Bewaren en Bewijzen

Ministerie van Economische Zaken

ECP NL
Platform voor eNederland

Bewaren en Bewijzen

Een productie van:

Ministerie van Economische Zaken

Colofon

Dit is een uitgave van ECP.NL. Deze uitgave is een volledige herziening van de uitgave 'Bewaren en bewijzen' (1998) van ECP.NL en het Nederlands Normalisatie-Instuut (NEN).

Teksten
ECP.NL werkgroep Bewaren en Bewijzen: zie bijlage 5.

Eindredactie
Marjolijn Durinck, ECP.NL
Inge Aarts, ECP.NL

Ontwerp omslag en binnenwerk:
ECP.NL / Efficiënta Offsetdrukkerij bv

Druk
Efficiënta Offsetdrukkerij bv

ISBN
978-90-76957-21-0

© ECP.NL, maart 2007

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorgaande schriftelijke toestemming van de maker.
Alhoewel de auteurs en uitgever uiterste zorgvuldigheid betracht hebben bij het samenstellen van deze uitgave aanvaarden zij geen aansprakelijkheid voor schade van welke aard ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede) gebaseerd zijn op de in deze uitgave vervatte informatie.

Inhoudsopgave

		Inleiding	5
		Doel van deze brochure	5
		Doelgroep	6
		Opbouw	6
1		**Digitale gegevens**	7
	1.1	Gevolgen van digitalisering	7
	1.2	Selectie, classificatie, vernietiging en bewaring	7
	1.3	Kwaliteitseisen aan gegevens	8
	1.4	Open standaarden voor opslag	10
2		**Bewaren van gegevens**	12
	2.1	Voor welke gegevens geldt een wettelijke bewaarplicht?	12
	2.2	Welke gegevens mogen worden bewaard?	13
	2.3	Specifieke categorie gegevens: persoonsgegevens	14
	2.4	Specifieke wet: Achiefwet	15
	2.5	Bewaartermijnen	16
	2.6	Vernietiging	17
3		**Bewijskracht van digitale gegevens**	19
	3.1	De elektronische onderhandse akte	19
	3.2	De elektronische handtekening	20
	3.3	De bewijsovereenkomst	22
	3.4	De Trusted Third Party	22
4		**In de praktijk: Bewaar- & Beveiligingsbeleid**	25
	4.1	Beveiliging van gegevens	25
	4.2	Beleid, organisatie en proces: Bewaar- & Beveiligingsbeleid	26
	4.3	Bewaren: ISO 15489 - Record management	27
	4.4	Beveiligen: Code voor Informatiebeveiliging	29
	4.5	Organisatorische maatregelen	32

5 **De Leidraad** 33
5.1 Doel 33
5.2 De Leidraad 33

Notenlijst 37

Bijlage 1 Verjaringstermijnen 38

Bijlage 2 Bewaartermijnen 40

Bijlage 3 Vernietigingstermijnen 42

Bijlage 4 Checklist Leidraad 44

Bijlage 5 Deelnemers ECP.NL werkgroep Bewaren en Bewijzen 45

Notities 46

Inleiding

De hoeveelheid gegevens binnen een organisatie is enorm. Naast papieren informatiestromen spelen elektronische informatiestromen steeds vaker een rol. Op papier georiënteerde processen, alsmede complete papieren administraties worden in snel tempo gedigitaliseerd.
Nieuwe authenticatiemethoden, zoals de elektronische handtekening, maken elektronische transacties (op afstand) mogelijk. Waar voorheen een fysiek document voorzien van een handtekening nodig was om authenticiteit, integriteit en controleerbaarheid te waarborgen, kunnen nu met één druk op de knop over grote afstanden overeenkomsten rechtsgeldig tot stand komen. Een digitale informatiehuishouding heeft consequenties voor de gehele organisatie en roept tal van vragen op.

Doel van deze brochure
Het doel van deze brochure is helderheid verschaffen in de beleidsmatige en juridische eisen en aanbevelingen voor de (digitale) opslag van gegevens en de bewijskracht van deze gegevens. Daarnaast krijgt u praktische en organisatorische handvatten hoe u risico's kunt ondervangen en gegevens veilig en betrouwbaar kunt bewaren zodat de bewijskracht gewaarborgd blijft. Hiermee kunt u de bewijskracht van opgeslagen (digitale) gegevens binnen en van uw organisatie verhogen.

In deze brochure krijgt u antwoord op de vragen:
- Welke gegevens moet ik bewaren en voor hoe lang?
- Welke processen horen er bij (digitale) opslag van gegevens en waarom?
- Hoe kan ik de antwoorden op bovenstaande vragen praktisch organisatorisch implementeren?

Buiten de scope van deze brochure vallen technische implementatie en sectorspecifieke gegevens.

Doelgroep

Deze brochure richt zich op iedereen die in publieke en particuliere organisaties verantwoordelijk is voor het genereren, verwerken, bewaren en vernietigen van gegevens met het doel rechten en verplichtingen te kunnen aantonen en wettelijk bewijs te kunnen verschaffen. Dit zijn juristen, archivarissen, ICT-ers en controllers. Maar tot de doelgroep behoren ook bestuurders, managers en andere leidinggevenden, die verantwoordelijk gesteld kunnen worden voor de mogelijkheid of onmogelijkheid van hun organisatie zichzelf te verantwoorden voor hun handelen. Evenals hun adviseurs of controleurs, zoals accountants of toezichthouders.

Opbouw

In Hoofdstuk 1 wordt ingegaan op gegevens in digitale vorm, de consequenties van digitalisering en de risico's die digitalisering met zich kan brengen. Hoofdstuk 2 bevat een overzicht van de bewaarverplichting van diverse categorieën van gegevens. In Hoofdstuk 3 komt de bewijskracht van digitale gegevens aan de orde. Tenslotte krijgt u in Hoofdstuk 4 handvatten hoe u de risico's kunt ondervangen en gegevens veilig en betrouwbaar kunt bewaren zodat de bewijskracht gewaarborgd blijft. Hoofdstuk 5 bevat een praktische leidraad die u helpt bij de organisatorische implementatie van het bewaren van (digitale) gegevens zodat de bewijskracht gewaarborgd blijft.

1 Digitale gegevens

Door de komst van de informatietechnologie zijn en worden steeds meer processen binnen bedrijven en overheidsorganen (van klein tot groot) gedigitaliseerd. Daarbij worden steeds veranderende en nieuwe elektronische communicatiekanalen ingezet zoals webservices, e-mail, internet, sms of MSN. Hierdoor groeit de uitwisseling van digitale gegevens en kunnen zaken veelal ook efficiënter en effectiever worden afgehandeld. Denk aan online kopen en verkopen, online betalen en elektronisch factureren. Papier als drager van informatie begint langzaam te verdwijnen en maakt plaats voor gegevens in digitale vorm.

1.1 Gevolgen van digitalisering

Deze overgang heeft echter wel gevolgen. Net als in de papieren wereld blijft ook in de digitale wereld verantwoording belangrijk. Iedere publieke en particuliere organisatie dient zich te kunnen verantwoorden. Op grond daarvan is het bewaren (maar ook het vernietigen) van gegevens noodzakelijk. Bestuurders en managers van organisaties kunnen persoonlijk ter verantwoording worden geroepen als hun organisatie niet in staat is onderbouwd te verklaren welke handelingen zijn verricht en waarom. Governance, due diligence en compliance vereisen dat bestuurders en managers aandacht schenken aan het bewaren van gegevens. De consequenties van het niet voldoen aan die verwachtingen lopen uiteen van boetes en verlies van publiek vertrouwen tot imagoschade en persoonlijke aansprakelijkheid.

1.2 Selectie, classificatie, vernietiging en bewaring

Het selecteren, vernietigen, classificeren en bewaren van digitale gegevens is dan ook onontbeerlijk. Iedere organisatie moet weten waarvoor en waarom welke informatie van belang is. Om te voorkomen -ook uit oogpunt van kostenbesparing- dat uw organisatie een enorme hoeveelheid gegevens bewaart, moet u

afwegen wat wel of niet moet worden bewaard, voor hoe lang en wat tijdig moet worden verwijderd of vernietigd.

De gegevens van de meeste organisaties zijn veelal naar eigen behoefte en gebruik gedefinieerd, op eigen wijze vergaard en van een verschillende actualiteit. Dit leidt bij beheer en uitwisseling van deze gegevens tot een groeiende administratieve belasting en mogelijk dubbel werk.

Over welke gegevens hebben we het in deze brochure?
1. Over gegevens gegenereerd door een organisatie verrichte transacties of handelingen;
2. Over gegevens die voortvloeien uit bedrijfsfuncties en -activiteiten;
3. Over gegevens die bewaard blijven vanwege hun verantwoordings- c.q. bewijswaarde.

Het gaat dus in alle gevallen om gegevens die in relatie staan met de uitgevoerde bedrijfsprocessen.

1.3 Kwaliteitseisen aan gegevens

Ervan uitgaande dat opgeslagen gegevens bewijskracht moeten hebben, zijn waarborgen nodig. Deze waarborgen richten zich vooral op het realiseren van twee aspecten:
1. het waarborgen van de kwaliteit van de vastgelegde gegevens;
2. het waarborgen van de kwaliteit van het gegevensbeheer.

De gegevens dienen te voldoen aan een aantal kwaliteitseisen om aan wet- en regelgeving te kunnen voldoen. Deze kwaliteitseisen zijn *niet afhankelijk* van de gebruikte informatiesystemen en de gebruikte informatievoorziening en realiseren de *historiciteit* van gegevens. Dit betekent dat de gegevens kunnen worden gereconstrueerd zoals ze ooit, op een eerder moment in de tijd, zijn gegenereerd. Gegevens dienen te blijven zoals ze oorspronkelijk zijn vastgesteld. Het gaat dus om een zodanige

vastlegging (conversie, bewaring en selectie) dat de blijvende juistheid en volledigheid in alle omstandigheden gewaarborgd is en, indien gegevens in de processen zijn gewijzigd, achteraf kan worden vastgesteld wie, wanneer welke wijzigingen heeft aangebracht.

De historiciteit van gegevens wordt bepaald door:

- **de integriteit**: de mate waarin de gegevens en de weergaven van gegevens zijn zoals ze waren, waarbij niets ten onrechte is toegevoegd, verdwenen, achtergehouden of veranderd;
- **de authenticiteit**: de mate waarin, ongeacht de gebruikte compressiemethodiek, de weergaven van gegevens de juiste oorspronkelijk vorm en inhoud bevatten;
- **de controleerbaarheid**: de mate waarin de gegevens en de weergaven van gegevens toetsbaar zijn.

Voor de kwaliteit van het gegevensbeheer kunt u verschillende instrumenten als uitgangspunt nemen, alleen of (bij voorkeur) in combinatie met elkaar. Wij noemen hier:

1. de NEN-ISO-norm 15489 1: 2001 Informatie- en Archiefmanagement;
2. de NEN-ISO/IEC-norm 17799: 2005 Code voor Informatiebeveiliging;
3. de NEN-ISO/IEC-norm 27001: 2005 Managementsystemen voor informatiebeveiliging;
4. het CobiT-framework;
5. het ITIL-framework.

Gegevens moeten meermalen, onafhankelijk van tijd, kunnen worden samengesteld, met dezelfde inhoud, presentatievorm en samenhang als op het moment van ontstaan of ontvangst. Tegelijkertijd is het voor de bewijswaarde belangrijk dat de omstandigheden waarin de gegevens zijn bewerkt en afgehandeld bekend zijn. Gedurende de tijd dat de gegevens als bewijs gebruikt worden moet het mogelijk zijn om de omstandigheden te reconstrueren waarin ze zijn ontstaan, bewerkt, afgehandeld en beheerd.

Om de kwaliteit van gegevens en van het beheer te waarborgen en te toetsen is transparantie nodig. Om dit te realiseren is het volgende noodzakelijk:

1. een beschrijving van de procedure van digitale opslag, bewaring en weergave van de gegevens;
2. het gebruik van technologie die waarborgt dat aan de genoemde kwaliteitseisen wordt voldaan;
3. een systematische en volledige registratie van gegevens;
4. het systematisch bewaren en rangschikken van de gegevens;
5. het beschermen van de gegevens tegen iedere vervalsing (= ongeoorloofde mutatie);
6. het vastleggen van de volgende gegevens:
   a. de identiteit van de verantwoordelijke;
   b. de identiteit van de verwerkers van de gegevens;
   c. de aard van de gegevens;
   d. het onderwerp van de gegevens;
   e. de datum van verwerking en/of opslag van gegevens;
   f. de plaats van verwerking en/of opslag;
   g. eventuele storingen tijdens verwerking en opslag.
7. de vastlegging en controle van de bevoegdheden tot toegang tot en gebruik van de gegevens en de mate waarin deze bevoegdheden zijn beperkt en worden gehandhaafd;
8. de controle van de gegevens en de transparantie van het proces van gegevensverwerking en -opslag.

1.4 Open standaarden voor opslag

Uw opslagstrategie moet gericht zijn op het gebruik van internationale (open) standaarden. Lange tijd is dat in de praktijk niet zo eenvoudig geweest. Vooral niet voor gegevensopslag. Talloze bestandsformaten zijn gangbaar (geweest) en een groot aantal daarvan is vandaag de dag niet meer leesbaar (te maken). Buiten de algemene opslagformaten ASCII, EBCDIC en Unicode zijn er een paar specifieke bestandsformaten internationaal gestandaardiseerd. Dit zijn Open Document Format (ODF)[i], Tagged Image File Format/Image Technology TIFF/IT[ii] en de Portable Document Formatie (PDF)-familie[iii].

ODF, volledig op XML gebaseerd en een belangrijke standaard voor interoperabiliteit, heeft het nadeel dat zowel de methode van weergave als de inhoud van de gegevens (zonder software-controle) makkelijk muteerbaar blijft. Hierdoor kan in principe niet voldaan worden aan de kwaliteitseisen van integriteit, authenticiteit en controleerbaarheid. Het formaat is dan ook (net als andere op XML-gebaseerde bestandsformaten, zoals Office Open XML) onbruikbaar in bewijsrechterlijke zin, aangezien de oorspronkelijke methode van weergave, inhoud en samenstelling daarbij een belangrijke rol spelen. Zowel TIFF/IT als PDF/A zijn in die zin de meest geëigende bestandsformaten voor gegevensopslag.

Ook voor de inrichting van metagegevens kunt u gebruikmaken van internationale standaarden: ISO/IEC 15836: 2003 en ISO/IEC 23081-1: 2006. Indien u gebruikmaakt van compressie zal de gebruikte methode de oorspronkelijke methode van weergave van die gegevens die van bewijsrechterlijk belang zijn, moeten kunnen reproduceren.

Bij het bewaren van gegevens is het altijd noodzakelijk dat in gebruik (geweest) zijnde opslagformaten leesbaar blijven of leesbaar gemaakt kunnen worden. Dit impliceert dat interfaces om dergelijke formaten te lezen beschikbaar moeten zijn, mits de mutatie ervan onmogelijk gemaakt wordt.

2 Bewaren van gegevens

Uw organisatie bewaart gegevens om zich te kunnen verantwoorden over het handelen en/of omdat deze gegevens kennis en ervaring bevatten die op bepaalde wijze duurzaam toegankelijk moeten blijven voor uw organisatie en soms ook voor derden. Verder kunnen deze gegevens van belang zijn voor de ontwikkeling en het beleid van uw organisatie en de implementatie van dat beleid. Sommige gegevens worden bewaard omdat zij vanwege hun cultuurhistorische waarde niet verloren mogen gaan. Denk bijvoorbeeld aan oude manuscripten en beeldmateriaal van bijzondere gebeurtenissen. Andere gegevens worden bewaard omdat ze kunnen aantonen dat aan een bepaalde verplichting is voldaan, bijvoorbeeld in het geval van een contractuele relatie. En soms worden gegevens bewaard, simpelweg omdat een bepaalde wettelijke bewaarplicht dient te worden nageleefd.
Bewaring van gegevens kan dus op grond van uiteenlopende redenen relevant zijn, zowel in juridisch als in bedrijfsmatig opzicht.

2.1 Voor welke gegevens geldt een wettelijke bewaarplicht?

Uw organisatie is wettelijk verplicht administratie te voeren van haar vermogenstoestand en haar werkzaamheden, naar de eisen die voortvloeien uit deze werkzaamheden. Ook de daartoe behorende boeken, bescheiden en andere gegevensdragers moeten worden bewaard. Op deze manier bestaat er altijd inzicht in:

1. **de rechten en verplichtingen van de organisatie**. De crediteuren- en debiteurenpositie en de vermogenspositie moet op elk moment snel inzichtelijk zijn of gemaakt kunnen worden. De administratie dient niet alleen de financiële resultaten van de organisatie te omvatten, maar ook de vastlegging van bestuurs- en beheersdaden, de interne organisatie in het algemeen, het interne berichtenverkeer en al wat daarmee samenhangt (algemene administratieverplichting)[iv].
2. **de gegevens die voor de heffing van belasting van belang zijn** (fiscale bewaarplicht)[v]. De administratie dient

aan de eisen van het bedrijf te voldoen. Daarbij moet rekening gehouden worden met de aard, omvang en ingewikkeldheid van de bedrijfsactiviteiten en de toegepaste administratieve techniek.

3. **de gegevens die voor de heffing van de rechten bij invoer van belang zijn**[vi].

Hoe moeten deze gegevens worden bewaard?
Bij een belastingcontrole moeten de gegevens van uw organisatie binnen redelijke termijn toegankelijk en controleerbaar zijn. In principe moet u de gegevens in *originele vorm* bewaren.

Slechts onder bepaalde voorwaarden mogen gegevens worden geconverteerd. Van conversie is bijvoorbeeld sprake als u een papieren administratie invoert in de computer, papieren facturen inscant of bestanden uit de computer overzet op microfiche. Van conversie is ook sprake als u van het ene computersysteem overgaat op een ander. Maar conversie is alleen toegestaan als:

- u alle gegevens overzet;
- u de gegevens inhoudelijk juist overzet;
- de nieuwe gegevensdrager tijdens de gehele bewaartermijn beschikbaar is;
- de geconverteerde gegevens binnen redelijke tijd ge(re)produceerd en leesbaar gemaakt kunnen worden;
- controle van de geconverteerde gegevens binnen redelijke tijd kan worden uitgevoerd;
- u de uitkomsten van de interne controle bewaart.[vii]

2.2 Welke gegevens mogen worden bewaard?

Naast de informatie die u verplicht moet bewaren, is het vanuit bewijsrechtelijk oogpunt aan te bevelen daarnaast ook andere gegevens te bewaren. In geval van een geschil kan het van belang zijn dat u behalve over een contract tevens over gegevens beschikt die inzicht geven in hoe het contract tot stand is gekomen. Daarbij speelt de wettelijke verjaringstermijn een rol. De algemene verjaringstermijn is twintig jaren tenzij de wet anders bepaalt[viii]. Voor een aantal in de wet genoemde rechtsvorderingen is de bewaartermijn vijf jaren[ix]. Na het verjaren van

deze termijnen is het bewaren van deze gegevens niet meer noodzakelijk.

In bijlage 1 vindt u een tabel met de belangrijkste verjaringstermijnen.

2.3 Specifieke categorie gegevens: persoonsgegevens

Persoonsgegevens vormen een specifieke categorie van gegevens die u vanuit bedrijfsmatig oogpunt bewaart of vernietigt. Omdat hierbij de privacy van degene van wie u de gegevens bewaart een rol speelt, gelden hier aparte voorschriften. Deze zijn te vinden in de **Wet bescherming persoonsgegevens**.

De Wet bescherming persoonsgegevens (Wbp) geldt voor de verwerking van gegevens van 'natuurlijke personen'. Op hoofdpunten kunnen we de Wbp samenvatten in enkele eisen die aan gegevensverwerking worden gesteld. Deze eisen zijn gericht aan de 'verantwoordelijke', ofwel de persoon of instantie die de verantwoordelijkheid draagt voor de gegevensverwerking.

(a) **Zorgvuldigheid**. De eerste eis betreft de zorgvuldigheid van de gegevensverwerking. Deze dient in overeenstemming met de wet en behoorlijk en zorgvuldig te gebeuren.
(b) **Grondslag voor de verwerking**. Persoonsgegevens mogen alleen worden verwerkt als hier een grondslag voor bestaat die duidelijk, uitdrukkelijk omschreven en gerechtvaardigd is. Grondslagen voor de verwerking zijn:
- de ondubbelzinnige toestemming van de persoon van wie de gegevens zijn;
- de noodzakelijkheid van gegevensverwerking voor het uitvoeren van een overeenkomst waarbij de betrokkene partij is;
- de behartiging van het gerechtvaardigde belang van de verantwoordelijke.

(c) **Doelbinding**. Persoonsgegevens mogen niet worden ver-

werkt op een wijze die onverenigbaar is met de doeleinden van de originele verkrijging. Met andere woorden: persoonsgegevens die met het oog op een bepaald doel zijn verzameld, mogen niet voor een ander doel gebruikt worden. Voorbeeld: het UWV mag geen gegevens uit de cliëntenadministratie verstrekken aan een deurwaarder.

(d) **Kwaliteit**. Persoonsgegevens mogen slechts worden verwerkt indien zij met het oog op het doel van de verwerking toereikend, ter zake dienend en niet bovenmatig zijn. Daarnaast moeten de gegevens juist en nauwkeurig zijn.

(e) **Beveiliging**. Wanneer persoonsgegevens worden verwerkt, dan dient de organisatie te zorgen voor een adequate beveiliging. Alle relevante delen van de gebruikte informatiesystemen moeten beveiligd zijn.

2.4 Specifieke wet: Achiefwet

Als uw organisatie valt onder de werking van de **Archiefwet 1995** (overheidsorganen) en daarmee samenhangende regelgeving, dan zijn er een aantal aanvullende eisen gesteld voor het bewaren van digitale gegevens die voor blijvende bewaring in aanmerking komen. Deze aanvullende eisen vragen vastlegging van:

1. inhoud, structuur en vorm van de gegevens bij ontstaan;
2. het moment waarop de gegevens zijn opgemaakt of ontvangen;
3. de taak waarop de gegevens betrekking hebben;
4. de samenhang met de andere ontvangen en opgemaakte gegevens;
5. een actueel, compleet en logisch samenhangend overzicht van de bij een overheidsorgaan berustende gegevens en de bestanden waarin deze bewaard worden;
6. gegevens over de gegevens bij ontstaan of ontvangst, waarbij minimaal worden vastgelegd: onderwerp, werkproces, afzender, datum en nummer;
7. het gebruikte standaardformaat bij het opslaan (uiterlijk bij overbrenging) van de gegevens;
8. de functionele eisen voor vorm, structuur en inhoud;
9. de volgende gegevens:
   a. de benaming van de toepassingsprogrammatuur waarmee de gegevens zijn ontvangen en opgemaakt, inclusief het versienummer;

b. de beschrijving van het platform, met naam en versie/type, van de besturingsprogrammatuur en de apparatuur;
c. de documentatie die aangeeft hoe de toepassingsprogrammatuur heeft gewerkt met inbegrip van de nieuwere versies;
d. een beschrijving van de opgeslagen bestanden die ten minste de volgende gegevens omvat:
   1. de naam van het overheidsorgaan dat de gegevens heeft ontvangen en opgemaakt en de benaming van het werkproces waarbinnen deze zijn ontvangen en opgemaakt;
   2. de benaming en omvang van elk opgeslagen bestand;
   3. een specificatie van de gegevens met begin- en einddatum;
   4. de relatie met andere bestanden;
   5. het opslagformaat;
   6. in voorkomende gevallen de toegepaste compressiemethode;
   7. de datum en het tijdstip van de opslag van het bestand op de gegevensdrager;
   8. in geval van een database: de documentatie over de structuur, die tenminste een compleet logisch datamodel met beschrijving van de entiteiten omvat.

Voor organisaties waar de Archiefwet 1995 op van toepassing is, is vervanging van gegevens mogelijk: gegevens mogen worden vervangen door substituten op andere dragers dan de oorspronkelijke.[x] Het kan dan gaan zowel om gegevens die op termijn vernietigbaar zijn als om gegevens die voor blijvende bewaring in aanmerking komen. De oorspronkelijke gegevens kunnen na substitutie worden vernietigd. Vervanging kan alleen plaatsvinden met behoud van *juiste en volledige weergave* van de gegevens.

Volgens het Archiefbesluit 1995 moet de vervanging van gegevens in een besluit vastliggen. Is er sprake van gegevens die voor blijvende bewaring in aanmerking komen, dan is machtiging van de betrokken minister of van Gedeputeerde Staten vereist. In beide gevallen moet u melding maken van hoe aan onderstaande twee voorschriften is voldaan:

1. De ingeschakelde deskundigen zijn bij de voorbereiding betrokken.

2. Er is rekeninggehouden met de taak van het overheidsorgaan, de waarde van de gegevens als cultureel erfgoed en het belang van de gegevens voor bedrijfsvoering, recht- en bewijszoekenden en historisch onderzoek.

Een machtiging tot vervanging is tot nu toe slechts eenmaal verstrekt[xi]. Vervanging vereist een volledig gecontroleerde omgeving, waarin de kwaliteitseisen die aan gegevens worden gesteld aantoonbaar worden gegarandeerd. Dat vereist een kwaliteitssysteem waarbinnen voortdurend sprake is van toetsing en verbetering.

2.5 Bewaartermijnen

Voor het bewaren van bepaalde gegevens gelden bepaalde bewaartermijnen. Het bepalen van deze bewaartermijnen vindt plaats met in acht neming van alle mogelijke (wettelijke) belangen. Het is belangrijk om hierbinnen te analyseren welke gegevens kunnen worden onderscheiden en welke bewaartermijnen daaraan zijn gekoppeld.

We kunnen onderscheid maken tussen bewaartermijnen voor de gegevens die noodzakelijk zijn voor vaststelling van fiscale verplichtingen en voor de gegevens van ander belang (intern, juridisch, historisch). Dit onderscheid is beschikbaar in:

1. de selectielijst opgesteld door de Nederlandse Vereniging van Bedrijfsarchivarissen (NVBA) voor particuliere bedrijven[xii].
2. de selectielijsten archiefbescheiden die op basis van de Archiefwet 1995 zijn vastgelegd voor rijks-, provinciale en (inter-)gemeentelijke organen.

In bijlage 2 vindt u een tabel met de belangrijkste bewaartermijnen.

2.6 Vernietiging

Gegevens uit de administratie

Administratieve gegevens moet u zeven jaar bewaren (zie bijla-

ge 2). In overleg met de Belastingdienst is het mogelijk bepaalde gegevens, die buiten de basisadministratie vallen, eerder te vernietigen. Hiervoor moet u afspraken maken met de Belastingdienst over:

1. welke gegevens voor de fiscale controle bewaard moeten blijven;
2. de invulling van de wettelijke begrippen 'leesbaar binnen een redelijke tijd' en 'controle binnen redelijke termijn';
3. de wijze waarop de gegevens benaderbaar gemaakt worden;
4. de wijze waarop de gegevens ter beschikking gesteld worden;
5. het verdichten van gegevens;
6. de invloed van systeemwijzigingen.

Geconverteerde gegevens

Als u controleerbaar aan de eisen van conversie voldoet (zie par. 3.2.1), hoeft u na een conversie de originele gegevens niet te bewaren en mag u ze vernietigen. Alleen de balans en de resultatenrekening moet u altijd op papier bewaren.

Persoonsgegevens

U mag persoonsgegevens niet langer bewaren dan noodzakelijk is voor het uitvoeren van het vooraf gespecificeerde doel. Als er voor de verwerking geen doel meer is, mag u de verzamelde gegevens niet bewaren. Dat impliceert dat u de gegevens moet vernietigen als het specifieke doel waarvoor ze werden verzameld, vervallen is.

Archiefwet

De bewaartermijnen die in de selectielijsten van de Archiefwet zijn opgenomen zijn *verplichtend* voor de overheidsorganen die vallen onder deze wet. Dat betekent dat na het verstrijken van de genoemde bewaartermijn vernietiging van de betrokken gegevens *moet* plaatsvinden.

In bijlage 3 vindt u een overzicht van de belangrijkste vernietigingstermijnen.

3 Bewijskracht van digitale gegevens

Wanneer twee partijen verwikkeld zijn in een geschil, dan kan dat leiden tot een juridische procedure. Partijen zullen dan voor de rechter hun stellingen aannemelijk moeten maken met bewijsmiddelen. Als hoofdregel geldt hierbij dat partijen met behulp van alle mogelijke middelen bewijs kunnen leveren. Dit is de zogenaamde *vrije bewijsleer*[xiii]. Partijen kunnen alle middelen gebruiken om iets te bewijzen, maar het is uiteindelijk de rechter die bepaalt wat er nou eigenlijk worden bewezen. Indien een partij kan aantonen dat de digitale gegevens die hij als bewijs aanlevert, op een betrouwbare wijze zijn vergaard en bewaard, dan kan de rechter hier uiteraard meer belang aan hechten dan aan digitale gegevens waarvan zulke garanties niet kunnen worden afgegeven.

In juridische procedures tussen civiele partijen kan een partij *dwingend bewijs* produceren. Dwingend bewijs houdt in dat de rechter verplicht is de inhoud van bepaalde bewijsmiddelen als waar aan te nemen, dan wel verplicht is de bewijskracht te erkennen die de wet aan bepaalde gegevens verbindt[xiv]. In de eerste plaats kan dwingend bewijs worden geproduceerd door middel van een *onderhandse akte*. Een onderhandse akte kan ook op elektronische wijze worden geproduceerd, hoewel de wijze waarop dat dient te geschieden nog niet geheel duidelijk is. In de tweede plaats kunnen partijen door middel van een *bewijsovereenkomst* afspreken dat een bepaald bewijsmiddel wordt uitgesloten of dat bepaald bewijs tot dwingend bewijs wordt bestempeld.

3.1 De elektronische onderhandse akte

Zoals gezegd kan dwingend bewijs worden geleverd met behulp van de onderhandse akte. Hoe deze akte op elektronische wijze kan worden vormgegeven, daar heeft de wetgever helaas nog onvoldoende over nagedacht. De wetgever heeft echter wel nieuwe wetgeving aangekondigd[xv]. Naar verwachting moet aan de volgende vereisten voldaan zijn om op elektronische wijze

een onderhandse akte te produceren (let wel; deze eisen kunnen uiteindelijk dus nog anders komen te luiden):[xvi]

- Het elektronisch document is voorzien van een voldoende betrouwbare elektronische handtekening. Er wordt automatisch aangenomen dat een elektronische handtekening voldoende betrouwbaar is indien er sprake is van een geavanceerde elektronische handtekening;
- Er moet voldaan zijn aan één of meer van de volgende vier vereisten:
  3. De gegevens dienen raadpleegbaar te zijn door partijen;
  4. De authenticiteit van de gegevens dient in voldoende mate te zijn gewaarborgd;
  5. Het moment van het opstellen van het elektronisch ondertekend document dient met voldoende zekerheid te kunnen worden vastgesteld;
  6. De identiteit van de betrokken partijen dient met voldoende zekerheid te kunnen worden vastgesteld.
- Het elektronisch ondertekend document dient te worden opgesteld met de bedoeling bewijs te produceren. Dit brengt mee dat het elektronisch ondertekend document ter beschikking moet zijn gesteld aan degene voor wie zij is opgemaakt.

3.2 De elektronische handtekening

Uit bovenstaande opsomming blijkt dat een elektronische handtekening mogelijk onderdeel wordt van de elektronische onderhandse akte. Een elektronische handtekening, de elektronische variant van een gewone handtekening, is voor de ontvanger het bewijs dat een elektronisch bericht inderdaad afkomstig is van de ondertekenaar en tijdens de verzending niet is gewijzigd. Of: een handtekening waarvan de elektronische gegevens zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie.[xvii] Een elektronische handtekening kan worden gezet met behulp van (technische) middelen als gebruikersnaam en wachtwoord, een ingescande handtekening of een elektronisch certificaat (al dan niet beveiligd met PIN-codes of biometrie).

Vanwege de snelle technologische ontwikkelingen worden door de wet geen specifieke technische eisen gesteld aan een elektronische handtekening. Dat betekent dat een elektronische handtekening met elke willekeurige techniek kan worden aangemaakt. Maar de betrouwbaarheid van de handtekening hangt natuurlijk wel af van de techniek die wordt gebruikt. Niet elke elektronische handtekening is even betrouwbaar.

De 'gewone' elektronische handtekening

Een 'gewone' elektronische handtekening is een handtekening die gekoppeld is aan andere elektronische gegevens (bijvoorbeeld een document of een e-mail) en wordt gebruikt als middel om de identiteit van de ondertekenaar vast te stellen. Een gewone elektronische handtekening is bijvoorbeeld een e-mailbericht waarin persoonsgegevens of een ingescande handtekening is opgenomen. Maar ook het intoetsen van een pincode of wachtwoord voor het bevestigen van een elektronische transactie is een gewone elektronische handtekening.

De geavanceerde elektronische handtekening

Een geavanceerde elektronische handtekening is daarentegen met meer waarborgen omkleed. Zij moet volgens de Wet elektronische handtekeningen aan eisen voldoen die meer zekerheid bieden ten aanzien van de identiteit en de wilsuiting van de ondertekenaar. Deze eisen zijn:

1. Zij is op een unieke wijze aan de ondertekenaar verbonden;
2. Zij maakt het mogelijk de ondertekenaar te identificeren;
3. Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging van de gegevens achteraf kan worden opgespoord.

Door deze eisen is de geavanceerde elektronische handtekening betrouwbaarder dan de 'gewone'.

De gekwalificeerde elektronische handtekening

Daarnaast kent de Wet elektronische handtekeningen de volgende twee aanvullende eisen:

1. de elektronische handtekening is gebaseerd op een gekwalificeerd certificaat dat voldoet aan eisen zoals gesteld in de Telecommunicatiewet, en
2. de elektronische handtekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen.

Een geavanceerde elektronische handtekening die ook aan deze laatste twee eisen voldoet, wordt ook wel aangeduid als een gekwalificeerde elektronische handtekening. De keuze voor een bepaalde soort elektronische handtekening is sterk afhankelijk van het doel waar de elektronische handtekening voor wordt gebruikt. Het belang van de juistheid en de zekerheid moet afgewogen worden tegen de kosten en het gemak.

3.3 De bewijsovereenkomst

Met een bewijsovereenkomst kunnen partijen afspreken of aan een bepaald bewijsmiddel dwingende bewijskracht toekomt, maar ook of in geval van een geschil de bewijslast op een bepaalde manier wordt verdeeld. Ook kunnen partijen in de bewijsovereenkomst bepaalde bewijsmiddelen uitsluiten. Ten aanzien van het leveren van bewijs met behulp van elektronische gegevens, kunnen partijen bijvoorbeeld overeenkomen om aan de registratie van gegevens van één der partijen dwingende bewijskracht toe te kennen. Zij zullen dan uiteraard in onderling overleg vast moeten stellen aan welke eisen deze registratie dient te voldoen.

3.4 De Trusted Third Party

Een Trusted Third Party (TTP) is een neutrale derde partij die ingezet kan worden bij de beveiliging van het elektronisch berichtenverkeer. De TTP kan zekerheid bieden over de te verzenden berichten door het nemen van bepaalde maatregelen. Een TTP kan diensten verlenen waarmee kan worden voldaan aan de eisen die gelden voor de elektronische onderhandse akte en kan op deze wijze bijdragen aan het produceren van dwingend bewijs.

Bewijs- en bewaardiensten van de TTP

a. *Bewijs van zending en ontvangst*. Partijen hebben behoefte aan een bewijs dat een bericht verzonden en/of ontvangen is. Om dit bewijs te verkrijgen zou A (verzender) zijn bericht via een TTP naar B (ontvanger) kunnen zenden. De organisatie van B kan een bericht van ontvangst sturen naar de TTP, die dit bericht weer (ondertekend) doorstuurt naar A. Zo is een dekkende constructie gebruikt om een bewijs van verzending te verkrijgen. Het feit dat het bericht bij de organisatie van B is aangekomen, wil nog niet zeggen dat B zelf het bericht ontvangen heeft. Om nu een bewijs van ontvangst te genereren zal B, zodra hij het bericht heeft gelezen, via de TTP, een bericht van ontvangst naar A moeten sturen. Het is weer de TTP die dit bericht ondertekent.

b. *Beheer van documenten en data recovery*. Indien partijen eventuele onenigheid vrezen over de werkelijke inhoud van een elektronisch document, dan kunnen zij bepalen dat een TTP een document zal beheren. Zou het daadwerkelijk tot onenigheid komen, dan is het document dat door de TTP wordt beheerd, het document dat uitkomst moet bieden. Om de originaliteit van het document te garanderen, kan de TTP het document digitaal ondertekenen en een tijdstempel meegeven.

c. *Tijdstempelen*. Om een tijdstempel aan een bericht toe te kennen, hoeft niet het gehele elektronische bericht aan de TTP te worden verstuurd. Volstaan kan worden met een *hash* van het bericht. Aan deze *hash* voegt de TTP de datum en de tijd waarop het bericht is ontvangen.

d. *Volgnummeren*. Om zekerheid te creëren over de volgorde waarin berichten worden verstuurd, kan de TTP volgnummers toekennen aan de berichten. Hierdoor kan onder andere gesignaleerd worden dat een berichtenstroom geschonden is, of dat een bericht meermalen verzonden is. Naast de TTP kan vaak ook het systeem zelf deze functie uitoefenen.

e. *Certificatiedienstverlening*. De TTP genereert elektronische sleutels en geeft elektronische certificaten uit waarin zij verklaart dat een bepaalde elektronische sleutel toebehoort aan een bepaald persoon. Vervolgens koppelt de TTP de sleutel aan een door deze persoon ondertekend digitaal certificaat.

Zo'n certificaat is een digitaal document dat de binding van een persoon of bedrijf met de elektronische sleutel bevestigt. Zo'n elektronische sleutel kan bijvoorbeeld worden gebruikt voor het zetten van een elektronische handtekening of het versleutelen van berichten.

4 In de praktijk: Bewaar- & Beveiligingsbeleid

In dit hoofdstuk leest u welke organisatorische maatregelen u moet treffen om bewaring van gegevens en de bewijskracht ervan te optimaliseren. Denk hierbij aan de beveiliging van uw bedrijfsnetwerk, het uitstippelen en implementeren van breed gedragen beveiligingsbeleid, het toekennen van taken en verantwoordelijkheden binnen de organisatie enzovoorts. Hiervoor kunt u gebruik maken van bestaande standaarden die in dit hoofdstuk worden besproken.

4.1 Beveiliging van gegevens

De beveiliging van gegevens en de media waarop deze bewaard worden, bestaat uit:

- Organisatorische maatregelen. Deze moeten leiden tot een intern beveiligings- en bewaarbeleid, adequate inrichting van het beveiligingsmanagement en het bevorderen van veilig gedrag bij (lijn)management en medewerkers (bijvoorbeeld door bewustwordingscampagnes).
- Fysieke beveiliging en controle daarvan (afsluitbare gebouwen, server ruimtes, kasten en meubilair, e.d.).
- Logische beveiliging van netwerken en informatie (logische toegangscontrole, encryptie, firewalls, virusscanners, e.d.).

Het geheel van beveiligingsmaatregelen in uw organisatie moet waarborgen dat:

- gegevens beschikbaar zijn op het moment van gebruik, uitsluitend voor een daartoe bevoegd persoon (beschikbaarheid);
- gegevens beschikbaar zijn op langere termijn;
- de blijvende integriteit (juistheid en volledigheid) van de gegevens is gewaarborgd en, indien gegevens in de processen zijn gewijzigd, achteraf kan worden vastgesteld wie, wanneer welke wijzigingen heeft aangebracht;
- de originaliteit en herkomst van gegevens kan worden vastgesteld (authenticiteit).

In wet- en regelgeving zijn geen concrete beveiligingsmaatregelen voorgeschreven, omdat deze snel verouderen. Vaak wordt gesproken over een 'adequate' beveiliging. Om aan te kunnen tonen dat de beveiliging adequaat is, moet u kijken naar welke risico's uw organisatie loopt en met behulp van welke maatregelen deze risico's worden beperkt.

4.2 Beleid, organisatie en proces: Bewaar- & Beveiligingsbeleid

Vertrekpunt voor een goede inrichting van 'Bewaren en beveiligen' is: een goede beheersorganisatie, procesborging en het toekennen van taken en verantwoordelijkheden. Dit is niet anders dan voor welk bedrijfsproces dan ook. De vastlegging hiervan, samen met de algemene doelstellingen van de organisatie voor Bewaren en Beveiligen, noemen we het *Bewaar & Beveiligingsbeleid*. Dit beleid kunt u onderbrengen bij het informatiebeleid of het beveiligingsbeleid. Een andere mogelijkheid is om dit beleid onder de brengen bij de Chief Information Officer (CIO)/ Informatiemanagement of bij de Chief Information Security Officer (CISO) / Informatiebeveiliging & risicomanagement. Gezien de belangrijke IT-component kunt u de uitvoering ook bij uw Automatiseringsafdeling neerleggen.

Gegevenseigenaar

Het begrip 'eigenaar' wordt vaak gehanteerd om aan te geven wie verantwoordelijk is voor bepaalde gegevens. Het eigenaarschap voor specifieke gegevens is doorgaans belegd in de lijn. Een lijnmanager treedt als eigenaar op van de gegevens in 'zijn' proces-sen, en stelt hier dus ook de eisen aan ten aanzien van Bewaren en Beveiligen. Het eigenaarschap voor gegevens die organisatiebreed worden ingezet, en die niet aan één lijnmanager zijn toe te wij-zen, wordt bepaald door degene bij wie het Bewaar- & Beveiligingsbeleid is ondergebracht (de portefeuillehouder 'Bewaren en Beveiligen'). Zoals reeds aangegeven is dit veelal de CIO of CISO.

Voor de inrichting van dit beheersproces kunt u twee standaarden als vertrekpunt gebruiken:
- Bewaren: ISO 15489 - Record Management
- Beveiligen: ISO 27001/ISO 17799 - Code voor Informatiebeveiliging

Deze twee standaarden worden hieronder besproken.

4.3 Bewaren: ISO 15489 - Record management

Inleiding

Deze standaard voor informatie-, documentatie- en archiefbeheer is een omschrijving van wat u allemaal moet doen om tot een adequate en op de uitvoering van taken afgestemde inrichting van de informatiehuishouding te komen. Onderwerpen die in de standaard aan de orde komen, zijn: beleid, toedeling van verantwoordelijkheden, voordelen van goed gegevensbeheer, een methode voor implementatie van de standaard, de verschillende processen van informatiebeheer, kwaliteitsbewaking, auditing en opleiding.

De standaard bestaat uit twee delen: 1. Algemeen en 2. Technische richtlijnen. De standaard biedt een algemeen geaccepteerd kader, waarop zowel overheidsorganisaties als bedrijven hun informatiehuishouding kunnen baseren. De hierin beschreven basisregels moeten nog worden vertaald naar de praktijk. De standaard heeft relatie met de NEN-ISO-standaard 9001 voor kwaliteitssystemen.

Beleid en verantwoordelijkheden

In deze standaard wordt aanbevolen dat organisaties een beleid voor informatie- en archiefmanagement vaststellen en documenteren. Het doel van het beleid behoort te zijn de totstandkoming en het beheer van authentieke, betrouwbare en bruikbare gegevens, die bedrijfsfuncties en -activiteiten kunnen ondersteunen zo lang als nodig is.

Uw organisatie moet het beleid afleiden van een analyse van de bedrijfsactiviteiten en moet gebieden definiëren waar wet- en

regelgeving, andere standaarden en best practices van toepassing zijn op gegevens in relatie tot de bedrijfsactiviteiten.
Ook moeten verantwoordelijkheden en bevoegdheden voor informatie- en archiefmanagement binnen uw organisatie worden vastgesteld en toegewezen. Deze verantwoordelijkheden moeten worden opgedragen aan alle medewerkers van de organisatie, inclusief informatiespecialisten, leidinggevenden en systeembeheerders.

Eisen aan informatie- en archiefmanagement

U moet vaststellen welke gegevens moeten worden vastgelegd. En u moet besluiten in welke vorm en structuur deze vastlegging moet plaatsvinden en welke technologieën daarvoor worden gebruikt. Daarnaast moet u duidelijk krijgen welke metagegevens worden gecreëerd over de vastgelegde bestanden, hoe wordt geordend en teruggezocht. Van belang is ook dat u het risico inschat bij ontbreken van gegevens en de zorg voor langdurige bewaring en tijdige vernietiging. Denk hierbij ook aan beveiligde omgevingen en continuïteitsplanning. Het is van belang hiervoor een risicoanalyse te verrichten.

Ontwerp en implementatie van een archiefsysteem

Een archiefsysteem moet aan bepaalde eisen voldoen. Een archiefsysteem behoort routinematig en systematisch gegevens over de bedrijfsactiviteiten op te nemen. Gegevensbestanden moeten worden geordend en beschermd, en moeten integer en toegankelijk zijn. In de standaard wordt aanbevolen bij het ontwerp van archiefsystemen aandacht te besteden aan een geschikte opslagomgeving en media, fysiek beschermende materialen, procedures voor behandeling, vernietiging en opslagsystemen. Denk hierbij ook aan tijdige conversie en migratie bij ICT-vernieuwingen. Momenteel wordt een norm uitgewerkt, NEN-ISO 2082, voor records management in bedrijfsapplicaties. Aan iedere applicatie waar gegevens worden gecreëerd en beheerd dienen namelijk archiefeisen te worden gesteld.

Processen en controles van informatie- en archiefmanagement

U moet bepalen welke gegevens in een archiefsysteem moeten worden opgenomen en hoe lang deze moeten worden bewaard.

Uw beslissingen dienen te zijn gebaseerd op de context van wet- en regelgeving, eisen van bedrijfsvoering en verantwoording en het risico dat men loopt. Het gaat daarbij om het onderkennen van huidige en toekomstige behoeften ten aanzien van de bedrijfsvoering. Denk hierbij aan het identificeren van, volgen van en de voortgangsbewaking op de gegevens.

Toezicht en controle
Uw organisatie moet regelmatig controleren of voldaan wordt aan de gestelde eisen om te garanderen dat de procedures en processen in archiefsystemen worden geïmplementeerd overeenkomstig de beleidslijnen en eisen en of deze voldoen aan de verwachte uitkomsten.

Opleiding
Uw organisatie behoort een permanent programma voor opleiding met betrekking tot informatie- en archiefmanagement op te zetten. Opleidingsprogramma's behoren gericht te zijn op het management, werknemers, contractanten en vrijwilligers.

Technische richtlijnen
NEN-ISO 15489-2 is een implementatiegids voor het eerste deel. Het voorziet in een methodologie die de implementatie van NEN-ISO 15489-1 mogelijk wil maken.

De volgende stappen worden beschreven:
1. Vooronderzoek.
2. Analyse van taken.
3. Identificatie van eisen aan gegevens.
4. Beoordeling van bestaande systemen.
5. Identificatie van strategieën om te voldoen aan eisen aan gegevens.
6. Ontwerp van een archiefsysteem.
7. Implementatie van een archiefsysteem.
8. Evaluatie na implementatie.

4.4 Beveiligen: Code voor Informatiebeveiliging

De Code voor Informatiebeveiliging (CvI) -ISO 17799 beschrijft de 'good practice' op het gebied van informatiebeveiliging en

risicomanagement. De ISO 17799 beschrijft in detail de controls (maatregelen voor beheersing en beveiliging). Het is een praktijkstandaard: de goede gebruiken van toonaangevende en ervaren organisaties op het gebied van informatiebeveiliging zijn naast elkaar gelegd en geïntegreerd. Veel bedrijven en instellingen zijn bezig hun organisatie voortdurend te verbeteren. Zij gebruiken daarvoor de Code voor Informatiebeveiliging als leidraad. De Code voor Informatiebeveiliging beschrijft zo'n 130 *best practices*. Deze beschrijven wat voor beveiligingsmaatregelen je in welke situaties zou kunnen nemen. Niet alles hoeft relevant te zijn voor elke organisatie; het is kunst hier praktisch mee om te gaan.

Ook bij de CvI is een goede inrichting van het proces met duidelijke taken, verantwoordelijkheden, bevoegdheden, rapportages en rapportagelijnen het vertrekpunt. Dit proces wordt aangeduid als het Information Security Management System, ISMS. Er is zelfs certificatie mogelijk van dit proces, zodat compliance niet alleen intern, maar ook naar de buitenwereld kan worden getoond.

Onderwerpen die in de standaard aan de orde komen zijn: beleid, organisatie, mens, fysiek, techniek en controle. Hieronder een korte uitwerking:

- *Beleid:* er moet een beleid zijn en worden onderhouden dat richting en ondersteuning geeft aan de procesinrichting. Dit document dient zowel als inrichtingsdocument als communicatiedocument.
- *Organisatie:*
  - Structuur: vanuit de top moet de structuur (control framework) voor taken, verantwoordelijkheden en bevoegdheden zijn vastgelegd. Er is een proces voor het toekennen daarvan. Duidelijk moet zijn wie welke verantwoordelijkheden heeft. De activiteiten moeten gecoördineerd worden uitgevoerd. Functiescheiding is ingericht.
  - Communicatie: geheimhouding is geregeld. Communicatie met belanghebbenden zoals klanten, overheid, partners, eigen personeel en wellicht het grote publiek, is ingericht.
  - Externe partijen: de risico's ten aanzien van de afhankelijkheid van derde partijen zijn beheerst. Ook externe partijen, inclusief klanten weten waar ze op kunnen rekenen.

- *Beheer van bedrijfsmiddelen:* de verantwoordelijkheden ten aanzien van bedrijfsmiddelen, zoals informatiebronnen, zijn belegd. Classificatie kán worden gebruikt om een bepaalde set maatregelen te koppelen aan een specifiek bedrijfsmiddel.
- *Personeel:* vóór, tijdens en na het dienstverband zijn er afspraken over hoe het personeel met gegevens om moet gaan. Het personeel wordt hierin ondersteund en getraind.
- *Fysieke beveiliging:* de fysieke beveiliging moet passen op de technische en personele beveiliging. De fysieke beveiliging is ingericht volgens zonering, met per zone toegangsbeheersing. Bepaalde voorzieningen, zoals voor elektriciteit naar laptops, vraagt extra aandacht. Ook moet er aandacht zijn voor verwijderen en vernietigen van informatiedragers.
- *Beheer van communicatie en bedieningsprocessen:*
  - Het operationele proces is gedocumenteerd. Ook het wijzigingenproces is gedocumenteerd met aandacht voor beveiliging. Er is voldoende scheiding tussen de ontwikkelomgeving enerzijds, en de productieomgeving anderzijds. Overdracht van de productieomgeving is beheerst.
  - Er is incident- en capaciteitsmanagement.
  - Dienstverlening door een derde partij is voldoende beheerst.
  - De integriteit van programmatuur en informatie is voldoende beschermd. Denk hierbij aan virussen, spam en 'mobile code'.
  - Reservekopieën: backup en restore zijn ingericht.
  - Netwerkbeveiliging: het 'eigen' netwerk is voldoende afgeschermd van niet-geautoriseerden. Geautoriseerde toegang is beheerst.
- *Vernietiging:* er moeten procedures zijn voor het lang genoeg, maar niet te lang, bewaren en veilig vernietigen van gegevens.
- *Uitwisselen van informatie met derden:* hier moeten afspraken over zijn.
- *E-commerce, internet:* de specifieke risico's rond het veilig (commercieel) gebruik zijn geïdentificeerd en voldoende beheerst.
- *Controle:* is ingericht om ongewenste activiteiten te voorkomen of te detecteren. Controle vindt plaats op verschillende

plaatsen in de organisatie: in de lijn, door interne auditing en door externe auditing.

- *Toegangsbeveiliging:* beheer van toegangsrechten van medewerkers en andere betrokkenen. De verantwoordelijkheden van deze gebruikers zijn bekend, waarbij bijzondere aandacht is voor direct aan de gebruikers ter beschikking gestelde middelen zoals laptops en organisers, alsmede telewerkvoorzieningen.
- *Verwerving, ontwikkeling en onderhoud van informatiesystemen:* beveiligingseisen zijn bekend, worden bewaakt en passen zo mogelijk in de beveiligingsarchitectuur. Ook in de ondersteunende processen voor verwerving, ontwikkeling en onderhoud is beveiliging geborgd.
- *Beveiligingsincidenten:* er is een beheerst proces rond het detecteren, melden en afwikkelen van beveiligingsincidenten.
- *Continuïteit:* eisen ten aanzien van continuïteit, beschikbaarheid en 'maximum dataverlies' zijn bekend voor de relevante bedrijfsmiddelen. Er is een proces voor continuïteitsmanagement, dat niet alleen de middelen, maar ook de processen betreft.
- *Naleving:* wettelijke verplichtingen zijn bekend en worden opgevolgd. Naleving van het beleid en de implementatie daarvan wordt geaudit.

4.5 Organisatorische maatregelen

Informatiebeveiliging is een proces. Om schijnbeveiliging te voorkomen moet u *periodiek* bekijken met welke (nieuwe) bedreigingen uw organisatie wordt geconfronteerd. Om informatiebeveiliging adequaat gestalte te geven, dient een samenhangend pakket beveiligingsmaatregelen te worden getroffen *en te worden onderhouden*. Informatiebeveiliging is een proces, dat pas optimaal functioneert als het tezamen met andere ondersteunende processen is geïntegreerd in de primaire bedrijfsprocessen.
Wilt u aan derden kenbaar maken dat u uw organisatie - in het bijzonder het management systeem voor informatiebeveiliging - op orde hebt, dan kunt u zich laten certificeren tegen de ISO 27001.

5 De Leidraad

5.1 Doel

De doelstelling van de Leidraad is om zodanige regels te formuleren dat het:

a. voor degenen die gegevens willen vastleggen, verwerken, beheren, bewaren en vernietigen mogelijk is om procedures en voorschriften te toetsen aan redelijk te stellen eisen;
b. voor diegenen die gebruik maken van deze gegevens mogelijk wordt een oordeel te vormen over de betrouwbaarheid en authenticiteit van de gegevens;
c. uitgangspunten biedt voor de toepassing van wettelijke regelingen inzake het vastleggen en bewaren van gegevens, zodat de bewijskracht van de gegevens wordt bevorderd.

Bij het inrichten van het kwaliteitssysteem geldt dat *niet* de gegevensdragers en de systemen uitgangspunt zijn, maar de gegevens *zelf*. De Leidraad richt zich dus op alle gegevens binnen een organisatie, *ongeacht de gegevensdrager*. De technische implementatie van de Leidraad valt dan ook *buiten het kader* van deze publicatie. Uitgangspunt is dat *ongeacht de gekozen technische uitwerking* de onderdelen van de Leidraad uit bewijstechnisch oogpunt noodzakelijk zijn. De gekozen technische oplossingen hebben hun eigen implicaties, die specifieke maatregelen vergen om de Leidraad te realiseren. Ongeacht de gebruikte technologie dient de Leidraad te worden gerealiseerd.

In bijlage 4 vindt u een checklist van onderstaande Leidraad waarmee u direct aan de slag kunt.

5.2 De Leidraad

(1) Een organisatie zorgt ervoor dat:
   a) de gegevens die worden verwerkt, geconverteerd, beheerd en uitgewisseld duidelijk zijn omschreven;

b) de gegevens systematisch zijn geordend op basis van een in een procedurebeschrijving vastgelegde structuur. De structuur maakt het ook voor een derde mogelijk binnen een redelijke termijn specifieke gegevens terug te vinden;
c) de systematische structuur binnen de gegevens wordt gehandhaafd en onderhouden;
d) van de verwerking van de gegevens een logboek wordt aangelegd, waarbij tenminste de volgende gegevens worden vastgelegd:
   (1) de identiteit van de verantwoordelijke;
   (2) de identiteit van de uitvoerder van de verwerking (i.c. de verantwoordelijke batchfile);
   (3) de aard van de verwerkte gegevens;
   (4) het onderwerp van de verwerkte gegevens;
   (5) de datum van verwerking;
   (6) de plaats van verwerking;
   (7) eventuele storingen die tijdens verwerking zijn opgetreden.

   Het logboek mag in geautomatiseerde vorm worden gevoerd; de audit-trail kan als logboek functioneren, mits voldaan wordt aan de gestelde voorwaarden én voor derden in begrijpelijk vorm toegankelijk is;
e) een index voor, tijdens en na de verwerking van gegevens wordt bijgehouden, omschreven in een procedurebeschrijving en genoteerd in het logboek;
f) de (ontvangen) gegevens voortdurend terug te voeren zijn op de (authentieke) bron en te benaderen zijn gedurende de bij deze gegevens behorende bewaartermijn. De aanwezigheid van het bestand binnen de gecontroleerde omgeving van het archief moet aantoonbaar zijn;
g) de gegevens (bij archivering en uitwisseling) voorzien worden van de nodige identificatiegegevens, waaronder de (eventueel) toegepaste bewijsvergrendeling (met name bij archivering van belang). Hierdoor kan worden vastgesteld dat er in een bepaald computerbestand geen veranderingen zijn doorgevoerd;
h) steekproefsgewijs de compleetheid en de kwaliteit van de gegevens gecontroleerd wordt. De opzet en uitvoering van deze steekproef worden omschreven in een proce-

durevoorschrift. De resultaten van de steekproef worden in het logboek of een bijlage daarvan vastgelegd;

i) voor de (archivering van) gegevens adequate voorzieningen van informatiebeveiliging worden getroffen (technische security-voorzieningen, inbraakpreventie, inbraaksignalering, bescherming tegen onbevoegde raadpleging, waterschade, uitval energievoorziening, vandalisme e.d.);

j) gegevens waarvan de bewaartermijn is verstreken worden vernietigd;

k) na geslaagde conversie of migratie de originelen worden vernietigd, met uitzondering van jaarverslagen, balansen en (authentieke) akten. Balans en winst- en verliesrekening dienen op papier te worden bewaard. Van deze conversie of migratie worden in het logboek vastgelegd:
   (1) de datum van conversie;
   (2) het oude en het nieuwe bestandsformaat;
   (3) (indien nodig) de verstrekte machtiging tot substitutie.

l) van een vernietiging van originelen een proces verbaal wordt opgemaakt, dat de volgende gegevens bevat:
   (1) de omschrijving van de vernietigde gegevens;
   (2) de wijze van vernietiging;
   (3) de datum van vernietiging;
   (4) ondertekening door tenminste twee personen, één namens de gegevensbeheerder, één namens de archiefvormer en, voor overheidsinstellingen noodzakelijk, één namens de archiefinspectie;
   (5) ondertekening door het management van de organisatie of de door deze gedelegeerde functionaris.

   m) het proces-verbaal van vernietiging onderdeel is van het logboek.

(2) Een organisatie stelt één of meer functionarissen aan die op de toepassing van de Leidraad toezien en verantwoordelijk zijn voor de controle. Deze functionarissen mogen niet belast zijn met dan wel verantwoordelijk gesteld zijn voor de inhoudelijke behandeling van de gegevens en -dragers of ressorteren onder een functionaris met een dergelijke verantwoordelijkheid, *tenzij* ze onderworpen zijn aan adequate interne controlemaatregelen betrekking hebbend op vol-

doende functiescheiding op dit punt. Het is van belang dat de interne controlemaatregelen aan continue rapportage onderhevig zijn, waardoor kan worden vastgesteld of de maatregelen effectief zijn.

(3) Een organisatie treft zodanige maatregelen dat alleen aan daartoe bevoegde personen gegevens ter beschikking worden gesteld en dat deze gegevens integer zijn en blijven. Dit betekent dat er bij de verstrekking van (toegang tot) digitale gegevens geen bevoegdheid wordt verstrekt om de gegevens te kunnen muteren, ook niet onbedoeld. Hierbij kunnen moeilijk muteerbare bestandsformaten als hulpmiddel worden gebruikt. De voorkeur hier heeft (voor gegevens in documentvorm) PDF/A (ISO/IEC 19005-1. Document Management - Electronic document file format for long-term preservation), of bestandsformaten die eenvoudig hiernaar te converteren zijn. Bij gegevens die niet in digitale vorm zijn verstrekt, worden er maatregelen getroffen die het retour ontvangen en weer op juiste wijze in het archief opnemen van gegevens waarborgen.

Notenlijst

i ISO/IEC 26300: 2006
ii ISO 12639: 2004
iii specifiek PDF/A (ISO 19005-1: 2005)
iv Burgerlijk Wetboek, Boek 2, art. 10, lid 1 en lid 3
v Algemene Wet inzake Rijksbelastingen, art. 47-57, met name art. 52; Wet op de Omzetbelasting 1968, art. 34 a
vi Douanewet, art. 8
vii Publicatie Uw geautomatiseerde administratie en de fiscale bewaarplicht, Belastingdienst december 2005
viii Burgerlijk Wetboek, boek 3, art. 306
ix Burgerlijk Wetboek, Boek 3, art. 307- 311, Boek 6, art.71
x Art 7 Archiefwet
xi Eerste officiële machtiging tot substitutie een feit, Timo ten Cate, Od, jaargang 60, juli/augustus 2006
xii Bewaartermijnen in een bedrijfsarchief, NVBA, 1993
xiii Rv, art. 152, lid 1
xiv Rv, art. 151, lid 1
xv Kamerstukken II 2005/06, 30 137, nr. 18. Zie ook J.H.M. ter Haar & E.D.C. Neppelenbroek, 'Het elektronisch ondertekend document: wel, niet of net zoiets als een akte', WPNR 2006-6655, p. 150-153
xvi Deze vereisten zijn ontleend aan de artikelen 3:15a BW, 6:227a BW en 156 lid 1 RV.
xvii Burgerlijk Wetboek, Boek 3, art. 15a, lid 4.

Bijlage 1 Verjaringstermijnen

Rechtsvorderingen	**Verjaartermijn**
Rechtsvorderingen tot vernietiging van een rechtshandeling ingeval van	
*onbekwaamheid	3 jaar
*bedreiging of misbruik van omstandigheden	3 jaar
*bedrog, dwaling of benadeling	3 jaar
*andere vernietigingsgrond	3 jaar
Rechtsvordering tot nakoming van een verbintenis uit overeenkomst	5 jaar
Rechtsvorderingen tot betaling van renten van geldsommen, lijfrenten, dividenden, huren, pachten en alles wat bij het jaar of een kortere termijn moet worden betaald	5 jaar
Rechtsvorderingen uit onverschuldigde betaling	5 jaar
Rechtsvorderingen tot vergoeding van schade of tot betaling van een bedongen boete	5 jaar
De rechtsvorderingen tot schadevergoeding van tegen de producent op basis van productaansprakelijkheid	3 jaar
Rechtsvorderingen tot ontbinding van een overeenkomst op grond van een tekortkoming in de nakoming of tot herstel van een tekortkoming	5 jaar

Deze verjaringstabel omvat een selectie van de verjaringstermijnen die wij als meest gebruikte of meest belangrijke hebben uitgezocht, maar mag niet als uitputtend worden beschouwd

Ingangsdatum	Juridische grondslag
nadat de onbekwaamheid is geëindigd, of, indien de onbekwame een wettelijke vertegenwoordiger heeft, drie jaren nadat de handeling ter kennis van de wettelijke vertegenwoordiger is gekomen	art 3:52 lid 1a BW
nadat deze invloed heeft opgehouden te werken	art 3:52 lid 1b BW
nadat het bedrog, de dwaling of de benadeling is ontdekt	art 3:52 lid 1c BW
nadat de bevoegdheid om deze vernietigingsgrond in te roepen, aan degene aan wie deze bevoegdheid toekomt, ten dienste is komen te staan.	art 3:52 lid 1d BW
vanaf de dag volgend op de dag dat de vordering opeisbaar is geworden	art 3:307 BW
vanaf de dag volgend op de dag dat de vordering opeisbaar is geworden	art 3:308 BW
vanaf de dag volgend op de dag dat de schuldeiser zowel met het bestaan van zijn vordering als met de persoon van de ontvanger bekend is geworden en in ieder geval 20 jaar nadat de vordering is ontstaan	art 3:309 BW
vanaf de dag volgend op de dag waarpp de benadeelde zowel met de schade of de opeisbaarheid van de boete als met de daarvoor aansprakelijke persoon bekend is geworden, en in ieder geval door verloop van 20 jaar nadat de gebeurtenis waardoor de schade is veroorzaakt of de boete opeisbaar is geworden. Of door verloop van 30 haar in geval van verontreiniging van lucht, water of bodem, gevaarlijke stoffen (6:175 BW) of beweging grond door mijnbouw (6:177 BW)	art 3:310 BW
vanaf de dag volgend op de dag waarop de benadeelde met de schade, het gebrek en de identiteit van de producent bekend is geworden of had moeten worden	art 6:191 BW
vanaf de dag, volgende op de dag waarop de schuldeiser met de tekortkoming bekend is geworden en in ieder geval twintig jaren nadat de tekortkoming is ontstaan.	art 3:311 BW

Bijlage 2 Bewaartermijnen

Documenten	Bewaartermijn
Jaarrekening, accountantverklaring ed	7 jaar
Algemene administratie waaronder in ieder geval grootboek, debiteuren- en crediteurenadministratie, in-en verkoopadministratie, voorraadadministratie en loonadministratie	7 jaar
Winst- en verliesrekening	7 jaar
Facturen ivm omzetbelasting	7 jaar
De boeken, bescheiden en andere gegevensdragers van een ontbonden rechtspersoon.	7 jaar
Van werknemers: loonbelastingverklaringen, identificatiebewijs, naam, adres, postcode, woonplaats, geboortedatum en sociaal fiscaal nummer	5 jaar
Loonstaten en loonadministratie	5 jaar
Administratie na ontbinding rechtspersoon	7 jaar
Gegevens bedrijfsmatig onroerend goed	9 jaar
Dividend nota's	5 jaar
Ledenadministratie cooperatie met aansprakelijkheid leden	10 jaar
Subsidie administratie	7 jaar
Werknemers die aan gevaarlijke stoffen worden blootgesteld: het arbeidsgezondheidskundig onderzoek en de lijsten van werknemers die zijn blootgesteld aan kankerverwekkende stoffen en asbest	40 jaar
Vervoer: persoonlijk controleboekje	1 jaar*
Vervoer: Register van werkboekjes	1 jaar*
Vervoer: Registratiebladen	1 jaar*
Voor Telecomaanbieders: Wetsvoorstel Bewaarplicht telecomgegevens	18 maanden

* Let op: dit is dan wel specifieke wetgeving, maar in veel gevallen vormen deze documenten voor de fiscus een belangrijk controlemiddel, en dan dienen deze documenten toch gewoon de 7 jaar bewaard te worden die is voorgeschreven in art 52 AWR en art 8 van de Douanewet!!

Deze bijlage bevat een selectie van de bewaartermijnen die wij als meest gebruikte en/of belangrijkste zien, maar is geenszins uitputtend.

Ingangsdatum	Juridische grondslag
vanaf datum opstellen	art. 2:394 BW lid 6
vanaf 1 januari na opstelling	art 2:10 lid 1 en 3 BW art 52 algemene wet inzake rijksbelastingen (AWR) art 8 lid 1 en 3 Douanewet
vanaf datum opstellen	art 2:10 lid 2 en 3 BW art 3:15i BW
na opstellen cq ontvangst	art 31 lid 6 Uitvoeringsbeschikking omzetbelasting
vanaf dat de rechtspersoon heeft opgehouden te bestaan	art 2:24 BW
vanaf het einde van het kalenderjaar waarin de dienstbetrekking is geeindigd	art 65 lid 3, 66 lid 4 en 105 lid 5 Uitvoeringsregeling loonbelasting 2001
Vanaf het einde van het kalenderjaar waarop zij betrekking hebben	art 6 Loonadministratiebesluit, Coordinatiewet sociale verzekering
na ontbinding	art 2:24 BW lid 1
volgend op het jaar dat men het goed is gaan gebruiken	art 34a Wet op de omzetbelasing
na opstellen	art 3 lid 1 uitvoeringsbeschikking dividendbelasting
vanaf aanvraag lidmaatschap	art 2:61 BW
vanaf datum opstellen	art 4:69 Algemene wet bestuursrecht (AWB)
vanaf beëindiging van de blootstelling aan gevaarlijke stoffen	art 4.10c Arbeidsomstandighedenbesluit
na de laatste aantekening	art. 12 AETR
na de laatste aantekening	art 25 Beschikking werkmap
na het gebruik	art 5 Beschikking gebruik tachograaf
vanaf het tijdstip waarop de gegevens voor de eerste keer zijn verwerkt	Wetsvoorstel Wijziging Telecommunicatiewet, op moment van schrijven in concept

Bijlage 3 Vernietigingstermijnen

Gegevens
Archiefwet
Selectielijsten voor de verschillende overheidsorganen geven de bewaar- en daarmee ook vernietigingstermijnen aan
Persoonsgegevens
Persoonsgegevens van leden en begunstigers van verenigingen, stichtingen en publiekrechtelijke beroepsorganisaties
Persoonsgegevens van sollicitanten
Persoonsgegevens van uitzendkrachten
Persoonsgegevens in de personeelsadministratie
Persoonsgegevens in de salarisadministratie
Persoonsgegevens in geval van uitkering bij ontslag
Persoonsgegevens in geval van pensioen en vervroegde uittreding
Persoonsgegevens van abonnementhouders
Persoonsgegevens van debiteuren en crediteuren
Persoonsgegevens van afnemers en leveranciers
Persoonsgegevens van huurders
Persoonsgegevens van clienten van juridische dienstverleners en accoutants

* tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht

Deze vernietigingstabel bevat vernietigingstermijnen die wij als meest gebruikt beschouwen, maar mag geenszins als uitputtend worden beschouwd

Vernietigingstermijn	Juridische grondslag
Afhankelijk van de taak van het overheidsorgaan, de verhouding tot andere overheidsorganen en het belang en de waarde van de gegevens	Selectielijsten, te vinden op de website van het Nationaal Archief (www.nationaalarchief.nl)
uiterlijk 2 jaar nadat het lidmaatschap is beëindigt of de begunstiger heeft aangegeven niet langer als begunstiger wil worden beschouwd*	Art 3 Vrijstellingsbesluit WBP
Wanneer de betrokkene daarom verzoekt, maar in ieder geval uiterlijk 4 weken nadat de sollicitatieprocedure is geeindigd, tenzij de betrokkene toestemming heeft gegeven de gegevens 1 jaar na de procedure te bewaren	Art 5 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat het dienstverband of de werkzaamheden zijn beeindigd*	Art 6 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat het dienstverband of de werkzaamheden zijn beeindigd*	Art 7 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat het dienstverband of de werkzaamheden zijn beeindigd*	Art 8 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat de aanspraken zijn beeidigd*	Art 9 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat de aanspraken zijn beeidigd*	Art 10 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar na het beeindigen van het abonnenment*	Art 11 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat de desbetreffende vordering is voldaan*	Art 12 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat de de transactie is afgehandeld*	Art 13 Vrijstellingsbesluit WBP
Uiterlijk 2 jaar nadat de huur is geeindigd, behalve de gegevens mbt de aanvraag en verstrekking van een huurtoeslag, deze worden uiterlijk 5 jaar na het eindigen van de huurtoeslag verwijderd*	Art 14 Vrijstellingsbesluit WBP
Wanneer de bewaartermijn volgens hun eigen gedrags- en beroepsregels eindigt of bij gebreke van zulke regels uiterlijk 2 jaar nadat de behandeling van de zaak is beeindigd*	Art 15 Vrijstellingsbesluit WBP

Bijlage 4 Checklist Leidraad

Stap	Beschrijving	J	N
1	Zijn alle gegevens in Uw organisatie beschreven ?		
2	Is bij al Uw gegevens aangegeven of zij zijn geconverteerd en/of uitgewisseld ?		
3	Zijn alle gegevens onderdeel van een systematische ordening ?		
4	Is deze systematische structuur vastgelegd in een procedurebeschrijving ?		
5	Is deze systematische structuur onderdeel van de toegankelijkheidsmiddelen?		
6	Bestaat er een onderhoudsorganisatie voor de systematische structuur ?		
7	Wordt van de verwerking van de gegevens een logboek bijgehouden ?		
8	Wordt in het logboek de identiteit van de verantwoordelijke functionaris voor de verwerking van de gegevens vastgelegd ?		
9	Wordt de identiteit van de uitvoerder van de bewerker of de verantwoordelijke batch-file daarvoor vastgelegd ?		
10	Worden in het logboek de aard en het onderwerp van de verwerkte gegevens vastgelegd ?		
11	Worden in het logboek de datum en de plaats van verwerking van de gegevens vastgelegd ?		
12	Worden storingen in de verwerking geregistreerd ?		
13	Indien de audit trail als logboek fungeert: voldoet de audit trail aan de voorwaarden zoals in 8-11 gedefinieerd ?		
14	Indien de audit trail als logboek fungeert: is de audit trail ook voor een derde toegankelijk, leesbaar en begrijpelijk ?		
15	Wordt een index van de gegevens bijgehouden ?		
16	Is deze index beschreven in een procedure ?		
17	Worden wijzigingen in de index door verwerking of verzending vastgelegd in het logboek ?		
18	Is bij de (ontvangen) gegevens duidelijk beschreven wat de authentieke bron is ?		
19	Zijn de gegevens gedurende de hele bewaartermijn leesbaar te presenteren ?		
20	Kan de beheersgeschiedenis van de gegevens in het archief aangetoond worden ?		
21	Zijn de gegevens voorzien van identificatiegegevens ?		
22	Is er bewijsvergrendeling toegepast ?		
23	Wordt periodiek de compleetheid en kwaliteit van de gegevens getoetst ?		
24	Is de opzet en uitvoering van de steekproef beschreven in een procedure ?		

Bijlage 5 Deelnemers ECP.NL werkgroep Bewaren en Bewijzen

De onderstaande partijen zijn betrokken geweest bij de totstandkoming van deze publicatie. De inhoud van deze publicatie geeft niet noodzakelijkerwijs de individuele mening van partijen weer.

Voorzitter: Bussel, G.J. van	Van Bussel Document Services
Aarts, I.M.	ECP.NL
Batenburg, Th.H.G.M.	DigiNotar BV
Bosch, S.	Hewlett Packard Nederland B.V.
Donkhorst, J.C.	Belastingdienst / CPP
Durinck, M.	ECP.NL
Eikelenboom, J.	Computer Associates B.V.
Glashouwer, B.	Het Expertise Centrum
Hoevers, M.	ECP.NL
Hof, S. van der	Universiteit van Tilburg
Hofman, H.	Nationaal Archief
Jongbloed, L.	Nederlandse Vereniging van Banken
Kuipers, J.H.B.	Belastingdienst Kantoor Arnhem
Leijten, M.	Computer Associates B.V.
Olthof, W.J.A.	NOREA
Overbeek, P.L.	OIS Information Risk & Security Management
Pasmooij, J.	Koninklijk NIVRA
Rietveld, J.C.J.	Ned. Normalisatie-instituut (NEN)
Samson, M.	Nederlandse Vereniging van Banken
Sinninghe Damste, W.A.	Sociale Verzekeringsbank
Stap, T. van der	Document@work (AIIM)
Viersma, M.	ECP.NL
Voulon, M.B.	Duthler Associates
Walgemoed, P.	Carelliance
Weezel, P. van	Belastingdienst / CPP
Wester, J.	Min. van Economische Zaken

Notities

Notities

Notities