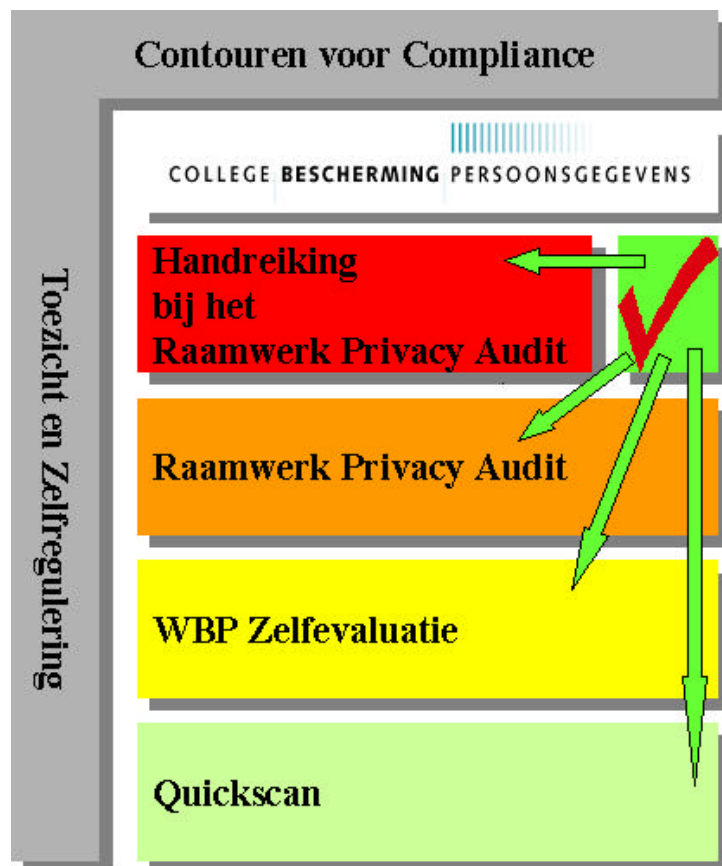


CONTOUREN voor COMPLIANCE

Overzicht van de Zelfreguleringsproducten





0 Inhoudsopgave

0	Inhoudsopgave	2
1	Toezicht en zelfregulering.....	3
1.1	<i>Zelfregulering</i>	<i>3</i>
1.2	<i>Status van de zelfreguleringsproducten.....</i>	<i>4</i>
2	Privacy-audit en kwaliteitsoordeel	4
3	Rol van de toezichthouder.....	5
3.1	<i>Het kwaliteitsoordeel.....</i>	<i>5</i>
3.2	<i>Toezicht</i>	<i>5</i>



1 Toezicht en zelfregulering

1.1 Zelfregulering

Onder de naam: **Contouren voor Compliance**¹ zijn vier zelfreguleringsproducten voor het verwerken van persoonsgegevens ontwikkeld. De hier onder beschreven producten bevatten in beginsel dezelfde hoofdthema's. De toenemende diepgang van de vraagstelling en de wijze van verwerking van de antwoorden is productspecifiek.

- **Quickscan**
doelstelling: hulpmiddel voor het bevorderen van het privacybewustzijn² in de organisatie van de verantwoordelijke en het bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- **WBP Zelfevaluatie**
doelstelling: hulpmiddel bij het verkrijgen van inzicht in het toepassen van de WBP in de organisatie van de verantwoordelijke en het nader bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- **Raamwerk Privacy Audit**
doelstelling: basis voor het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking.
- **Handreiking bij het Raamwerk Privacy Audit**
doelstelling: handreiking bij het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking. De handreiking is gebaseerd op het Raamwerk Privacy Audit en geeft aan hoe een concretisering van de wettelijke norm kan plaatsvinden.

Elke verwerking van persoonsgegevens waarop de Wet bescherming persoonsgegevens (WBP) als algemene kaderwet van toepassing is, kan onderzocht worden op basis van het Raamwerk Privacy Audit. Het Raamwerk Privacy Audit biedt namelijk een handvat voor het opstellen van een onderzoeksplan dat is toegesneden op de specifieke situatie van de organisatie. Wanneer er sprake is van aanpalende wetgeving, wordt deze meegenomen in het onderzoeksplan.

In het raamwerk is geen normering aangegeven voor de criteria die de wet stelt aan organisaties als het gaat om de bescherming van persoonsgegevens. Een handreiking voor het concretiseren van de wettelijke norm is beschreven in het document 'Handreiking bij het Raamwerk Privacy Audit'. Dit document is opgesteld met het doel richting te geven aan het gebruik van het raamwerk. De professionele oordeelsvorming van de onderzoeker blijft een grote rol spelen bij de beoordeling, gezien de open normen binnen de WBP.

Het object van onderzoek betreft één specifiek door de verantwoordelijke benoemde verwerking van persoonsgegevens. De beoordeling heeft betrekking op de wijze waarop de verantwoordelijke de verwerking van persoonsgegevens heeft ingericht. Het kwaliteitsoordeel heeft, in het algemeen, geen betrekking op de inhoud van de producten en de diensten die de verantwoordelijke levert in relatie tot deze

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

² In Contouren voor Compliance wordt onder 'privacy' verstaan de bescherming van persoonsgegevens.



verwerking van persoonsgegevens. Indien binnen het product of de dienst persoonsgegevens zijn opgenomen, wordt wel een beoordeling gegeven over het in overeenstemming zijn met de privacywet- en regelgeving³ verwerken van die persoonsgegevens.

1.2 Status van de zelfreguleringsproducten

Het College bescherming persoonsgegevens (CBP) stelt de zelfreguleringsproducten ter beschikking aan de vrije markt, voor zowel het bedrijfsleven als de overheid. De producten worden aan de hand van evaluaties periodiek inhoudelijk en redactioneel bijgesteld. Het CBP stelt zich op het standpunt dat een privacy-audit geen wettelijke verplichting mag zijn. Het staat aan een ieder vrij om een geheel of gedeeltelijk compliance onderzoek uit te (laten) voeren.

De producten zijn bedoeld als hulpmiddel bij de toetsing op het voldoen aan relevante privacywet- en regelgeving. Omdat de toepasselijkheid van wet- en regelgeving afhankelijk is van een veelheid van factoren kan geen eenduidig kader gegeven worden. In de praktijk betekent dit dat de toepasselijke wet- en regelgeving altijd kaderstellend is boven de zelfreguleringsproducten.

Een compliance onderzoek kan bijvoorbeeld uitgevoerd worden door:

- de toezichthouder;
- een Functionaris voor de Gegevensbescherming;
- een onafhankelijke derde zoals een accountant of een auditor;
- een interne auditor of een medewerker van een interne kwaliteitsafdeling.

2 Privacy-audit en kwaliteitsoordeel

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

Volgens het CBP geeft een afgegeven kwaliteitsoordeel zekerheid binnen het maatschappelijk verkeer wanneer aan de aandachtspunten beschreven in de onderstaande tekst wordt voldaan.

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

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

³ Hieronder worden verstaan alle op de te beoordelen verwerking van persoonsgegevens van toepassing zijnde wetten en regels, waarin bepalingen ten aanzien van de bescherming van persoonsgegevens zijn opgenomen.



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

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

Tot slot is het raadzaam eisen te stellen aan een zorgvuldige opdrachttuitvoering (opdrachtformulering, uitvoering, oordeelsvorming, rapportage en dossieropbouw).

3 Rol van de toezichthouder

3.1 Het kwaliteitsoordeel

Een kwaliteitsoordeel wordt afgegeven door een onderzoeker op basis van een uitgevoerd onderzoek en heeft betrekking op de kwaliteit van het stelsel van maatregelen en procedures gericht op het beschermen van persoonsgegevens over de gehele verwerking.

Het CBP moedigt het verkrijgen van een (positief) kwaliteitsoordeel over een verwerking van persoonsgegevens aan omdat de verantwoordelijke daarmee aan geeft belang te hechten aan de bescherming van de persoonsgegevens. Het feit dat een verantwoordelijke een verwerking van persoonsgegevens heeft laten beoordelen, betekent niet dat daarmee de bevoegdheid van het CBP tot het instellen van een onderzoek vervalt. In geval van twijfel aan de rechtmatigheid van een verwerking zal het CBP eigen onderzoek instellen. Het CBP kan in zijn toezichtsbeleid wel rekening houden met een afgegeven kwaliteitsoordeel.

Een (ambtshalve) onderzoek van het CBP heeft een andere scope, diepgang en doel en moet niet verward worden met een privacy-audit of compliance onderzoek. Het CBP voert geen compliance onderzoeken uit in het kader van zelfregulering zoals hier bedoeld en geeft geen kwaliteitsoordelen af.

3.2 Toezicht

Het CBP ziet toe op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Het CBP stimuleert zelfregulering van overheid en bedrijfsleven voor een adequate privacybescherming. Het CBP geeft daarmee aan zich te willen opstellen als tweedelijnsorganisatie. Die rol is alleen mogelijk indien de eerste lijn beschikt over kennis van zaken en zich bewust is van de eigen verantwoordelijkheid.



Het CBP heeft vanuit die visie de afgelopen jaren een tweetal projecten gestart:

- het ontwikkelen van producten in het kader van zelfregulering;
- het ontwikkelen van een systeem dat voorziet in een handreiking voor compliance onderzoeken.

In samenwerking met marktpartijen (accountantsorganisaties, adviesbureaus en beroepsorganisaties) is een viertal zelfreguleringsproducten ontwikkeld waarmee overheid en bedrijfsleven, zelfstandig of met behulp van een (externe) adviseur, kunnen nagaan hoe zij er voorstaan bij de implementatie en naleving van de privacywet- en regelgeving.

De WBP gaat uit van de eigen verantwoordelijkheid van overheid en bedrijfsleven voor een adequate privacybescherming en geeft de maatstaven daarvoor aan in een stelsel van rechten en verplichtingen. Een ander uitgangspunt van de WBP is dat de burger primair voor zijn eigen rechten moet opkomen. Die eigen verantwoordelijkheid aan beide kanten zal door het CBP worden gevoed door voorlichting, normontwikkeling en stimulering van 'privacyvriendelijke' technologieën in de vorm van Privacy-Enhancing Technologies (PET) en Privacy by Design (het meenemen van privacybeschermende maatregelen in de architectuurfase). Daarbij past het bevorderen van zelfregulering via gedragscodes en de aanstelling van een Functionaris voor de Gegevensbescherming (FG), die in de WBP een prominente plaats hebben gekregen.

Het gebruik van de bevoegdheden tot handhaving komt in deze benadering pas aan de orde indien andere middelen falen of ongeschikt blijken.