Toezichtplan Functionaris Gegevensbescherming 2021

Inleiding	3
Doelstelling FG Toezichtplan	3
Positie FG	3
Overleg	3
Rapportage	3
Toezichtpunten 2021	4

Inleiding

Dit document bevat het FG toezichtplan van de Functionaris voor Gegevensbescherming (FG) van het CAK voor de periode januari 2021 – december 2021. De Algemene Verordening Gegevensbescherming (AVG) verplicht het CAK om een FG aan te stellen. De FG is de persoon binnen een organisatie die toezicht houdt op de toepassing en naleving van de AVG. De FG heeft een breed takenpakket, waaronder het creëren van privacy-bewustzijn in de organisatie en het actief betrokken zijn bij de wijze waarop de organisatie omgaat met gegevens. De FG fungeert als eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP). Kenmerkend voor de FG is dat deze een onafhankelijke rol heeft binnen de organisatie. De FG rapporteert rechtstreeks aan de voorzitter van de RvB van het CAK. De FG ziet binnen het CAK dus toe op de omgang met persoonsgegevens. Om dit te kunnen doen, kan hij:

- informatie verzamelen over gegevensverwerkingen binnen de organisatie;
- deze verwerkingen analyseren en beoordelen of ze aan de wet voldoen;
- informatie, adviezen en aanbevelingen geven aan de organisatie.

De FG werkt nauw samen met de Coördinerend Privacy Officer (CPO). Zij hebben echter wel twee inhoudelijk verschillende rollen. De CPO is verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid. Tevens biedt de CPO ondersteuning bij de uitvoering van dit beleid. De CPO speelt een grote rol binnen de organisatie, door te fungeren als aanspreekpunt voor privacyvraagstukken die spelen in de organisatie. De FG controleert vervolgens of inderdaad gesproken kan worden van een rechtmatige gegevensverwerking.

Doelstelling FG toezichtplan

Doel van het FG toezichtplan is om het CAK aantoonbaar te kunnen laten voldoen aan de vereisten van privacy regelgeving door middel van het toetsen van en het adviseren over de inrichting van het risicobeheersingsraamwerk op het privacy management. In 2019 heeft PWC een aantal aanbevelingen rondom informatiebeveiliging en privacy gedaan. Hoewel informatiebeveiliging en privacy nauw met elkaar verweven zijn ziet dit toezichtplan enkel op privacy. Het CIO office heeft het “Strategisch Informatiebeveiligingsbeleid CAK 2020 – 2022” opgesteld en rapporteert afzonderlijk met betrekking tot informatiebeveiliging.

Taken FG

De FG dient nauw betrokken te worden bij al hetgeen verband houdt met de privacy organisatie. Dit houdt onder meer maar niet uitsluitend in dat de FG om advies wordt gevraagd bij geschillen, wordt geraadpleegd in geval van een datalek of dergelijk incident en dat relevante auditrapporten ten aanzien van gegevensbescherming en/of informatiebeveiliging integraal en proactief met de FG worden gedeeld. Verder vervult de FG een onafhankelijke rol, dit heeft tot gevolg dat de FG daar ook naar moet kunnen handelen (door o.a. ondersteuning en toegangsverschaffing).

Overleg

Maandelijks vindt een overleg plaats tussen de FG, de CPO en de coördinator datalekken van het CAK. Tevens neemt de FG deel aan het tweewekelijks overleg Security en Privacy met de Chief Information Security Officer (CISO), Information Security Officer (ISO) en de CPO van het CAK. Ook is de FG aanwezig bij de overleggen van het Privacy & Security gilde. Buiten het CAK neemt de FG deel aan het overleg Functionaris Gegevensbescherming Manifestgroep (IND, SVB, Belastingdienst, ministerie van Justitie & Veiligheid, ministerie van Financiën en CBR) en het FG overleg met ZonMw, Nza, Dopingautoriteit, CIZ, ZiNL, VWS.

Rapportage

De FG brengt gelijk aan de P&C cyclus per kwartaal aan de voorzitter van de Raad van Bestuur een rapportage uit over de voortgang van dit toezichtplan en over de stand van zaken met betrekking tot de bescherming van persoonsgegevens binnen het CAK. Aan het einde van ieder jaar biedt de FG een

jaarverslag aan de voorzitter van de Raad van Bestuur van het CAK aan. In genoemde rapportages zal in ieder geval worden aangegeven in hoeverre de verwerkingen van persoonsgegevens door het CAK voldoen aan de Algemene Verordening Gegevensbescherming (AVG). In het jaarverslag wordt daarnaast teruggekeken naar het afgelopen jaar. Wat heeft het CAK bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te (blijven) voldoen aan de AVG? Ook worden aanbevelingen gedaan om gegevensbescherming en privacy in het komende jaar naar een hoger niveau te tillen. Over de contacten die de FG met AP heeft gehad zal ook worden gerapporteerd.

Aan de hand van de volgende thema's zal de FG dit jaar toezien op de naleving van de AVG binnen het CAK:

1. **Beleid**
   Het Privacybeleid CAK biedt het kader waarin het CAK aangeeft aan welke principes het zich houdt. Het laat zien hoe het CAK omgaat met persoonsgegevens en welke maatregelen het treft om te voldoen aan de wet- en regelgeving.

   Acties komend jaar:
   De FG ziet er op toe dat het Privacybeleid CAK volledig en actueel is en of binnen het CAK gehandeld wordt naar hetgeen daarin is bepaald.

2. **Processen**
   De verwerkingen van persoonsgegevens van het CAK dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan het CAK in gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren.

   Acties komend jaar:
   De FG zal bekijken in hoeverre privacy wordt meegenomen in het ontwerpen/aanpassen van o.a. producten, systemen of processen (privacy by design en default). Tevens zal de FG steeksproefsgewijs toetsen, beoordelen en rapporteren hoe het DPIA proces verloopt en of de aanbevelingen uit de verrichte DPIA's ook daadwerkelijk zijn uitgevoerd en resultaat opleveren.

3. **Organisatorische inbedding**
   Voor een goede en juiste uitvoering is het van belang dat eenieder binnen het CAK op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren. Vrijwel iedere regeling of stafafdeling heeft een contactpersoon bij wie medewerkers terecht kunnen met vragen over het verwerken van persoonsgegevens. Samen met de privacy officer en de CISO vormen zij het Privacy & Security gilde.

   Acties komend jaar:
   De FG ziet er op toe dat de diverse contactpersonen die zich met privacy bezig houden hun kennis van privacy onderhouden, bijvoorbeeld door middel van het volgen van opleidingen. Ook zal de FG bezien of de rol van de privacyfunctionarissen formeel is ingebed in het functiehuis. Clusteruitvoering heeft medio december een plan van aanpak opgeleverd om te zorgen dat de clusters in control komen. De FG ziet er op toe dat deze plannen van aanpak worden uitgevoerd en bewaakt. Daarnaast is het van belang dat zij ook daadwerkelijk door de organisatie in de gelegenheid worden gesteld om hun taken naar behoren te kunnen vervullen. Binnen het CAK wordt op verschillende manieren aan privacy bewustwording gedaan, bijvoorbeeld door het

aanbieden van e-learnings. Bewustwording kan verder vergroot worden door meer berichtgeving over privacy op de CAK intranetsite en het houden van bijeenkomsten met privacy als onderwerp.

4. **Rechten van betrokkenen**
Het CAK dient degene waar de gegevens van verwerkt worden (de betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen genomen worden om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten, waaronder het inzagerecht controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Acties komend jaar:
De FG zal er op toezien dat het voldoen aan verzoeken van betrokkenen procesmatig goed wordt geborgd.

5. **Samenwerking**
Het CAK werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. Het CAK dient dan ook afspraken te maken met deze andere partijen. Afspraken worden vastgelegd in verwerkersovereenkomsten en convenanten. In het verwerkingenregister worden het aantal verwerkingen geregistreerd.

Acties komend jaar:
Komend jaar wordt er hard doorgewerkt aan een beter systeem waarin het aantal verwerkingen wordt geregistreerd. De FG zal toezien op een juiste en tijdige implementatie. Door steekproeven en reviews zal de FG nagaan of in voorkomende gevallen ook daadwerkelijke een verwerkersovereenkomst is afgesloten en de inhoud van de verwerkersovereenkomsten beoordelen.

6. **Beveiliging**
Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat het CAK passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Acties komend jaar:
Zoals hierboven onder “Doelstelling FG toezichtplan” al opgemerkt zal CIO office er op toezien dat het CAK passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. De FG zal echter wel beoordelen hoe het datalekkenproces verloopt.

Aanbiedingsformulier RvB – RvB Directieraad

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: bestuurssecretaris@hetcak.nl
Memo's kunnen uitsluitend worden ingediend door een manager of directeur die direct aan de RvB rapporteert (N-1).

1	**Indiener**	[redacted]
2	**Titel**	Functionaris Gegevensbescherming (FG)
3	**Datum behandeling RvB / RvB Directieraad**	*DD / MM / JJJJ*
4	**Aard van de behandeling** *Vakje aanklikken.*	☐ **Ter advisering** ☐ **Ter besluitvorming** ☒ **Ter bespreking** ☐ **Ter kennisname** ☐ **Ter ondertekening** ☐ **Anders:**
5	**Vertrouwelijk behandelen?**	☐ **ja** ☒ **nee**
6	**Eerder behandeld in/met** *Gremium of functie noemen.*	☐ **Raad van bestuur** ☐ **Raad van bestuur - Directieraad**

Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie:

☐ **Overeenstemming** *(geen toelichting vereist)*

☐ **Geen overeenstemming, toelichting:**

7 **Korte samenvatting**

In het Toezichtplan Functionaris Gegevensbescherming 2021 staat beschreven hoe de FG zijn rol het komend jaar wil gaan invullen. Meer specifiek staat in het toezichtplan beschreven op welke punten de FG toezicht gaat houden, hoe hij dat doet en op welke wijze hij daarover rapporteert. Doel van het toezichtplan is om het CAK aantoonbaar te kunnen laten voldoen aan de vereisten van de privacy regelgeving.

8 **Gevraagd besluit**

Indien van toepassing.

9 **Betrokkenheid Ondernemingsraad**

- [x] **Geen**
- [ ] **Adviesplichtig**
- [ ] **Instemmingsplichtig**

10 **Adviezen intern**

Elk besluitmemo moet voorzien zijn van een intern advies

		N-1:	Advies overgenomen ja/nee inclusief motivering
A	Regelingen (Wmo/ZvW/ WLZ/BTL)	RD	
B	Risk/Compliance	R&C	
C	ICT en informatievoorziening	CIO	De aanvullingen van de Coördinerend Privacy Officer en de Chief Information Security Officer zijn in het toezichtplan opgenomen.
D	ICT en informatievoorziening	ICT	
E	Strategisch / beleidsmatig	S&B	
F	Financieel - beheerskosten	Control	
G	Personele zaken	HR	
H	Corporate juridisch en politiek-bestuurlijk	Bestuurs-zaken	
I	Privacy	FG	
J	Overig, nl		

Aanbiedingsformulier RvB – RvB C/ K MT CAK

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: [redacted]
Memo's kunnen uitsluitend worden ingediend door een manager of directeur die direct aan de RvB rapporteert.

1	Indiener	[redacted]
2	Titel	AVG kwartaalrapportage en stand van zaken 2021 naleving AVG Rijk
3	Datum behandeling RvB / RvB MT CAK	0 2 1 1 2 0 2 1 *DD / MM / JJJJ*
4	Aard van de behandeling *Vakje aanklikken*	☐ Ter advisering ☑ Ter besluitvorming ☐ Ter bespreking ☑ Ter kennisname ☐ Ter ondertekening ☐ Anders:
5	Vertrouwelijk behandelen	☐ Ja ☑ Nee
6	Eerder behandeld in/met *Gremium of functie noemen*	☐ Raad van Bestuur ☐ Raad van Bestuur – MT CAK Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie: ☐ Overeenstemming *(geen toelichting vereist)* ☐ Geen overeenstemming, toelichting: <Toelichting>

7	Korte samenvatting	De Q3 2021 kwartaalrapportage AVG is ter kennisname en heeft ten doel de RvB te informeren over de status van de werking van het privacy stelsel. De rapportage is met betrokkenen binnen de clusters besproken. De stand van zaken (2021) van de naleving van AVG Rijk betreft een jaarlijkse uitvraag vanuit VWS. De privacy officer heeft dit overzicht met de RD's besproken.
8	Gevraagd besluit *Indien van toepassing*	De RvB wordt gevraagd de stand van zaken (2021) van de naleving AVG Rijk vast te stellen zodat verzending aan VWS kan volgen.
9	Betrokkenheid ondernemingsraad	☑ Geen ☐ Adviesplichtig ☐ Instemmingsplichtig

10 Adviezen intern

Elk besluitmemo moet voorzien zijn van een intern advies

		N-1:	Advies overgenomen ja/nee inclusief motivering
A	Regelingen (Wmo/Zvw/Wlz/Btl)	RD	Ja
B	Risk/Compliance	R&C	n.v.t.
C	ICT en informatievoorziening	CIO	Opsteller
D	ICT en informatievoorziening	ICT	n.v.t.
E	Strategisch / beleidsmatig	S&B	n.v.t.
F	Financieel - beheerskosten	Control	n.v.t.
G	Personele zaken	HR	n.v.t.
H	Corporate juridisch en politiek-bestuurlijk	Bestuurs-zaken	n.v.t.
I	Privacy	FG	n.v.t.
J	Overig, nl		n.v.t.

Aanbiedingsformulier RvB – RvB MT CAK

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: [redacted]
Memo's kunnen uitsluitend worden ingediend door een manager of directeur die direct aan de RvB rapporteert.

1	Indiener	[redacted]
2	Titel	Advies uitstel AVG audit
3	Datum behandeling RvB / RvB MT CAK	2 2 1 2 2 0 2 0 *DD / MM / JJJJ*
4	Aard van de behandeling *Vakje aanklikken*	☑ Ter advisering ☐ Ter besluitvorming ☐ Ter bespreking ☐ Ter kennisname ☐ Ter ondertekening ☐ Anders:
5	Vertrouwelijk behandelen	☐ Ja ☑ Nee
6	Eerder behandeld in/met *Gremium of functie noemen*	☐ Raad van Bestuur ☐ Raad van Bestuur – MT CAK Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie: ☐ Overeenstemming *(geen toelichting vereist)* ☐ Geen overeenstemming, toelichting: <Toelichting>

7	Korte samenvatting	Gezien de resultaten van een beperkte deelwaarneming adviseert afdeling IA de RvB in de eerste helft van 2021 opdracht te geven voor wederom een beperkt onderzoek naar implementatie AVG welke, bij positieve resultaten, kan worden omgezet naar een volledige audit.
8	Gevraagd besluit *Indien van toepassing*	<Gevraagd besluit>
9	Betrokkenheid ondernemingsraad	☑ Geen ☐ Adviesplichtig ☐ Instemmingsplichtig

10 Adviezen intern

Elk besluitmemo moet voorzien zijn van een intern advies

	Onderwerp:	Wie:	Advies overgenomen ja/nee inclusief motivering
A	Regelingen (Wmo/Zvw/Wlz/Btl)	RD	<A>
B	Risk/Compliance	R&C	<B>
C	ICT en informatievoorziening	CIO	<C>
D	ICT en informatievoorziening	ICT	<D>
E	Strategisch / beleidsmatig	S&B	<E>
F	Financieel - beheerskosten	Control	<F>
G	Personele zaken	HR	<G>
H	Corporate juridisch en politiek-bestuurlijk	Bestuurs-zaken	<H>
I	Privacy	FG	<I>
J	Overig, nl		<J>

Aanbiedingsformulier RvB – RvB MT CAK

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: [redacted]
Memo's kunnen uitsluitend worden ingediend door een manager of directeur die direct aan de RvB rapporteert.

1	Indiener	[redacted]
2	Titel	auditrapport GRC AVG Controlepunten
3	Datum behandeling RvB / RvB MT CAK	0 7 0 9 2 0 2 1 *DD / MM / JJJJ*
4	Aard van de behandeling *Vakje aanklikken*	☐ Ter advisering ☐ Ter besluitvorming ☐ Ter bespreking ☑ Ter kennisname ☐ Ter ondertekening ☐ Anders:
5	Vertrouwelijk behandelen	☐ Ja ☑ Nee
6	Eerder behandeld in/met *Gremium of functie noemen*	☐ Raad van Bestuur ☐ Raad van Bestuur – MT CAK Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie: ☐ Overeenstemming *(geen toelichting vereist)* ☐ Geen overeenstemming, toelichting: <Toelichting>

7	Korte samenvatting	Het oordeel van de audit op AVG controlepunten per 6 januari 2021 luidt: **onvoldoende**. Internal Audit heeft de bevindingen overgedragen aan CIO Office. Op 8 juli 2021 heeft IA de opvolging van de bevindingen beoordeeld. De conclusie is dat waar verbetering heeft plaatsgevonden, de controlepunten nu van voldoende niveau zijn. Het merendeel van de controlepunten is echter niet of onvoldoende verbeterd. Hierdoor biedt de huidige set aan AVG controlepunten in onvoldoende mate de juiste randvoorwaarden voor een effectieve monitoring van AVG normen in KCD.
-	Gevraagd besluit *Indien van toepassing*	–
9	Betrokkenheid ondernemingsraad	☑ Geen ☐ Adviesplichtig ☐ Instemmingsplichtig

10 Adviezen intern

Elk besluitmemo moet voorzien zijn van een intern advies

	Onderwerp:	Wie:	Advies overgenomen ja/nee inclusief motivering
A	Regelingen (Wmo/Zvw/Wlz/Btl)	RD	<A>
B	Risk/Compliance	R&C	<B>
C	ICT en informatievoorziening	CIO	<C>
D	ICT en informatievoorziening	ICT	<D>
E	Strategisch / beleidsmatig	S&B	<E>
F	Financieel - beheerskosten	Control	<F>
G	Personele zaken	HR	<G>
H	Corporate juridisch en politiek-bestuurlijk	Bestuurs-zaken	<H>
I	Privacy	FG	<I>
J	Overig, nl		

Aanbiedingsformulier RvB

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: [redacted]
Memo's kunnen uitsluitend worden ingediend door een manager of directeur die direct aan de RvB rapporteert.

1	Indiener	[redacted]
2	Titel	Informerend memo datalekken WAN
3	Datum behandeling RvB	0 7 1 2 2 0 2 1 *DD / MM / JJJJ*
4	Aard van de behandeling *Vakje aanklikken*	☐ Ter advisering ☐ Ter besluitvorming ☐ Ter bespreking ☑ Ter kennisname ☐ Ter ondertekening ☐ Anders:
5	Vertrouwelijk behandelen	☐ Ja ☑ Nee
6	Bespreking in aanwezigheid van	☑ Indiener ☐ Andere gasten naast indiener, namelijk:
7	Eerder behandeld in/met *Gremium of functie noemen*	☐ Raad van Bestuur ☐ Raad van Bestuur – MT CAK Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie: ☐ Overeenstemming *(geen toelichting vereist)* ☐ Geen overeenstemming, toelichting: <Toelichting>

8	Korte samenvatting	In de regeling wanbetalers zijn in bepaalde situaties onjuiste broninhouders aangeschreven. Het gaat hierbij om 2 situaties: 1 Nieuwe aanmeldingen: de polisadministratie van UWV was hierbij niet actueel. Met FG is afgestemd dat dit een 'geaccepteerd datalek' is. 2 Herstart van broninhouding: hierbij wordt de laatst bekende werkgever/uitkeringsinstantie aangeschreven, maar het kan zijn dat dit niet juist is voor de actuele situatie van de klant. Maatregelen om dit risico te mitigeren worden in gang gezet. Bij de AP is een voorlopige melding gemaakt. Op de 1e situatie vindt nog afstemming plaats met FG's van andere organisaties. Afhankelijk daarvan zal de voorlopige melding aan AP worden ingetrokken of worden aangevuld met een nadere toelichting en mitigerende maatregelen. Tot slot zal het proces rondom deze datalekken geëvalueerd worden.
9	Gevraagd besluit *Indien van toepassing*	Niet van toepassing
10	Betrokkenheid ondernemingsraad	☑ Geen ☐ Adviesplichtig ☐ Instemmingsplichtig

11 Adviezen intern

Elk besluitmemo moet voorzien zijn van een intern advies

	Onderwerp:	Wie:	Advies overgenomen ja/nee inclusief motivering
A	Regelingen (Wmo/Zvw/Wlz/Btl)	RD	nvt
B	Risk/Compliance	R&C	nvt
C	ICT en informatievoorziening	CIO	Privacy officer betrokken in traject
D	ICT en informatievoorziening	ICT	nvt
E	Strategisch / beleidsmatig	S&B	Advies overgenomen
F	Financieel - beheerskosten	Control	nvt
G	Personele zaken	HR	nvt
H	Corporate juridisch en politiek-bestuurlijk	Bestuurs-zaken	In rol van FG; advies overgenomen
I	Privacy	FG	Advies overgenomen
J	Overig, nl		Datalekmanager tevens betrokken bij traject.

Datalekken bij aanschrijven broninhouders wanbetalersregeling

RvB

[redacted] – Manager UR, [redacted] – Manager KC, [redacted] – Regelingadviseur, [redacted] – Strategisch adviseur S&B, [redacted] – Datalekmanager, [redacted] – Privacy officer, [redacted] – Functionaris gegevensbescherming, [redacted] – Teammanager V&B2, [redacted] – Teammanager MB, [redacted] – Business Consultant

[redacted] – directeur Zvw

Datalekken bij aanschrijven broninhouders wanbetalers-regeling

n.v.t.

2 december 2021

1.0

Het bestuur is recent door de datalekmanager en de directeur Zvw geïnformeerd over een mogelijk datalek in de regeling Wanbetalers. Het datalek raakt mogelijk ook de kern van uitvoering door het CAK; als broninformatie die niet up to date is leidt tot datalekken, heeft dit CAK-breed grote impact.

Omdat op dat moment nog analyse en afstemming plaatsvond of het daadwerkelijk om datalekken ging, kon dit op dat moment nog niet met zekerheid aangegeven worden. Inmiddels heeft de analyse plaatsgevonden en is vastgesteld dat er inderdaad sprake is van een datalek en is hiervan ook een voorlopige melding gemaakt bij de Autoriteit Persoonsgegevens (AP).

Met dit memo wordt informatie gegeven over de oorzaken, de impact en risico's van dit type datalekken. Ook worden de mitigerende maatregelen toegelicht om het aantal datalekken in de toekomst te reduceren en wordt ingegaan op de afspraken die zijn gemaakt voor afstemming met de AP en evaluatie van het interne proces rondom datalekken.

Aanleiding

Op basis van gegevens uit de polisadministratie van het UWV worden werkgevers aangeschreven met het verzoek de bestuursrechtelijke premie in te houden op het salaris van de werknemer die bij ons is aangemeld door de zorgverzekeraar. De werkgever wordt gevraagd dit bedrag, tot nader bericht van het CAK of tot uitdiensttreding van de werknemer, maandelijks naar het CAK over te maken. Mocht de werknemer uit dienst gaan wordt de werkgever tevens verzocht dit aan het CAK door te geven.

Naar aanleiding van een gesignaleerd verbeterpunt is in juli een analyse uitgevoerd naar het aantal beschikkingen dat naar 'oude' broninhouders (BI) verstuurd is. Na terugmeldingen van BI's via telefoon, email of middels retourzendingen van beschikkingen zijn in eerste instantie 71 gevallen geconstateerd (± 1% van het totale aantal verstuurde beschikkingen over dezelfde periode). Van het totale aantal beschikkingen komt dus ongeveer 99% wel bij de actuele BI's terecht. Een deel van de BI's heeft de uitdienstmelding pas doorgegeven nadat het HAD-proces (herinneren, aanmanen, deurwaarder) richting de BI al is opgestart.

Tijdens de analysefase is de vraag gerezen of sprake is van data incidenten of datalekken. In afwachting van het intern onderzoek is op 25 november jl. een voorlopige melding van een datalek bij AP gedaan.

Oorzaken

Er zijn twee oorzaken waardoor beschikkingen niet naar de actuele BI worden gestuurd:

1. Nieuwe aanmeldingen:
   Dit betreft de eerste aanschrijving richting de BI voor een werknemer/uitkeringsgerechtigde die voor het eerst is aangemeld in de wanbetalersregeling. Hierbij kan het gebeuren dat uitgevraagde brondata van UWV Polisadministratie niet actueel is. Dit betrof circa 10% van de eerdergenoemde 1% onjuiste aanschrijvingen.
2. Bestaande aanmeldingen:
   Dit betreft klanten die eerder in de wanbetalersregeling zaten en waar inhouding op salaris of uitkering plaatsvond. De betreffende klant heeft een betalingsregeling getroffen met de zorgverzekeraar, waardoor geen bestuursrechtelijke premie meer wordt opgelegd. Als deze betalingsregeling mislukt, wordt hij/zij weer bij het CAK aangemeld en wordt broninhouding opnieuw gestart. Het kan daarbij gebeuren dat gegevens van de BI's in OHI niet meer actueel zijn. Dit betrof circa 90% van eerdergenoemde 1% onjuiste aanschrijvingen.

In onderstaande paragrafen wordt nader toegelicht wat de aanleiding is van het datalek, welke risico's er zijn en welke maatregelen worden getroffen om het risico te mitigeren.

Nieuwe aanmeldingen

Het CAK maakt voor de uitvoering van de wanbetalersregeling gebruik van brongegevens uit de basisregistraties, waaronder de Basisregistratie Inkomens (de UWV Polisadministratie, gevuld vanuit de loonaangifteketen). De actualiteit van deze gegevens loopt per definitie enige maanden achter op de werkelijke situatie in Nederland. Na analyse van bovengenoemde 1% (71 gevallen) is gebleken dat dit in ongeveer 10% van de gevallen de oorzaak is dat niet de juiste BI wordt aangeschreven. Om daar rekening mee te houden wordt de inhoudingsplichtige (brongegeven) altijd verzocht om het CAK te informeren wanneer de burger van hem geen actueel inkomen meer ontvangt. Soms verzuimen werkgevers dat (tijdig) te doen waardoor het CAK een herinneringstraject start. Eerst dan geeft de werkgever door dat hij niet meer de actuele bron is.

Risico en maatregelen

Vanuit uitvoeringsperspectief moet uitgegaan kunnen worden van de betrouwbaarheid van de brondata van ketenpartners. Dat deze data mogelijk verouderd is, en daarmee vanuit het CAK een datalek kan ontstaan, wordt gezien als een risico. Dit heeft CAK-breed grote impact op de uitvoerbaarheid van de verschillende regelingen en het aantal datalekken dat hieruit voort kan vloeien.

Omdat er geen andere bron is voor de benodigde informatie, en dit ook de toegewezen bron moet zijn voor de uitvoering, is met de functionaris gegevensbescherming (FG) en de datalekmanager afgestemd dat hier sprake van een 'geaccepteerd risico op datalekken'. Voorwaarde daarbij is dat meteen actie wordt ondernomen met verzoek tot vernietigen van de beschikking en het aanschrijven van de juiste BI. Dit type datalek wordt intern geregistreerd, maar hoeft niet bij de AP gemeld te worden.

Met dit risico wordt de kern van de uitvoering geraakt en dit zal ook impact hebben op de overige regelingen bij het CAK. Door de FG wordt daarom met overige uitvoeringsorganisaties afgestemd hoe elders hiermee wordt omgegaan. Afhankelijk van die uitkomst wordt vervolgens CAK-breed de impact bepaald en een CAK-brede werkwijze afgestemd, zodat dit op eenduidige wijze wordt afgehandeld.

Bestaande aanmeldingen
Zodra een betalingsregeling is getroffen met de zorgverzekeraar wordt de premie-inning door het CAK opgeschort. Bij niet-nakoming daarvan wordt de BI geheractiveerd. Het geautomatiseerde proces is nu zodanig ingericht dat, onafhankelijk van de duur van opschorting, weer gebruik wordt gemaakt van de reeds bekende gegevens van de BI in OHI. In ongeveer 90% van de geconstateerde gevallen in juli, is het niet meer actueel zijn van deze gegevens de oorzaak dat beschikkingen niet naar de, op dat moment, juiste BI worden verstuurd. Sinds de introductie van betalingensregeling bij de zorgverzekeraar en de huidige geautomatiseerde inregeling van het proces, is dit helaas het geval. Sindsdien is overigens geen enkele keer uit informatie gebleken dat burgers zich met deze klacht rechtstreeks hebben gemeld. BI melden daarentegen wel via mail, telefoon of per brief dat wanbetalers uit dienst zijn gegaan.

Risico en maatregelen
Om het risico te beperken dat een onjuiste aanschrijving plaatsvindt, wordt bij klanten waarbij inning via het CJIB loopt het proces 'heruitvraag broninhouding' (HUB) uitgevoerd. Hiermee wordt periodiek bekeken of er voor de betreffende persoon inmiddels een werkgever/uitkeringsinstantie is, zodat BI gestart kan worden. Dit is echter een arbeidsintensief proces, waarvoor in de begroting 2022 structureel extra fte is aangevraagd. Op moment van aanvraag was echter nog niet bekend dat het aanschrijven van de vorige BI als datalek geclassificeerd moest worden. De urgentie van het aannemen van extra collega's om dit proces uit te voeren is daarmee nu toegenomen. Om dit proces ook uit te voeren voor de mislukte betalingsregeling zal extra inzet vragen. De impact hiervan wordt nog nader vastgesteld.

Het HUB-proces is echter geen structurele oplossing. De exacte reductie van het aantal datalekken is o.a. afhankelijk van de frequentie waarmee de heruitvraag wordt gedaan en kan het nooit 100% oplossen. Een mogelijke oplossing zou zijn om dit proces te automatiseren, echter door de overvolle planning van het OHI team kan deze niet op korte termijn worden. Daarbij komt ook dat real-time gegevensuitwisseling binnen de loonaangifteketen voorlopig nog vanwege de complexiteit en haalbaarheid een utopie is.

Als aanvullende maatregel wordt de communicatie richting de BI herzien, waarbij bekeken wordt of voldoende duidelijk blijkt dat het CAK tijdig geïnformeerd dient te worden als wanbetalers uit dienst treden.

Met de FG is afgestemd dat dit type datalek intern wordt geregistreerd. Afgesproken werkwijze is dat direct na melding actie wordt ondernomen met verzoek tot vernietigen van de beschikking. De huidige gevallen dienen gemeld te worden, omdat momenteel onvoldoende adequate acties zijn uitgezet om deze datalekken te voorkomen. Zolang de maatregelen nog niet zijn getroffen, worden meldingen wel aan de AP gemeld.

In afwachting van het intern onderzoek is op 25 november jl. een voorlopige melding van een datalek bij AP gedaan. Uiterlijk 31 december a.s. dient de voorlopige melding gecompleteerd te worden. In gezamenlijk overleg zijn de volgende acties voor de FG afgesproken:

- Raadplegen van collega FG's hoe om te gaan met het niet altijd actueel zijn van uitgevraagd brongegevens van basisregistraties.
- Informeel contact leggen met AP en bespreken hoe omgegaan dient te worden met dit type datalekken.

Afhankelijk van de terugkoppeling van de FG zal de voorlopige melding datalekken aan AP worden ingetrokken of worden aangevuld met een nadere toelichting en mitigerende maatregelen.

Sinds het constateren van dit type data incidenten, is de vraag gerezen hoe en door wie bepaald wordt of er sprake is van een datalek, hoe met dit soort meldingen omgegaan dient te worden, hoe deze gekwalificeerd dienen te worden en welke acties noodzakelijk zijn. Er heeft een relatief lange termijn gezeten tussen constatering van het verbeterpunt en de vraag of er sprake is van een datalek, tot het moment dat dit was vastgesteld en duidelijk was welke acties nodig waren. Ook is in het proces en over het type datalek onduidelijkheid ontstaan over het al dan niet binnen 72 uur moeten melden aan de AP.

Vanuit verschillende interne ontwikkelingen (werkdruk in de teams, reorganisatie, vertrek van riskofficer, nieuwe aangestelde datalekmanager, etc) is dit alles te verklaren, maar voor de toekomst zijn hier verbeteringen in nodig. Er zal nog een evaluatie op het proces plaatsvinden, zodat hier leerpunten uit gehaald kunnen worden.

Advies Strategie en Beleid (Strategisch adviseur, [redacted])
Het CAK maakt voor de uitvoering van de wanbetalerswet gebruik van brongegevens uit de basisregistraties, waaronder de Basisregistratie Inkomens (de UWV Polisadministratie, gevuld vanuit de loonaangifteketen). Deze verzameling en registratie vindt zijn borging in de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). De gegevensleveringen vanuit de polisadministratie aan het CAK zijn geborgd in artikel 5.7 sub b van het Besluit SUWI.

De actualiteit van gegevens vanuit de polisadministratie loopt per definitie enige maanden achter op de werkelijke situatie In Nederland. Om daar rekening mee te houden verzoeken wij de inhoudingsplichtige (brongegeven) altijd om ons te informeren wanneer de burger van hem geen actueel inkomen meer ontvangt. Soms verzuimen werkgevers dat (tijdig) te doen waardoor het CAK een herinneringstraject start. Eerst dan geeft de werkgever door dat hij niet meer de actuele bron is.
Het heraanschrijven (herinnering/aanmaning) van de bron is noodzakelijk omdat het CAK een vordering heeft op de bron. Daarnaast is er geen sprake van nieuwe informatie vanuit het CAK over de status van de burger, deze status (het is een wanbetaler Zvw) is immers altijd in de eerdere broninhoudingsperiode ook al gedeeld met de werkgever.

Het opnieuw aanschrijven van de bij ons bekende bron gebeurt ook als de premie-inning tijdelijk is gepauzeerd omdat er een betalingsregeling tussen wanbetaler en zorgverzekeraar is gesloten. Bij niet-nakoming daarvan heractiveren wij de bron door hem aan te schrijven (herhaling van de eerdere status). Daar zijn overigens (voor de toekomst!) nog wel verbetermogelijkheden in aan te brengen door na een langere periode van pauzering eerst nog een controle op actualiteit van de bron uit te voeren, maar dit zit veel meer in de sfeer van de verdere optimalisatie van de dienstverlening.

Advies Functionaris Gegevensbescherming (Adviseur bestuurlijke & juridische zaken, [redacted])
Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Daar is in dit geval sprake van. Immers, de persoonsgegevens van burgers die in de wanbetalersregeling zitten, zijn verzonden naar 'oude' broninhouders. Of een datalek gemeld moet worden, is afhankelijk van de

(potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. Daarbij zijn een aantal factoren van belang, zoals de aard van de inbreuk, de aard en gevoeligheid van de persoonsgegevens. In dit geval is sprake van persoonsgegevens van een kwetsbare groep, namelijk burgers die in de wanbetalersregeling zitten omdat zij vanwege hun (financiële) niet in staat zijn om hun ziektekosten te betalen. Dit maakt dat dit datalek van genoemde 71 gevallen (alsnog) gemeld moet worden bij de AP.

Een datalek moet echter worden gemeld binnen 72 uur bij de AP. Dit betekent dus dat in dit geval sprake is van een te late melding. Naar aanleiding van een gesignaleerd verbeterpunt in juli had immers al een melding moeten worden gemaakt. De AP zal overigens voor de te late melding alleen een boete opleggen als je door ernstig verwijtbare nalatigheid niet tijdig hebt gemeld. Daarvan is alleen sprake als je willens en wetens de regels overtreedt met als doel om daar financieel beter van te worden (anders dan het voorkomen van een boete). Daar is hier geen sprake van. Een melding kan ertoe leiden dat de AP onderzoek gaat doen. Dat hoeft echter niet het geval te zijn en is mede afhankelijk van de capaciteit bij de AP en de afwegingen die zij maakt. Mocht er toch een onderzoek komen waarbij de AP concludeert dat wij inderdaad niet juist hebben gehandeld dan kan de AP een bindende aanwijzing geven en bij het niet opvolgen daarvan zal bij een volgende te late melding een boete kunnen worden opgelegd.

In dit geval is echter wel sprake van een bijzondere situatie aangezien het CAK afhankelijk is de levering van betrouwbare brondata van ketenpartners. Het is niet ondenkbaar dat deze situatie zich ook voordoet bij andere (overheids)instanties die afhankelijk zijn van brondata van ketenpartners voor de verzending van uitingen aan hun klanten. Zoals hierboven in dit memo al vermeld heb ik hierover contact opgenomen met enkele collega FG's uit de Functionaris Gegevensbescherming Manifestgroep (FG-MFG). Op het moment dat dit memo tot stand kwam heb ik nog geen reacties mogen ontvangen.

Ik sluit mij daarbij aan bij de hierboven voorgestelde mitigerende maatregelen. Aanvullend daarop adviseer ik nog om in gesprek te gaan met het UWV over de gegevensleveringen om te bezien of er nog (extra) waarborgen ingebouwd kunnen worden die ervoor zorgen dat de brondata betrouwbaarder zijn.

Rapportage status privacy stelsel Q3 2021

Raad van Bestuur CAK

[redacted]

[redacted]
Privacy officer CIO-office

Status privacy stelsel CAK

Geen

22-10-2021

1.0

In 2020 is het privacy stelsel ingericht. Het stelsel bestaat uit een samenhangende set van kaders, richtlijnen en inrichtingsdocumenten die door de clusters gebruikt worden om in control te komen. Hiertoe stelt elk cluster minimaal 1 privacy specialist aan, die zorgt voor toepassing van het privacy stelsel. Het privacy stelsel is sinds september 2020 in gebruik.
Vanuit het privacy gilde werken de privacy specialisten samen aan privacyvraagstukken.
Deze rapportage wordt elk kwartaal uitgebracht om de RvB te informeren over de status van de werking van het stelsel.

Stapje voor stapje

De aandacht voor privacy neemt toe, tevens constateren we ook dat de voortgang van verbeteringen achter blijft doordat met de reorganisatie (juli 2021) en alle nieuwe initiatieven de nog beschikbare privacy deskundigen moeite hebben voldoende tijd vrij te maken voor alle werkzaamheden.

Bemensing

Na de tweede reorganisatie (juli 2021) zijn een aantal riskofficer formatieplaatsen (bij wie deze privacy taken belegd waren) vervallen.
Oorspronkelijk waren er 6 FTE's en 1 parttime medewerker beschikbaar bij de regeling clusters welke zich met privacy en AVG bezighielden.
Hier zijn na de reorganisatie nog 3 FTE's en 1 parttimer van overgebleven, die ook nog voor andere taken worden ingezet.
Dit is een zorgelijke ontwikkeling gezien de omvang van de activiteiten die we nog moet verrichten om in control te komen.

Begin oktober zijn er overleggen ingepland tussen de privacy officer van CIO-office en de regeling directeuren om de voortgang van de implementatie van de AVG te bespreken. Daar zal (onder andere) de omgang met de consequenties van de gekrompen bemensing op de agenda staan.

Thema sessies privacy gilde

De privacy officer heeft in 2021 vier themasessies georganiseerd voor de leden van het privacy gilde. Tijdens deze sessies wordt steeds een belangrijk onderdeel van de AVG belicht en besproken. Hierna hebben de gilde leden extra handvatten om het betreffende onderdeel in het regelingcluster te implementeren. Waar nodig ondersteunt de privac officer met toelichting op en advisering over de kaders en richtlijnen.

Datalekken

Per 1 september jl. is de nieuwe datalekkenmanager gestart. Deze is gepositioneerd onder de manager klantservices. Met het aanstellen van de

datalekkenmanager is een doorstart gemaakt met het verder inrichten van het datalekkenproces, inclusief rapportages.
De datalekkenmanager neemt ook deel aan het 2-wekelijks overleg met de FG en de privacy-officer zodat knelpunten en bijzondere datalekken besproken kunnen worden.

Verwerkingenregister en PIA's

De clusters Wlz, Wmo, Btl en CIO-office hebben de verwerkingen op orde. Voor het cluster Zvw wordt een inhaalslag gemaakt. Cluster Zvw heeft naar verwachting eind Q4 haar verwerkingen op orde.
De volgende stap is het op orde brengen van het PIA-register. Dit zal, in tegenstelling tot wat in Q2 werd gerapporteerd, naar verwachting niet eind 2021 gerealiseerd zijn. In 2022 moeten 36 PIA's, die in 2019 zijn uitgevoerd, worden herzien ; bij de geringere beschikbare capaciteit vraagt dit versterkte prioriteit binnen de clusters.

Bemensing

Specialist privacy bij de clusters

Bedrijfsvoering, de staven en HR hebben gezamenlijk een privacy deskundige aangesteld.. Deze deskundige beschikt nog over onvoldoende kennis en ervaring m.b.t. AVG en privacy en zal dus "on the job" verder getraind worden.

Risicomanagement Tooling

Inrichting Tooling

De inrichting van het GRC verloopt nog niet conform de verwachtingen vanwege technische inrichtingsproblemen; de leverancier is hier meermaals op aangesproken en is fouten aan het herstellen. Met o.a. de riskofficer Wmo en Internal Audit is overleg hoe de geïdentificeerde risico's vanuit de PIA's bewaakt kunnen worden vanuit het GRC.

Sturing

De privacy officer van CIO-office overlegt elk kwartaal met de deskundigen van de regeling clusters over de voortgang van de werkzaamheden en over de knelpunten.
Opvallend punt uit deze gesprekken:

- voor de clusters is in augustus 2020 een KPI-rapportage ontwikkeld, waarmee de riskofficer (van een cluster) aan de RD toelicht in hoeverre het cluster in control is m.b.t. privacy en de RD dit in de standaard maandrapportage rapporteert. Het stuurmiddel wordt echter nog in geen enkel cluster toegepast. Dit punt zal begin oktober met de RD's worden besproken.

Privacy By Design

In Q4 gaat de privacy officer in overleg met de besturing van de ART. in de ART moeten concreet stappen worden gezet om privacy by design te borgen, zodat elke EPIC die wordt gerealiseerd (aantoonbaar) voldoet aan de AVG.
Tevens is er overleg met de architecten om dit onderwerp ook binnen architectuur prominenter op de agenda te krijgen.

Awareness

Privacy Gilde

Een PIA heeft een geldigheidstermijn van 3 jaar. In 2022 verloopt de geldigheid van ca. 36 PIA's.

Maandelijks is er een regulier overleg onder voorzitterschap van de privacy officer waar dagelijkse zaken en problemen worden besproken en de verbeterkoers besproken wordt. Maandelijks organiseert de privacy officer een themasessie waarbij met het privacy gilde een specifiek aspect van de AVG en privacy wordt besproken.
In 2021 zijn tot nu toe de onderwerpen Privacy by Design, Lifecyclemanagement van data, Verwerkersovereenkomsten en Rechten van betrokkenen behandeld.

CAK-breed De intranetsite van privacy is ingericht (Volg hier de link naar de site) Hier worden zeer regelmatig nieuwsberichten geplaatst welke de privacy-awareness bevorderen.
- opleidingscoördinator van HR stuurde actief op een 100% score voor het maken van de verplichte e-learning en rapporteerde hier ook over aan de RD's. De medewerker die de e-learning heeft gebouwd en het onderhoud hiervan deed is uit dienst. Hiermee is onderhoud (voorlopig) niet meer mogelijk.

Datalekken

Gemelde datalekken

Per 1 april zijn clustercoördinatoren datalekken aangewezen. De clustercoördinatoren zijn verantwoordelijk voor de coördinatie van het analyseren en oplossen van datalekken. Hierdoor worden oorzaken duidelijk.
De laatste 3 maanden ligt het aantal intern gemelde datalekken tussen de 250 en 400. Dit betreft overwegend adresproblemen.
Oorzaken o.a.:

- Kwaliteit van de adresbestanden door fouten in het primaire proces;
- Achterstanden bij het verwerken klantmeldingen;
- Synchronisatieproblemen tussen systemen;
- Onvoldoende gebruik naken van de terugmeld-voorziening BRP;
- Wijze waarop retourpost wordt afgehandeld.

De cluster coördinatoren proberen in samenspraak met de datalekkenmanager deze problematiek op de kalender van het programma "continue verbeteren" te krijgen.

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

Organisatieonderdeel	Het CAK
Naam hoofd van dienst	[redacted]
Naam privacy officer	[redacted]
Rapportagedatum	30-9-2021

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	Voor diensten ingericht. Toepassing in de Agile Realease Train (ART) is onderhanden.
		pag. 20	De organisatie kan aantonen dat bij nieuwe systemen, beleid en diensten een Quick Scan IB en P en zondig een PIA is uitgevoerd.	*geen verduidelijking noodzakelijk*	Volledig	
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*	Deels	Protocol beschikbaar. Inbedding in de lijn (werkinstructies) is onderhanden.
		pag. 10	De organisatie gebruikt vastgestelde modellen voor afhandeling van AVG verzoeken en bezwaar.	*geen verduidelijking noodzakelijk*	Deels	Protocol beschikbaar, per cluster vrijheid voor de praktische invulling. Naar verwacht zal via het privacy gilde wel een zoveel mogelijk
		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.	Deels	Inrichting onderhanden middels centrale rapportage. Wordt daarna een agendapunt voor het overleg FG/privacy officer.
		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).	Volledig	Algemeen privacyverklaring en regeling specifieke verdere toelichting op de CAK-website
		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	
		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	Indien dit van toepassing wordt wordt er uiteraard aandacht aan besteed
				Voor alle verwerkingen waarbij sprake is van geautomatiseerde besluitvorming op basis van profilering is een PIA uitgevoerd.	Geen	
				Alle betrokkenen zijn vooraf aantoonbaar geïnformeerd over de geautomatiseerde besluitvorming, de mogelijke gevolgen die dit met zich meebrengt en welke bewaartermijn worden gehanteerd.	Geen	
				De organisatie heeft een proces ingericht dat betekenisvolle menselijke tussenkomst in de besluitvorming borgt, en waar de betrokkene een beroep op kan doen.	Geen	
		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*	Volledig	Bijv. opnemen telefoongesprekken en klant tevredenheidsonderzoeken.
		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	Communicatie verloopt altijd via de wettelijke vertegenwoordiger van de minderjarige.
4	Privacy beleid	pag. 13	De organisatie beschikt over privacy beleid welke door of namens de SG is vastgesteld.	*geen verduidelijking noodzakelijk*	Volledig	Wordt jaarlijks vastgesteld
		pag. 13	Het privacy beleid wordt minimaal een keer in de drie jaar geëvalueerd en geactualiseerd. Zo nodig wordt het beleid opnieuw vastgesteld.	*geen verduidelijking noodzakelijk*	Volledig	Wordt jaarlijks vastgesteld.
		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	
		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	Verplicht eleaning en berichten op intranet.
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.	Volledig	Bijlage bij het privacy beleid.
		pag. 14	De organisatie heeft een kwaliteitscyclus ingericht voor gegevensbescherming en privacy om de blijvende goede omgang met persoonsgegevens te waarborgen.	*geen verduidelijking noodzakelijk*	Geen	Nog in te richten.
		pag. 15	De organisatie toetst haar verwerkers regelmatig op de naleving van de eisen van de AVG	*geen verduidelijking noodzakelijk*	Geen	Nog in te richten.
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	
		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	Allemaal beschikbaar, maar niet als bijlage. Registertoool is hier niet geschikt voor.

		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	Kaders beschikbaar, inrichting in ART nog onderhanden.
			De organisatie heeft in kaart gebracht bij welke verwerkingen sprake is van verwerking van persoonsgegevens waaruit ras of etnische afkomst kan blijken.	*geen verduidelijking noodzakelijk*	Niet van toepassing	
		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*	Niet van toepassing	Cak is ZBO.
7	Risico gestuurd beveiligen van persoonsgegevens	pag. 19	De organisatie heeft per verwerking de noodzakelijke technische en organisatorische maatregelen geïdentificeerd en geïmplementeerd en neemt de controle op de werking van deze maatregelen op in het periodieke proces van kwaliteitscontrole op het register.	*geen verduidelijking noodzakelijk*	Deels	Verbetering is mogelijk. Managen van risico's en maatregelen is nog onvolwassen.
		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*	Volledig	Melding aan CPOVWS geschiedt door de FG, indien deze dit noodzakelijk acht.
		pag. 20	De organisatie houdt een register bij van al haar datalekken als verwerker en als verwerkingsverantwoordelijke.	*geen verduidelijking noodzakelijk*	Volledig	Topdeskregistratie.
		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*	Deels	Gebeurt 2 wekelijks in overleg FG/Privacy-officer/datalekkenmanager. Verbetering is mogelijk.
		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.	Volledig	
				Iedere PIA is voorzien van een advies van de FG en een beschrijving hoe opvolging is gegeven aan het advies.	Volledig	
				Er is gebruik gemaakt van het rijks brede model voor de PIA. Tevens is gewaarborgt dat iedere Pia elke drie jaar wordt geactualiseerd.	Volledig	
		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*	Deels	Per PIA wordt vastgesteld welke functionarissen nodig zijn.
		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*	Volledig	
		pag. 20	Er is een procesbeschrijving voor het uitvoeren van PIA's en het opvolgen van uitkomsten.	*geen verduidelijking noodzakelijk*	Deels	Opvolgen uitkomsten is onderhanden.
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.	Volledig	
		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.	Volledig	
		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.	Volledig	
		(nog) geen onder-deel van AVG handreiking pag. 22	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 ieders 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.	Volledig	
			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).	Volledig	