Wet bescherming persoonsgegevens

Samenwerkingsverband Audit Aanpak / Werkgroep Zelfevaluatie

WBP Zelfevaluatie

Disclaimer

Dit product 'WBP Zelfevaluatie' is met de grootste zorg ontwikkeld door het 'Samenwerkingsverband Audit Aanpak', waarbij de wettelijke regels gesteld bij of krachtens de Wet bescherming persoons-gegevens 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 'WBP Zelf-evaluatie' geen rekening kon worden gehouden, geschiedt het gebruik van de 'WBP Zelfevaluatie' steeds geheel voor risico van de gebruiker.

WBP Zelfevaluatie

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 via 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 2 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 privacy-certificaat worden afgegeven.

Vaststellen

Voordat is overgegaan tot het vaststellen van de WBP Zelfevaluatie 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 Accountants & Adviseurs;
- BESTUUR & MANAGEMENT CONSULTANTS (BMC);
- Continuity Planning Associates (CPA);
- 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

II . 1 Positionering zelfevaluatie (al dan niet met review)

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 is overigens beperkter dan het kwaliteitsspectrum van de gegevensverwerking in brede zin (veilig, efficiënt, effectief, exclusief, integer, continu en controleerbaar).

Het samenwerkingsverband 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 een 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 CBP, Achtergrondstudie en Verkenning (A&V), nummer 23 ‘Beveiliging van persoonsgegevens’ uitgegeven. Deze uitgave beschrijft de noodzakelijke beveiligingsmaatregelen die aan de verwerking van persoonsgegevens, in verschillende situaties, worden gesteld. Deze uitgave is bij het CBP te bestellen.

De onderlinge verhouding tussen deze drie producten 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 product WBP Zelfevaluatie. WBP Zelfevaluatie is een systematische methode waarbij de organisatie zelfstandig de kwaliteit van de bescherming van persoonsgegevens in kaart brengt en kan beoordelen. De zelfevaluatie geeft antwoord op de volgende twee vragen:

- wat is de huidige situatie?
- wat is de gewenste situatie?

Hoofdstuk IV bevat ter ondersteuning van deze aanpak een handreiking voor de wijze waarop een zelfevaluatie kan worden uitgevoerd.

II . 2 Privacybescherming als onderdeel van de managementcyclus

Het realiseren van bedrijfsdoelstellingen vindt doorgaans plaats via een bepaalde managementcyclus. Gebruikelijk is dat dergelijke cycli uit drie onderdelen bestaan: de organisatie van de processen (inclusief de beleidsvoering), de processen zelf en een evaluatie en bijsturing van de processen. De bescherming van persoonsgegevens dient een onlosmakelijk element van de managementcyclus te zijn. De aanpak en werkwijze die aan de ontwikkeling van de WBP Zelfevaluatie ten grondslag hebben gelegen, sluiten aan op de hiervoor geschetste situatie.

Het voeren van beleid gericht op privacybescherming past in het streven van het management naar totale kwaliteit en maatschappelijk verantwoord ondernemen.

Kern van deze aanpak is dat bij het uitvoeren van een WBP Zelfevaluatie met behulp van vragen wordt nagegaan waar en op welke wijze de eisen van de WBP reeds in de operationele organisatie worden geborgd en welke aanvullende voorzieningen eventueel nog moeten worden getroffen om een toereikende bescherming van persoonsgegevens te verzekeren.

De WBP Zelfevaluatie bevat daarvoor in hoofdstuk V negen hoofdvragen die refereren aan de, op grond van de WBP, noodzakelijk in ogenschouw te nemen aandachtspunten.

II . 3 Belang WBP Zelfevaluatie

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 op het eerste oog relatief onschuldige persoonsgegevens een andere betekenis krijgen.
Deze ontwikkelingen worden maatschappelijk slechts geaccepteerd binnen bepaalde grenzen. Die grenzen zijn door 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. De WBP Zelfevaluatie geeft organisaties met een redelijke mate van zekerheid inzicht in de wijze waarop en de mate waarin de organisatie zorgvuldig omgaat met de verwerking van persoonsgegevens. Daarnaast kan via het instrument van de zelfevaluatie de bewustwording rond het thema privacybescherming in positieve zin beïnvloed worden.

Het realiseren van een op een specifieke situatie toegesneden privacybescherming is geen sinecure. Gedacht zou kunnen worden dat de WBP Zelfevaluatie uitsluitend bestemd is voor grootschalige gegevensverzamelingen en grote organisaties. Niets is minder waar. Ook in kleinschaliger situaties waarin sprake is van het verwerken van persoonsgegevens, kan een zelfevaluatie nuttig en wenselijk zijn. Een eenduidig model voor de afweging van het nut en de noodzaak van het uitvoeren van een zelfevaluatie kan niet worden opgesteld. 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.

II . 4 Opzet WBP Zelfevaluatie

Het product WBP Zelfevaluatie biedt de leiding van een organisatie een hulpmiddel om in enkele dagen een overzicht te verkrijgen van de wijze waarop de organisatie invulling heeft gegeven aan de bescherming van persoonsgegevens. Tevens biedt dit instrument de leiding de mogelijkheid om een ambitieniveau te bepalen op basis waarvan deze een groeipad kan opstellen om, vanuit de huidige situatie, dit ambitieniveau te realiseren. Het definiëren van een ambitieniveau heeft voor organisaties die privacybescherming expliciet tot hun organisatiedoelstellingen rekenen grote betekenis. Een gedegen risicoanalyse dient de basis te zijn voor een weloverwogen keuze van het ambitieniveau. De WBP Zelfevaluatie kan daarmee worden gekenschetst als een diagnosemodel.

Het product WBP Zelfevaluatie kan worden toegepast op alle typen organisaties. Uit ervaring met soortgelijke instrumenten en tests met de WBP Zelfevaluatie blijkt dat het hanteren van dit instrument, na gedegen voorbereiding, een tijdbeslag van 1 à 2 dagen vergt.

Deze WBP Zelfevaluatie kan desgewenst met een review worden uitgebreid. De doelstelling van de review is de waarde van de interne meting te verhogen door een in- of externe deskundige de uitkomsten van de zelfevaluatie te laten beoordelen aan de hand van onderliggende dokumenten. Het management krijgt door het laten uitvoeren van de review een uitkomst voorgelegd gebaseerd op een onafhankelijke toetsing van daadwerkelijk getroffen maatregelen. Een uitkomst die mogelijk in het proces te rooskleurig of te negatief is voorgesteld, kan hiermee gecorrigeerd worden.

De opzet van de WBP Zelfevaluatie is gebaseerd op het INK model. Dit model is ontwikkeld door het Instituut Nederlandse Kwaliteit. Dit model beoogt de leiding van een organisatie zelf te laten vaststellen hoe de organisatie presteert en hoe de organisatie is ingericht voor haar taak. Deze doelstellingen zijn in dit document WBP Zelfevaluatie specifiek toegesneden op de analyse van de wijze waarop de bescherming van persoonsgegevens in een organisatie zich verhoudt tot de WBP.

Het product WBP Zelfevaluatie is beschikbaar op de website van het CBP (www.cbpweb.nl).

II . 5 Uitvoering WBP Zelfevaluatie

In het document is voor de volgende indeling gekozen. Op de rechterpagina van het document zijn opgenomen:

- de vertaling van de inhoud van de WBP naar negen hoofdvragen;
- de nadere onderverdeling van de hoofdvragen in subvragen;
- een toelichting op de hoofd- en subvragen;
- ruimte voor het noteren van de sterke punten binnen de organisatie en de punten voor verbetering van het in de hoofd-/subvraag behandelde aandachtspunt.
- op de achterflap een kader waarin per hoofd- of subvraag op een schaal van 1 tot en met 5 kan worden aangegeven wat:
  - de inschatting van de beoordeling van de antwoorden op de vragen door de uitvoerder(s) is, en
  - het ambitieniveau van de organisatie is.

Op de linkerpagina van dit document zijn de reviewvragen opgenomen. De reviewvragen bevatten (niet limitatief) aan de WBP gerelateerde specifieke aandachtspunten die de invulling vormen van een hoofd- of subvraag. Deze aandachtspunten zijn bij de review de basis voor de beoordeling van:

- de volledigheid van de invulling van de zelfevaluatie door de uitvoerder(s);
- de zorgvuldigheid waarmee de zelfevaluatie is verricht.

Op de achterflap is een totaaloverzicht opgenomen waarin de confrontatie tussen de feitelijke situatie en het ambitieniveau is weergegeven. Hieruit kan worden afgeleid welke aanvullende voorzieningen moeten worden getroffen om het gewenste ambitieniveau te realiseren, respectievelijk in hoeverre het ambitieniveau moet of kan worden aangepast.

Bij de uitvoering van de WBP Zelfevaluatie kan ervoor gekozen worden om de reviewvragen al dan niet ter beschikking te stellen aan de uitvoerders.

De zelfevaluatie wordt door eigen medewerkers op organisatie- of afdelingsniveau uitgevoerd onder verantwoordelijkheid van het management, het afdelingshoofd, de beveiligingsdeskundige etc. De rapportage van de zelfevaluatie moet geadresseerd worden aan het hoogste managementniveau (bestuur/directie).

De zelfevaluatie kan worden aangevuld met een review door een in- of externe deskundige gespecialiseerd in audit en de WBP die, voor wat betreft de interne reviewer, onafhankelijk is van het organisatieonderdeel dat de zelfevaluatie heeft uitgevoerd. Voor een externe reviewer spreekt het aspect van onafhankelijkheid voor zich.

Belangrijk is te onderkennen dat het begrip 'verwerking' zoals dat wordt gehanteerd in de WBP Zelfevaluatie een ruimere definitie kent dan het begrip verwerking in de gebruikelijke ICT betekenis. Volgens de definitie in de WBP vallen alle handelingen die persoonsgegevens in een organisatie ondergaan, daaronder. Te denken valt daarbij aan handelingen zoals het verzamelen, vastleggen, bewaren, bewerken, wijzigen, veranderen, vernietigen en verspreiden van persoonsgegevens. Overigens vallen ook handmatig verwerkte persoonsgegevens onder de WBP. Zie voor definitie van het begrip verwerking B/2.2.

Methodiek WBP Zelfevaluatie

III . 1 Inleiding

De negen hoofdvragen van de WBP Zelfevaluatie sluiten aan op het door het samenwerkingsverband ontwikkelde Raamwerk Privacy Audit. Voor de duidelijkheid zijn de in de WBP Zelfevaluatie geformuleerde hoofdvragen waar nodig gespecificeerd in een aantal subvragen. Het is noodzakelijk om alle vragen uit de WBP Zelfevaluatie ook daadwerkelijk in de beschouwing te betrekken om, met een redelijke mate van zekerheid, inzicht te kunnen verkrijgen over de wijze waarop en de mate waarin er sprake is van een toereikende bescherming van de persoonsgegevens.

Getracht is de vragen zodanig te formuleren dat zij ook voor niet juridisch geschoolde medewerkers te begrijpen zijn. Niettemin is bij de formulering van de reviewvragen bewust gekozen voor de juridische terminologie zoals die in de WBP gebruikt wordt. Vandaar dat de reviewers over gedegen kennis van de WBP dienen te beschikken. Ter ondersteuning van de beantwoording van de vraagstelling is de A&V studie 'Beveiliging van persoonsgegevens', uitgegeven door het CBP, beschikbaar op de website van het CBP.

Ter onderbouwing van de vragen en ten behoeve van de beantwoording is in het onderdeel review een aantal aandachtspunten opgenomen waarvoor geldt dat een organisatie hiervan minimaal moet nagaan of wordt voldaan aan deze aandachtspunten dan wel dat er redenen zijn waarom deze punten niet van toepassing zijn. Deze afwijkingen moeten worden gemotiveerd en vastgelegd. De wijze van implementatie van de wet kan namelijk per organisatie sterk verschillen.

Het is van groot belang dat een organisatie die de WBP Zelfevaluatie uitvoert, vaststelt welke wettelijke vereisten vanuit de WBP, maar ook vanuit andere toepasselijke wetgeving (GBA, Politiewet, etc.) van toepassing zijn op de verwerking van persoonsgegevens binnen de organisatie. In de bijlage zijn de hoofdlijnen van de WBP uiteengezet. Het is goed denkbaar dat specifieke bepalingen (bijvoorbeeld over de verwerking door een bewerker en gegevensverkeer met landen buiten de Europese Unie) voor een organisatie niet van toepassing zijn, omdat deze situaties zich niet voordoen.

III . 2 Hoofdvragen

De negen hoofdvragen die in dit instrument aan de orde komen hebben betrekking op de volgende onderwerpen:

1 Melding
2 Transparantie
3 Doelbinding
4 Rechtmatige grondslag
5 Kwaliteit
6 Rechten
7 Beveiliging
8 Bewerker
9 Niet EU-landen

Bij het in beeld brengen van de huidige situatie (de beoordeling) en de gewenste situatie (het ambitieniveau) wordt gebruik gemaakt van een indeling in vijf niveaus. Deze vijf niveaus zijn vermeld onder het kopje 'Beoordeling' dat bij elke vraag is opgenomen na de toelichting op de betreffende vraag. De opbouw van de vijf niveaus is oplopend qua zwaarte en kan als volgt worden weergegeven:

Niveau	Wijze omgaan met WBP	Zwaarte
1	*Niets vastgelegd en niets bekend*	+
2	*Niets vastgelegd maar wel bekend*	++
3	*Vastgelegd en bekend*	+++
4	*Vastgelegd, bekend en nageleefd*	++++
5	*Vastgelegd, bekend, nageleefd en gecontroleerd*	+++++

Op basis van dit stramien is in relatie tot elke vraag aangegeven wat verstaan wordt onder elk van de vijf niveaus.

III . 3 Toepassing WBP Zelfevaluatie

Het verdient aanbeveling de WBP Zelfevaluatie volgens onderstaand stramien te laten verlopen:

- Het beoordelen van de stand van zaken in de organisatie. In hoofdstuk IV is als voorbeeld een stappenplan opgenomen dat daarvoor kan worden gebruikt. De reviewvragen zijn bedoeld om de feitelijke beoordeling te ondersteunen.
  Vanzelfsprekend zal bij de uitvoering van de WBP Zelfevaluatie moeten worden nagegaan welke beheersmaatregelen de organisatie reeds getroffen heeft en in welke mate deze bijdragen aan de bescherming van persoonsgegevens.
- Het bepalen van het ambitieniveau voor de verwerking van de persoonsgegevens in de organisatie. Voor een goede bepaling van het ambitieniveau is een adequate risicoanalyse noodzakelijk. De risico's die voor de betreffende organisatie specifiek te onderkennen zijn, bepalen in belangrijke mate het gewenste ambitieniveau. De inschatting van de risico's is onder meer afhankelijk van: de aard en omvang van de organisatie, de aard en omvang van de gebruikte persoonsgegevens, het beoogde en feitelijke gebruik en verstrekking van persoonsgegevens, de wijze van verwerking en de verwerkingsomgeving. Daarnaast kunnen de ambitieniveaus per vraag verschillen. Ook spelen factoren als technologische ontwikkelingen en de maatschappelijke en persoonlijke visie een rol. Zo zal een hogere risicoklasse volgens A&V nr. 23 'Beveiliging van persoonsgegevens' (zie website CBP) moeten leiden tot een hoog ambitieniveau. Wanneer gekozen wordt voor specifieke controle op de naleving van afspraken kan dit via de bepaling van het ambitieniveau (zie niveau 5) worden vormgegeven.

- Het laten uitvoeren van een review op de zelfevaluatie door een in- of externe deskundige op basis van kennisneming van de kwaliteit van daadwerkelijk getroffen maatregelen. Bij de review vindt een beoordeling plaats van:
  - de uitkomsten en waardering van de beoordeling;
  - de in de rubrieken 'Sterke punten' en 'Punten voor verbetering' opgenomen opmerkingen;
  - het ingeschatte ambitieniveau.
- Het bepalen door het management van de eventueel te nemen vervolgstappen om het ambitieniveau en de uitkomst van de beoordeling op één lijn te brengen.

Handreiking bij de voorbereiding en uitvoering WBP Zelfevaluatie

Dit hoofdstuk geeft een toelichting op de aanpak en werkwijze die als handreiking kan dienen voor het voorbereiden en uitvoeren van een zelfevaluatie. Uiteraard kunnen ook andere in de organisatie gebruikte methodieken worden gehanteerd (bijvoorbeeld projectmanagement). De reviewvragen dienen als onderbouwing voor de WBP Zelfevaluatie.

IV . 1 Samenwerking

De ervaring met soortgelijke zelfevaluaties en de uitgevoerde testen leert dat de kracht van de zelfevaluatie als instrument ligt in het groepsproces. Onder verantwoordelijkheid van het management dienen verschillende sleutelfunctionarissen (zoals bijvoorbeeld systeembeheerder, applicatiebeheerder(s), controller, hoofd personeelszaken, hoofd juridische zaken) de zelfevaluatie uit te voeren. Zo kunnen zij in betrekkelijk korte tijd een goed beeld van de kwaliteit van de huidige organisatie krijgen en kan ook een grote sprong worden gemaakt in het proces van bewustwording rond de bescherming van persoonsgegevens binnen de organisatie. In dat kader zou ook een vertegenwoordiging van de Ondernemingsraad deel kunnen uitmaken van het team zelfevaluatie.

Door bij de uitvoering van de WBP Zelfevaluatie expliciet de sterke punten en de verbeterpunten te identificeren, kan een goede basis worden gelegd voor vervolgactiviteiten. De bevindingen van de WBP Zelfevaluatie kunnen zo de start vormen van een verbetertraject voor de bescherming van persoonsgegevens. Hiermee kan tevens een goede basis worden gelegd voor het laten uitvoeren van een Privacy Audit, waarmee een onafhankelijk oordeel (al dan niet in de vorm van een privacycertificaat) kan worden verkregen over de mate waarin de organisatie voldoet aan de wettelijke bepalingen voor de bescherming van persoonsgegevens. Nadere informatie over de betekenis en inhoud van een Privacy Audit staat op de website van het CBP (www.cbpweb.nl).

IV . 2 Stapsgewijze aanpak

De voorbereiding en uitvoering van de WBP Zelfevaluatie dient op gestructureerde wijze plaats te vinden. Dit waarborgt een effectieve en efficiënte uitvoering van de zelfevaluatie. In het algemeen kunnen onderstaande stappen worden onderscheiden.

Stap 1 Stel vast of de WBP van toepassing is

Allereerst moet worden vastgesteld of de WBP op de verwerking van persoonsgegevens binnen de organisatie van toepassing is. De hoofdlijnen van de WBP en de wettelijke context zijn opgenomen in B/I en B/II.

De WBP is van toepassing op persoonsgegevens die met een computersysteem of handmatig worden verwerkt of die op een andere manier bestemd zijn om in een bestand te worden opgenomen. Daarnaast zijn er organisaties waarvoor aanvullende specifieke wetgeving (o.a. politieregisters) van toepassing is.

Stap 2 **Stel een geschikt team samen**

Stel het team samen dat de WBP Zelfevaluatie gaat uitvoeren. Voor de optimale samenstelling van dit team wordt verwezen naar de inleiding van dit hoofdstuk. Aan het team kan een interne (of externe) deskundige toegevoegd worden die als procesbegeleider moet zorgen voor een goede procesgang. Indien de WBP Zelfevaluatie wordt uitgevoerd voor één of een beperkt aantal verwerkingen van persoonsgegevens (dus niet organisatiebreed) zal de samenstelling van het team hierop moeten aansluiten.

De omvang van een team kan variëren. Bij zelfevaluaties waarbij een team uit bijvoorbeeld meer dan zeven personen bestaat, is het aan te raden om de bespreking van de diverse vragen in subgroepen te laten plaatsvinden. De uitkomsten kunnen vervolgens plenair worden teruggekoppeld. Tegelijk kan dan worden vastgesteld of er consensus bestaat. Vanzelfsprekend is de omvang van het team afgestemd op de grootte van de organisatie. Binnen een kleine organisatie is het heel goed mogelijk dat het team uit twee personen zal bestaan.

Stap 3 **Voorbereiding en planning**

Organiseer een bijeenkomst waarin de volgende onderwerpen aan de orde komen:

- de reden om met de WBP Zelfevaluatie aan de slag te gaan;
- een korte uitleg over de WBP en het instrument WBP Zelfevaluatie;
- de gekozen aanpak en werkwijze;
- de wijze van communicatie;
- het eventueel geplande vervolgtraject.

Zorg ervoor dat de begrippen die in dit product worden gehanteerd voor iedereen helder zijn en zorg voor voldoende kennis binnen het team.

Stap 4 **Voer (individueel) de WBP Zelfevaluatie uit**

Elk teamlid gaat voor zichzelf aan de hand van de vragen in hoofdstuk V na hoe de organisatie in werkelijkheid scoort op de genoemde vragen en welk ambitieniveau wenselijk is voor het betreffende onderwerp.
Daarbij noteert ieder teamlid de naar zijn of haar mening sterke punten en de geconstateerde punten die voor verbetering vatbaar zijn. Het is wenselijk dat elk teamlid zijn of haar bevindingen kort motiveert.

Stap 5 **Vorm een gezamenlijk oordeel**

Vergelijk in het team de individuele scores en bevindingen. Inventariseer de overeenkomsten en de verschillen. Discussieer grondig over de verschilpunten op basis van argumenten en feiten en raadpleeg daarbij de aantekeningen en de beschrijvingen uit stap 4.
Plaats de gemeenschappelijke uitkomsten van de scores van de vragen van hoofdstuk V tot slot in de profielschets die is opgenomen op de achterflap.

Bij een grotere groep (zeven personen of meer) is het raadzaam de discussies te laten plaatsvinden in subgroepen. In de subgroepen worden de individuele scores op dezelfde wijze besproken als in de situatie met één groep.

Stap 6 Beoordeel de resultaten opnieuw

Kijk als team nogmaals kritisch naar de uitkomsten van de WBP Zelfevaluatie. Ga na of de keuzes ten opzichte van een buitenstaander, zoals een in- of externe auditor, met feiten en voorbeelden kunnen worden onderbouwd. Bepaal of de uitkomst geldt voor de gehele organisatie of slechts voor delen van de verwerking van persoonsgegevens binnen de organisatie. Afstemming met de managers op alle niveaus van de bedrijfsvoering en alle betrokken afdelingen is gewenst voor het creëren van draagvlak voor te nemen vervolgacties. Pas de score zonodig aan.

Stap 7 Besluitvorming hoogste management

Voordat er besloten kan worden tot het plannen van vervolgacties dient het hoogste management binnen de organisatie een besluit te nemen of, en zo ja welke vervolgstappen op basis van de WBP Zelfevaluatie zullen worden gezet.

Stap 8 Plan vervolgacties

Stel gezamenlijk een plan op voor vervolgacties. Belangrijke aandachtspunten bij een plan van aanpak voor de vervolgacties op de WBP Zelfevaluatie zijn:

- heldere formulering van conclusies door het hoogste management over de uitkomsten van de zelfevaluatie en de noodzaak tot verdere vervolgstappen, waarbij aandacht wordt geschonken aan de prioriteitstelling van de vervolgstappen;
- het realiseren van het vervolgtraject via een adequate projectmanagementmethode teneinde voldoende draagvlak en afstemming binnen de organisatie te creëren;
- zorgdragen voor adequate communicatie binnen de gehele organisatie over het waarom van en de wijze waarop de vervolgacties gestalte gaan krijgen;
- een goede voortgangsbewaking van de geplande vervolgacties.

Vragen WBP Zelfevalutatie

De onderstaande vragen hebben betrekking op de melding en het voorafgaand onderzoek. Deze vragen zijn gebaseerd op hoofdstuk 4 van de WBP (de artikelen 27 tot en met 32).

a *Heeft u maatregelen getroffen waarin de stappen zijn vastgelegd vanaf het voornemen tot de verwerking van persoonsgegevens tot aan het melden van die verwerking?* ○ ja ○ nee

b *Heeft u onderzocht of de verwerking is vrijgesteld van de meldingsplicht bij het CBP of de functionaris voor de gegevensbescherming* ○ ja ○ nee

c *Heeft u de vrijstelling schriftelijk vastgelegd in een besluit?* ○ ja ○ nee

d *Als de melding van de verwerking bij het CBP niet is vrijgesteld, heeft u dan de verplichte melding bij de functionaris voor de gegevensbescherming of het CBP gedaan en komt die melding overeen met de werkelijkheid?* ○ ja ○ nee

Zo ja,
bevat de melding:

_____ *de naam en het adres van de verantwoordelijke?* ○ ja ○ nee

_____ *een concrete beschrijving van het doel of de doeleinden van de verwerking?* ○ ja ○ nee

_____ *een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die betrekking hebben op de melding?* ○ ja ○ nee

_____ *de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt?* ○ ja ○ nee

_____ *de voorgenomen doorgiften van gegevens naar landen buiten de Europese Unie?* ○ ja ○ nee

_____ *een algemene beschrijving van de maatregelen en procedures die de beveiliging van de verwerking waarborgen?* ○ ja ○ nee

_____ *bepalingen over bewaartermijnen?* ○ ja ○ nee

e *Heeft u zich ervan vergewist dat de aanmelding van de verwerking in bepaalde gevallen onderhevig is aan voorafgaand onderzoek door het CBP?* ○ ja ○ nee

Zo nee,
zijn de volgende situaties op de voorgenomen verwerking van toepassing:

_____ *ander gebruik van een identificatienummer dan waarvoor het wettelijk is bedoeld om deze gegevens in verband te brengen met gegevens die worden verwerkt door een andere verantwoordelijke?* ○ ja ○ nee

_____ *vastlegging van gegevens op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen?* ○ ja ○ nee

_____ *verwerken van strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag ten behoeve van derden zonder vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus?* ○ ja ○ nee

Vervolg op pagina 22

Melding

Toelichting

Het verwerken van persoonsgegevens in de organisatie moet vooraf goed worden geregeld. Wanneer men van plan is persoonsgegevens te gaan verwerken, moet worden onderzocht of de voorgenomen verwerking moet worden gemeld bij het College bescherming persoonsgegevens (CBP) of een functionaris voor de gegevensbescherming respectievelijk of de verwerking is vrijgesteld van deze verplichting. Wanneer daarom wordt verzocht, moeten inlichtingen over de verwerking gegeven kunnen worden.

In hoeverre heeft uw organisatie maatregelen en procedures getroffen met stappen vanaf het voornemen om persoonsgegevens te gaan verwerken tot en met het melden van de verwerking en het verstrekken van inlichtingen?

Beoordeling

1 Er zijn geen procedures vastgelegd en de verplichte melding bij het CBP of de functionaris voor de gegevensbescherming vond niet plaats.

2 Er zijn geen procedures vastgelegd maar de verplichte melding bij het CBP of de functionaris voor de gegevensbescherming vond wel plaats.

3 Er zijn procedures vastgelegd en de melding bij het CBP of de functionaris voor de gegevensbescherming vond plaats.

4 Er zijn procedures vastgelegd en de melding bij het CBP of de functionaris voor de gegevensbescherming vond plaats. Voorzien is het doorvoeren van wijzigingen in procedures en aanmelding. Aan de medewerkers worden instructies gegeven en dit wordt periodiek herhaald.

5 Er zijn procedures vastgelegd en de melding bij het CBP of de functionaris voor de gegevensbescherming vond plaats. Voorzien is het doorvoeren van wijzigingen in procedures en aanmelding. Aan de medewerkers worden instructies gegeven en dit wordt periodiek herhaald. Er wordt gecontroleerd of de individuele medewerkers de maatregelen en procedures naleven.

Ambitie

U geeft aan welke maatregelen voor verwerking en melden van de verwerking u wilt nemen.

Sterke punten | Punten voor verbetering

f *Wordt door u op een centraal punt in de organisatie een register bijgehouden van de verwerkingen?* ( ) ja ( ) nee

Zo ja,
bevat dit register dan tenminste:

_____ *de gegevens die relevant zijn ingeval van een vrijstelling of melding?* ( ) ja ( ) nee

_____ *van gemelde verwerkingen de ontvangstbevestiging van het CBP?* ( ) ja ( ) nee

g *Kan het register kosteloos worden geraadpleegd?* ( ) ja ( ) nee

h *Heeft u maatregelen getroffen voor het verstrekken van inlichtingen over de gemelde en daarvan vrijgestelde verwerkingen? (art. 30, derde lid, WBP)* ( ) ja ( ) nee

Zo ja,
bevatten die inlichtingen de volgende gegevens:

_____ *degene die verantwoordelijk is voor de verwerking?* ( ) ja ( ) nee

_____ *de verwerkte gegevens of categorieën van gegevens?* ( ) ja ( ) nee

_____ *de categorieën van betrokkenen?* ( ) ja ( ) nee

_____ *het doel of de doeleinden van de verwerking?* ( ) ja ( ) nee

_____ *de ontvangers of categorieën van ontvangers aan wie de gegevens worden verstrekt?* ( ) ja ( ) nee

_____ *bewaartermijnen?* ( ) ja ( ) nee

i *Wanneer u geen inlichtingen verstrekt, doet u dan een beroep op het belang van:* ( ) ja ( ) nee

_____ *de veiligheid van de staat?* ( ) ja ( ) nee

_____ *de voorkoming, opsporing en vervolging van strafbare feiten?* ( ) ja ( ) nee

_____ *gewichtige economische en financiële belangen van de staat en andere openbare lichamen?* ( ) ja ( ) nee

_____ *het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de genoemde belangen?* ( ) ja ( ) nee

_____ *de bescherming van de betrokkene of rechten van vrijheden van anderen?* ( ) ja ( ) nee

a *Geeft u de betrokkene informatie over uw identiteit, het doel en de bestemming van de gegevens wanneer zij hiervan niet op de hoogte zijn?* ○ ja ○ nee

Zo ja,
geeft u de informatie:

_____ *voorafgaande aan de verkrijging?* ○ ja ○ nee
_____ *op het moment van de vastlegging van de gegevens?* ○ ja ○ nee
_____ *uiterlijk op het moment van eerste verstrekking?* ○ ja ○ nee

Zo nee,
om welke reden(en) geeft u de informatie niet? Omdat:

_____ *deze mededeling onmogelijk is of een onevenredige inspanning kost.* ○ ja ○ nee
_____ *indien u de vorige vraag met ja heeft beantwoord, legt u dan de herkomst van de gegevens vast?* ○ ja ○ nee

Of meent u dat die handelwijze noodzakelijk is in het belang van:

_____ *de veiligheid van de staat?* ○ ja ○ nee
_____ *de voorkoming, opsporing en vervolging van strafbare feiten?* ○ ja ○ nee
_____ *gewichtige economische en financiële belangen van de staat en andere openbare lichamen?* ○ ja ○ nee
_____ *de bescherming van de betrokkene of van de rechten en vrijheden van anderen?* ○ ja ○ nee

b *Instrueert u uw medewerkers over de informatieverplichting?* ○ ja ○ nee

c *Wordt het nakomen van de informatieverplichting gecontroleerd?* ○ ja ○ nee

d *Verstrekt u bij of krachtens de wet voorgeschreven gegevens?* ○ ja ○ nee

Zo ja,

_____ *informeert u de betrokkene wanneer hij daarom vraagt over dat wettelijk voorschrift?* ○ ja ○ nee

Transparantie

Toelichting

De gegevensverwerking in de organisatie moet voor de betrokkene transparant zijn. Dit betekent onder meer dat de betrokkene voorafgaande aan de verkrijging op de hoogte moet worden gesteld van de identiteit van de organisatie en het doel waarvoor de gegevens worden verwerkt. Indien de gegevens niet rechtstreeks van de betrokkene worden verkregen moet de betrokkene worden geïnformeerd op het moment van de vastlegging van diens gegevens of wanneer de gegevens bestemd zijn om aan een derde te worden verstrekt. Indien persoonsgegevens voor commerciële of charitatieve doeleinden worden verwerkt gelden er bijzondere voorwaarden. Op de voorgaande regels zijn weer uitzonderingen van toepassing.

Wordt er in uw organisatie voor gezorgd dat de verwerking van de persoonsgegevens voor de betrokkenen transparant is en wordt aan de betreffende informatieverplichting voldaan?

Beoordeling

1 Er zijn geen procedures vastgelegd en de verplichting tot informeren van de betrokkene is niet in de organisatie bekend.

2 Er zijn geen procedures vastgelegd maar de verplichting tot informeren van de betrokkene is in de organisatie bekend.

3 Er zijn geen procedures vastgelegd maar de betrokkenen worden wel geïnformeerd.

4 Er zijn procedures vastgelegd en de verplichting tot informeren van de betrokkene wordt nageleefd.

5 Er zijn procedures vastgelegd en de verplichting tot informeren van de betrokkene wordt nageleefd en deze naleving wordt gecontroleerd.

Ambitie

U geeft aan welke mate van transparantie van de gegevensverwerking u wilt bereiken.

Sterke punten

Punten voor verbetering

V / 3 *Reviewvragen*

a *Heeft u maatregelen getroffen die waarborgen dat het verwerken van persoonsgegevens plaatsvindt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden?* ○ ja ○ nee

Zo ja,

_____ *zijn deze doeleinden concreet vastgelegd?* ○ ja ○ nee

b *Verwerkt u gegevens voor andere doeleinden dan waarvoor zij zijn verzameld?* ○ ja ○ nee

Zo ja,
wordt daarbij rekening gehouden met:

_____ *de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen?* ○ ja ○ nee

_____ *de aard van de betreffende gegevens?* ○ ja ○ nee

_____ *de gevolgen van de beoogde verwerking voor de betrokkene?* ○ ja ○ nee

_____ *de wijze waarop de gegevens zijn verkregen?* ○ ja ○ nee

_____ *de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen?* ○ ja ○ nee

_____ *een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift dat verwerking in de weg kan staan?* ○ ja ○ nee

c *Voor het geval niet verenigbaar met het doel wordt gewerkt kan dan gemotiveerd aangegeven worden of dit gebeurt in het belang van:* ○ ja ○ nee

_____ *de voorkoming, opsporing en vervolging van strafbare feiten?* ○ ja ○ nee

_____ *gewichtige economische en financiële belangen van de staat en andere openbare lichamen?* ○ ja ○ nee

_____ *het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen?* ○ ja ○ nee

_____ *de bescherming van de betrokkene of van de rechten en vrijheden van anderen?* ○ ja ○ nee

_____ *de veiligheid van de staat?* ○ ja ○ nee

d *Verwerkt u gegevens voor historische, statistische of wetenschappelijke doeleinden?* ○ ja ○ nee

Zo ja,

_____ *heeft u de nodige maatregelen getroffen om te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden?* ○ ja ○ nee

e *Heeft u maatregelen getroffen om te waarborgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de realisering van het doel waarvoor ze worden verzameld of vervolgens worden verwerkt?* ○ ja ○ nee

Doelbinding

Toelichting

Het verzamelen en het verdere gebruik van persoonsgegevens is aan specifieke regels gebonden. Het verzamelen is mogelijk voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verzamelde persoonsgegevens worden alleen verder verwerkt als dit verenigbaar is met het doel waarvoor ze zijn verkregen. Op deze regels zijn weer uitzonderingen van toepassing. De organisatie dient bekend te zijn met de voorschriften voor de verwerking. Het management draagt zorg dat er volgens die voorschriften wordt gewerkt.

Worden de persoonsgegevens in uw organisatie voor een specifiek doel verzameld en verder verwerkt op een manier die verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen?

Beoordeling

1 Er zijn geen procedures voor het verzamelen en verder verwerken vastgelegd en de regels voor het verzamelen en verder verwerken zijn niet in de organisatie bekend.

2 Er zijn geen procedures vastgelegd maar de regels voor het verzamelen en verder verwerken zijn wel in de organisatie bekend.

3 Er zijn procedures vastgelegd en de regels voor het verzamelen en verder verwerken zijn in de organisatie bekend.

4 Er zijn procedures vastgelegd, de regels voor het verzamelen en verder verwerken zijn in de organisatie bekend en worden nageleefd.

5 Er zijn procedures vastgelegd, de regels voor het verzamelen en verder verwerken zijn in de organisatie bekend, worden nageleefd en deze naleving wordt gecontroleerd.

Ambitie

U geeft aan in welke mate u de doelbinding van uw gegevensverwerking middels procedures wilt vastleggen.

Sterke punten | Punten voor verbetering

Het verwerken van persoonsgegevens kan slechts rechtmatig plaatsvinden wanneer een beroep kan worden gedaan op een grondslag die in de wet wordt genoemd (artikel 8 WBP).

a *Heeft u maatregelen getroffen om vast te stellen of er een grondslag is in de wet om gegevens te verwerken?* ○ ja ○ nee

Zo ja,
verwerkt u persoonsgegevens op basis van één of meer van de volgende gronden:

_____ *de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend?* ○ ja ○ nee

_____ *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 noodzakelijk zijn voor het sluiten van een overeenkomst?* ○ ja ○ nee

_____ *de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is?* ○ ja ○ nee

_____ *de gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene?* ○ ja ○ nee

_____ *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?* ○ ja ○ nee

_____ *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?* ○ ja ○ nee

b *Verwerkt u gegevens 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?* ○ ja ○ nee

Zo ja,

_____ *heeft u gecontroleerd of dit in overeenstemming is met de WBP?* ○ ja ○ nee

Rechtmatige grondslag

Toelichting

Voor het rechtmatig verwerken van persoonsgegevens is een grondslag nodig. De WBP geeft limitatief aan in welke gevallen persoonsgegevens mogen worden verwerkt. Voor bepaalde gegevens - de bijzondere gegevens als bedoeld in artikel 16 WBP - geldt dat het verwerken verboden is tenzij aan specifieke voorwaarden is voldaan. 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.

Worden de (bijzondere) persoonsgegevens in uw organisatie voor een specifiek doel verwerkt op grond van de in de WBP genoemde grondslagen?

Beoordeling

1 Er zijn geen procedures voor het bepalen van de rechtmatige grondslag van verwerking vastgelegd en de regels zijn niet in de organisatie bekend.

2 Er zijn geen procedures voor het bepalen van de rechtmatige grondslag van verwerking vastgelegd maar de regels voor de rechtmatige grondslag van verwerking zijn wel in de organisatie bekend.

3 Er zijn procedures voor het bepalen van de rechtmatige grondslag van verwerking vastgelegd en de regels zijn in de organisatie bekend.

4 Er zijn procedures voor het bepalen van de rechtmatige grondslag van verwerking vastgelegd, de regels zijn in de organisatie bekend en worden nageleefd.

5 Er zijn procedures voor het bepalen van de rechtmatige grondslag van verwerking vastgelegd, de regels zijn in de organisatie bekend, worden nageleefd en deze naleving wordt gecontroleerd.

Ambitie

U geeft aan in welke mate u de rechtmatige grondslag van uw gegevensverwerking in procedures wilt vastleggen.

Sterke punten | Punten voor verbetering

a *Heeft u procedures en maatregelen getroffen waarmee de kwaliteit van de gegevensvoorbereiding en de invoer van gegevens gewaarborgd kan worden?* ○ ja ○ nee

Zo ja,
is hierbij aandacht besteed aan:

_____ *Gegevensvoorbereiding door de gebruikersorganisatie.*
Persoonsgegevens worden alleen verzameld en verder verwerkt voor het doel waarvoor ze zijn bestemd. De persoonsgegevens zijn terzake dienend, niet bovenmatig, juist en nauwkeurig. Invoerformulieren en invoerschermen waarborgen onder meer dat fouten en het achterwege laten van invoer wordt geminimaliseerd? ○ ja ○ nee

_____ *Autorisatie van brondocumenten.*
Brondocumenten worden gemaakt door geautoriseerd personeel. Er is voldoende functiescheiding met betrekking tot de oorsprong en goedkeuring van een brondocument? ○ ja ○ nee

_____ *Gegevens verzamelen voor brondocumenten.*
Alle geautoriseerde brondocumenten worden tijdig, volledig, accuraat en juist verantwoord en verwerkt? ○ ja ○ nee

_____ *Foutbehandeling brondocumenten.*
Tijdens het opstellen van gegevens worden fouten en onregelmatigheden ontdekt, gemeld en gecorrigeerd? ○ ja ○ nee

_____ *Handhaven brondocumenten.*
Originele brondocumenten blijven in bezit van de organisatie of zijn binnen een acceptabele termijn te verkrijgen indien reconstructie of herstel van gegevens nodig is en om te voldoen aan de wettelijke eisen? ○ ja ○ nee

_____ *Autorisatieprocedures gegevensinvoer.*
Gegevens worden alleen door geautoriseerde personeelsleden ingevoerd? ○ ja ○ nee

_____ *Foutenafhandeling tijdens gegevensinvoer waarborgt dat fouten e.d. worden ontdekt, gemeld en gecorrigeerd?* ○ ja ○ nee

_____ *Juistheid-, volledigheids- en autorisatiecontroles.*
Ingevoerde gegevens worden gecontroleerd op juistheid, volledigheid en autorisatie. Tevens worden de ingevoerde gegevens zo dicht mogelijk bij de bron gevalideerd en bewerkt? ○ ja ○ nee

_____ *Herstelprocedure gegevensinvoer.*
Herstelprocedures zorgen voor correctie van onjuiste invoer van gegevens? ○ ja ○ nee

Vervolg op pagina 32

Kwaliteit

Toelichting

Voor de kwaliteit van de verwerking van persoonsgegevens gelden bepaalde kwaliteitseisen. Persoonsgegevens worden voor een bepaald doel verzameld en verder verwerkt. Voor dat doel behoren de persoonsgegevens toereikend, ter zake dienend en niet bovenmatig te zijn. Dat betekent onder meer dat niet meer gegevens mogen worden verzameld dan nodig is. De persoonsgegevens moeten tevens juist en nauwkeurig zijn. Dat betekent dat er maatregelen moeten zijn genomen om de juistheid van de gegevens te waarborgen. Hiermee worden fouten in de invoer en verwerking voorkomen. Eenmaal gemaakte fouten moeten tijdig ontdekt en hersteld worden.

Heeft u voorzien in procedures waarin de kwaliteit van de verwerking van persoonsgegevens wordt gewaarborgd?

Beoordeling

1 Er zijn geen procedures vastgelegd en de regels voor de kwaliteit van persoonsgegevens zijn niet in de organisatie bekend.

2 Er zijn geen procedures vastgelegd maar de regels voor de kwaliteit van persoonsgegevens zijn wel in de organisatie bekend.

3 Er zijn procedures vastgelegd en de regels voor de kwaliteit van persoonsgegevens zijn in de organisatie bekend.

4 Er zijn procedures vastgelegd, de regels voor de kwaliteit van het verwerken van persoonsgegevens zijn in de organisatie bekend en worden nageleefd.

5 Er zijn procedures vastgelegd, de regels voor de kwaliteit van het verwerken van persoonsgegevens zijn in de organisatie bekend, worden nageleefd en deze naleving wordt gecontroleerd.

Ambitie

U geeft aan in welke mate u de kwaliteit van de verwerking van persoonsgegevens wilt waarborgen.

Sterke punten | Punten voor verbetering

b *Heeft u procedures en maatregelen getroffen waarmee de kwaliteit van de gegevensverwerking gewaarborgd kan worden?* ( ) ja ( ) nee

Zo ja,
is hierbij aandacht besteed aan:

_____ *Validatie van gegevensverwerking en bewerking.*
Validatie van de gegevensverwerking, authenticatie en bewerking vindt zo dicht mogelijk bij de plaats van ontstaan plaats? ( ) ja ( ) nee

_____ *Integriteit van de gegevensverwerking.*
Functiescheiding en het controleren van de verwerking van persoonsgegevens in de vorm van bijvoorbeeld (geprogrammeerde) verbanden en totalen, mutatie- en andere verwerkingscontroles? ( ) ja ( ) nee

_____ *Foutafhandeling bij gegevensverwerking.*
Onjuiste transacties worden vastgelegd en geïdentificeerd zonder dat ze verwerkt worden of dat andere juiste transacties vervallen of worden onderbroken? ( ) ja ( ) nee

c *Heeft u procedures en maatregelen getroffen waarmee de kwaliteit van de uitvoer en de integriteit van gegevensbestanden gewaarborgd kan worden?* ( ) ja ( ) nee

Zo ja,
is hierbij aandacht besteed aan:

_____ *Beoordelen van uitvoer.*
De juistheid van de uitvoerverslagen wordt gecontroleerd door de verstrekker en de relevante gebruikers? De afhandeling van fouten in de uitvoer wordt beheerst? ( ) ja ( ) nee

_____ *Behandelen en behouden van uitvoer.*
Uitvoerformulieren uit de informatiesystemen worden behandeld en indien onjuist niet verstrekt? ( ) ja ( ) nee

_____ *Vergelijken en herstellen uitvoer.*
De uitvoer wordt automatisch vergeleken met relevante controletotalen. Audit trails worden ter beschikking gesteld voor het traceren van verwerkte gegevens en herstellen van verminkte gegevens? ( ) ja ( ) nee

_____ *Librarybeheer.*
De inhoud van de gegevens opgeslagen in de bibliotheek wordt systematisch geïnventariseerd en de integriteit van de bewaarde media wordt instandgehouden? ( ) ja ( ) nee

a *Inzage*

Is er in uw organisatie een procedure die het omgaan met het verzoek van de betrokkene om inzage in diens persoonsgegevens regelt? ( ) ja ( ) nee

Zo ja,
wordt hierin geregeld:

_____ *hoe en waar het verzoek moet worden ingediend?* ( ) ja ( ) nee

_____ *dat betrokkene binnen vier weken schriftelijk wordt meegedeeld of persoonsgegevens over hem worden verwerkt?* ( ) ja ( ) nee

_____ *dat een volledig overzicht van persoonsgegevens wordt gegeven in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers en de informatie over de herkomst van de gegevens?* ( ) ja ( ) nee

_____ *dat, indien een derde naar verwachting bedenkingen zal hebben, die derde in de gelegenheid wordt gesteld zijn zienswijze naar voren te brengen, tenzij dit onmogelijk is of een onevenredige inspanning kost?* ( ) ja ( ) nee

_____ *dat, indien de betrokkene daarom verzoekt mededelingen worden gedaan over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de betreffende gegevens?* ( ) ja ( ) nee

_____ *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?* ( ) ja ( ) nee

_____ *voor een bericht volgend op een verzoek ten hoogste tien gulden in rekening wordt gebracht?* ( ) ja ( ) nee

Zo nee,
beroept u zich dan op het belang van:

_____ *de voorkoming, opsporing en vervolging van strafbare feiten?* ( ) ja ( ) nee

_____ *gewichtige economische en financiële belangen van de staat en andere openbare lichamen?* ( ) ja ( ) nee

_____ *het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de voornoemde belangen?* ( ) ja ( ) nee

_____ *de bescherming van de betrokkene of van de rechten en vrijheden van anderen?* ( ) ja ( ) nee

_____ *de veiligheid van de staat?* ( ) ja ( ) nee

Vervolg op pagina 36

Rechten

Toelichting

De betrokkene heeft recht op inzage, verbetering, aanvulling, verwijdering of afscherming van diens persoonsgegevens. Op de bedoelde rechten zijn weer uitzonderingen. Van de organisatie wordt verwacht dat er procedures zijn die waarborgen dat de rechten van de betrokkenen zijn verzekerd. De organisatie is met die rechten en procedures bekend.

In hoeverre worden in uw organisatie de rechten van betrokkenen gegarandeerd?

Beoordeling

1 Er zijn geen procedures vastgelegd en de regels voor rechten van betrokkenen zijn niet bekend binnen de organisatie.

2 Er zijn geen procedures vastgelegd maar de regels voor de rechten van betrokkenen zijn wel in de organisatie bekend.

3 Er zijn procedures vastgelegd en de regels voor de rechten van betrokkenen zijn in de organisatie bekend.

4 Er zijn procedures vastgelegd, de regels voor de rechten van betrokkenen zijn in de organisatie bekend en worden nageleefd.

5 Er zijn procedures vastgelegd, de regels voor de rechten van betrokkenen zijn in de organisatie bekend, worden nageleefd en deze naleving wordt gecontroleerd.

Ambitie

U geeft aan in welke mate u de rechten van betrokkenen wilt garanderen.

Sterke punten	Punten voor verbetering

b *Verbeteren, aanvullen, verwijderen en afschermen*

Heeft uw organisatie een procedure voor de afhandeling van 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? ○ ja ○ nee

Zo ja,
wordt in de procedure aandacht besteed aan de vraag of:

_____ *het verzoek de aan te brengen wijzigingen bevat?* ○ ja ○ nee

_____ *de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk wordt bericht of, dan wel in hoeverre aan het verzoek wordt voldaan?* ○ ja ○ nee

_____ *een weigering op het verzoek met redenen is omkleed?* ○ ja ○ nee

_____ *een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd?* ○ ja ○ nee

_____ *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?* ○ ja ○ nee

_____ *indien er persoonsgegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd, de derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis wordt gegeven van de verbetering, aanvulling, verwijdering of afscherming, tenzij gemotiveerd is dit dat dit onmogelijk blijkt of een onevenredige inspanning kost?* ○ ja ○ nee

_____ *indien de betrokkene dit verzoekt opgave wordt gedaan van degenen aan wie de mededeling is gedaan?* ○ ja ○ nee

_____ *de vergoeding wordt teruggegeven in geval er op het verzoek, op aanbeveling van het CBP of op bevel van de rechter tot verbetering, aanvulling, verwijdering of afscherming is overgegaan?* ○ ja ○ nee

c *Relatief verzet (toekennen na belangenafweging)*

Is er in uw organisatie sprake van:

_____ *gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt?* ○ ja ○ nee

_____ *gegevensverwerking die noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert?* ○ ja ○ nee

Zo ja,

_____ *heeft u dan een procedure waarlangs de betrokkene te allen tijde verzet kan aantekenen in verband met zijn bijzondere persoonlijke omstandigheden?* ○ ja ○ nee

Vervolg op pagina 38

Zo ja,
wordt in die procedure geregeld:

_____ *dat binnen vier weken na ontvangst van het verzoek om verzet wordt beoordeeld of het verzet gerechtvaardigd is vanwege de bijzondere persoonlijke omstandigheden van verzoeker?* ○ ja ○ nee

_____ *dat indien het verzet gerechtvaardigd is, de verwerking terstond wordt beëindigd?* ○ ja ○ nee

_____ *dat de voor het in behandeling nemen van het verzet de gevraagde vergoeding van kosten niet hoger mag zijn dan een bedrag dat bij of krachtens algemene maatregel van bestuur is vastgesteld?* ○ ja ○ nee

_____ *dat de vergoeding teruggegeven wordt als het verzet gegrond wordt bevonden?* ○ ja ○ nee

d *Absoluut verzet (altijd toekennen)*

Verwerkt u gegevens voor direct marketing of charitatieve doeleinden? ○ ja ○ nee

Zo ja,

_____ *heeft u maatregelen getroffen om de betrokkene te wijzen op de mogelijkheid zich hiertegen te verzetten?* ○ ja ○ nee

_____ *vindt deze bekendmaking plaats via bladen?* ○ ja ○ nee

_____ *vindt deze bekendmaking tenminste 1 maal per jaar plaats?* ○ ja ○ nee

_____ *wijst u de betrokkene op het recht van verzet, wanneer een boodschap naar betrokkene wordt gezonden?* ○ ja ○ nee

_____ *kan het verzet kosteloos worden gedaan?* ○ ja ○ nee

_____ *wordt de verwerking terstond beëindigd?* ○ ja ○ nee

e *Geautomatiseerde besluiten*

Is er in uw organisatie sprake van het nemen van besluiten op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van iemands persoonlijkheid? ○ ja ○ nee

Zo ja,
heeft u een procedure waarin aandacht wordt besteed aan de vraag 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;* ○ ja ○ nee

_____ *de betrokkene in de gelegenheid is gesteld over het besluit zijn zienswijze naar voren te brengen?* ○ ja ○ nee

_____ *de grondslag te vinden is in een wet waarin maatregelen zijn vastgelegd die strekken tot bescherming van het gerechtvaardigde belang van de betrokkene?* ○ ja ○ nee

_____ *de betrokkene de logica wordt medegedeeld die ten grondslag ligt aan de geautomatiseerde verwerking?* ○ ja ○ nee

Vervolg op pagina 40

f *Bijzonderheden*

De verzoeken tot inzage en correctie worden ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt, en ten aanzien van onder curatele gestelden gedaan door hun wettelijke vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijke vertegenwoordigers.

Controleert u dit? ○ ja ○ nee

Bent u een organisatie voor wetenschappelijk, statistisch of historisch onderzoek? ○ ja ○ nee

Zo ja,

_____ *heeft u voorzieningen getroffen zodat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt?* ○ ja ○ nee

_____ *Bent u op de hoogte van de uitzonderingen op de rechten van betrokkenen?* ○ ja ○ nee

a *Stelt u periodiek beleid vast voor beveiliging en de daarbij behorende normen, procedures en maatregelen?* ○ ja ○ nee

Zo ja,

_____ *is er een bij het beleidsplan behorend communicatieplan?* ○ ja ○ nee

_____ *instrueert u alle medewerkers, ook de tijdelijke, over het beveiligingsbeleid, de bijbehorende normen, procedures en maatregelen?* ○ ja ○ nee

_____ *worden beleid, normen, procedures en maatregelen schriftelijk verstrekt?* ○ ja ○ nee

_____ *toetst u of medewerkers de procedures en maatregelen kennen en zich overeenkomstig gedragen?* ○ ja ○ nee

_____ *is er een procedure om vast te stellen dat het personeel het beveiligingsbeleid heeft begrepen en opgevolgd?* ○ ja ○ nee

_____ *wordt het management jaarlijks geïnformeerd over het beveiligingsbewustzijn van de medewerkers?* ○ ja ○ nee

_____ *is er een systeem waarbij sprake is van continue bewaking en vernieuwing/verbetering van de procedures?* ○ ja ○ nee

b *Tekenen alle medewerkers, ook de tijdelijke, een geheimhoudingsverklaring?* ○ ja ○ nee

c *Moeten nieuwe medewerkers een verklaring omtrent het gedrag overleggen?* ○ ja ○ nee

d *Wordt bij navraag van referenties de omgang met persoonsgegevens nagetrokken?* ○ ja ○ nee

e *Is informatiebeveiliging onderwerp gedurende functioneringsgesprekken en beoordelingen?* ○ ja ○ nee

f *Zijn de verantwoordelijkheden voor informatiebeveiliging in de functieomschrijvingen en arbeidscontracten opgenomen?* ○ ja ○ nee

g *Is er voor gezorgd dat taken of functies die onverenigbaar zijn met het oog op beveiliging, niet door dezelfde medewerker worden uitgevoerd (functiescheiding)?* ○ ja ○ nee

h *Worden alle medewerkers incl. derden en uitzendkrachten getraind?* ○ ja ○ nee

Zo ja,

_____ *wordt deze training ook voor nieuwe medewerkers herhaald?* ○ ja ○ nee

_____ *is er een overzicht van alle medewerkers die deze training gevolgd hebben?* ○ ja ○ nee

_____ *gebruikt u bij trainingen voor informatiesystemen en beveiligingsmaatregelen uitsluitend gegevens over fictieve personen?* ○ ja ○ nee

Vervolg op pagina 44

Beveiliging / Bewustzijn

Toelichting

Informatiebeveiliging heeft geen effect als ze alleen maar op papier bestaat. De medewerkers zullen beveiligingsmaatregelen daadwerkelijk moeten uitvoeren 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, zowel bij indiensttreding van personeel, als bij de dagelijkse functieuitoefening door bestaande personeelsleden. Zo kan er al bij de werving van personeel gelet worden op de kennis van beveiliging en de houding van de sollicitant ten aanzien daarvan.
Verder moet de aandacht voor dit onderwerp terugkomen in communicatie-(plannen) van de organisatie en opleidingstrajecten.

Uiteraard moeten alle medewerkers regelmatig op de hoogte worden gehouden van de afgesproken procedures en maatregelen voor de informatiebeveiliging. Dat kan schriftelijk, maar ook door middel van instructies, voorlichting of door het onderwerp aan de orde te brengen in periodieke beoordelingsgesprekken. Het moet daarbij duidelijk zijn dat informatiebeveiliging niet vrijblijvend is. Controle op de naleving is belangrijk. Bij de medewerkers moet duidelijk zijn dat er sancties staan op het niet-naleven van de regels.

Vervolg op pagina 43

i	*Worden beveiligingsincidenten door de verantwoordelijke medewerkers direct gerapporteerd aan hun manager en aan de voor de beveiliging verantwoordelijke functionaris?*	○ ja ○ nee
j	*Neemt u disciplinaire maatregelen wanneer een personeelslid de geheimhoudingsverklaring schendt of procedures en maatregelen niet correct uitvoert?*	○ ja ○ nee

Bevordert uw organisatie actief het beveiligingsbewustzijn bij de medewerkers?

Beoordeling

1 Er wordt hiervoor geen inspanning geleverd. Er zijn ook geen procedures voor het vaststellen van de mate waarin de WBP begrepen is en of er behoefte is aan opleiding en training op dit terrein.

2 De medewerkers worden geïnformeerd over informatiebeveiliging. Beveiliging komt reeds ter sprake tijdens de sollicitatieprocedure. Er zijn eerste aanzetten voor de vaststelling van de mate waarin de WBP begrepen is en er is sprake van enige identificatie van de behoefte aan training en opleiding op dit terrein.

3 De medewerkers worden geïnformeerd over informatiebeveiliging en zij ontvangen instructies. Het komt ter sprake tijdens de sollicitatieprocedure en er worden gerichte vragen gesteld aan sollicitanten. Er is een systeem voor de bepaling van de mate waarin de WBP begrepen is en de meting van behoefte aan opleiding en training.

4 De medewerkers worden geïnformeerd over informatiebeveiliging en ontvangen daarover instructies. Er wordt regelmatig gecontroleerd of de medewerkers de maatregelen naleven. Beveiliging wordt ter sprake gebracht tijdens de sollicitatie-procedure en daarover worden gerichte vragen gesteld aan sollicitanten. De ant-woorden van de sollicitanten worden nagetrokken. De naleving van het systeem van meting van opleiding en training wordt bewaakt.

5 De medewerkers worden geïnformeerd over informatiebeveiliging, zij ontvangen instructies. Er wordt regelmatig gecontroleerd of de medewerkers de maatregelen naleven. Bij niet-naleving worden maatregelen getroffen tegen de betreffende medewerkers. Beveiliging komt ter sprake tijdens de sollicitatieprocedure en er worden gerichte vragen gesteld aan sollicitanten. Beveiligingsbewustzijn is een selectiecriterium.

Ambitie

U geeft aan hoe uw organisatie het beveiligingsbewustzijn stimuleert.

Sterke punten | Punten voor verbetering

a *Worden voor uw organisatie systemen en software ontwikkeld?* ○ ja ○ nee

Zo ja,

_____ *controleert u of de maatregelen en procedures voor beveiliging in overeenstemming zijn met het informatiebeveiligingsbeleid?* ○ ja ○ nee

b *Wordt bij aanschaf van apparatuur en systemen rekening gehouden met de benodigde graad van beveiliging?* ○ ja ○ nee

c *Heeft u het beheer van informatietechnologie binnen uw organisatie gedocumenteerd?* ○ ja ○ nee

Zo ja,
bevat de documentatie de volgende onderdelen:

_____ *datamodellen?* ○ ja ○ nee

_____ *software?* ○ ja ○ nee

_____ *datacommunicatieprotocollen?* ○ ja ○ nee

_____ *procesbeschrijvingen?* ○ ja ○ nee

_____ *autorisatieschema?* ○ ja ○ nee

d *Zijn er in geval van calamiteiten en incidenten of problemen bij de gegevensverwerking procedures opgesteld?* ○ ja ○ nee

Zo ja,

_____ *worden bij uitvoering van deze procedures alle handelingen vastgelegd?* ○ ja ○ nee

e *Wordt door derden onderhoud aan systemen en sofware verricht?* ○ ja ○ nee

Zo ja:

_____ *is in het onderhoudscontract met derden de vertrouwelijke omgang met persoonsgegevens vastgelegd?* ○ ja ○ nee

_____ *is bij het onderhoud door derden de toegankelijkheid tot persoonsgegevens beperkt?* ○ ja ○ nee

_____ *worden bij het testen van systemen gegevens gebruikt die betrekking hebben op bestaande personen?*

Beveiliging / IT-voorzieningen

Toelichting

Voor de bedrijfsvoering is het belangrijk dat een organisatie goed bijhoudt over welke voorzieningen ze beschikt. Ook voor de informatiebeveiliging is een dergelijk beheer van de IT-voorzieningen nodig. Onder IT-voorzieningen kan alle hardware en software worden verstaan. De aanwezige hardware en software moet duidelijk beschreven zijn en er moeten duidelijke afspraken zijn over onderhoud en wijzigingen in de voorzieningen. Er moet duidelijk beschreven zijn wie de bevoegdheid en verantwoordelijkheid voor deze taken heeft. In de beheerprocedures moet speciale aandacht worden besteed aan eventuele calamiteiten.

Bij het ontwikkelen en de aanschaf van software en hardware moet altijd worden beoordeeld of de producten voldoende beveiligingsmogelijkheden bieden. Bij het beschrijven van de IT-voorzieningen hoort ook het classificeren van gegevensdragers. Deze moeten, in elk geval voor de hoogste risicoklasse, worden gemarkeerd of gelabeld, zodat de klasse van de gegevens duidelijk te zien is.

Zijn er binnen uw organisatie afspraken gemaakt over het beheer van de informatietechnologie?

Beoordeling

1 Er zijn hier geen afspraken over gemaakt.

2 Er zijn formele afspraken over het beheer van de IT.

3 Er zijn gestandaardiseerde en gedocumenteerde procedures voor het beheer van IT.

4 Er zijn gestandaardiseerde en gedocumenteerde procedures voor het beheer van IT en deze worden regelmatig herzien.

5 Er zijn gestandaardiseerde en gedocumenteerde procedures voor het beheer van IT die regelmatig worden herzien. Het beheer van IT wordt als een essentieel kwaliteitskenmerk van de organisatie gezien.

Ambitie

U geeft aan welke afspraken u binnen uw organisatie wilt maken over het beheer van de informatietechnologie.

Sterke punten | Punten voor verbetering

a	*Heeft u vastgelegd wie toegang heeft tot welke systemen en bestanden?*	ja	nee
b	*Heeft u vastgelegd wie binnen uw organisatie bevoegd is om medewerkers autorisaties te geven voor de verwerking van persoonsgegevens?*	ja	nee
———	*Zo ja, heeft u een procedure vastgesteld om deze autorisaties toe te kennen?*	ja	nee
c	*Controleert u in de operationele situatie/praktijk of de toegangscontrole volledig overeenkomt met de toegekende autorisaties?*	ja	nee
d	*Maakt u gebruik van bevoegdheidsprofielen?*	ja	nee
e	*Beperkt u de autorisatiebevoegdheidsprofielen die u aan een medewerker of groep van medewerkers toekent, tot uitsluitend die bevoegdheden die voor het uitoefenen van de taak nodig zijn?*	ja	nee
f	*Worden de autorisaties die aan de medewerkers zijn toegekend regelmatig gecontroleerd?*	ja	nee
g	*Heeft u procedures vastgesteld voor de herziening van autorisaties in geval van van ontslag, vertrek en wijziging van functie ?*	ja	nee
h	*Heeft u voor derden en tijdelijke medewerkers een vergelijkbare procedure opgesteld ?*	ja	nee
i	*Is uw computercentrum in een aparte ruimte ondergebracht?*	ja	nee
j	*Is het aantal medewerkers met toegang tot deze ruimte tot het absolute minimum beperkt?*	ja	nee
k	*Is deze ruimte voorzien van een brandblusinstallatie?*	ja	nee
———	*Zo ja, wordt deze brandblusinstallatie regelmatig getest?*	ja	nee
l	*Is er een Uninterrupted Power Supply (UPS) aanwezig om korte stroomonderbrekingen op te vangen?*	ja	nee
m	*Is er een noodstroomaggregaat aanwezig dat in geval van langdurige uitval van de stroomvoorziening automatisch wordt opgestart?*	ja	nee
———	*Zo ja, wordt dit noodstroomaggregaat regelmatig getest?*	ja	nee

Vervolg op pagina 48

Beveiliging / Toegangsbeveiliging

Toelichting

Het is van groot belang dat de organisatie maatregelen en procedures heeft om te voorkomen dat onbevoegden toegang krijgen tot locaties, informatiesystemen en gegevensbestanden. Wanneer iemand met weinig moeite een gebouw, applicatie of gegevensbestand kan binnendringen waar zich persoonsgegevens bevinden, zal het risico op ongeautoriseerde kennisneming en ongeoorloofde mutaties in persoonsgegevens sterk toenemen. Fysieke en logische toegangsbeveiliging is daarom noodzakelijk. Dit houdt in dat maatregelen moeten worden getroffen om ruimtes te kunnen afsluiten en om te controleren wie tot welke ruimtes toegang heeft. Daarnaast moet worden voorkomen dat onbevoegde personen die toegang hebben verkregen tot een gebouw of rekencentrum ook toegang krijgen tot; informatiesystemen en gegevensbestanden. Naast de logische toegangsbeveiliging dient ook de fysieke beveiliging adequaat te zijn om verlies van persoonsgegevens te voorkomen.

In hoeverre heeft uw organisatie maatregelen en procedures getroffen om te voorkomen dat onbevoegden toegang krijgen tot locaties, informatiesystemen en gegevensbestanden?

Beoordeling

1 Er zijn geen procedures en er wordt volstaan met standaard beveiligingsmaatregelen.

2 Er zijn procedures en maatregelen vastgelegd. De beveiliging van locaties, informatiesystemen en gegevensbestanden wordt daarin beschreven.

3 Er zijn procedures en maatregelen vastgelegd en deze worden regelmatig herzien.

4 Er zijn procedures en maatregelen vastgelegd en deze worden regelmatig herzien. Aan de medewerkers worden instructies gegeven en dit wordt periodiek herhaald.

5 Er zijn procedures en maatregelen vastgelegd en deze worden regelmatig herzien. Aan de medewerkers worden instructies gegeven en dit wordt periodiek herhaald. Er wordt gecontroleerd of de individuele medewerkers de maatregelen en procedures naleven.

Ambitie

U geeft aan welke maatregelen voor toegangsbeheer en -controle u wilt nemen.

Sterke punten | Punten voor verbetering

n *Wordt bij de inlogprocedure gebruik gemaakt van een gebruikersnaam en een wachtwoord?* ( ) ja ( ) nee

Zo ja,
zijn er afspraken gemaakt met betrekking tot:

_____	*geldigheid periode van een wachtwoord?*	( ) ja	( ) nee
_____	*hergebruik van wachtwoorden?*	( ) ja	( ) nee
_____	*keuze van wachtwoorden?*	( ) ja	( ) nee
_____	*lengte van wachtwoorden?*	( ) ja	( ) nee
_____	*het maximaal aantal inlogpogingen dat is toegestaan?*	( ) ja	( ) nee
_____	*is de controle op de naleving van deze afspraken geautomatiseerd?*	( ) ja	( ) nee

o *Heeft u uw medewerkers geïnstrueerd over gebruik en toepassing van het wachtwoord?* ( ) ja ( ) nee

p *Is het vrijgeven van een geblokkeerde systeemtoegang uitsluitend toegestaan door een geautoriseerde functionaris?* ( ) ja ( ) nee

q *Wordt elke poging om toegang te krijgen tot een systeem vastgelegd in een log-file?* ( ) ja ( ) nee

Zo ja,
wordt er ten aanzien hiervan:

_____	*een bewaartijd in acht genomen?*	( ) ja	( ) nee
_____	*regelmatig een analyse op bijzonderheden gemaakt?*	( ) ja	( ) nee
_____	*schriftelijk gerapporteerd over incidenten?*	( ) ja	( ) nee

r *Wordt bij het verstrekken van toegang tot persoonsgegevens via een computernetwerk gebruikersnaam en wachtwoord ook het tijdstip en de gebruikte apparatuur gecontroleerd?* ( ) ja ( ) nee

Zo ja,

_____	*wordt hiervan een registratie bijgehouden in een logbestand?*	( ) ja	( ) nee

s *Wordt er aan de verantwoordelijke onmiddellijk gerapporteerd indien het aantal toegestane pogingen om toegang te krijgen tot het informatiesysteem wordt overschreden?* ( ) ja ( ) nee

t *Is het mogelijk om zonder toestemming van de daarvoor verantwoordelijke bevoegdheden over te dragen?* ( ) ja ( ) nee

a	*Maakt u gebruik van datacommunicatie via netwerken?*			○ ja	○ nee
	Zo ja,				
	welke van de hieronder vermelde mogelijkheden is/zijn voor uw organisatie van toepassing:				
_____	*LAN (Local Area Network)?*	○ ja	○ nee		
_____	*WAN (Wide Area Network)?*	○ ja	○ nee		
_____	*Internet?*	○ ja	○ nee		
b	*Heeft u in een procedure vastgelegd op welke wijze datacommunicatie behoort plaats te vinden?*			○ ja	○ nee
c	*Maakt u gebruik van de beveiligingsmogelijkheden die uw netwerk-apparatuur en software bieden (antivirusprogrammatuur en firewalls)?*			○ ja	○ nee
	Zo ja,				
_____	*heeft u een antivirusprogramma geïnstalleerd?*	○ ja	○ nee		
_____	*heeft u een zogenaamde screen-saver geïnstalleerd waardoor gebruikers automatisch worden afgesloten nadat de gebruiker z'n Terminal/PC niet heeft gebruikt?*	○ ja	○ nee		
d	*Heeft u maatregelen getroffen om te voorkomen dat medewerkers eigen apparatuur, bijv. PC's, aan het netwerk aansluiten?*			○ ja	○ nee
e	*Maakt u gebruik van een koppeling tussen uw netwerk en publieke netwerken?*			○ ja	○ nee
	Zo ja,				
_____	*heeft u deze koppelingen beveiligd door bijvoorbeeld firewalls?*	○ ja	○ nee		
f	*Houdt u bij de aanschaf van netwerkapparatuur en netwerksoftware rekening met beveiligingseisen?*			○ ja	○ nee
g	*Bevinden kwetsbare netwerkcomponenten (zoals hubs, routers) zich in afgesloten ruimten?*			○ ja	○ nee
h	*Heeft u maatregelen getroffen waaruit blijkt dat de datacommunicatie alleen plaatsvindt tussen u en de door u vertrouwde netwerkvoorzie-ningen?*			○ ja	○ nee
i	*Zijn er maatregelen getroffen om te controleren of over netwerken getransporteerde persoonsgegevens ongewijzigd zijn overgebracht?*			○ ja	○ nee
j	*Verzendt u persoonsgegevens over publieke netwerken?*			○ ja	○ nee
	Zo ja,				
_____	*maakt u daarbij gebruik van encryptietechnieken?*	○ ja	○ nee		
_____	*heeft u procedures opgesteld voor het beheer van de cryptografische sleutels?*	○ ja	○ nee		
_____	*houdt u een registratie bij van alle verzonden en ontvangen berichten?*	○ ja	○ nee		

Beveiliging / Netwerken

Toelichting

Voor het transporteren van gegevens wordt vaak gebruik gemaakt van computer- of telefoonnetwerken. Deze datacommunicatie kan binnen de organisatie zijn, al dan niet binnen één locatie, maar ook met andere locaties/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. Bij netwerken die gekoppeld zijn met externe netwerken, denk aan internet, ontstaat een extra risico. Via deze koppeling kan, wanneer sprake is van ontoereikende beveiliging, van buitenaf het informatiesysteem worden binnengedrongen, met risico voor de integriteit van persoonsgegevens die zich daarin bevinden. Beveiliging van deze koppelingen is daarom extra belangrijk.

In hoeverre heeft uw organisatie maatregelen getroffen om te voorkomen dat onbevoegden toegang krijgen tot persoonsgegevens bij datacommunicatie?

Beoordeling

1 Er zijn hiervoor geen maatregelen en procedures.

2 Er zijn maatregelen en procedures vastgelegd voor het verzenden en ontvangen van berichten.

3 Er zijn maatregelen en procedures vastgelegd voor het verzenden en ontvangen van berichten. Deze maatregelen en procedures worden regelmatig geactualiseerd.

4 Er zijn maatregelen en procedures vastgelegd voor het verzenden en ontvangen van berichten. Deze maatregelen en procedures worden regelmatig geactualiseerd en de naleving ervan wordt gecontroleerd.

5 Er zijn maatregelen en procedures vastgelegd voor het verzenden en ontvangen van berichten. Deze procedures worden regelmatig herzien en de naleving ervan wordt gecontroleerd. Er is een toereikend niveau van beveiliging van het gegevensverkeer.

Ambitie

U geeft aan welk niveau van beveiliging van uw communicatie u wilt bereiken.

Sterke punten | Punten voor verbetering

a *Heeft u maatregelen getroffen zodat alleen daartoe bevoegde personen kunnen beschikken over de verwijderbare gegevensdragers?* ○ ja ○ nee

b *Worden er back-ups gemaakt van bestanden?* ○ ja ○ nee

Zo ja,

_____ *is er een back-up cyclus vastgesteld?* ○ ja ○ nee

Zo ja,

_____ *is deze in een procedure vastgelegd?* ○ ja ○ nee

_____ *wordt gecontroleerd of deze procedure wordt nageleefd?* ○ ja ○ nee

_____ *is er een bewaartermijn voor back-ups vastgesteld?* ○ ja ○ nee

_____ *wordt er een exemplaar van de back-ups op een externe locatie bewaard?* ○ ja ○ nee

c *Worden de gegevensdragers met persoonsgegevens bewaard in afsluitbare ruimten?* ○ ja ○ nee

Zo ja,

_____ *zijn deze ruimten voorzien van een beveiliging tegen inbraak?* ○ ja ○ nee

d *Worden de gegevensdragers in een inbraakwerende kluis bewaard?* ○ ja ○ nee

Zo ja,

_____ *is de ruimte waarin de kluis staat voorzien van een inbraakdetectiesysteem?* ○ ja ○ nee

e *Zijn de persoonsgegevens op de gegevensdragers extra beveiligd zodat onbevoegden hiervan geen kennis kunnen nemen (bijvoorbeeld door encryptie)?* ○ ja ○ nee

f *Is bij het vernietigen van persoonsgegevens geregeld dat:*

_____ *gegevens niet fysiek aanwezig blijven op de gegevensdragers?* ○ ja ○ nee

_____ *speciale vernietigingsmethoden worden gehanteerd voor gegevens die op optische media zijn vastgelegd?* ○ ja ○ nee

_____ *de verantwoordelijke eerst toestemming moet geven alvorens de gegevens daadwerkelijk worden vernietigd?* ○ ja ○ nee

_____ *het verwijderen van tussen- en testresultaten die bij de gegevensverwerking horen eveneens plaatsvindt?* ○ ja ○ nee

_____ *dit pas plaatsvindt na een vastgestelde bewaartermijn voor persoonsgegevens?* ○ ja ○ nee

g *Is er voorgeschreven dat er een administratie wordt bijgehouden van de gegevens die worden vernietigd?* ○ ja ○ nee

Zo ja,
wordt vastgelegd:

_____ *door wie de gegevens zijn vernietigd?* ○ ja ○ nee

_____ *het tijdstip waarop de gegevens zijn vernietigd?* ○ ja ○ nee

_____ *in opdracht van wie de gegevens zijn vernietigd?* ○ ja ○ nee

Beveiliging / Bewaring en vernietiging

Toelichting

Persoonsgegevens kunnen op verschillende media, zogenaamde gegevensdragers worden bewaard. Gegevensdagers bestaan onder meer uit papieren dossiers, elektromagnetische media (magneetbanden, diskettes, harddisks) of optische media (CD-ROM'S). Het veilig bewaren van gegevensdragers is van belang voor de beveiliging van persoonsgegevens. Regelmatig moeten, op vaste tijdstippen, back-ups gemaakt worden van de systemen. De gevolgen van storingen en calamiteiten worden hierdoor beperkt. Het maken van back-ups moet in duidelijke procedures zijn vastgelegd, waarvan de naleving wordt gecontroleerd. Voor de beschikbaarheid is het belangrijk dat de 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. Het is nodig dat gegevensdragers zorgvuldig worden bewaard en getransporteerd, zodat onbevoegde personen ze niet kunnen meenemen of de gegevens inzien. Gegevensdragers die gegevens uit hoge risicoklassen (denk aan gevoelige of bijzondere gegevens) bevatten, moeten in ruimtes worden bewaard die afgesloten kunnen worden en voorzien zijn van adequate inbraakbeveiliging.

Wanneer persoonsgegevens niet meer gebruikt worden, moeten ze zorgvuldig worden vernietigd. Eventueel kan dit gebeuren na inachtneming van een gestelde bewaartermijn. Wanneer de gegevens niet tijdig worden vernietigd, bestaat alsnog de mogelijkheid voor zowel bevoegden als onbevoegden om kennis te nemen van de gegevens. Vernietiging van gegevens betekent veelal het fysiek vernietigen van de gegevensdragers waarop ze staan dan wel het wissen van gegevens op gegevensdragers. Het is daarbij belangrijk dat de verantwoordelijkheden duidelijk zijn vastgelegd en worden nageleefd.

Vervolg op pagina 55

Zijn er in uw organisatie procedures voor het bewaren en vernietigen van gegevens?

Beoordeling

1 Nee, er zijn hiervoor geen procedures.

2 Er zijn informele procedures voor het bewaren en vernietigen van gegevens.

3 Er zijn formele procedures vastgelegd voor het bewaren en vernietigen van gegevens.

4 Er zijn formele procedures vastgelegd voor het bewaren en vernietigen van gegevens en de medewerkers worden regelmatig geïnstrueerd.

5 Er zijn formele procedures vastgelegd voor het bewaren en vernietigen van gegevens. De medewerkers worden regelmatig geïnstrueerd. De naleving van de procedures wordt regelmatig gecontroleerd.

Ambitie

U geeft aan welke maatregelen u wilt treffen met betrekking tot het bewaren en vernietigen van gegevens.

Sterke punten	Punten voor verbetering

V / 7.6 *Reviewvragen*

a	*Is er binnen uw organisatie een calamiteitenplan?*			○ ja ○ nee
	Zo ja,			
	bevat het de volgende onderdelen:			
_____	*preventie van calamiteiten?*	○ ja	○ nee	
_____	*ontruiming?*	○ ja	○ nee	
_____	*continuïteit van de gegevensverwerking?*	○ ja	○ nee	
_____	*noodvernietiging?*	○ ja	○ nee	
b	*Wordt het calamiteitenplan regelmatig geactualiseerd?*			○ ja ○ nee
c	*Wordt het plan regelmatig geoefend?*			○ ja ○ nee
d	*Is er een herstelprocedure (recovery procedure) om na calamiteiten de gegevensverwerking te hervatten?*			○ ja ○ nee
	Zo ja,			
_____	*wordt deze procedure regelmatig getoetst en herzien?*	○ ja	○ nee	

Beveiliging / Calamiteitenplan

Toelichting

Elke organisatie kan te maken krijgen met calamiteiten, zoals brand, waterschade of ernstige computerstoringen. Dergelijke calamiteiten kunnen ervoor zorgen dat de bedrijfsvoering wordt onderbroken. In het ernstigste geval komt het voortbestaan van een organisatie in gevaar. Ook voor de aanwezige persoonsgegevens kan een calamiteit ernstige gevolgen hebben, bijvoorbeeld verlies van (alle) gegevens. Als regel moet iedere organisatie een calamiteitenplan 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.

Welke voorzorgen heeft uw organisatie getroffen in het geval zich calamiteiten voordoen?

Beoordeling

1 Er zijn geen bijzondere voorzorgen.
2 Er is een calamiteitenplan opgesteld.
3 Er is een calamiteitenplan opgesteld. Dit plan wordt regelmatig geactualiseerd.
4 Er is een calamiteitenplan opgesteld. Dit plan wordt regelmatig geactualiseerd. De medewerkers worden regelmatig geïnstrueerd.
5 Er is een calamiteitenplan opgesteld. Dit plan wordt regelmatig geactualiseerd. De medewerkers worden regelmatig geïnstrueerd. Er vinden regelmatig oefeningen plaats.

Ambitie

U geeft aan welke maatregelen u wilt nemen met betrekking tot herstel na calamiteiten.

Sterke punten | Punten voor verbetering

a *Is er een contract tussen de verantwoordelijke en de bewerker van de gegevens opgesteld?* ○ ja ○ nee

Zo ja,
is hierin vastgelegd:

_____ *dat verwerking van persoonsgegevens slechts in opdracht van de verantwoordelijke kan plaatsvinden, behoudens afwijkende wettelijke bepalingen?* ○ ja ○ nee

_____ *dat de verantwoordelijke en de bewerker zich aan de beveiligingseisen zullen houden (vergelijk vraag 7.1 tot en met 7.6)* ○ ja ○ nee

_____ *dat de beveiligingsmaatregelen schriftelijk worden vastgelegd?* ○ ja ○ nee

b *Stelt u zich op de hoogte van het daadwerkelijke beveiligingsniveau bij de bewerker?* ○ ja ○ nee

c *Hebben alle medewerkers van de bewerker een geheimhoudingsplicht?* ○ ja ○ nee

d *Is er een calamiteitenplan?* ○ ja ○ nee

e *Wordt jaarlijks het niveau van beveiliging bij de bewerker gecontroleerd?* ○ ja ○ nee

Zo ja,

_____ *wordt hierover gerapporteerd?* ○ ja ○ nee

Bewerker

Toelichting

In veel gevallen zal een organisatie niet alle verwerkingen van persoonsgegevens zelf uitvoeren maar geheel of gedeeltelijk uitbesteden aan opdrachtnemers. Voor de beveiliging van persoonsgegevens geldt dat de opdrachtnemer dezelfde beveiliging moet garanderen als de verantwoordelijk organisatie. In de contracten met opdrachtnemers moet de beveiliging van de gegevens daarom expliciet opgenomen worden. Ook is het verplicht dat de opdrachtnemer een geheimhoudingsverklaring tekent. Wanneer de opdrachtnemer gegevens uit de hoogste risicoklasse verwerkt zal er ook actief toezicht moeten worden gehouden op de beveiligingsmaatregelen die zijn genomen, bijvoorbeeld in de vorm van periodieke controles.

Heeft uw organisatie (delen van de) gegevensverwerking uitbesteed?

Beoordeling

1 Ja, maar er is geen contract opgesteld met de opdrachtnemer(s).

2 Ja, er is een contract opgesteld met opdrachtnemer(s).

3 Ja, er is een contract opgesteld met opdrachtnemer(s). Hierin is een clausule opgenomen over de verplichting tot informatiebeveiliging.

4 Ja, er is een contract opgesteld met opdrachtnemer(s). Hierin is een clausule opgenomen over de verplichting tot informatiebeveiliging. Er is ook een geheimhoudingsverklaring.

5 Ja, er is een contract opgesteld met opdrachtnemer(s). Er zijn in het contract duidelijke afspraken vastgelegd over de verantwoordelijkheid voor de informatiebeveiliging. Periodiek wordt dit in overleg met de opdrachtnemer getoetst en aangepast.

Ambitie

U geeft aan hoe u met betrekking tot privacywaarborgen de uitbesteding van verwerkingen wilt regelen.

Sterke punten | Punten voor verbetering

a *Heeft uw organisatie voor het doorgeven van persoonsgegevens om deze verder te bewerken in landen buiten de Europese Unie een procedure vastgesteld?* ○ ja ○ nee

Zo ja,

_____ *wordt hierin gemotiveerd weergegeven op grond van welke gevallen het gegevensverkeer plaatsvindt?* ○ ja ○ nee

Het betreffende land waarborgt een passend beschermingsniveau. Bij die beoordeling is gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevens van invloed zijn. In het bijzonder is rekening gehouden met de aard van de gegevens, met de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen bestaan. ○ ja ○ nee

Het betreffende land biedt geen waarborgen voor een passend beschermingsniveau, maar aan één of meer van de volgende voorwaarden is voldaan:

_____ *de betrokkene heeft zijn ondubbelzinnige toestemming gegeven voor verwerking?* ○ ja ○ nee

_____ *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 die noodzakelijk zijn voor het sluiten van een overeenkomst?* ○ ja ○ nee

_____ *de doorgifte is noodzakelijk voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst?* ○ ja ○ nee

_____ *de doorgifte is noodzakelijk vanwege een zwaarwegend algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht?* ○ ja ○ nee

_____ *de doorgifte is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene?* ○ ja ○ nee

_____ *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?* ○ ja ○ nee

_____ *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?* ○ ja ○ nee

Niet EU-landen

Toelichting

De organisatie kan persoonsgegevens vanuit Nederland ook verder laten verwerken in een land buiten de Europese Unie. Persoonsgegevens kunnen bijvoorbeeld vanuit Nederland worden doorgegeven naar de Verenigde Staten om daar met andere gegevens te worden samengebracht. Dit kan niet zonder meer en hiervoor gelden aanvullende en bijzondere voorwaarden. Het land buiten de Europese Unie dient namelijk een passend beschermingsniveau voor de verwerking van de persoonsgegevens te waarborgen.

Realiseert de organisatie zich dat het verwerken van persoonsgegevens in een land buiten de Europese Unie aan aanvullende en bijzondere regels is gebonden en worden persoonsgegevens conform die regels verwerkt?

Beoordeling

1 Er zijn geen procedures vastgelegd en de regels voor het verwerken van persoonsgegevens in landen buiten de Europese Unie zijn niet in de organisatie bekend.

2 Er zijn geen procedures vastgelegd maar de regels voor het verwerken van persoonsgegevens in landen buiten de Europese Unie zijn wel in de organisatie bekend.

3 Er zijn procedures vastgelegd en de regels voor het verwerken van persoonsgegevens in landen buiten de Europese Unie zijn in de organisatie bekend.

4 Er zijn procedures vastgelegd, de regels voor het verwerken van persoonsgegevens in landen buiten de Europese Unie zijn in de organisatie bekend en worden nageleefd.

5 Er zijn procedures vastgelegd, de regels voor het verwerken van persoonsgegevens in landen buiten de Europese Unie zijn in de organisatie bekend, worden nageleefd en de naleving wordt gecontroleerd.

Ambitie

U geeft aan in hoeverre u bij de verwerking van persoonsgegevens in een land buiten de Europese Unie aan de specifieke regels die daarvoor gelden, wilt voldoen.

Sterke punten | Punten voor verbetering

Bijlagen

Hoofdlijnen WBP

Met het in werking treden van de WBP in 2001 voldoet Nederland aan de eis van de EG privacyrichtlijn 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, omschreven 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 de juiste mensen op het juiste tijdstip en voor het juiste doel 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 Wet bescherming persoonsgegevens stelt een College bescherming persoonsgegevens (CBP) in dat toezicht houdt op het naleven van deze privacywetgeving. Het CBP heeft de bevoegdheid een onderzoek in te stellen naar de wijze waarop in de aanwezige verwerking van persoonsgegevens invulling wordt gegeven aan de geldende privacywetgeving.

Juridisch kader voor privacybescherming

2 . 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 in de lidstaten moet worden omgegaan met de verwerking van persoonsgegevens.

2 . 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 hier weergegeven (artikel 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 begrippenkaders, 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*
1onder 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 Meldingsbesluit;
- het Vrijstellingsbesluit;
- de procedure voor het melden van een verwerking van persoonsgegevens.

Samenvatting uitkomsten WBP Zelfevaluatie

Nadat de WBP Zelfevaluatie is uitgevoerd aan de hand van de in hoofdstuk V opgenomen vragen is het gewenst het management een samenvatting te verstrekken van de bevindingen. Daarin wordt aangegeven hoe de feitelijke implementatie/naleving van de bescherming van persoonsgegevens in de organisatie zich verhoudt tot het gedefinieerde ambitieniveau.
In onderstaand schema worden, door het plaatsen van een kruisje in het betreffende vakje, het ambitieniveau en de uitkomsten van de beoordeling op overzichtelijke wijze met elkaar geconfronteerd.

Uitkomsten Hoofdstuk V

V /		Beoordeling					Ambitie				
1	Melding	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
2	Transparantie	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
3	Doelbinding	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
4	Rechtmatige grondslag	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
5	Kwaliteit	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
6	Rechten	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.1	Beveiliging / Bewustzijn	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.2	Beveiliging / IT-voorzieningen	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.3	Beveiliging / Toegangsbeveiliging	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.4	Beveiliging / Netwerken	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.5	Beveiliging / Bewaring en vernietiging	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
7.6	Beveiliging / Calamiteitenplan	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
8	Bewerker	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5
9	Niet-EU landen	0 1	0 2	0 3	0 4	0 5	0 1	0 2	0 3	0 4	0 5

De uitkomsten weergegeven in dit schema vormen voor het management de basis voor het definiëren van de te nemen vervolgstappen en de prioriteiten die daarbij moeten worden gehanteerd, dan wel bijstelling van het ambitieniveau.

Indien het management ervoor heeft gekozen om de WBP Zelfevaluatie door een in- of externe deskundige te laten reviewen zal de uitkomst van deze review uiteraard in de besluitvorming dienen te worden betrokken.

Colofon

Samenstelling
Samenwerkingsverband Audit Aanpak
Werkgroep Zelfevaluatie

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