**Doe het zelf met privacybescherming**

**Een toelichting op de Audit Aanpak**

**College bescherming persoonsgegevens**

Het College bescherming persoonsgegevens – CBP – (onder de Wet bescherming persoonsgegevens de rechtsopvolger van de Registratiekamer) houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen.

**Advies, bemiddeling en onderzoek**
Het College adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Zij toetst gedragscodes en privacyreglementen en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan de toezichthouder onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet.

**Publicaties**
Over haar werkzaamheden en bevindingen brengt het CBP jaarlijks een openbaar verslag uit. Daarnaast geeft zij publicaties uit over de resultaten van verricht onderzoek.

**Informatie**
Voor juridisch advies kunt u gebruik maken van het telefonisch spreekuur, op werkdagen van 9.00 – 12.30 uur, telefoon (070) 381 13 00.

College bescherming persoonsgegevens
Prins Clauslaan 20
Postbus 93374
Telefoon (070) 381 13 00
Fax (070) 381 13 01
E-mail mail@cbpweb.nl

**Inhoud**

**Colofon**

Uitgave: College bescherming persoonsgegevens
Ontwerp: Miriam Monster (Proforma)
Druk: Sdu grafisch bedrijf bv
Datum: 2001

## 1. Inleiding

Door de technologische ontwikkeling kunnen organisaties omvangrijke hoeveelheden persoonsgegevens verwerken (zoals verzamelen, registreren en aanwenden voor verschillende doeleinden). Het wordt steeds eenvoudiger gegevensbestanden te koppelen. Op deze wijze kunnen op het eerste oog relatief onschuldige persoonsgegevens een andere betekenis krijgen. Verder raken individuele personen het zicht en hun zeggenschap kwijt over hun persoonsgegevens.

De bescherming van persoonsgegevens in Nederland wordt vanaf 1 september 2001 geregeld in de Wet bescherming persoonsgegevens (WBP). Deze wet, als opvolger van de Wet persoonsregistraties (WPR), stelt eisen aan de wijze waarop organisaties persoonsgegevens mogen verwerken. Vrijwel elke organisatie in Nederland doet dat en heeft dus te maken met de WBP. De eisen in de WBP zijn veranderd en uitgebreid ten opzichte van de WPR. Dit betekent dat een organisatie die voldoet aan de wettelijke bepalingen van de WPR niet zonder meer voldoet aan alle WBP bepalingen.

Vooruitlopend op de invoering van de Wet bescherming persoonsgegevens (WBP) heeft de voorloper van het CBP eind 1999 het initiatief genomen om in een samenwerkingsverband een aantal producten te ontwikkelen. Dit initiatief past binnen de beleidsfilosofie van het CBP tot het stimuleren van zelfregulering. Uit dit project komen de audit producten die organisaties in staat stellen om de kwaliteit van de getroffen maatregelen voor de bescherming van persoonsgegevens in hun organisatie te (laten) beoordelen.

*Zelfregulering en Viersporenbeleid*
Het beleid van het CBP is mede gericht op het bevorderen van de bescherming van persoonsgegevens door zelfregulering. Degenen die verantwoordelijk zijn voor het verwerken van persoonsgegevens, dienen deze bescherming als een vanzelfsprekendheid te ervaren en in hun werkzaamheden te vertalen. Daartoe heeft het CBP een viersporenbeleid ontwikkeld dat zich richt op bewustwording, normontwikkeling, technologie en handhaving.

Door middel van publicatie van Achtergrondstudies en Verkenningen, brochures en algemene (publieks)voorlichting draagt het CBP bij aan de bewustwording van de privacybescherming in Nederland. Ook de inmiddels ontwikkelde audit producten zijn instrumenten die bijdragen aan een adequaat niveau van bewustwording binnen organisaties. Bewustwording is een eerste stap op weg naar een toereikende bescherming van persoonsgegevens.

Hoewel de wet een duidelijk raamwerk geeft voor de bescherming van persoonsgegevens is de feitelijke invulling van deze bescherming niet altijd eenvoudig te realiseren. Via wetgevingsadviezen, jurisprudentie, het toetsen van gedragscodes, het Raamwerk Privacy Audit en de studie ‘Beveiliging van persoonsgegevens’ schept het CBP een normatief kader dat als referentie kan dienen voor de feitelijke invulling van de privacybescherming.

De technologische ontwikkelingen bieden zowel kansen als bedreigingen voor de privacybescherming. Inzicht in de risico's bij verwerking van persoonsgegevens door middel van informatietechnologie en de mogelijkheden van de technologie (in het bijzonder Privacy-Enhancing Technologies) dragen bij tot een goed niveau van bescherming van persoonsgegevens binnen organisaties.

Tot slot beschikt het College bescherming persoonsgegevens (CBP) in de nieuwe wet (WBP) over meer mogelijkheden tot handhaving van de wet. Via onderzoeken en Privacy Audits vult het CBP deze taak in. Daarbij heeft het CBP een eigen verantwoordelijkheid, welke het uiteraard moet kunnen verdedigen op grond van het mandaat dat het bij wet heeft meegekregen en de nadere invulling van die wet in haar eigen beleidsvorming.

Het initiatief rond de Audit Aanpak past heel goed bij het viersporenbeleid van het CBP:
- Is er voldoende privacybewustzijn in de organisatie?
- Wordt er gewerkt volgens wettelijke normen c.q. zelfregulering?
- Wordt het gebruik van Privacy-Enhancing Technologies (PET) gestimuleerd?
- Wordt het voorgaande voldoende beheerst en gecontroleerd door de verantwoordelijke?

*Audit producten*
Het Samenwerkingsverband Audit Aanpak bestaat uit marktpartijen, zoals audit- en adviesorganisaties, koepelorganisaties van auditors, werknemers-, werkgevers- en consumentenorganisaties en de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties. Dit samenwerkingsverband heeft drie audit producten ontwikkeld: Quickscan, WBP Zelfevaluatie (eventueel met review) en Raamwerk Privacy Audit. Tussen de verschillende audit producten bestaat een verschil in diepgang, zodat een goede afweging gemaakt moet worden bij de keuze tussen de audit producten.

De Quickscan is een beknopte vragenlijst waarmee functionarissen binnen een organisatie snel inzicht kunnen verkrijgen in de mate waarin men zich bewust is van de bescherming van persoonsgegevens.

Via de WBP Zelfevaluatie kan een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van de maatregelen voor de bescherming en beveiliging van persoonsgegevens beoordelen. De WBP Zelfevaluatie kan door organisaties ook gebruikt worden bij de implementatie van de WBP binnen de organisatie of de overgang van WPR naar WBP. 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.

Het Raamwerk Privacy Audit is bedoeld voor het opstellen van een werkplan voor het uitvoeren van een Privacy Audit door een (privacy)deskundige auditor. De Privacy Audit geeft de leiding van een organisatie met een hoge mate van zekerheid een objectief oordeel over de naleving van de wettelijke bepalingen en daarmee ook inzicht in de sterke en zwakke punten van de bescherming van persoonsgegevens.

Uit onderstaand schema blijkt de relatie tussen de verschillende audit producten:

*Overzicht diepgang productenset*

| **Behoefte/diepgang** | **Product** |
|---|---|
| Globale indruk | Quickscan |
| Interne meting | WBP Zelfevaluatie |
| Interne meting + externe beoordeling | WBP Zelfevaluatie + review |
| Onafhankelijk onderzoek + certificaat | Privacy Audit |

De audit producten zijn voor burgers, verantwoordelijken en auditors beschikbaar gesteld op de website van het CBP.

*Het Samenwerkingsverband*
De Audit Aanpak is ontwikkeld in het Samenwerkingsverband Audit Aanpak dat bestaat uit het CBP, diverse koepelorganisaties en verschillende marktpartijen van audit- en adviesorganisaties. Het CBP is eindverantwoordelijk voor de geleverde producten. Wijzigingen in de producten komen echter pas tot stand na besluitvorming door het Samenwerkingsverband.

De audit producten zijn tijdens de ontwikkeling uitgebreid getest bij verschillende typen van organisaties. De ervaringen en bevindingen bij het gebruik van de audit producten zullen gebruikt worden voor verdere optimalisering van de nu ontwikkelde producten.

*Een privacycertificaat?*
In aansluiting op de audit producten is een project gestart om de haalbaarheid van een privacycertificaat te onderzoeken. Een privacycertificaat kan als keurmerk een belangrijke rol vervullen bij zelfregulering door organisaties. Het CBP stelt daarbij als eis dat een toekomstig privacycertificaat voldoet aan hoge kwaliteitseisen. Naar verwachting zal er eind 2001 meer duidelijkheid bestaan over de haalbaarheid van een privacycertificaat.

## 2. Managementcyclus en de bescherming van persoonsgegevens

Het realiseren van bedrijfsdoelstellingen, via de managementcyclus, verloopt in het algemeen via de volgende drie fasen: de organisatie van de processen (inclusief de beleidsvoering), de processen zelf en een evaluatie en bijsturing van de processen. De bescherming van persoonsgegevens dient een onlosmakelijk element van de managementcyclus te zijn.

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 of Privacy Audit 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 passende bescherming van persoonsgegevens te verzekeren.

Het proces om tot een goede privacybescherming te komen gaat niet van vandaag op morgen. Een organisatie heeft tijd nodig om het bewustwordingsproces op gang te brengen. Het proces vraagt ook om begeleiding. De auditor kan vanuit zijn natuurlijke adviesfunctie hierin voorzien. Daarnaast is het voor het management dat belast is met de implementatie van de WBP raadzaam één of meerdere contactpersonen aan te stellen die verantwoordelijk zijn voor onder meer de coördinatie van de te treffen voorzieningen en de evaluatie van de getroffen voorzieningen. Hierbij kan onder meer gedacht worden aan de functionaris voor de gegevensbescherming[1].

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

Het is van groot belang dat een organisatie die de WBP Zelfevaluatie of Privacy Audit uitvoert, vaststelt welke wettelijke vereisten vanuit de WBP, maar ook vanuit andere wetgeving (GBA, Politiewet, etc.) van toepassing zijn op de verwerking van persoonsgegevens binnen de organisatie. 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 relevant zijn, omdat deze situaties zich niet voordoen.

[1] Brochure

## 3. Basisniveau van privacybescherming

Voor het rechtmatig verwerken van persoonsgegevens en het zorgvuldig omgaan met persoonsgegevens schrijft de WBP een aantal dwingende normen voor. Deze normen zijn uitgewerkt in een aantal basisvoorwaarden. Deze basisvoorwaarden vormden het uitgangspunt bij het ontwikkelen van de audit producten.

1. *Voornemen en melden*
   De verwerking van persoonsgegevens moet vooraf worden gemeld bij het College bescherming persoonsgegevens (CBP) of een functionaris voor de gegevensbescherming, tenzij de verwerking daarvan is vrijgesteld.

2. *Transparantie*
   De betrokkene, dat is de persoon wiens persoonsgegevens worden verwerkt, moet kunnen overzien door wie en voor welk doel zijn gegevens worden verwerkt.

3. *Doelbinding*
   Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

4. *Rechtmatige grondslag*
   De verwerking van persoonsgegevens moet berusten op een in de WBP genoemde grondslag, zoals toestemming, overeenkomst, wettelijke plicht, gerechtvaardigd belang en dergelijke. Voor bijzondere gegevens (onder meer ras, gezondheid, seksuele geaardheid) gelden striktere normen.

5. *Kwaliteit*
   De persoonsgegevens moeten zoveel mogelijk juist, nauwkeurig, toereikend, terzake dienend en niet bovenmatig zijn.

6. *Rechten van de betrokkenen*
   De betrokkenen hebben het recht om kennis te nemen van hun gegevens en te laten verbeteren of te laten verwijderen. Tevens hebben zij er recht op om bezwaar te maken tegen het verwerken van persoonsgegevens.

7. *Beveiliging*
   Passende maatregelen van technische en organisatorische aard vormen het noodzakelijke sluitstuk van een rechtmatige verwerking.

8. *Verwerking door een bewerker*
   Als de verwerking wordt uitbesteed aan een bewerker, moet worden verzekerd dat deze zich houdt aan de aanwijzingen van de verantwoordelijke.

9. *Gegevensverkeer met landen buiten de EU*
   Het verkeer van persoonsgegevens naar een land buiten de Europese Unie (EU) is in principe alleen toegestaan als dat land een passend niveau van bescherming heeft.

## 4. Audit Aanpak

De ontwikkelde audit producten kennen zowel gelijksoortige (identieke) als specifieke elementen. In de producten komen dezelfde hoofdthema's aan de orde. De mate waarin de hoofdthema's naar objecten en deelobjecten worden gedifferentieerd is per product echter anders. Zo kent de Quickscan naast de hoofdthema's weinig deelobjecten. Het Raamwerk Privacy Audit kent kent daarentegen de meeste deelobjecten.

Alle producten bevatten in beginsel dezelfde hoofdthema's. De toenemende diepgang van de vraagstelling en de wijze van verwerking van de antwoorden is productspecifiek bepaald. De hoofdthema's zijn:

- behoorlijke en zorgvuldige verwerking van persoonsgegevens;
- beveiliging van persoonsgegevens;
- Privacy-Enhancing Technologies;
- de rechten van betrokkenen waarborgen.

*Specifieke kenmerken Quickscan*
Het doel van de Quickscan is het bevorderen van het privacybewustzijn in de organisatie van de verantwoordelijke en het bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking. De Quickscan bestaat uit dertien korte vragen. De Quickscan kan ook als opstap worden gezien naar de WBP Zelfevaluatie.

*Specifieke kenmerken WBP Zelfevaluatie*
Het doel van de WBP Zelfevaluatie is het bevorderen van privacybewustzijn en inzicht in privacynormen in de organisatie van de verantwoordelijke en het nader bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking. Met de WBP Zelfevaluatie wordt gestreefd naar een verdieping van het privacybewustzijn ten opzichte van de Quickscan. Ook beoogt het een toename van het inzicht in relevante normen. Belangrijk is dat het managementteam het nut om verbeteringen aan te brengen onderkent, naar de organisatie uitdraagt en tenslotte initieert.

*Specifieke kenmerken WBP Zelfevaluatie met review*
Aanvullend aan de uitgangspunten die voor de WBP Zelfevaluatie gelden, heeft de review de objectivering van de WBP Zelfevaluatie tot doel en de positiebepaling van de organisatie binnen de maatschappij voor wat betreft de kwaliteit van de privacybescherming.

Daarom kan het nuttig zijn om de uitkomsten van de zelfevaluatie door een externe deskundige te laten reviewen. De review biedt de verantwoordelijke een bepaalde mate van zekerheid over de kwaliteit van de privacybescherming binnen een beperkt budget. De WBP Zelfevaluatie kan gebruikt worden als opstap naar de Privacy Audit.

*Specifieke kenmerken Raamwerk Privacy Audit*
De Privacy Audit heeft tot doel de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerkingsketen te beoordelen. De uitvoering dient te geschieden door een gecertificeerde deskundige. Het CBP kan gezien haar taak ook zelf een Privacy Audit conform het Raamwerk Privacy Audit uitvoeren. De mogelijkheden worden bezien voor het afgeven van een privacycertificaat nadat een Privacy Audit met een positief oordeel is uitgevoerd.

## 5. Quickscan

De Quickscan is een beknopte vragenlijst waarmee functionarissen binnen een organisatie snel inzicht kunnen verkrijgen in de mate waarin men zich bewust is van de bescherming van persoonsgegevens. De vragen zijn geclusterd in vier categorieën:

- privacybewustzijn in de organisatie;
- uitvoering van wettelijke bepalingen;
- beveiliging;
- controle.

De uitkomsten van de Quickscan geven een globale indruk hoe het met de privacybescherming in een organisatie gesteld is. De vragenlijst is echter beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens zoals die in de WBP zijn bepaald. Het instrument is met name geschikt voor het creëren van bewustwording en kan het begin zijn van een verbetertraject in de organisatie.

De Quickscan bevat een duidelijke toelichting op het gebruik en kan door alle werknemers in een organisatie ingevuld worden. De uitkomsten zijn nuttig voor de leiding, de ondernemingsraad en, indien benoemd, voor de functionaris voor de gegevensbescherming. Op de website van de het CBP is een uitgebreide toelichting op de verschillende mogelijke antwoorden beschikbaar. Aan de hand van deze toelichting kunnen de mogelijke vervolgstappen bepaald worden.

Na het bekend worden van de uitkomsten van de vragenlijst kan de organisatie een gericht onderzoek uitvoeren naar de concrete invulling van de privacyeisen binnen de organisatie. Daarvoor is in eerste instantie een uitgebreide WBP Zelfevaluatie te verkrijgen. Via deze zelfevaluatie kunnen medewerkers in een organisatie zelfstandig de kwaliteit van de maatregelen ter bescherming van persoonsgegevens beoordelen en nagaan op welke gebieden noodzakelijke maatregelen ontbreken of ontoereikend zijn. Daarmee vergroot de verantwoordelijke het vertrouwen van relaties in de zorgvuldige omgang met persoonsgegevens binnen een organisatie.

Als bijlage in deze brochure is de Quickscan opgenomen. Om voor de verspreiding van de Quickscan zorg te dragen zal het CBP deze opnemen in de daartoe geëigende brochures.

## 6. WBP Zelfevaluatie

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 het verwerken van persoonsgegevens. Daarnaast kan de WBP Zelfevaluatie bijdragen aan bewustwording van het belang van privacybescherming. Organisaties kunnen de WBP Zelfevaluatie ook gebruiken bij de implementatie van de WBP of bij de overgang van WPR naar WBP. 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.

Via de WBP Zelfevaluatie kan een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van de maatregelen voor de bescherming en beveiliging van persoonsgegevens beoordelen. De methode is gebaseerd op het INK-model, dat beoogt de leiding van een organisatie zelf te laten vaststellen hoe de organisatie presteert en hoe de organisatie is ingericht op haar taak. De WBP Zelfevaluatie geeft inzicht in de huidige en de gewenste situatie. De organisatie kan hierdoor haar ambitieniveau voor de bescherming van persoonsgegevens aangeven en de feitelijke situatie beoordelen.

De bepalingen van de WBP zijn overzichtelijk geclusterd in negen aandachtsgebieden die alle aspecten van de WBP afdekken. Per aandachtsgebied worden ook de sterke punten en de punten voor verbetering geïdentificeerd. Tot slot worden alle bevindingen samengevat, waarbij in één oogopslag duidelijk wordt hoe de feitelijke naleving van de bescherming van persoonsgegevens zich verhoudt ten opzichte van het gedefinieerde ambitieniveau.

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), verantwoordelijke, 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. De rapportage van de zelfevaluatie moet gericht worden aan het hoogste managementniveau (bestuur/directie).

*Ambitieniveau*
De WBP Zelfevaluatie biedt de leiding van een organisatie een hulpmiddel om in een beperkte tijd 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 (risico)analyse dient de basis te zijn voor een weloverwogen keuze van het ambitieniveau. De WBP Zelfevaluatie kan daarmee worden gekenschetst als een diagnosemodel.

*Review*

De 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 externe deskundige de uitkomsten van de zelfevaluatie te laten beoordelen. 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, wordt hiermee gecorrigeerd. Een externe deskundige die gespecialiseerd is in auditing en de WBP kan de review uitvoeren.

## 7. Raamwerk Privacy Audit

Het Raamwerk Privacy Audit is bedoeld voor het uitvoeren van een Privacy Audit door een (privacy)deskundige externe auditor. De Privacy Audit geeft de leiding van een organisatie met een hoge mate van zekerheid een objectief beeld van de naleving van de wettelijke bepalingen en daarmee ook inzicht in de sterke en zwakke punten van de bescherming van persoonsgegevens. Het CBP is met beroepsorganisaties van auditors in overleg over een applicatiecursus voor Registeraccountants en IT-auditors die Privacy Audits willen uitvoeren.

De Privacy Audit is een breed opgezette 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. Een Privacy Audit heeft de grootste diepgang van alle genoemde producten en is derhalve het meest uitgebreide onderzoek.

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

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

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

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

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

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

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

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

## 8. Conclusie

Het CBP kan er niet alleen voor zorgen dat in de Nederlandse samenleving alle persoonsgegevens beschermd worden. Dat pretenderen we dan ook niet. Daarom heeft de toezichthouder op de privacywetgeving een tweedelijnsstrategie ontwikkeld: de privacybescherming dient vooral door organisaties zelf gerealiseerd te worden.

Dat roept de vraag op: hoe beschermen we in onze eigen organisatie de bij ons aanwezige persoonsgegevens? Om die vraag te beantwoorden heeft het CBP relevante partijen uitgenodigd. Het doel was om gezamenlijk producten te ontwikkelen die het organisaties mogelijk maken de privacywet na te leven.

Met behulp van de drie ontwikkelde audit producten is het management van een organisatie die persoonsgegevens verwerkt in staat een zelfonderzoek uit te voeren en weet vooraf welke normen bij een extern ingesteld onderzoek gehanteerd worden.

Dankzij de inspanning van alle partijen zijn er kwalitatief hoogwaardige producten ontwikkeld. Het Samenwerkingsverband hoopt dat ze vaak gebruikt zullen worden en dat ze een bijdrage mogen leveren aan het bewustzijn dat we zuinig moeten zijn op onze persoonsgegevens.

## 9. Meer informatie

Mocht u meer informatie willen over de audit producten of over het omgaan met persoonsgegevens in het algemeen dan kunt u de internetsite van het CBP raadplegen. Via deze website kunt u de audit producten downloaden. Ook kunt u tussen 09.00 en 12.30 uur bellen met een adviseur van het CBP op tel. (070) 381 13 00. U kunt ook faxen (070) 381 13 01 of e-mailen: mail@cbpweb.nl.

Het Samenwerkingsverband Audit Aanpak houdt zich aanbevolen voor reacties. 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*

Het CBP heeft in de serie Achtergrondstudies en Verkenningen als nummer 23 *Beveiliging van persoonsgegevens* uitgegeven. Deze uitgave beschrijft de noodzakelijke beveiligingsmaatregelen die aan de verwerking van persoonsgegevens, in verschillende situaties, worden gesteld.

Voor het beveiligen van persoonsgegevens wordt in bovengenoemde studie aangegeven dat er een wettelijke basis bestaat voor het toepassen van technologische maatregelen. Het betreft hier de zogenaamde Privacy-Enhancing Technologies (PET). In Achtergrondstudies en Verkenningen nummer 11 “Privacy-Enhancing Technologies – The Path to Anonymity” wordt de theorie rond PET uitgebreid beschreven. Daarnaast geeft het CBP de brochure “Mag het een bitje minder zijn?” uit waarin een praktische handleiding tot het gebruik van PET wordt gegeven.

## Bijlage Quickscan bescherming persoonsgegevens

**Wet bescherming persoonsgegevens**
De privacybescherming in Nederland wordt sinds 2001 geregeld in de Wet bescherming persoonsgegevens (WBP). Deze wet, als opvolger van de Wet Persoonsregistraties (WPR), stelt eisen aan de wijze waarop organisaties persoonsgegevens verwerken. Vrijwel elke organisatie in Nederland doet dat en heeft dus te maken met de WBP. De eisen in de WBP zijn veranderd en uitgebreid ten opzichte van de WPR. Dit betekent dat als uw organisatie voldoet aan de wettelijke bepalingen van de WPR dit niet zonder meer betekent dat zij voldoet aan alle WBP-bepalingen. Het College bescherming persoonsgegevens (CBP) is als opvolger van de Registratiekamer belast met het toezicht op de naleving van de WBP.

**Doel van de Quickscan**
*Als u vindt dat personeelsleden, klanten, debiteuren, bezoekers en andere relaties vertrouwen moeten hebben in uw organisatie dan moet uw organisatie dat vertrouwen verdienen en vervolgens waarmaken. Een zorgvuldige verwerking van persoonsgegevens draagt bij aan dit vertrouwen. Het is daarom belangrijk vast te stellen hoe uw organisatie persoonsgegevens verwerkt. Een eerste stap hierbij is het creëren van voldoende bewustzijn over het belang van de zorgvuldige omgang met persoonsgegevens binnen uw organisatie. Om het proces van bewustwording te stimuleren, is een korte privacyvragenlijst opgesteld. De uitkomsten van deze vragenlijst geven een globale indruk hoe het met de privacybescherming binnen uw organisatie is gesteld. De uitkomsten van de vragenlijst zijn nuttig voor de leiding van de organisatie die verantwoordelijk is voor de naleving van de privacywetgeving, maar ook voor de ondernemingsraad en, indien benoemd de functionaris voor de gegevensbescherming. Ook in werkoverleg kan aandacht besteed worden aan de uitkomsten van deze vragenlijst.*
**Let op:** De vragenlijst is beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens, zoals die in de WBP zijn geregeld.

**Hoe werkt de vragenlijst?**
Elke medewerker in een organisatie kan de vragenlijst zelfstandig invullen. De vragenlijst bestaat uit dertien vragen. U kunt de vragen beantwoorden met ‘ja’ of ‘nee’. Door een vraag met ‘ja’ te beantwoorden, geeft u aan dat uw organisatie aandacht heeft voor het onderwerp van die vraag. Of er in voldoende mate en op de juiste wijze aandacht wordt besteed, kan pas worden gezegd na gericht onderzoek. Indien u ‘nee’ heeft geantwoord dan vraagt het betreffende onderwerp om nadere aandacht binnen uw organisatie. Mogelijk schiet uw organisatie tekort in het naleven van de wettelijke bepalingen. Op welke wijze de organisatie hier vervolg aan kan geven, vraagt eveneens om meer gericht onderzoek.
Op de website van het CBP (www.cbpweb.nl) vindt u per vraag een toelichting op de antwoordmogelijkheden van deze vragenlijst. Via deze toelichting kunt u zelf de voor uw organisatie beste vervolgstap bepalen.

*Vervolgstap*
Na het bekend worden van de uitkomsten van de vragenlijst kan de organisatie een gericht onderzoek uitvoeren naar de concrete invulling van de privacyeisen binnen de organisatie. Daarvoor is in eerste instantie een uitgebreide WBP Zelfevaluatie te verkrijgen. Via deze zelfevaluatie kunnen medewerkers van uw organisatie zelfstandig de kwaliteit van de maatregelen ter bescherming van persoonsgegevens beoordelen en nagaan op welke gebieden noodzakelijke maatregelen ontbreken of ontoereikend zijn. Daarmee vergroot u het vertrouwen van relaties in de zorgvuldige omgang met persoonsgegevens binnen uw organisatie.

*Meer informatie?*
Mocht u meer informatie willen over deze Quickscan of over het omgaan met persoonsgegevens in het algemeen dan kunt u de internetsite van het College bescherming persoonsgegevens (www.cbpweb.nl) raadplegen. Via deze website kunt u ook de WBP Zelfevaluatie downloaden. Op de website treft u ook het Raamwerk Privacy Audit aan. Op basis van dit raamwerk kan een interne of externe auditor een gedetailleerd onderzoek uitvoeren naar de wijze waarop en de mate waarin uw organisatie omgaat met de bescherming van persoonsgegevens. Ook kunt u tussen 09.00 en 12.30 uur bellen met een adviseur van het CBP via tel. (070) 381 13 00. U kunt ook faxen (070) 381 13 01 of e-mailen: mail@cbpweb.nl.

*Van wie is de vragenlijst afkomstig?*
De vragenlijst is ontwikkeld in een samenwerkingsverband bestaande uit het CBP, diverse koepelorganisaties en verschillende marktpartijen van audit- en adviesorganisaties.

**Vragen:**
*Het is mogelijk dat u geen zicht heeft op de totale organisatie waarin u werkzaam bent. In dat geval kunt u voor onderstaande vragen voor het woord organisatie ook de afdeling lezen waarin u werkzaam bent.*

***Privacybewustzijn in de organisatie***
Voor het realiseren van een goede bescherming van de persoonsgegevens in een organisatie is privacybewustzijn en het proces van privacybewustwording van belang.

1. Is in uw bedrijf voorlichting gegeven over de nieuwe privacywet (WBP)? Ja Nee

2. Heeft de directie of leiding uitgesproken dat de organisatie de privacy van personen moet respecteren?
   Ja Nee

De directie of leiding van een organisatie kan op verschillende manieren de privacy bij haar medewerkers onder de aandacht brengen. Daarbij kan gedacht worden aan: informatiesessies over privacy, een privacyrichtlijn voor medewerkers, specifieke acties en maatregelen ter bescherming van de privacy.

3. Wordt er op uitvoerend niveau binnen uw organisatie aandacht besteed aan privacybescherming?
   Ja Nee

***Uitvoering wettelijke bepalingen***
Onder het verwerken van persoonsgegevens wordt onder meer verstaan het, zowel geautomatiseerd als handmatig, verzamelen, vastleggen, bewerken, bewaren, verstrekken, verwijderen en vernietigen van persoonsgegevens door organisaties.

De wet beperkt het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn, zoals door de organisatie vooraf geformuleerd, en doelstellingen die daarmee verenigbaar zijn.

4. Beperkt uw organisatie het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn en doelstellingen die daarmee verenigbaar zijn? Ja Nee

Het verwerken van persoonsgegevens kan uitsluitend plaatsvinden als daarvoor een rechtmatige grondslag aanwezig is. De WBP geeft aan op welke gronden verwerking toegestaan is.

5. Vindt het verwerken van persoonsgegevens binnen uw organisatie plaats in overeenstemming met de grondslagen van de WBP? Ja Nee

Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt.

6. Zijn er regels vastgesteld voor het verwerken van persoonsgegevens binnen uw organisatie?
   Ja Nee

De wet stelt strengere eisen aan de verwerking van bijzondere persoonsgegevens. Dit betreft gegevens over: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

7. Zijn er specifieke regels vastgesteld voor het verwerken van bijzondere persoonsgegevens binnen uw organisatie? Ja Nee

Voor een zorgvuldige verwerking moeten de persoonsgegevens die in uw organisatie worden verwerkt, correct zijn.

8. Controleert uw organisatie persoonsgegevens op juistheid en volledigheid? Ja Nee

De WBP legt organisaties die persoonsgegevens verwerken een informatieplicht op. Daardoor weten de personen (betrokkenen) van wie persoonsgegevens worden verwerkt hoe de organisatie met hun persoonsgegevens omgaat.

9. Leeft uw organisatie de informatieplicht naar betrokkenen na? Ja Nee

De WBP kent aan personen (betrokkenen) van wie persoonsgegevens worden verwerkt bepaalde rechten toe. Dit betreft het recht tot inzage, wijziging en verwijdering van persoonsgegevens en het recht op verzet tegen het verwerken van persoonsgegevens.

10. Komt uw organisatie de rechten van betrokkenen na? Ja Nee

***Beveiliging***

Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt. Dit betekent dat niet iedereen in een organisatie toegang mag hebben tot persoonsgegevens of deze mag bewerken, verstrekken of verwijderen.

11. Heeft uw organisatie bevoegdheden aan medewerkers toegekend zodat uitsluitend geautoriseerde medewerkers toegang hebben tot persoonsgegevens? Ja Nee

De WBP stelt dat een organisatie passende technische en organisatorische maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, met inbegrip van onnodige verwerking.

12. Heeft uw organisatie maatregelen getroffen die verlies en onrechtmatige verwerking van persoonsgegevens tegengaan? Ja Nee

***Controle***

Controle op de naleving van de maatregelen die de organisatie getroffen heeft, bij de onderwerpen van de vragen 4 tot en met 12, is belangrijk voor een goede bescherming van de persoonsgegevens.

13. Wordt de naleving van de maatregelen voor privacybescherming binnen uw organisatie van tijd tot tijd gecontroleerd? Ja