NIVRA

NOREA
de beroepsorganisatie van IT-auditors

Richtlijn 3600

Assurance-opdrachten met betrekking tot de bescherming van persoongegevens (Privacy-audits)

Juli 2006

Koninklijk Nederlands Instituut van Registeraccountants

Inhoudsopgave

Bijlagen

Inleiding

1. Deze Richtlijn heeft ten doel grondslagen vast te stellen en aanwijzingen te geven voor de uitvoering van assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy-audit).

2. Deze Richtlijn is een gezamenlijke richtlijn van het Nederlands Instituut van Registeraccountants (NIVRA)[1] en de Nederlandse Orde van Register EDP-auditors (NOREA) en is gebaseerd op:
   - De Gedrags en Beroepsregels voor Registeraccountants (GBR-1994) en de Richtlijnen voor assurance-opdrachten van het NIVRA;
   - De Gedrags en Beroepsregels voor Register EDP-auditors (GBRE) en de Richtlijnen in het kader van de Attestfunctie “Opdrachtformulering en –aanvaarding”, “Dossiervorming en –beheer” en “Rapportage” van de NOREA.

3. Deze Richtlijn is in eerste instantie gericht op de externe privacy-auditor aan wie het is voorbehouden of opgedragen een assurance-opdracht met betrekking tot de bescherming van persoonsgegevens uit te voeren met als doel het afgeven van een assurance-rapport voor het maatschappelijk verkeer (‘open verkeer’). Indien, op basis van deze richtlijn, een privacyonderzoek wordt uitgevoerd door interne privacy-auditors[2], mag het rapport uitsluitend voor interne doeleinden worden gebruikt en niet in het maatschappelijk verkeer worden gebracht.

4. Een privacy-audit heeft tot doel belanghebbenden, op basis van een door een privacy-auditor uitgevoerd onderzoek, zekerheid te verschaffen over de mate waarin het door een verantwoordelijke opgezet stelsel van maatregelen en procedures gericht op de bescherming van persoonsgegevens van een aangegeven verwerking, voldoet aan de eisen die zijn gesteld door de Wet bescherming persoonsgegevens (Wbp) en alle overige op de verwerking van persoonsgegevens van toepassing zijnde wet- en regelgeving.

Begrippen en definities

5. In deze richtlijn wordt verstaan onder:

   Betrokkene: degene op wie een persoonsgegeven betrekking heeft[3] [4].

   College bescherming persoonsgegevens (Cbp): Het college dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde[5].

   Opdrachtgever: degene die de opdracht tot het uitvoeren van een privacy-audit verstrekt. Meestal zal dit de “verantwoordelijke” zijn. Het kan echter zijn dat een andere partij opdrachtgever is.

   Privacy-audit: de werkzaamheden die in het kader van een assurance-opdracht, in opdracht van de opdrachtgever, door een privacy-auditor worden uitgevoerd teneinde belanghebbende zekerheid te verschaffen over de mate waarin het stelsel van maatregelen en procedures gericht op een aangegeven verwerking van persoonsgegevens van een verantwoordelijke, voldoet aan de eisen die gesteld worden door de Wbp en alle overige op de verwerking van persoonsgegevens bij de verantwoordelijke van toepassing zijnde wet- en regelgeving.

   Privacy-auditor: de Registeraccountant (RA) die optreedt als accountant in de zin van art. 2 lid1 GBR of de Register EDP-auditor (RE), die de eindverantwoordelijkheid draagt voor de uitvoering van een privacy-audit.

---

1 Deze Richtlijn geldt niet voor NOvAA-leden.

2 Hieronder worden ook begrepen auditors in dienst van de overheid.

3 Het recht op privacybescherming stoelt op de Grondwet artikel 10 en is verder uitgewerkt in de Wbp van 6 juli 2000. Deze wet is gebaseerd op de Europese Richtlijn 95/46/EG van 25 oktober 1995.

4 Wbp, art. 1

5 Wbp, art. 51

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt[6].

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder 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[7].

Normenkader (suitable criteria): de benchmarks die worden gebruikt voor het evalueren of toetsen van het object van onderzoek waaronder, voor zover van belang, die voor presentatie en toelichting. Criteria kunnen formeel of minder formeel zijn. Toepasbare criteria zijn noodzakelijk voor een redelijk consistente evaluatie of toetsing van het object van onderzoek binnen de context van vakkundige oordeelsvorming.

Invulling van een privacy-audit

6. Een privacy-audit kan zich richten op:
   - Het stelsel van maatregelen en procedures gericht op een specifiek aangegeven verwerking van persoonsgegevens;
   - een bestuursverklaring van de verantwoordelijke die aangeeft welke maatregelen en procedures (het stelsel) gericht op een specifiek aangegeven verwerking van persoonsgegevens door de verantwoordelijke zijn getroffen.

   Het stelsel van maatregelen en procedures omvat “de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen” [8]. Het gaat om één specifiek benoemde verwerking van persoonsgegevens;

7. Het onderzoek wordt afgerond met een assurance-rapport waarin een conclusie is opgenomen die met een redelijke mate van zekerheid aangeeft of:
   - de opzet en het bestaan op enige datum, danwel de werking van het stelsel van maatregelen en procedures gericht op de bescherming van persoonsgegevens van een aangegeven verwerking over een aangegeven periode heeft voldaan aan de eisen zoals opgenomen in het normenkader (paragraaf 12);
   - het gestelde in de bestuursverklaring juist is.

Opdrachtaanvaarding

8. **Bij de aanvaarding van een opdracht dient de privacy-auditor na te gaan of:**
   - **de desbetreffende verwerking van persoonsgegevens eenduidig is gespecificeerd en gemeld bij het Cbp.** Indien de verwerking van persoonsgegevens op grond van het Vrijstellingsbesluit Wbp niet behoeft te worden gemeld, is het noodzakelijk dat dit alsnog door de verantwoordelijke vrijwillig gebeurt bij het Cbp, zodat het object van onderzoek duidelijk en eenduidig is gedefinieerd en afgebakend;
   - **hij beschikt over de vereiste deskundigheid**

   In het geval dat het assurance-rapport bestemd is voor het maatschappelijk verkeer dient de privacy-auditor na te gaan of hij onafhankelijk is van de verantwoordelijke (paragraaf 3).

---

6 Wbp, art. 1
7 Wbp, art. 1
8 Wbp, art. 2

9. **De privacy-auditor dient de opdrachtvoorwaarden vast te leggen in een schriftelijke opdrachtbevestiging.** Onderwerpen die hierin minimaal moeten worden behandeld zijn:
   - De doelstelling van de opdracht;
   - De namen van de opdrachtgever en opdrachtnemer;
   - De verantwoordelijke;
   - De doelgroep;
   - Het object van onderzoek; de aangegeven verwerking van persoonsgegevens, inclusief de afbakening daarvan, zoals aan het Cbp (proforma) gemeld op grond van de Wbp artikel 27;
   - Een verwijzing naar de te gebruiken normstellingen en standaarden; zie paragrafen 2 en 12, of de desbetreffende bestuursverklaring;
   - De mate van zekerheid (redelijk);
   - De reikwijdte van het onderzoek;
   - De hoofdlijnen van de aanpak en aard van de werkzaamheden;
   - De afspraken met betrekking tot de eindrapportage;
   - Het feit dat de te verrichten werkzaamheden dienen te resulteren in een conclusie
   - De planning;
   - De privacy-auditor die verantwoordelijk is voor de uitvoering;
   - De kosten.

   Indien het assurance-rapport bedoeld is voor het maatschappelijk verkeer en gebruik zal worden gemaakt van het 'logo' of keurmerk:
   - Voorwaarden voor openbaarmaking;
   - Voorwaarden verbonden aan het gebruik van het 'logo' of keurmerk.

Deskundigheidseisen en het gebruikmaken van deskundigen

10. **De privacy-auditor dient te beschikken over:**
    a. voldoende kennis en ervaring op het terrein van ICT-controls;
    b. voldoende juridische en praktische kennis van de Wbp en overige relevante wet- en regelgeving.

11. Indien een privacy-auditor niet in voldoende mate beschikt over de vereiste kennis zoals aangegeven in paragraaf 10, kan hij gebruikmaken van deskundigen uit de eigen organisatie of van derden. **De privacy-auditor dient te allen tijde zelf over een zodanig algemeen inzicht te beschikken met betrekking tot de deskundigheidsgebieden ICT, IT-auditing en privacybescherming, dat hij zijn functie als privacy-auditor kan rechtvaardigen.**

Het normenkader

12. **De privacy-auditor dient bij zijn beoordeling normen te hanteren.** Deze zijn vastgelegd in de navolgende documenten[9]:
    - Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen;
    - Achtergrondstudies & Verkenningen nummer 23, "Beveiliging van Persoonsgegevens" uitgegeven door de Registratiekamer (nu CBP), gepubliceerd in 2001;
    - Raamwerk Privacy Audit, uitgegeven door het samenwerkingsverband Audit Aanpak, gepubliceerd in 2001 (hoofdstuk V);
    - Contouren voor Compliance, Handreiking bij het Raamwerk Privacy Audit, CBP 2005 (het hoofdstuk 3, V.I. t/m V.9)
    - De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes, jurisprudentie en publieke afspraken[10].

[9] Deze documenten zijn beschikbaar op de websites van het Cbp, het NIVRA en de NOREA.

[10] Voor een nadere toelichting zie "Contouren voor Compliance", V.I

Aanpak en uitvoering van de werkzaamheden

13. **De privacy-auditor dient bij de aanpak en de uitvoering van de werkzaamheden rekening te houden met:**
    - **de voor de beroepsgroep van toepassing zijnde gedrags en beroepsregels (zie paragraaf 2);**
    - **de aangegeven aanpak neergelegd in het "Raamwerk Privacy Audit" en de "Contouren voor Compliance, Handreiking bij het Raamwerk Privacy Audit" (hoofdstukken 2.2 t/m 2.5, 3.1 t/m 3.6, 3.7 en 3.8);**
    - **de in de opdracht vastgelegde specifieke punten.**

Oordeelsvorming

14. Bij het beoordelen van de toereikendheid van het stelsel van maatregelen en procedures gericht op een verwerking van persoonsgegevens vergelijkt de privacy-auditor de feitelijk aangetroffen situatie met het normenkader. **Bij de oordeelsvorming dient de privacy-auditor gebruik te maken van de guidance die is opgenomen in "Contouren voor Compliance, Handreiking bij het Raamwerk Privacy audit".** In deze handreiking is aangegeven welk gewicht moet worden toegekend aan geconstateerde afwijkingen en op welke wijze deze afwijkingen in de eindbeoordeling moeten meewegen.

Rapportering en openbaarmaking

15. **Een assurance-rapport dient te voldoen aan de voor de beroepsgroep van toepassing zijnde gedrags en beroepsregels (zie paragraaf 2) en minimaal de volgende elementen te bevatten;**
    - **Opschrift;**
    - **De geadresseerde;**
    - **De doelstelling van de opdracht;**
    - **De namen van de opdrachtgever en opdrachtnemer;**
    - **De verantwoordelijke organisatie;**
    - **Het object van onderzoek; de aangegeven verwerking van persoonsgegevens, inclusief de afbakening daarvan (opzet en bestaan of opzet, bestaan en werking), zoals aan het Cbp (proforma) gemeld op grond van de Wbp artikel 27;**
    - **Een verwijzing naar het gebruikte normenkader en de gebruikte richtlijnen; zie paragrafen 2 en 13;**
    - **De reikwijdte van het onderzoek;**
    - **De hoofdlijnen van de aard van de werkzaamheden;**
    - **De verantwoordelijkheden van de privacy-auditor.**
    - **De conclusie, inclusief toelichting;**
    - **De datering;**
    - **De naam en vestigingsplaats van de privacy-auditor.** Ondertekening met de eigen naam plus de naam van de organisatie van de privacy-auditor is toegestaan.

16. Onder verwijzing naar de "Contouren voor Compliance; Handreiking bij het Raamwerk Privacy audit", vormen aard en omvang van de geconstateerde afwijkingen de basis voor het uiteindelijke oordeel (professional judgement) van de privacy-auditor. Het af te geven oordeel kan slechts zijn:
    - Positief: Een positief oordeel houdt in dat de privacy-auditor tot het oordeel komt dat het beoordeelde stelsel voldoet aan het normenkader;
    - Negatief: Een negatief oordeel houdt in dat de privacy-auditor tot het oordeel komt dat het beoordeelde stelsel niet voldoet aan het normenkader.

    De privacy-auditor dient in de formulering van het oordeel tot uiting te laten komen of het om een positief of negatief oordeel gaat.

17. **In de formulering van een negatief oordeel dienen de woorden "voldoet niet aan het normenkader" te worden gebruikt.**

18. Op grond van een assurance-rapport met een positief oordeel bestemd voor het maatschappelijk

verkeer wordt de verantwoordelijke de mogelijkheid geboden – onder voorwaarden – een 'logo' of keurmerk te vermelden op het briefpapier, brochures en dergelijke, en op het openbaar deel van de website van de organisatie. De voorwaarden zijn opgenomen in "Gebruiksvoorwaarden en –reglement 'logo' of keurmerk (NAAM KEURMERK>", beschikbaar op de website van het NIVRA en NOREA. Toestemming voor het gebruik van het bedoelde 'logo' of keurmerk wordt door het NIVRA/NOREA verleend. Voor welke verwerkingen van persoonsgegevens toestemming is verleend voor het gebruik van het 'logo' of keurmerk is aangegeven in het door het NIVRA en de NOREA beheerd register "Gecertificeerde verwerkingen" dat beschikbaar is op www.nivra.nl en www.norea.nl.

Dossiervorming

19. **De dossiervorming van de uitgevoerde assurance-opdracht dient plaats te vinden in overeenstemming met de aanwijzingen zoals opgenomen Richtlijn 230 Dossiervorming of Register EDP-auditors (Richtlijn "Dossiervorming en -beheer").**

Bijlage 1

Voorbeeld van een assurance-rapport met betrekking tot de bescherming van persoonsgegevens

Aan: Opdrachtgever

Betreft: Assurance-rapport met betrekking tot de bescherming van persoonsgegevens

Opdracht
In gevolge uw opdracht <VERWIJZING NAAR DE OPDRACHT> hebben wij een onderzoek ingesteld naar de opzet en het bestaan van het stelsel van maatregelen en procedures gericht op de bescherming van de verwerking van persoonsgegevens <OMSCHRIJVING> die onder de verantwoordelijkheid van <NAAM ORGANISATIE> plaats vindt, zoals door de verantwoordelijke <NAAM ORGANISATIE> is gemeld aan het College bescherming persoonsgegevens onder Meldingsnummer <X>, naar de stand op <DATUM> . OPTIONEEL: Tevens hebben wij een onderzoek ingesteld naar de werking van dit stelsel over de periode van <DATUM> tot <DATUM>.

Werkzaamheden
Ons onderzoek heeft tot doel ten behoeve van belanghebbenden met een redelijke mate van zekerheid een oordeel te geven of het door organisatie <NAAM VERANTWOORDELIJKE> ingerichte stelsel van maatregelen en procedures gericht op de bescherming van persoonsgegevens van verwerking <X>, voldoet aan de eisen zoals vastgelegd in de navolgende documenten:

- Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen;
- Achtergrondstudies & Verkenningen nummer 23, “Beveiliging van Persoonsgegevens” uitgegeven door de Registratiekamer (nu Cbp), gepubliceerd in 2001;
- “Raamwerk Privacy Audit’, uitgegeven door het samenwerkingsverband Audit Aanpak, gepubliceerd in 2001;
- “Contouren voor Compliance, Handreiking bij het Raamwerk Privacy-Audit”, CBP 2005;
- De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes, jurisprudentie en publieke afspraken, te weten ……

Ons onderzoek is verricht in overeenstemming met de Richtlijn “Assurance-opdrachten met betrekking tot de bescherming van persoongegevens (Privacy-audits)”. In het kader van ons onderzoek zijn als de belangrijkste werkzaamheden uitgevoerd:

- Het verkrijgen van inzicht in de kenmerken van de organisatie en de branche waarin deze opereert, in relevante maatschappelijke issues en wet- en regelgeving;
- Het onderkennen van risico’s in de externe omgeving en organisatie zelf, en onderzoeken in hoeverre deze risico’s worden afgedekt door het beoordeelde stelsel;
- Het beoordelen van het stelsel in opzet en bestaan op basis van een uitgevoerde risico-analyse.
- Het wegen van de geconstateerde afwijkingen in relatie tot de eisen zoals opgenomen in het normenkader;

OPTIONEEL INDIEN OOK DE WERKING IS BEOORDEELD:

- Voor zover relevant voor onze beoordeling, het testen van de interne beheersmaatregelen op hun effectieve werking gedurende de beoordeelde periode.

Conclusie
Op grond van onze werkzaamheden concluderen wij dat de opzet en het bestaan van het stelsel van maatregelen en procedures gericht op de bescherming van de persoonsgegevens van verwerking <X> naar de stand <DATUM> heeft voldaan aan het normenkader. OPTIONEEL INDIEN OOK DE WERKING IS BEOORDEELD: Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de persoonsgegevens van verwerking <X> over de periode van <DATUM> tot <DATUM> heeft voldaan aan het normenkader.

Plaats, datum
Ondertekening

Bijlage behorend bij het assurance-rapport

Toelichting bij de conclusie

Ons onderzoek was gericht op het geven van een oordeel met een redelijke mate van zekerheid over het stelsel van maatregelen en procedures van een aangegeven verwerking. Incidentele inbreuken op het stelsel die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving behoeven daarom niet altijd te zijn geconstateerd. Het assurance-rapport heeft alleen betrekking op de met het meldingsnummer aangeduide verwerking van persoonsgegevens.

Wij kunnen niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures.

Hoewel het bij de beoordeling gehanteerde normenkader door het Cbp, in samenwerking met marktpartijen is opgesteld, mag een positief oordeel van de privacy-auditor niet worden uitgelegd als een positief oordeel van het Cbp.

Bijlage 2

Voorbeeld van een bestuursverklaring met betrekking tot de bescherming van persoonsgegevens

Bestuursverklaring met betrekking tot de bescherming van persoongegevens van verwerking <X>

Verantwoordelijkheid
De <NAAM VERANTWOORDELIJKE> is verantwoordelijk voor het opzetten en handhaven van een stelsel van maatregelen en procedures gericht op de bescherming van de verwerking van persoonsgegevens <OMSCHRIJVING> die onder de verantwoordelijkheid van <NAAM ORGANISATIE> plaats vindt, zoals door de verantwoordelijke <NAAM ORGANISATIE> is gemeld aan het College bescherming persoonsgegevens onder Meldingsnummer <X>, naar de stand op <DATUM> .

Het stelsel van maatregelen en procedures
Het stelsel van maatregelen en procedures is ontworpen om een redelijke mate van zekerheid te bieden dat de bescherming van de persoongegevens van verwerking <X>, onder verantwoordelijkheid van organisatie <NAAM VERANTWOORDELIJKE>, voldoet aan de eisen zoals vastgelegd in de navolgende documenten:

- Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen;
- Achtergrondstudies & Verkenningen nummer 23, “Beveiliging van Persoonsgegevens” uitgegeven door de Registratiekamer (nu Cbp), gepubliceerd in 2001;
- “Raamwerk Privacy Audit’, uitgegeven door het samenwerkingsverband Audit Aanpak, gepubliceerd in 2001;
- “Contouren voor Compliance, Handreiking bij het Raamwerk Privacy-Audit”, CBP 2005;
- De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes, jurisprudentie en publieke afspraken, te weten ……

Een stelsel van maatregelen en procedures, hoe goed ontworpen ook, bevat inherente beperkingen en kan derhalve alleen een redelijke mate van zekerheid bieden met betrekking tot het voldoen aan de eisen. Daarnaast kan de effectiviteit gedurende de tijd verschillen vertonen, bijvoorbeeld tengevolge van (tijdelijke of permanente) veranderingen of omstandigheden.

Bestuursverklaring
Wij bevestigen onze verantwoordelijkheid voor het stelsel van maatregelen en procedures zoals uiteengezet in de twee bovenstaande paragrafen. Wij hebben ons vergewist van de opzet en het bestaan van het stelsel. OPTIONEEL: de opzet, het bestaan en de werking van het stelsel.
Op grond daarvan verklaren wij dat – voor zover wij dat redelijkerwijze hebben kunnen constateren – de opzet en het bestaan van het stelsel van maatregelen en procedures gericht op de bescherming van de persoonsgegevens van verwerking <X> op <DATUM> heeft voldaan aan de gestelde eisen.
OPTIONEEL INDIEN OOK DE WERKING ONDERDEEL UITMAAKT VAN DE VERKLARING: Op grond daarvan verklaren wij dat – voor zover wij dat redelijkerwijze hebben kunnen constateren – het stelsel van maatregelen en procedures gericht op de bescherming van de persoonsgegevens van verwerking <X> over de periode van <DATUM> tot <DATUM> heeft voldaan aan de gestelde eisen.

Plaats en datum
Ondertekening door de verantwoordelijke

Bijlage 3

Voorbeeld van een assurance-rapport inzake een bestuursverklaring met betrekking tot de bescherming van persoonsgegevens

Aan: Opdrachtgever

Betreft: Assurance-rapport inzake een bestuursverklaring met betrekking tot de bescherming van persoonsgegevens

Opdracht
In gevolge uw opdracht <VERWIJZING NAAR DE OPDRACHT> hebben wij een onderzoek ingesteld naar de juistheid van de bijgevoegde bestuursverklaring met betrekking tot het stelsel van maatregelen en procedures gericht op de bescherming van persoongegevens van de verwerking <OMSCHRIJVING> die onder de verantwoordelijkheid van <NAAM ORGANISATIE> plaats vindt.

Het stelsel van maatregelen en procedures
Het stelsel van maatregelen en procedures is ontworpen om een redelijke mate van zekerheid te bieden dat de bescherming van de persoongegevens van verwerking <X>, onder verantwoordelijkheid van organisatie <NAAM VERANTWOORDELIJKE>, voldoet aan de eisen zoals vastgelegd in de navolgende documenten:

- Wet bescherming persoonsgegevens, de wet van 6 juli 2000, Staatsblad 302, houdende regels inzake de bescherming van persoonsgegevens, inclusief alle onderliggende besluiten en regelingen;Achtergrondstudies & Verkenningen nummer 23, “Beveiliging van Persoonsgegevens” uitgegeven door de Registratiekamer (nu Cbp), gepubliceerd in 2001;
- “Raamwerk Privacy Audit’, uitgegeven door het samenwerkingsverband Audit Aanpak, gepubliceerd in 2001;
- “Contouren voor Compliance, Handreiking bij het Raamwerk Privacy-Audit”, CBP 2005;
- De formeel van toepassing zijnde sectorale wetgeving, andere wetgeving, gedragscodes, jurisprudentie en publieke afspraken, te weten ……

Werkzaamheden
Ons onderzoek is verricht in overeenstemming met de Richtlijn “Assurance-opdrachten met betrekking tot de bescherming van persoongegevens (Privacy-audits)”. Volgens deze Richtlijn is ons onderzoek zodanig ingericht en uitgevoerd, dat een redelijke mate van zekerheid is verkregen dat het gestelde in de bestuursverklaring geen onjuistheden van materieel belang bevat. In het kader zijn als de belangrijkste werkzaamheden uitgevoerd:

- Het verkrijgen van inzicht in de kenmerken van de organisatie en de branche waarin deze opereert, in relevante maatschappelijke issues en wet- en regelgeving;
- Het onderkennen van risico’s in de externe omgeving en organisatie zelf, en onderzoeken in hoeverre deze risico’s worden afgedekt door het beoordeelde stelsel;
- Het beoordelen van het stelsel in opzet en bestaan op basis van een uitgevoerde risico-analyse.
- Het wegen van de geconstateerde afwijkingen in relatie tot de eisen zoals opgenomen in het normenkader.

OPTIONEEL INDIEN OOK DE WERKING IS BEOORDEELD:

- Voor zover relevant voor onze beoordeling, het testen van de interne beheersmaatregelen op hun effectieve werking gedurende de beoordeelde periode.

Conclusie
Op grond van onze werkzaamheden concluderen wij dat de bestuursverklaring van <NAAM ORGANISATIE> per <DATUM ONDERZOEK> juist is.

Plaats, datum

Ondertekening

Bijlage behorend bij het assurance-rapport

Toelichting bij de conclusie

Ons onderzoek was gericht op het geven van een oordeel met een redelijke mate van zekerheid over de juistheid van de bestuursverklaring met betrekking tot het stelsel van maatregelen en procedures van een aangegeven verwerking. Incidentele inbreuken op het stelsel die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving behoeven daarom niet altijd te zijn geconstateerd. Het assurance-rapport heeft alleen betrekking op de met het meldingsnummer aangeduide verwerking van persoonsgegevens.

Wij kunnen niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures en daarmee de juistheid van het gestelde in de bestuursverklaring.

Hoewel het bij de beoordeling gehanteerde normenkader door het Cbp, in samenwerking met marktpartijen is opgesteld, mag een positief oordeel van de privacy-auditor niet worden uitgelegd als een positief oordeel van het Cbp.

Koninklijk Nederlands Instituut van Registeraccountants

A.J. Ernststraat 55
Postbus 7984
1008 AD Amsterdam
T 020 301 03 01
E nivra@nivra.nl
I www.nivra.nl

de beroepsorganisatie van IT-auditors

A.J.Ernststraat 55
1083 GR Amsterdam
Tel: 020 - 3010 380
Fax: 020 - 3010 302
e-mail: norea@norea.nl
Internet: www.norea.nl