Criteria voor het monitoren van de naleving van de AVG gebaseerd op de Handreiking Naleving AVG Rijksoverheid

Organisatieonderdeel: VWS kerndepartement
Naam hoofd van dienst:
Naam privacy officer:
Rapportagedatum: 5.1.2.c

Legenda
Volledig
Deels
Geen
Niet van toepassing

	KPI		KPI	Dit houdt in:	Meetwaarde	Toelichting
2	Privacy	pag. 17	De organisatie heeft alle verwerkingen voorzien van tenminste een van de in art 6 van de AVG opgenomen grondslagen en opgenomen in het register van verwerkingen.	*geen verduidelijking noodzakelijk*	Volledig	
		pag. 9	De organisatie past privacy by design en privacy by default toe bij op te stellen beleid of ontwerp van een nieuw systeem of dienst in een vroeg stadium. Hierin betrekt de organisaties thema's zoals dataminimalisatie, doelbinding, proportionaliteit, subsidiariteit en bewaartermijnen.	De organisatie beschikt over privacy by design beleid en evalueert deze periodiek.	Deels	Er is weinig kennis binnen het kerndepartement over Privacy by Design en Privacy by Default on is onderdeel van mijn jaarplan. In het afgelopen jaar zijn er twee directies die dit heeft meegenomen.
		pag. 20	De organisatie kan aantonen dat bij nieuwe systemen, beleid en diensten een Quick Scan IB en P en zonodig een PIA is uitgevoerd.	*geen verduidelijking noodzakelijk*	Geen	Dit wordt niet uitgevoerd en is niet geborgd in de inkoopprocessen.
3	Rechten van betrokkenen	pag. 10	De organisatie beschikt over procedure(s) om de rechten van de betrokkene(n) snel en adequaat af te handelen.	*geen verduidelijking noodzakelijk*	Geen	Er is nog geen procedure.
		pag. 10	De organisatie gebruikt vastgestelde modellen voor afhandeling van AVG verzoeken en bezwaar.	*geen verduidelijking noodzakelijk*	Geen	Er is geen vastgesteld model.
		pag. 10	De organisatie beoordeelt de ontvangen verzoeken periodiek op vlotte en juiste afhandeling. Zo nodig worden procedures aangepast.	Er wordt aantoonbaar (denk aan een gespreksverslag) periodiek een evaluatie van de afgehandelde AVG-verzoeken ingericht.	Geen	Dit proces is nog niet ingericht.
		pag. 10	De organisatie informeert betrokkenen op transparante wijze over de verwerking van persoonsgegevens.	Per verwerking is aantoonbaar de informatieplicht in kaart gebracht en daarin worden de toepasselijke wettelijke vereisten (art 13 en 14 van de AVG) meegenomen.(dit kan opgenomen worden in het opmerkingenveld in het verwerkingenregister).	Geen	Ik begrijp hier de toelichting niet.
		pag. 10	De organisatie heeft op al haar websites een privacy verklaring geplaatst. Deze verklaring is eenvoudig vindbaar, zichtbaar, voldoende specifiek en makkelijk toegankelijk.	*geen verduidelijking noodzakelijk*	Volledig	Bijna alle websites hebben een privacy-verklaring.
		pag. 11	De organisatie heeft aantoonbaar inzichtelijk gemaakt waar gebruik wordt gemaakt van geautomatiseerde besluitvorming op basis van profilering en op basis van welke grondslag dat gebeurt.	*geen verduidelijking noodzakelijk*	Niet van toepassing	Er zijn geen systemen bekend met geautomatiseerde besluitvorming.
				Voor alle verwerkingen waarbij sprake is van geautomatiserde besluitvorming op basis van profilering is een PIA uitgevoerd.	Niet van toepassing	
				Alle betrokkenen zijn vooraf aantoonbaar geinformeerd over de geautomatiseerde besluitvorming, de mogelijke gevolgen die dit met zich meebrengt en welke bewaartermijn worden gehanteerd.	Niet van toepassing	
				De organisatie heeft een proces ingericht dat betekenisvolle menselijke tussenkomst in de besluitvorming borgt, en waar de betrokkene een beroep op kan doen.	Niet van toepassing	
		pag. 12	Als de organisatie persoonsgegevens verder wil gaan verwerken voor een ander doel dan waarvoor de gegevens zijn verzameld, informeert hij aantoonbaar de betrokkene, voor aanvang van de verdere verwerking, over dat andere doel.	*geen verduidelijking noodzakelijk*	Geen	Geen inzicht of dit bij ons het geval is, heb het vermoeden van wel.
		pag. 12	De organisatie heeft in kaart gebracht bij welke verwerkingen sprake is van contact met kinderen en zij heeft voor deze contactmomenten duidelijke, eenvoudige, begrijpelijke en beknopte taal gehanteerd in een toegankelijke vorm.	*geen verduidelijking noodzakelijk*	Niet van toepassing	
4	Privacybeleid	pag. 13	De organisatie beschikt over privacy beleid welke door of namens de SG is vastgesteld.	*geen verduidelijking noodzakelijk*	Volledig	VWS beleid, geen beleid voor KD
		pag. 13	Het privacybeleid wordt minimaal een keer in de drie jaar geëvalueerd en geactualiseerd. Zo nodig wordt het beleid opnieuw vastgesteld.	*geen verduidelijking noodzakelijk*	Niet van toepassing	
		pag. 13	De organisatie ziet toe op periodieke trainingen van nieuw en bestaand personeel dat betrokkenen is bij de verwerking.	De organisatie kent een opleidingsplan om het kennisniveau van de AVG op peil te houden.	Deels	Er wordt niet op directie niveau getraind aan de hand van de verwerkingen. Er is een schema voor trainingen IB- en P-coordinatoren gemaakt.
		pag. 13	De organisatie organiseert jaarlijks een bewustwordingscampagne voor de naleving van de AVG.	De organisatie kent een jaarlijks bewustwordingsplan om de naleving van de AVG te waarborgen en maakt gebruik van meetinstrumenten om het bewustwordingsniveau en de impact van de bewustwordingsmiddelen in kaart te brengen.	Deels	Dit proces is nog niet ingericht. Wel het verzoek GoodHabitz module Privacy te volgen, maar dat is voor een klein deel opgevolgd door directies.
5	Organisatie van privacy	pag. 14	De organisatie heeft haar privacy governance in kaart gebracht waarin in ieder geval de verschillende rollen zoals omschreven in hoofdstuk 5 van de Handreiking naleving AVG in zijn opgenomen. Deze governance is kenbaar gemaakt bij de betrokken partijen en vastgesteld door de hoofd van dienst.	De organisatie kent een privacy governance document en actualiseert deze periodiek. Dit kan ook opgenomen zijn in het privacy beleid.	Geen	Dit document is nog niet gemaakt voor KD.
		pag. 14	De organisatie heeft een kwaliteitscyclus ingericht voor gegevensbescherming en privacy om de blijvende goede omgang met persoonsgeevens te waarborgen.	*geen verduidelijking noodzakelijk*	Deels	Dit proces is niet ingericht, wel bij directie OBP
		pag. 15	De organisatie toetst haar verwerkers regelmatig op de naleving van de eisen van de AVG	*geen verduidelijking noodzakelijk*	Geen	Dit proces is niet ingericht!
6	Register van verwerkingsactiviteiten	pag. 17	De organisatie houdt een register bij van verwerkingsactiviteiten (in haar rol als verwerkingsverantwoordelijk en eventueel ook als verwerker) en zorgt dat deze voldoet aan het Voorschrift Informatiebeveiliging Rijksdienst bijzondere informatie (VIR BI). In het register zijn slechts gegevens opgenomen tot en met het niveau departementaal vertrouwelijk.	*geen verduidelijking noodzakelijk*	Volledig	Ik zal nog dubbelchecken of de VIR-BI is aangehouden.
		pag. 17	Per verwerking zijn minimaal de volgende bijlagen opgenomen: PIA's/quickscan IB&P, verwerkersovereenkomsten of afspraken, advies van de FG en andere voor de verwerking relevante documentatie.	*geen verduidelijking noodzakelijk*	Deels	Alleen PIA's en verwerkersovereenkomsten. De quickscans en andere relevante documentatie wordt opgeslagen in het ISMS.
		pag. 17	De organisatie heeft een proces ingericht om de juistheid en de volledigheid van het register te waarborgen en periodiek te controleren. In dit proces is minimaal aandacht voor wijzigende wet- en regelgeving, IT-architectuur, onderkende informatiesystemen bij informatiebeveiliging en het ordeningsplan/selectielijst.	In dit proces is minimaal aandacht voor wijzigende wet- en regelgeving, IT-architectuur, onderkende informatiesystemen bij informatiebeveiliging en het ordeningsplan/selectielijst.	Deels	Dit proces is niet ingericht, wel deels bij OBP. Echter niet op het niveau als hiernaast omschreven.
		pag. 18	In het kader van transparantie en het streven naar een open overheid publiceert de Rijksoverheid vastgestelde verwerkingen *in beginsel* op internet.	*geen verduidelijking noodzakelijk*	Deels	Er is een achterstand in reviewen en publiceren, daarnaast zijn veel verwerkingen nog niet opgenomen in het register.
7	Risicogestuurd beveiligen van persoonsgegevens	pag. 19	De organisatie heeft per verwerking de noodzakelijke technische en organisatorische maatregelen geidentificeerd en geimplementeerd en neemt de controle op de werking van deze maatregelen op in het periodieke proces van kwaliteitscontrole op het register.	*geen verduidelijking noodzakelijk*	Geen	Dit proces is niet ingericht.
		pag. 20	De organisatie beschikt over een procedure meldplicht datalekken. Deze procedure is makkelijk te vinden voor medewerkers. Hierin is opgenomen dat het datalek wordt gerapporteerd aan het juiste managementniveau in de organisatie en in geval melding bij de AP tevens aan de CPO VWS.	*geen verduidelijking noodzakelijk*	Deels	Procedure VWS concern, van KD is in de maak, evenals incidentenregister + handleiding medewerkers
		pag. 20	De organisatie houdt een register bij van al haar datalekken als verwerker en als verwerkingsverantwoordelijke.	*geen verduidelijking noodzakelijk*	Volledig	zie bijlage incidenten 2020
		pag. 20	Periodiek wordt het voorkomen en de afhandeling inclusief registratie van datalekken geanalyseerd. Hierover wordt gerapporteerd aan het management. Zo nodig worden aanvullende maatregelen genomen ter voorkoming van datalekken.	*geen verduidelijking noodzakelijk*	Geen	Dit proces is niet ingericht. Alles wordt ad hac afgehandeld, er is geen ruimte voor analyse.
		pag. 20	De organisatie voert een PIA uit voor alle verwerkingen die hiervoor in aanmerking komen. Of een PIA is aangewezen wordt bepaald aan de hand van een Quick Scan IB en P.	De definitieve PIA's zijn opgeslagen in het register gegevensverwerking en zijn van handtekening voorzien van de verwerkingsverantwoordelijke of de hiervoor gemandateerde ambtenaar.	Deels	Voor de verwerkingen waar een quickscan IB & P is uitgevoerd, is dit correct. Er zijn echter heel veel verwerkingen die nog een quickscan dienen te krijgen.
				Iedere PIA is voorzien van een advies van de FG en een beschrijving hoe opvolging is gegeven aan het advies.	Deels	Dit gebeurt in de praktijk, maar nog niet efficient. Met name de opvolging.
				Er is gebruik gemaakt van het rijksbrede model voor de PIA. Tevens is gewaarborgt dat iedere Pia elke drie jaar wordt geactualiseerd.	Deels	Rijkspia model ja, evaluatie per drie jaar is nog niet juist ingericht.
		pag. 20	Bij de uitvoering van de PIA zijn minimaal de volgende medewerkers betrokken: (gedelegeerd) eigenaar van het informatiesysteem of -proces en de gemandateerd medewerker, de medewerker die betrokken is bij de uitvoering van het relevante werkproces, de medewerker met expertise op het gebied van privacy, en, indien relevant, informatiebeveiliging en de betreffende projectleider en -deskundigen.	*geen verduidelijking noodzakelijk*	Volledig	Als er dan een PIA wordt uitgevoerd, ja, dan gaat dit wel goed :-)
		pag. 20	Het inkoopproces is zo ingericht dat bij de inkoop van diensten of systemen waarbij persoonsgegevens worden verwerkt standaard een PIA wordt overwogen.	*geen verduidelijking noodzakelijk*	Geen	Nee, dit proces is nog niet goed ingericht, knelpunt is tijd, geen tijd voor quickscans.
		pag. 20	Er is een procesbeschrijving voor het uitvoeren van PIA's en het opvolgen van uitkomsten.	*geen verduidelijking noodzakelijk*	Geen	Nee, dit proces is nog niet ingericht.
					Geen	
8	Doorgifte van persoonsgegevens aan derde landen of en internationale organisatie	pag. 15	De organisatie schakelt alleen verwerkers in indien deze voldoende garanties bieden dat zij aan de wettelijk vereisten voor gegevensbescherming voldoen.	Dit is aantoonbaar ingericht doordat privacy een standaard onderdeel is in het programma van eisen bij een aanbesteding of inkooptraject.	Deels	Nee, dit is het grootste knelpunt. Inkooptraject is niet centraal belegd en veroorzaakt risico's voor de organisatie. Sommige inkooptrajecten gaan zoals het hoort.
		pag. 15	Met alle verwerkers binnen de Staat der Nederlanden is een verwerkersafspraak afgesloten.	Daarbij is gebruikgemaakt van het verwerkersafspraakmodel zoals te vinden op het Rijksportaal.	Deels	Nee, dit is helaas niet het geval.
		pag. 15	Met alle verwerkers buiten de Staat der Nederlanden is een verwerkersovereenkomst afgesloten.	Daarbij is gebruikgemaakt van het Arvodi-model, het Arbit-model en het Ariv-model zoals opgenomen in PIANOo en op rijksportaal gepubliceerd.	Deels	Nee, dit is helaas niet het geval.
		(nog) geen onderdeel van AVG handreiking	Is er sprake van gezamenlijke verwerkingsverantwoordelijkheid, wat voorkomt als twee of meerdere partijen doel en middelen van verwerken bepalen, moeten ook de onderlinge verhoudingen tot die verwerking worden gedocumenteerd (in leders register van verwerkingsactiviteiten, maar tevens in de afsprakenkaders).	Dit speelt o.a. bij verwerken van persoonsgegevens tussen ketenpartijen. Partijen kijken in deze sfeer tevens naar de ketensamenwerking daarbij, zodanig dat ieders privacy administratie op elkaar aansluit. Een verwerker die zelf zijn middelen kiest om daar vorm aan te geven is daarmee overigens géén gezamenlijk verwerkingsverantwoordelijke. Kernpunt daarvoor ligt in de eindbeslissingsbevoegdheid.	Geen	hier wordt mee geworsteld, zie laatste Privacykring meeting.
		pag. 22	Ook bij doorgifte van persoonsgegevens aan een derde land (landen buiten de EEG) of internationale organisaties wordt de privacy en gegevensbescherming gewaarborgd. Hierbij is aandacht voor alle daarbij vereiste waarborgen waaronder doorgifte plaatsvindt zoals adequaatheidsbesluiten, passende waarborgen en, bindende bedrijfsvoorschriften.	Er moet duidelijkheid zijn (register van verwerkingsactiviteiten) welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd. Er wordt rekening gehouden met de consequenties van de actualiteit van wetgevingskaders die op doorgifte kunnen inwerken (denk aan de recente uitspraak over het onrechtmatig zijn van de Privacy Shield overeenkomst in relatie tot gegevensdeling met Amerikaanse bedrijven).	Geen	Ik heb nog geen goed beeld of hier sprake van is.