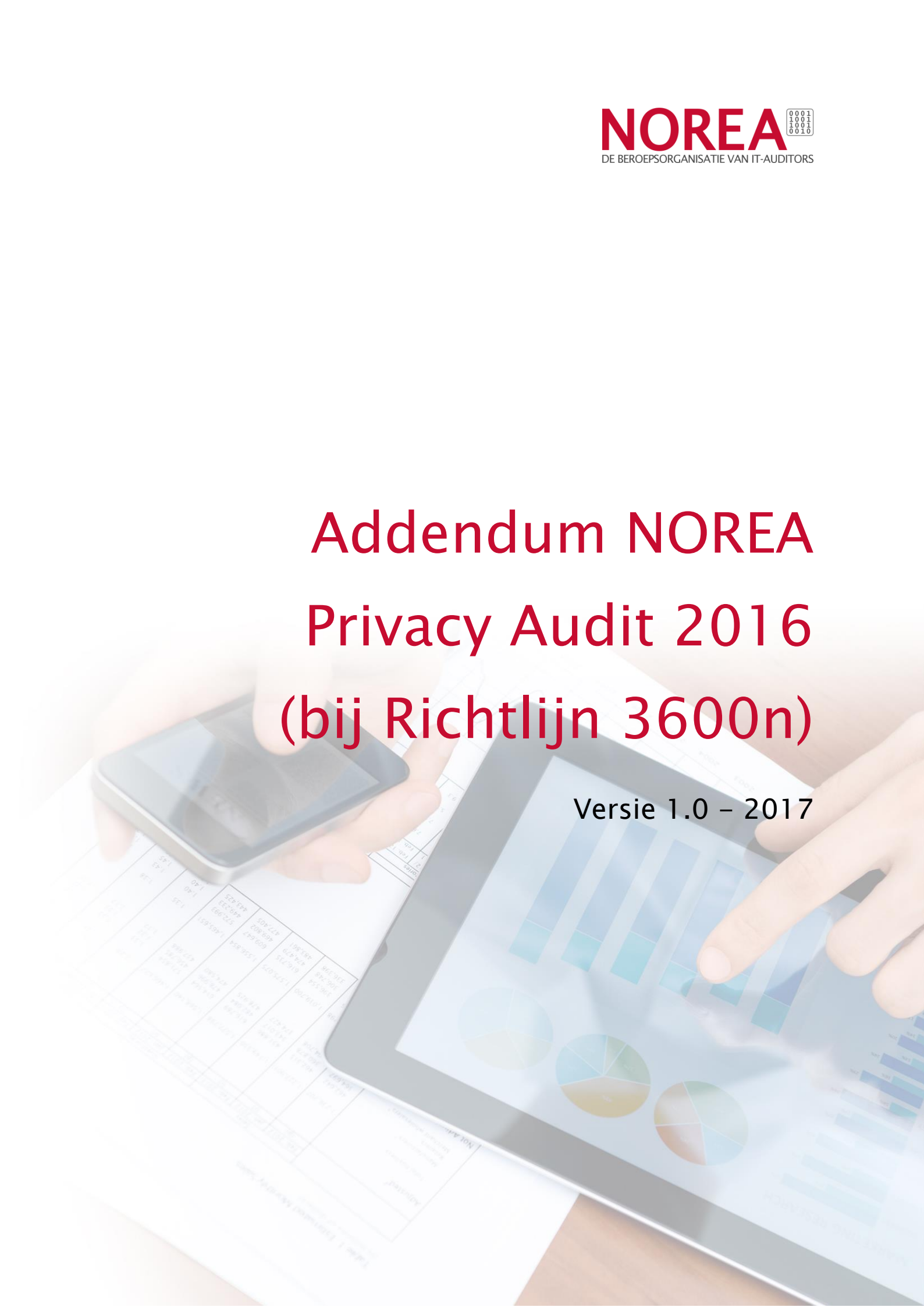
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Addendum NOREA Privacy Audit 2016 (bij Richtlijn 3600n)

Versie 1.0 – 2017



Inhoud

1 Introductie

De NOREA standaard 3600n wordt tot op heden gebruikt voor het uitvoeren van privacy audits. Na een positief oordeel, wat inhoudt dat de privacy-auditor tot het oordeel komt dat het beoordeelde stelsel voldoet aan het normenkader, wordt het keurmerk 'privacy audit proof' afgegeven door het NOREA. Er zijn momenteel (stand 2016) 5 organisaties die het 'privacy audit proof' certificaat mogen voeren, namelijk: stichting Bureau Krediet Registratie, Centraal Bureau voor de Statistiek, Liander, Nationaal Forensisch Instituut en de Rijksdienst Wegverkeer.

Het gebruik van de 3600n standaard is nader geanalyseerd vanwege het in werking treden van de meldplicht datalekken per 1 januari 2016 en de introductie van de Richtsnoeren Beveiliging van Persoonsgegevens door de AP, als opvolger van Achtergrondstudies en Verkenningen nr. 23 (AV-23). In dit addendum op NOREA standaard 3600n worden de uitkomsten van deze verschillenanalyse toegelicht en wordt beschreven hoe omgegaan dient te worden met deze wijzigingen.

2 Achtergrond huidige controleprotocol 3600n

Bij het uitvoeren van een privacy audit op basis van de huidige NOREA standaard 3600n dienen de volgende documenten als uitgangspunt gehanteerd te worden:

- 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 en verkenningen 23, Beveiliging van Persoonsgegevens (AV-23), Registratiekamer, 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.

De huidige beoordelingscriteria in bovenstaande documenten (en wetgeving) zijn ontoereikend om een beslissing op privacycertificering te kunnen onderbouwen. Hoewel de wijziging van de Wet bescherming persoonsgegevens formeel nog steeds de wet van 6 juli 2000 wordt genoemd, is een specifieke referentie naar de meldplicht datalekken gewenst. De Achtergrondstudies en verkenningen 23 is inmiddels vervallen en opgevolgd door de Richtsnoeren Beveiliging van Persoonsgegevens.

In de huidige praktijk worden deze tekortkomingen van de 3600n standaard opgelost door in de rapportage te vermelden welke aanpassingen er zijn gedaan aan het raamwerk om dit in lijn te brengen met de huidige standaarden en de wet- en regelgeving.

3 Verschillenanalyse AP Richtsnoeren en AV-23

In de Richtsnoeren wordt uitgelegd waarom afstand is genomen van AV-23. AV-23 schreef op basis van een risicoclassificatie beveiligingsmaatregelen voor. De risicoclassificatie was gebaseerd op de aard van de verwerkte persoonsgegevens in combinatie met de hoeveelheid verwerkte persoonsgegevens en de complexiteit van de verwerking. Een risicogerichte benadering, waarbij op basis van analyse van de risico's gericht beveiligingsmaatregelen worden getroffen, ontbrak. Als gevolg daarvan is AV-23, in ieder geval waar het gaat om concreet treffen van beveiligingsmaatregelen, in de loop der jaren steeds verder af komen te staan van de beveiligingspraktijk. In de Richtsnoeren Beveiliging van Persoonsgegevens heeft de AP gekozen voor een methodiek die aansluit bij de gangbare praktijk van de informatiebeveiliging en die verantwoordelijken de flexibiliteit biedt om passende beveiligingsmaatregelen te treffen.

In onderstaande tabel is een verwijzing opgenomen van de eisen vanuit de AP richtsnoeren naar AV-23. Wij merken nadrukkelijk op dat de tekst van AV-23 niet toereikend is, maar slechts nuttig kan zijn bij het formuleren van te treffen maatregelen.

ID	Eisen vanuit de AP richtsnoeren	Verwijzing AV-23
	Plan-do-check-act	
	1. Beoordeel de risico's 2. Maak gebruik van geaccepteerde beveiligingsstandaarden 3. Controleer en evalueer regelmatig	
	Beoordelen risico's	
	Schat de risico's voor beschikbaarheid, integriteit en vertrouwelijkheid in (laag, midden, hoog) op basis van 2 assen: Risico's voor betrokkenen en Risico's die de verwerking met zich meebrengt.	
1	**Informatiebeveiliging**	
1.1	Beleidsdocument voor informatiebeveiliging	4.1
1.2	Toewijzen van verantwoordelijkheden voor informatiebeveiliging	4.2
1.3	Beveiligingsbewustzijn	4.3
1.4	Fysieke beveiliging en beveiliging van apparatuur	4.5; 4.8
1.5	Toegangsbeveiliging (need to know / need to have)	4.7

ID	Eisen vanuit de AP richtsnoeren	Verwijzing AV-23
1.6	Logging en controle (activiteiten die worden uitgevoerd met persoonsgegevens, pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens)	4.1; 4,7; 4.10
1.7	Correcte verwerking in toepassingssystemen (controle op invoer, verwerking en uitvoer voldoen aan vooraf gestelde eisen)	4.6; 4.10
1.8	Beheer van technische kwetsbaarheden	4.6
1.9	Incidentenbeheer	4.1; 4.6
1.10	Afhandeling van datalekken en beveiligingsincidenten	4.1; 4.3; 4.6
1.11	Continuïteitsbeheer	4.6; 4.10; 4.13
2	**Geheimhouding**	
2.1	Beleid m.b.t. gegevensbescherming en geheimhouding van persoonsgegevens	4.3; 4.4
2.2	Geheimhoudingsovereenkomsten (intern & extern)	4.3; 4.4; 4.12;4.14
3	**Toepassing van PET**	
3.1	Encryptie (versleuteling) en hashing bij *verzending via internet, bij opslag op draagbare apparatuur, en op verwijderbare media*	4.5; 4.8
3.2	Omgang met e-waste (afgedankte apparatuur en opslagmedia)	4.12
4	**Controle op naleving**	
4.1	Controle op naleving van de maatregelen binnen de organisatie (procedureel), d.m.v. werkplekcontrols, social engineering tests	4.1
4.2	Controle op technische naleving (technische systemen) d.m.v. beoordeling van beveiligingsmaatregelen in toepassingssystemen (code review), tests van nieuwe en gewijzigde informatiesystemen, beveiligingsassessments	4.1
5	**Verwerking door een bewerker**	

ID	Eisen vanuit de AP richtsnoeren	Verwijzing AV-23
5.1	Bewerkersovereenkomst dient te bevatten: - Beveiligingseisen - Differentiatie van de verwerkte persoonsgegevens (welke eisen van toepassing op welke gegevens) - Dienstverlening door de bewerker - Betrouwbaarheidseisen van toepassing op de verwerking - Beveiliging door de bewerker - Transparantie over de beveiliging (inhoud en frequentie van rapportages, right to audit) - Transparantie over opgetreden beveiligingsincidenten - Verwerking door subbewerkers - Verwerking van persoonsgegevens buiten Nederland - Voorwaarden voor heronderhandeling of beëindiging van de overeenkomst	4.14
5.2	Toezicht op naleving: - Controle en beoordeling van de dienstverlening door bewerker - Beoordeling en afhandeling van beveiligingsincidenten en datalekken - Beheer van wijzigingen in de dienstverlening door de bewerker	4.14

4 Risicoanalyse op de gegevensverwerking

De organisatie die persoonsgegevens verwerkt dient voorafgaand aan de verwerking een analyse uit te voeren waarin de risico's van de verwerking worden vastgesteld. In de beschrijving van deze analyse wordt aangenomen dat er al eerder is vastgesteld dat er sprake is van een rechtmatige verwerking van persoonsgegevens.

Een dergelijke analyse kent een aantal stappen:

1. het inventariseren van de processen waarin persoonsgegevens worden verwerkt (artikel 1b Wbp);
2. het vaststellen van de aard van de persoonsgegevens in combinatie met de omvang en het gebruik. De evaluatie dient mede aan de hand van de Wbp plaats te vinden: gegevens die in de Wbp als bijzondere persoonsgegevens worden aangemerkt, leveren een hoger risico op (artikel 16 Wbp; zie paragraaf 3.1);
3. het inventariseren van de mogelijke vormen van onbevoegde of onzorgvuldige verwerking van de gegevens, zoals: verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking (art. 13 Wbp);

4. het bepalen van de risicoklasse. Dit is het product van de kans op ongewenste gevolgen en de schade die dit kan veroorzaken voor de betrokkene, de verantwoordelijke of de bewerker. Hierbij moet worden uitgegaan van situaties die redelijkerwijs te verwachten zijn.

De laatste stap van deze analyse, toegepast op persoonsgegevens, levert een risico op. De gevonden factor bepaalt de mate van risico van de gegevens. Het is de verantwoordelijkheid van de verwerkende organisatie om de risico's en de risicoklassen te bepalen. De gehanteerde risicoklassen volgen het model zoals destijds in Achtergrondstudies & Verkenningen 23 is opgezet of een vergelijkbaar door de organisatie gehanteerd model. Indien de organisatie een ander model hanteert, is het de verantwoordelijkheid van de privacy auditor om een vertaling te maken naar de risicoklassen zoals deze hier gehanteerd worden.

De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij die hogere risicoklasse:

- Risicoklasse 0 publiek niveau;
- Risicoklasse I basis niveau;
- Risicoklasse II verhoogd risico;
- Risicoklasse III hoog risico.

Risicoklasse 0 publiek niveau

Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. De persoonsgegevens behoeven ten aanzien van de vertrouwelijkheid van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Als gevolg van de Wbp worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld dan welke al noodzakelijk zijn voor een zorgvuldige bedrijfsvoering.

Risicoklasse I basis niveau

De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeids-relaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.

Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school – leerling, verhuurder – huurder, hotel – gast, vereniging – lid, organisatie – deelnemer.

Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan dient de beveiliging van persoonsgegevens tenminste te worden ondergebracht in risicoklasse II.

Risicoklasse II verhoogd risico

De uitkomst van de analyse toont aan dat de impact voor de betrokkene groter is bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De te nemen (informatie) beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basisniveau.

In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkene);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.

Soms moet de verwerking van bijzondere gegevens vanwege een hoge gevoeligheidsgraad in het maatschappelijk verkeer, bijvoorbeeld wanneer het gegevens over levensbedreigende ziektes betreft, ondergebracht worden in risicoklasse III.

Risicoklasse III hoog risico.

Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate grote impact voor de betrokkene dat het gerechtvaardigd is deze verwerking van persoonsgegevens in risicoklasse III te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen.

De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien

dit onzorgvuldig of onbevoegd geschiedt. Bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse.

Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse. Deze geheimhoudingsplicht kan zowel wettelijk of anderszins formeel zijn geregeld door de overheid of door een private organisatie zijn ingevoerd voor haar medewerkers.

In relatie tot de indeling van persoonsgegevens in risicoklassen, wordt ook in het kader van een bewuste omgang met die persoonsgegevens, gebruik gemaakt van markering. Markering is het aangeven van de risicoklasse die van toepassing is op de persoonsgegevens die op deze gegevensdrager zijn vastgelegd. De gegevensdrager wordt dus, indien technisch mogelijk, voorzien van een redelijkerwijs zichtbaar kenmerk dat aangeeft hoe de persoonsgegevens op die drager behandeld dienen te worden. Gegevensdragers zijn alle media waarin of waarop de persoonsgegevens kunnen worden vastgelegd, zoals papier, CD-ROM's, diskettes en tapes, schijven en intern geheugen.

De functie van markering is dat de risicoklasse van de persoonsgegevens direct zichtbaar is. Hierop dienen de maatregelen voor het bewaren en gebruik van de gegevensdragers te worden afgestemd. Markering van persoonsgegevens tot en met risicoklasse II is optioneel. Markering van de persoonsgegevens behorende bij risicoklasse III is noodzakelijk.

5 Aanvullend te toetsen maatregelen in het Raamwerk Privacy Audit

De AP richtsnoeren leiden tot de volgende aanvulling op het Raamwerk Privacy Audit.

- Meldplicht Datalekken.
- Binnen de organisatie zijn processen ingericht om meldingen te maken van datalekken. De organisatie dient te beschikken over een formeel vastgestelde procedure inzake de meldplicht datalekken. Daarnaast dient de organisatie een registratie bij te houden van alle gemelde incidenten omtrent datalekken.
- Voor een concreet controleprogramma verwijzen we naar de bijlage "Werkprogramma Meldplicht Datalekken"
- Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen van materiële omvang. Bij het uitvoeren van een risicoanalyse dient de impact van boetes te worden meegenomen.
- Voorts wordt benadrukt dat de Richtsnoeren meer aandacht vragen voor de kwaliteit van encryptie en het gebruik van Privacy Enhanced Technieken (PET).

- Tenslotte willen we ook de PIA noemen als instrument voor het bepalen van de impact van privacyrisico's van een project, in een vroeg stadium en op een gestructureerde en heldere manier.

6 Evaluatie van de geconstateerde afwijkingen

Bij het beoordelen van een verwerking van persoonsgegevens zal de privacy auditor een vergelijking maken tussen de norm en de aangetroffen situatie. Indien geen verschil wordt vast-gesteld, functioneert het (deel)object conform de norm. Indien verschillen worden aangetroffen maakt het toetsingskader onderscheid in drie situaties:

- Non-conformiteit;
- Deficiëntie;
- Incident.

Non-conformiteit

Een structurele (stelselmatige), materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van de persoonsgegevens van een of meer betrokkene(n) in ernstige mate is of kan worden geschaad.

Deficiëntie

Een structurele (stelselmatige), niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van persoonsgegevens van een of meer betrokkene(n) niet in ernstige mate is of kan worden geschaad.

Incident

Een incidentele, niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscode waardoor de bescherming van persoons-gegevens van een of meer betrokkene(n) niet in ernstige mate is of kan worden geschaad.

De privacy auditor kan afhankelijk van de specifiek aangetroffen situatie besluiten tot een op- of afwaardering van de ernst van de afwijking. Het onderscheid tussen een materiële en een niet-materiële tekortkoming wordt bepaald door de mate waarin de betrokkene geschaad wordt in de bescherming van zijn persoonlijke levenssfeer. Dit is ter beoordeling van de privacy auditor.

7 Tot slot

Tot slot wordt nog opgemerkt dat de Algemene Verordening Gegevensbescherming op 18 mei 2018 in werking treedt. Dat betekent dat organisaties en instellingen vanaf die datum aan deze Verordening moeten voldoen.

Bijlage: Werkprogramma Wet Meldplicht Datalekken