STAATSCOURANT

Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.

Nr. 252

30 december 2008

Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegevens voorschriften (Regeling periodieke audit politiegegegevens)

De Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie;

Gelet op artikel 6:5 van het Besluit politiegegevens;

Besluiten:

Artikel 1. Definities

In deze regeling wordt verstaan onder:
a. *wet:* de Wet politiegegevens.
b. *besluit:* het Besluit politiegegevens;
c. *verantwoordelijke:* de verantwoordelijke, bedoeld in artikel 1, onderdeel f, van de wet;
d. *privacy audit:* de audit, bedoeld in artikel 33 van de wet;
e. *auditinstelling:* het onderzoeksbureau dat is aangewezen om de privacy audit uit te voeren;
f. *auditor:* de medewerker van de auditinstelling die de privacy audit namens de auditinstelling uitvoert;
g. *auditee:* het regionaal politiekorps, het Korps landelijke politiediensten, de Rijksrecherche of de Koninklijke marechaussee, of het onderdeel daarvan, dat onderworpen wordt aan een audit;
h. *interne audit:* de interne audit, bedoeld in artikel 6:5, vijfde lid, van het besluit;
i. *interne auditor:* de voor het uitvoeren van een interne audit gekwalificeerde ambtenaar van politie bedoeld in artikel 1, onderdeel k, van de wet;
j. *hercontrole:* de hercontrole, bedoeld in artikel 33, derde lid, van de wet.

Artikel 2. Privacy audit (artikel 6:5, eerste lid)

1. De privacy audit wordt uitgevoerd door middel van een Electronic Data Processing (EDP) audit, ook wel IT-audit genoemd.

2. De privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee:
   a. de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
   b. de werking van de getroffen maatregelen en procedures.

3. De resultaten van de interne audits worden betrokken bij de privacy audit.

4. Indien de verantwoordelijke de toegang tot bepaalde gegevens wenselijk noch noodzakelijk acht voor een goede uitvoering van de privacy audit, kan hij de toegang daartoe weigeren, dan wel aan beperkende voorwaarden verbinden. De verantwoordelijke deelt de auditor schriftelijk en gemotiveerd zijn beslissing mede.

5. De resultaten van de privacy audit worden in een auditrapportage vermeld. De auditrapportage bevat ten minste:
   a. een beschrijving van de bij het uitvoeren van de audit gevolgde aanpak;
   b. een beschrijving van de resultaten van de privacy audit;
   c. het oordeel en de aanbevelingen van de auditor;
   d. indien uit de resultaten van de privacy audit blijkt dat niet of niet geheel wordt voldaan aan het bij of krachtens de wet bepaalde, de aanbeveling van de auditor inzake de uitvoering van een hercontrole door een externe dan wel interne auditor.

6. Na afronding van de privacy audit wordt de rapportage onverwijld aangeboden aan de verantwoordelijke.

Artikel 3. Interne audit (artikel 6:5, vijfde lid)

1. De verantwoordelijke draagt zorg dat, mede ter voorbereiding op de privacy audit, tenminste jaarlijks een interne audit plaatsvindt.

2. De interne audit wordt uitgevoerd door middel van een Electronic Data Processing (EDP) audit, ook wel IT-audit genoemd.

3. De interne audit heeft betrekking op één dan wel een aantal onderdelen van de wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee:
   a. de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
   b. de werking van de getroffen maatregelen en procedures.

4. De interne audit vindt plaats aan de hand van en overeenkomstig een auditplan. In het auditplan komen minimaal de volgende elementen aan de orde:
   a. het doel van de interne audit;
   b. de inhoud/object van de interne audit;
   c. de doorlooptijd van de interne audit;
   d. de onderzoeksinstrumenten die bij de interne audit worden ingezet en de bijdrage daarvan;
   e. de wijze waarop en de termijn waarbinnen wordt gerapporteerd;
   f. de beveiliging van de ten behoeve van de interne audit verzamelde informatie;
   g. de geheimhoudingsplicht waartoe een ieder die betrokken is bij een interne audit verplicht is;
   h. de aanbieding en verspreidingskring van de interne auditrapportage.

5. Indien de verantwoordelijke de toegang tot bepaalde gegevens noodzakelijk noch wenselijk acht voor een goede uitvoering van de interne audit, kan hij de toegang daartoe weigeren, dan wel aan beperkende voorwaarden verbinden. De verantwoordelijke deelt de interne auditor schriftelijk en gemotiveerd zijn beslissing mede.

6. De resultaten van de interne audit worden in een auditrapportage vermeld. De auditrapportage bevat minimaal:
   a. een beschrijving van de bij het uitvoeren van de audit gevolgde werkwijze;
   b. een beschrijving van de resultaten van de privacy audit;
   c. het oordeel en de aanbevelingen van de auditor.

7. Na afronding van de interne audit wordt de rapportage onverwijld aangeboden aan de verantwoordelijke.

Artikel 4. Hercontrole (artikel 6:5, vierde lid)

1. Indien bij het uitvoeren van de privacy audit tekortkomingen zijn geconstateerd stelt de verantwoordelijke binnen drie maanden een verbeterrapport op waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de geconstateerde tekortkomingen.

2. Op basis van het verbeterrapport vindt de hercontrole plaats. De hercontrole heeft alleen betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tekortkomingen zijn geconstateerd en heeft tot doel op systematische wijze te toetsen of door de verantwoordelijke zodanige maatregelen zijn getroffen dat aan de uitvoering van het onderdeel of de betreffende onderdelen van de wet thans op adequate wijze uitvoering is gegeven.

3. De hercontrole wordt uitgevoerd door een externe auditor indien de auditor daartoe heeft geadviseerd. In alle andere gevallen wordt de hercontrole door een interne auditor uitgevoerd.

4. De resultaten van de hercontrole worden in een rapportage vastgelegd.

5. Na afronding van de hercontrole wordt de rapportage onverwijld aangeboden aan de verantwoordelijke.

Artikel 5. De auditor (artikel 6:5, derde lid)

1. De auditor is ingeschreven als Register EDP-auditor bij de Nederlandse Orde van Register EDP-Auditors, dan wel bij een internationaal of Europees equivalent daarvan.

2. De auditor beschikt over gedegen en aantoonbare kennis en vaardigheden op het gebied van:
   a. de politieorganisatie;
   b. de informatievoorziening en processen van verwerking van politiegegevens;
   c. de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens, het Besluit politiegegevens en de Wet bescherming persoonsgegevens.

3. De auditor is onafhankelijk ten opzichte van de auditee.

4. De auditor is verplicht tot volledige geheimhouding van de informatie die hij in de loop van zijn auditactiviteiten verkrijgt, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht. Hij legt daartoe een geheimhoudingsverklaring af.

5. De functie van auditor kan worden voorgedragen voor aanwijzing als vertrouwensfunctie ingevolge artikel 3 van de Wet veiligheidsonderzoeken.

Artikel 6. De interne auditor

1. De interne auditor heeft een auditorenopleiding van de politie gevolgd.

2. De interne auditor beschikt over voldoende kennis en vaardigheden op het gebied van:
   a. geautomatiseerde informatiesystemen en methoden en technieken rond EDP/IT- auditing;
   b. de politieorganisatie;
   c. de informatievoorziening en processen van verwerking van politiegegevens;
   d. de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens, het Besluit politiegegevens en de Wet bescherming persoonsgegevens.

3. De interne auditor stelt zich onafhankelijk op ten opzichte van de auditee.

Artikel 7. Inwerkingtreding

Deze regeling treedt in werking met ingang van 1 januari 2009.

Artikel 8. Citeertitel

Deze regeling wordt aangehaald als: Regeling periodieke audit politiegegevens.

Deze regeling, met de daarbij behorende toelichting, zal in de Staatscourant worden geplaatst.

De Minister van Justitie,
E.M.H. Hirsch Ballin.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst.

De Minister van Defensie,
E. van Middelkoop.

TOELICHTING

1. Algemeen

Ter controle op de naleving van de bij of krachtens de Wet politiegegevens (Stb. 2007, 300) gegeven voorschriften, voorziet deze wet in een systeem van toezicht. Met behulp daarvan dient de verantwoordelijke na te gaan of de getroffen verwerkingsmaatregelen en -procedures en beleid in voldoende mate waarborgen dat de verwerking van politiegegevens conform de wettelijke normen geschiedt en, in het geval de resultaten van de uitgevoerde controles daartoe aanleiding geven, voor correctie dan wel aanpassing van de getroffen maatregelen en procedures te zorgen.

Artikel 33 van de Wet politiegegevens geeft de hoofdlijnen van het toezichtsysteem van de wet: de verantwoordelijke is verplicht tot het periodiek laten uitvoeren van privacy audits en, indien uit de controleresulaten van de privacy audits blijkt dat niet aan de wet wordt voldaan, van een hercontrole. Als toezichthouder op de wet ontvangt het College Bescherming Persoonsgegevens een afschrift van de controleresulaten. In artikel 6:5 van het Besluit politiegegevens (Besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens) zijn de auditcyclus en de inhoud van de privacy audits nader uitgewerkt. Volgens deze bepaling vindt eenmaal in de vier jaren een privacy audit plaats en heeft de controle betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures. Tevens voorziet artikel 6:5 van het besluit in de mogelijkheid dat, ter voorbereiding op de privacy audits, interne audits plaatsvinden. De verdere uitwerking van het toezichtstelsel geschiedt in deze regeling.

2. Artikelsgewijs

Artikel 2. Privacy audit

De privacy audit vindt eenmaal in de vier jaren plaats, zo mogelijk in het jaar voorafgaand aan het begin van een volgende cyclus in het kader van het Stelsel kwaliteitszorg binnen de politie. Op deze manier kunnen de resultaten van de privacy audit meegenomen worden bij de controles in het kader van kwaliteitszorg binnen de politie.

De verplichting van de verantwoordelijke tot het door middel van een privacy audit periodiek doen controleren van de uitvoering van de wet houdt in dat de verantwoordelijke tijdig opdracht verstrekt aan een auditinstelling om de privacy audit uit te voeren. Bij de selectie van de auditinstelling neemt de verantwoordelijke in acht de in deze regeling gestelde voorwaarden inzake werkwijze, deskundigheid en betrouwbaarheid waar de auditor aan dient te voldoen (artikel 5). Voorts is het van belang om vooraf zicht te hebben op de geraamde waarde van de opdracht. Immers, in het geval de geraamde waarde de zogenaamde door de Europese Commissie vastgestelde ‘drempelwaarde’ overschrijdt (zie Verordening 1422/2007waarbij de drempelwaarden recentelijk zijn gewijzigd en de Europese aanbestedingsrichtlijnen 2004/17/EG en 2004/18/EG), dient de verantwoordelijke de opdracht Europees aan te besteden. In voorkomend geval dient de verantwoordelijke er rekening mee te houden dat een Europese aanbestedingsprocedure overeenkomstig vaste termijnen en aan de hand van strakke kaders verloopt. Doorgaans neemt een dergelijke procedure 8 à 12 maanden in beslag. Naar het zich laat aanzien is de kans gering dat een opdracht ten behoeve van de uitvoering van de privacy audit, de desbetreffende Europese drempelwaarde zal overschrijden.

De privacy audit heeft, zoals gezegd, als doel te toetsen of, en in welke mate de organisatiestructuur en verwerkingsmaatregelen en -procedures in hun opzet, bestaan en werking aan de naleving van de wettelijke voorschriften bijdragen. Daarbij worden de gegevensverwerkingen beoordeeld op de naleving van de uit de wettelijke voorschriften voortvloeiende technische en juridische verplichtingen.

Bij de aanvang van de privacy audit maken de auditor en de verantwoordelijke afspraken over de doorlooptijd van de privacy audit en de termijn waarbinnen de auditrapportage afgerond en uitgebracht dient te worden. Voor het overige bedient de auditor zich, voor de aanpak en uitvoering van de privacy audit, van de EDP/IT-methode, waaronder begrepen de op de auditor toepasselijke reglementen en richtlijnen van de Nederlandse Orde van Register EDP-Auditors (NOREA).

De beoordeling geschiedt met behulp van de voor een EDP-audit – thans ook wel IT-audit genoemd – gebruikelijke onderzoeksinstrumenten, zoals mondelinge en/of schriftelijke enquêtes of vragenformulieren en interviews met daarvoor geselecteerde respondenten.
Daar de jaarlijkse interne audits door middel van dezelfde methodiek, de EDP/IT-methode, worden uitgevoerd als de privacy audit, kunnen de resultaten daarvan eenvoudig worden betrokken bij de privacy audit en kan de auditor de inhoud van de privacy audit afstemmen op die van de interne

audits. Aldus, indien uit de resultaten van de interne audits blijkt dat bepaalde aspecten van de gegevensverwerkingen verbetering behoeven, gaat de auditor na of deze inmiddels zijn doorgevoerd. Andersom: indien bepaalde verwerkingen in het kader van de interne audit(s) reeds voldoende zijn gecontroleerd en volgens de interne auditors niet aangepast dienen te worden, kan dit aanleiding zijn om deze verwerkingen in het kader van de privacy audit slechts beperkt te controleren.

De toetsing door de auditor vindt voorts plaats aan de hand van de toepasselijke regelgeving, de relevante (beleids)documenten, organisatiebeschrijvingen, werkinstructies en overige relevante documenten inzake de structuur en organisatie van de auditee enerzijds en aan de hand van de informatie die de verantwoordelijke, op grond van de zogenaamde protocolplicht, schriftelijk dient vast te leggen anderzijds. In artikel 32, eerste lid, van de Wet politiegegevens wordt bepaald welke gegevens door de verantwoordelijke dienen te worden vastgelegd. Dit betreft de doelen van verwerkingen op grond van artikel 9 (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) en artikel 13 (ondersteunende taken), de toekenning van autorisaties, de verstrekking van politiegegevens aan derden en de verwerkingen ten aanzien waarvan er aanwijzingen zijn voor onbevoegd of onrechtmatig gebruik en de geautomatiseerde vergelijking van politiegegevens met andere gegevens. In artikel 6:4 van het Besluit politiegegevens wordt de opsomming van artikel 32 van de wet nader uitgewerkt. In het tweede lid daarvan wordt voorts – in aanvulling op het in artikel 32 bepaalde, de verplichting neergelegd tot vastlegging van bepaalde gegevens rond de geautomatiseerde vergelijking en het in combinatie met elkaar verwerken van politiegegevens op grond van artikel 11, eerste, tweede, vierde en vijfde lid van de wet.
Met name voor de beoordeling van de werking in de praktijk van de getroffen verwerkingsmaatregelen en -procedures is de op grond van de protocolplicht vastgelegde informatie relevant. De auditor controleert de schriftelijke vastleggingen door middel van steekproeven.

Alhoewel de meeste verwerkingen van politiegegevens geautomatiseerd geschieden, worden ook handmatige handelingen met betrekking tot politiegegevens verricht. Ook deze verwerkingen dienen te worden meegenomen in de in het kader van de privacy audit te verrichten beoordeling.

Krachtens artikel 4, vijfde lid, van de Wet politiegegevens verstrekt de verantwoordelijke de auditor toegang tot de gegevensbestanden of datasystemen die onder zijn beheer worden verwerkt, voor zover de auditor deze behoeft voor de uitvoering van de privacy audit. Aangezien het voor een goede uitvoering van de privacy audit niet noodzakelijk is dat de auditor toegang krijgt tot alle politiegegevens maakt de voorliggende regeling het mogelijk om de toegang tot bepaalde gegevens te weigeren dan wel aan beperkende voorwaarden te binden. Deze beslissing is aan de verantwoordelijke voorbehouden. Als voorwaarde hiervoor geldt dat de toegang tot de gegevens noodzakelijk noch wenselijk wordt geacht. Hierbij kan worden gedacht aan gevoelige politiegegevens zoals gegevens betreffende informanten (zie artikel 12 van de wet) en andere door de Criminele Inlichtingeneenheid (CIE) verwerkte gegevens. De verantwoordelijke is verder gehouden zijn beslissing terzake schriftelijk en gemotiveerd mede te delen aan de auditor.

Het staat de auditor vrij om, in het belang van de privacy audit, voor bepaalde onderdelen of aspecten van de privacy audit een beroep te doen op (een) andere externe deskundige(n). Inschakeling van een dergelijke deskundige vindt plaats onder de verantwoordelijkheid van de auditor, in die zin dat hij in alle gevallen integraal verantwoordelijk blijft voor de kwaliteit van de onderzoeksresultaten en de auditrapportage.

Na afronding van het onderzoek stelt de auditor een auditrapportage op. De rapportage bevat minimaal vier onderdelen. In het eerste deel beschrijft de auditor de gevolgde aanpak en eventueel de opdracht en voornaamste aanbevelingen. In het tweede deel van het rapport beschrijft de auditor objectief en nauwkeurig (zo mogelijk per onderzocht onderdeel) de situatie zoals die is aangetroffen en de resultaten van zijn onderzoek. In het derde deel formuleert de auditor zijn oordeel inzake de naleving van de wettelijke voorschriften. Het oordeel van de auditor is gebaseerd op de onderzoeksresultaten. Daarnaast formuleert hij aanbevelingen betreffende de wijze waarop geconstateerde tekortkomingen weggenomen kunnen worden. Mochten de resultaten van het onderzoek daartoe aanleiding geven, geeft de auditor in het vierde deel een aanbeveling inzake de uitvoering van de hercontrole door een externe dan wel interne auditor.

Overeenkomstig het bepaalde in artikel 33, tweede lid, van de Wet politiegegevens wordt een afschrift van de auditrapportage gezonden aan het College Bescherming Persoonsgegevens.

Artikel 3. Interne audit

De verantwoordelijke dient jaarlijks een interne audit te laten uitvoeren. Aangezien de privacy audit eens in de vier jaren plaatsvindt, zullen binnen een auditcyclus minimaal drie interne audits moeten worden uitgevoerd. Wil de verantwoordelijke aan deze verplichting kunnen voldoen, dan zal dat een

belangrijke plaats moeten innemen in het beleids- en beheerscyclus van de desbetreffende organisatie. Tevens is het van groot belang dat de verantwoordelijke tijdig opdracht verstrekt aan de interne auditor om de interne audit uit te voeren.

De methodiek, werkwijze en doelstelling van de interne audit komen grotendeels overeen met die van de externe audit: de interne audit wordt uitgevoerd door middel van de EDP/IT-methode, maakt gebruikt van de voor een EDP/IT-audit gebruikelijke onderzoeksinstrumenten en vindt eveneens plaats aan de hand van de in deze toepasselijke regelgeving, relevante documenten inzake de structuur en organisatie van de auditee en de informatie die op grond van de protocolplicht schriftelijk is vastgelegd. Doelstelling van de interne audit is ook om te toetsen of de getroffen verwerkingsmaatregelen en -procedures in voldoende mate waarborgen dat de verwerking van politiegegevens conform de wettelijke normen geschiedt. Voorts, en behoudens gemotiveerde beslissing van de verantwoordelijke dat de toegang tot de gegevens noodzakelijk noch wenselijk wordt geacht, heeft de interne auditor, net als de externe auditor, toegang tot de gegevensbestanden of datasystemen voor zover hij deze behoeft voor de uitvoering van de interne audit. De resultaten van de interne audit worden verder in een rapportage vermeld welke – met uitzondering van het onderdeel inzake de uitvoering van een hercontrole – op gelijke wijze is opgebouwd als die betreffende de externe audit.

De interne audit vindt plaats aan de hand van een auditplan. Het auditplan, dat een jaar-, danwel een meerjarenplan kan zijn, is opgesteld door de interne auditor en dient ter voorbereiding op de audit. De verantwoordelijke stelt het auditplan vast. In het auditplan worden de belangrijkste elementen van de interne audit vastgelegd. Hierna wordt op een aantal daarvan ingegaan.

Het object

Anders dan de externe audit heeft de interne audit betrekking op één dan wel een aantal onderdelen van de te auditen wettelijke normen, en niet het geheel daarvan. De audit kan met andere woorden worden beperkt tot bepaalde categorieën verwerkingen, bijvoorbeeld de verwerkingen op grond van artikel 9 van de Wet politiegegevens (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) of op grond van artikel 13 (ondersteunende taken). Ook is het mogelijk om de interne audit te beperken tot een deel van de organisatie van de auditee. Wel is het de bedoeling dat, aan het einde van de vierjarige auditcyclus, de belangrijkste aspecten van de gegevensverwerkingen aan een interne audit zijn onderworpen. Indien nodig, kan ervoor worden gekozen om binnen de auditcyclus, bepaalde gevoelige verwerkingen niet één maar meerdere keren te laten controleren. Gelet op het bovenstaande is het van belang om van tevoren het object van de interne audit zo nauwkeurig mogelijk te beschrijven.

De doorlooptijd

Van tevoren dient een zo realistisch mogelijk inschatting te worden gemaakt van de tijd dat voor het uitvoeren van de audit noodzakelijk is. Het lijkt aangewezen om per onderdeel van de wet dat wordt gecontroleerd, een tijdsplanning te maken.

De wijze waarop en de termijn waarbinnen wordt gerapporteerd

Er worden afspraken gemaakt over de vraag of de interne auditor tussenrapportages zal uitvoeren inzake de voortgang van de interne audit, danwel volstaat met een eindrapportage. Het verdient voorts de voorkeur om een uiterste termijn af te spreken waarbinnen de rapportage afgerond dient te worden.

De beveiliging en geheimhouding

De informatie die tijdens de interne audit wordt verzameld dient vertrouwelijk te worden behandeld. Om de vertrouwelijkheid te garanderen worden van tevoren afspraken gemaakt over de wijze waarop tijdens de audit en na de afronding daarvan met de informatie wordt omgegaan. Anders dan voor de auditor het geval is, wordt van de interne auditor niet vereist dat hij een geheimhoudingsverklaring aflegt. Als ambtenaar van politie heeft de interne auditor immers reeds een ambtseed/belofte afgelegd. Daarnaast is hij krachtens artikel 7, eerste lid, van de Wet politiegegevens gehouden tot een geheimhouding wanneer hij de beschikking krijgt over politiegegevens.

Andere aspecten waarover in het auditplan afspraken kunnen worden gemaakt betreffen de ondersteuning van de interne auditor door een auditteam en de samenstelling daarvan, de personele en materiele kosten die met het uitvoeren van de audit zijn gemoeid.

Artikel 4. Hercontrole

Indien uit de resultaten van de privacy audit onverhoopt zou blijken dat de verwerking van politiegegevens op onderdelen niet voldoet aan de wettelijke normen, dient binnen één jaar een hercontrole te worden uitgevoerd op het of de onderdelen waar het resultaat onvoldoende voor was.
De hercontrole wordt door een externe dan wel een interne auditor uitgevoerd. Zo mogelijk vindt de hercontrole plaats tegelijkertijd met de eerste interne audit van de nieuwe auditcyclus.

Artikel 5. De auditor

Als belangrijkste voorwaarde voor de auditor geldt dat hij als Register EDP-auditor ingeschreven staat bij de beroepsorganisatie voor EDP/IT-auditors 'NOREA'. Bij NOREA ingeschreven Register EDP-auditors wordt een aantal verplichtingen opgelegd op het gebied van opleiding (postdoctoraal EDP/IT-auditing), ervaring (minimaal drie jaar relevante werkervaring) en permanente educatie. Daarnaast zijn Register EDP-auditors gebonden aan gedrags- en beroepsregels (waaronder regels inzake integriteit en objectiviteit), een tuchtregeling en richtlijnen over opdrachtaanvaarding, dossiervorming en rapportage. De betrouwbaarheid en deskundigheid van de auditor op het gebied van informatietechnololgie en -systemen kunnen met andere woorden worden ontleend aan zijn inschrijving als Register EDP-auditor bij NOREA. Dit is niet anders wanneer ingevolge een Europese aanbestedingsprocedure gekozen wordt voor een Europese auditinstelling cq. auditor. In de regeling is immers bepaald dat de auditor dan bij een Europees equivalent van NOREA moet zijn ingeschreven. De verantwoordelijke zal in een dergelijk geval zich ervan moeten vergewissen dat de desbetreffende beroepsorganisatie, vergelijkbare eisen stelt op het gebied van opleiding, ervaring, permanente educatie, integriteit en objectiviteit.

Buiten het voorgaande worden in de regeling eisen gesteld betreffende de specifieke voor het uitvoeren van een audit binnen de politieorganisatie vereiste kennis van de auditor: hij dient te beschikken over kennis en vaardigheden op het gebied van de informatievoorziening en processen van verwerking van politiegegevens, de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens, het Besluit politiegegevens en de Wet bescherming persoonsgegevens en uiteraard de politieorganisatie. Wat de betrouwbaarheid betreft is in de regeling de mogelijkheid opgenomen dat de functie van auditor voorgedragen wordt voor aanwijzing als vertrouwensfunctie. Het is aan de verantwoordelijke om te bepalen of, gelet op de concrete inhoud van de audit, een dergelijke voordracht nodig is.

Aangezien EDP/IT-auditors conform de zgn. EDP/IT-methode, en met behulp van de voor een EDP/IT-audit gebruikelijke onderzoeksinstrumenten te werk gaan, betekent dit voorts dat met de voorwaarde dat de auditor als Register EDP-auditor moet zijn ingeschreven, tevens de werkwijze van de auditor is bepaald. Om die reden wordt in de regeling niet nader ingegaan op dit aspect.

De auditor dient voorts onafhankelijk te zijn ten opzichte van de auditee. Als zodanig is van belang dat hij zich niet in laat met activiteiten die strijdig kunnen zijn met de onafhankelijkheid van zijn oordeel en dat hij vrij is van commerciële, financiële en andere druk die zijn oordeel zou kunnen beïnvloeden.

Tenslotte is de auditor krachtens artikel 7, tweede lid, van de Wet politiegegevens gehouden tot geheimhouding van de informatie die hij tijdens de audit verkrijgt. Om te waarborgen dat de auditor zich daadwerkelijk bewust is van deze verplichting en gelet op het belang daarvan, is in aanvulling op de bepaling van artikel 7 van de Wet politiegegevens, in de regeling vastgelegd dat de auditor een geheimhoudingsverklaring aflegt.

Artikel 6. De interne auditor

Op dezelfde wijze als voor de interne auditors in het kader van het Stelsel van kwaliteitszorg binnen de politie en de auditors informatiebeveiliging (Regeling informatiebeveiliging politie) het geval is, wordt door de politie voor de functie van interne auditor een auditorenopleiding ontwikkeld. Deze opleiding wordt ontwikkeld en verzorgd door de politie in overleg met de Koninklijke marechaussee en deze zal voor zowel ambtenaren van politie als van de Koninklijke marechaussee toegankelijk zijn. Teneinde te waarborgen dat alle voor beide organisaties belangrijke aspecten aan bod komen, wordt de inhoud van de opleiding in gezamenlijk overleg bepaald. Alleen ambtenaren van politie en van de Koninklijke marechaussee die de auditorenopleiding hebben gevolgd en met succes hebben afgerond, kunnen als interne auditors fungeren. Hiermee wordt gewaarborgd dat de interne auditor over de nodige kennis en vaardigheden beschikt op het gebied van informatietechnologie en -systemen en methoden en technieken rond de uitvoering van EDP/IT-audits. Daarnaast, net zoals voor de auditor geldt, worden in de regeling eisen gesteld betreffende de specifieke voor het uitvoeren van een audit binnen de politieorganisatie vereiste kennis van de interne auditor. Analoog aan het bepaalde in artikel 2:9 van het Besluit politiegegevens kunnen deze eisen, indien noodzakelijk, bij regeling van de Minister van

Justitie, de Minister van Binnenlandsze Zaken en Koninkrijksrelaties en de Minister van Defensie nader worden vastgesteld.

De interne auditor dient zich onafhankelijk op te stellen ten opzichte van de auditee. Zo mogelijk behoort hij daarom niet tot de auditee. Ten slotte zorgen de politie en de Koninklijke marechaussee voor het accuraat houden van een bestand van interne auditors waaruit ten behoeve van de interne audit gekozen kan worden.

De Minister van Justitie,
E.M.H. Hirsch Ballin.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst.

De Minister van Defensie,
E. van Middelkoop.