Bijlage 5. Risicomodel

Als basis voor het risicomodel heb ik mede gebruik gemaakt van het 'Adviesrapport voorbereiding archiefsector op de AVG' van Mathieu Paapst, 30 april 2018.

Nr	Omschrijving	Gevolg	Kans	Beheers	Maatregel
Risico's m.b.t. de wetgeving					
1	Het begrip 'algemeen belang' is multi-interpretabel.				Met welke maatregel kunnen we dit risico beheersen? En wat is het precieze verschil tussen 'algemeen belang' en 'gerechtvaardigd belang'? Dat is me nog niet helemaal duidelijk.
	Een verzoek tot verwijdering van persoonsgegevens wordt gehonoreerd.				In de metadata duidelijk maken welke persoonsgegevens vastgelegd zijn of het systeem *full text* doorzoekbaar maken.
	Het is onduidelijk of de selectielijst en/of het SDI moet worden aangepast i.v.m. de AVG.				
	Het is onduidelijk of verlenging van de bewaartermijnen toegestaan is i.r.t. de AVG.				
	De AVG regelt niet wat er moet gebeuren als een verwerking ophoudt te bestaan.				Totdat regelgeving anders besluit blijft de verwerking vermeld in het register.
Organisatorische aspecten					
	DIM wordt in de verwerkingsovereenkoms-ten die met marktpartijen gesloten worden niet meegenomen.				Contact opnemen met Security Center en bespreken hoe DIM een plaats krijgt in het model.
	DIM wordt aangesproken op de informatieplicht.				Contact opnemen met Security Center en juridische zaken.
	De documentatieplicht dient gearchiveerd te worden. Welk selectiecriterium is hierop van toepassing?				

	RWS moet i.h.k.v. aanbestedingen of samenwerkingsverband en informatie uit de archieven verstrekken aan derden (marktpartijen en/of andere organisatie).				Welke verantwoordelijkheid heeft de afdeling DIM in zulke gevallen? Onze stelling was tot nu toe dat dit de verant-woordelijkheid van het primair proces is.

	Het is onduidelijk wie verwerkingsverantwoorde-lijke is van de DMS-en die bij primair proces in gebruik zijn.				Met welke maatregel kunnen we dit risico beheersen?
	De afspraken met verwerker bestaan niet, of voldoen niet.				Als ze niet bestaan: afspraken alsnog maken en vastleggen. Als ze niet voldoen, dan……(zie verderop)…
DIM-proces					
	Bij invoer van personeelsgegevens wordt AVG vergeten.				Regelmatig (1 of 2x per jaar?) het archiefsysteem onderzoeken op persoonsgegevens (bijv. kopieën van paspoorten) Regelmatig de medewerkers er aan herinneren dat persoonsgegevens zo min mogelijk moeten worden opgeslagen.
	Bij de overdracht van projectarchieven zitten nog persoonsgegevens.				Projectarchieven controleren en opschonen voordat overgedragen wordt. Resultaat van deze actie als opmerking opnemen in de Verklaring van Overdracht.
	Documenten met persoonsgegevens worden bijgehouden door systemen die niet onder DIM vallen, maar wel onder de AVG en de Archiefwet.				Security Center adviseren over deze documenten en systemen.
	RWS websites die gearchiveerd worden bevatten persoonsgegevens.				Opnemen in de richtlijn webarchivering hoe hier mee moet worden omgegaan.

	Het is onduidelijk welke processen welke categorieën persoonsgegevens worden verwerkt, bewaartermijn en beveiliging.				De inventarisatie die nu door de DIM-werkgroep gedaan wordt herhalen.
	Archiefbewerking wordt uitbesteed aan een derde				Verwerkingsovereenkomst van de derde partij

	partij.				(DocDirekt, marktpartij) vragen.
	De afspraken met verwerker voldoen niet.				Met welke maatregel of sanctie kunnen we dit risico beheersen? (zie ook kopje organisatorische aspecten).
	Te bewaren archiefbescheiden worden niet overgebracht conform afspraak met Nationaal Archief (bijv.tekeningen en berekeningen).				Vermelden in het register.
Verwerkingsgronden					
	Doelbinding en of de looptijd van de doelbinding van de verwerkte persoonsgegevens is niet duidelijk.				Met welke maatregel kunnen we dit risico beheersen?
	Correcte doelbinding wordt niet nageleefd.				
	Geen controle of doelbinding nog valide is.				

P = preventie — maatregelen waardoor het risico niet meer kan optreden

R = reductie — maatregelen waardoor ofwel de kans van optreden kleiner wordt, ofwel de gevolgen worden beperkt

O = overdracht — het risico wordt bij een andere partij neergelegd (die dat wel wil dragen, bijv. een verzekeraar)

A = acceptatie — kost niets; liever bewust een risico accepteren dan het helemaal niet onderkennen

N = noodscenario — maatregelen die je neemt als het risico (toch) optreedt, om te redden wat je redden kunt

G = groot

M = middel

K = klein