	**1**	**2**	**3**
aantal x gewicht:										
• Op basis van het aantal van 13 aandachtsgebieden bij de twee evaluatie-eisen voor persoonsgegevens bedraagt het maximale aantal '(straf)punten':			**13**	**26**	**52**	**104**	**13**	**13**	**26**	**39**

Totale beoordeling								
Maximaal totaal van V en E	46	92	184	368	46	46	92	138
Oordeel: (totaal punten deficiënties en incidenten)								
• afgeven, verlengen, niet intrekken van de verklaring								
• opschorten van de geldigheid van de verklaring								