



Bewaren

en Bewijzen



Ministerie van Economische Zaken



ECP

Platform voor de
InformatieSamenleving

Jelle.attema@ecp.nl

ECP

Platform voor de
InformatieSamenleving

122 Deelnemers

35,7%

BEDRIJVEN MEER DAN 500
WERKNEMERS

21,7%

BEDRIJVEN MINDER DAN 500
WERKNEMERS

24%

INTERMEDIAIRE ORGANISATIES

10,8%

OVERHEDEN/PUBLIEKE SECTOR

6,2%

ONDERWIJSINSTELLINGEN

1,6%

KENNISPARTNERS

Voorzitter: Busse, G.J. van	Van Busse 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 

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			

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 ?		

Leidraad

- Beschrijving bewaarde data
- Beheer data (beveiliging, audittrails en logboeken)
- Toegankelijkheid (bv. index)
- Toetsing kwaliteit procedures en data

Een update voor Bewaren & Bewijzen?

- Juridisch: weinig veranderingen.
- Veranderende praktijk:
 - Conversie, scan&herken, native-digital (xml, PDF),
 - Cloud: beheer van documenten/data uitbesteden.
 - Papier dezelfde (onbetrouwbare) status als digitaal: fotoshop, kopieerapparatuur
 - Duurzame toegankelijkheid: domein B&B en operationaal informatiebeheer vallen samen: authenticiteit/integriteit, kwaliteit, vertrouwelijkheid enz..

Rechtvaardiging

“Het bepalen welke documenten behoren te worden opgenomen in een archiefsysteem, is gebaseerd op een analyse van de context van wet- en regelgeving, eisen van bedrijfsvoering en verantwoording en het risico indien geen archiefbescheiden worden vastgelegd.”

Bron:[NEN15489] NEN-ISO 15489, norm 7.1 en 9.1.

(DUTO, versie 0.1, 13 maart 2015)

- Kan de leidraad nog helpen bepalen
 - welke documenten in een archiefsysteem moeten worden opgenomen
 - met oog op “eisen bedrijfsvoering en verantwoording” en
 - “risico’s van niet bewaren”?

Voorbeeld Belastingdienst

- Veranderende eisen aan bewaren & bewijzen (“eisen aan verantwoording en bedrijfsvoering”):
 - Documenten/data genereren/bewaren die aantonen dat een transactie echt heeft plaatsgevonden,
 - Dat alle voor toezichthouder relevante transacties zijn geadministreerd,
 - Dat documenten/data authentiek (herkomst) en integer zijn,
 - Controleerbaarheid (auditfiles, toetsing, toegankelijkheid).
- Bewaren en bewijzen is techniek onafhankelijk. Kan dat nog wel?
 - gestructureerde data opgeslagen in (verspreide) databases bij verschillende serviceproviders (webwinkels, payment service provider, administratieve software, marketingpartijen)
 - Data uit workflow, documentmanagementsystemen, ERP.
 - Ongestructureerde data: foto, film, office-documenten, mail, social media.
 - Gegeneerde documenten: (geo, jaarrekening, catalogi, websites, spreadsheets met formules, worddocumenten gegenereerd met macro's)
 - Omgang met persoonsgegevens (cookiewet, wet datalekken)
 - Uitgefaseerde en nieuwe informatiesystemen: portabiliteit/continuïteit.

Is Bewaren en Bewijzen nog goed genoeg?

- NEE:
 - Bewaren & Bewijzen niet meer geborgd door goed beheer van informatie uit werkprocessen. Werkprocessen moeten gericht (meta)informatie genereren/bewaren met oog op bewijskracht.
 - Aandacht voor technische verschillen: omgang met (semi)gestructureerde informatie, en ongestructureerde (mails, word-documenten, excelsheets)
 - Aandacht voor privacy/datalekken, portabiliteit en continuïteit tijdens gebruik van data en bij bewaren.
 - ???
- JA:
 - Scope van Bewaren en Bewijzen is beperkt en die scope is nog prima.
 - ???
- Graag uw mening