Memo

Datalekmeldingen juli tot en met december 2019

RvB

[redacted] (FG)
(opsteller)

Datalekmeldingen juli tot en met december 2019

Geen

22-01-2020

1.0

Inleiding

In deze memo wordt inzicht gegeven in alle datalekmeldingen van de periode juli tot en met december 2019. Deze memo is een vervolg op de memo van het eerste halfjaar van 2019. Het gaat om alle datalekmeldingen die middels de Self Service Portal door medewerkers zijn gemeld. Alle meldingen zijn ingedeeld in veel voorkomende categorieën, waarbij allereerst per categorie de aantallen worden weergeven. Vanwege het regeling gericht werken bevat deze memo tevens een overzicht van alle meldingen per regeling. Daarnaast volgt een overzicht van de belangrijkste oorzaken, (voorgestelde) verbeteringen en maatregelen. Wij sluiten af met een overzicht waarin de gegevens van heel 2019 zijn verwerkt.

Aantal datalekmeldingen 2019 (per maand)

In de periode juli tot en met december zijn **369** datalekken gemeld. Onderstaand overzicht geeft inzage in het aantal datalekmeldingen per maand, onderverdeeld in de meest voorkomende categorieën (algemeen overzicht). Aansluitend volgt een overzicht van het aantal datalekmeldingen per regeling (Wmo, Wlz, Zvw en Buitenland). De categorie 'overig' heeft betrekking op datalekmeldingen die niet onder één van de regelingen valt.

Algemeen overzicht datalekmeldingen (juli 2019):

Datalekken bij de AP gemeld (klantgegevens)	53
Datalekken bij de AP gemeld (medewerkersgegevens)	1
Datalekmeldingen die betrekking hebben op de huishoudsamenstelling	6
Datalekmeldingen met betrekking tot de ex-partnersproblematiek	7
Datalekmeldingen die na analyse géén datalek blijken te zijn	11
Totaal	**78**

Datalekmeldingen per regeling (juli 2019):

Wmo	42
Wlz	12
Zvw	6
Buitenland (Schengen inbegrepen)	10
Overig	8
Totaal	**78**

Algemeen overzicht datalekmeldingen (augustus 2019):

Datalekken bij de AP gemeld (klantgegevens)	47
Datalekmeldingen die betrekking hebben op de huishoudsamenstelling	1
Datalekmeldingen met betrekking tot de ex-partnersproblematiek	2
Datalekmeldingen die na analyse géén datalek blijken te zijn	19
Totaal	**69**

Datalekmeldingen per regeling (augustus 2019):

Wmo	34
Wlz	19
Zvw	9
Buitenland (Schengen inbegrepen)	3
Overig	4
Totaal	**69**

Algemeen overzicht datalekmeldingen (september 2019):

Datalekken bij de AP gemeld (klantgegevens)	38
Datalekken bij de AP gemeld (medewerkersgegevens)	1
Datalekmeldingen met betrekking tot de ex-partnersproblematiek	5
Datalekmeldingen die na analyse géén datalek blijken te zijn	22
Totaal	**66**

Datalekmeldingen per regeling (september 2019):

Wmo	37
Wlz	15
Zvw	4
Buitenland	4
Overig	6
Totaal	**66**

Algemeen overzicht datalekmeldingen (oktober 2019):

Datalekken bij de AP gemeld (klantgegevens)	42
Datalekken bij de AP gemeld (medewerkersgegevens)	1
Datalekmeldingen die betrekking hebben op de huishoudsamenstelling	1
Datalekmeldingen met betrekking tot de ex-partnersproblematiek	3
Datalekmeldingen die na analyse géén datalek blijken te zijn	12
Totaal	**59**

Datalekmeldingen per regeling (oktober 2019):

Wmo	28
Wlz	20
Zvw	4
Buitenland	3
Overig (Wtcg inbegrepen)	4
Totaal	**59**

Algemeen overzicht datalekmeldingen (november 2019):	
Datalekken bij de AP gemeld (klantgegevens)	47
Datalekken bij de AP gemeld (medewerkersgegevens)	2
Datalekmeldingen die na analyse géén datalek blijken te zijn	17
Totaal	**66**
Datalekmeldingen per regeling (november 2019):	
Wmo	33
Wlz	17
Zvw	9
Buitenland	5
Overig	2
Totaal	**66**

Algemeen overzicht datalekmeldingen (december 2019):	
Datalekken bij de AP gemeld (klantgegevens)	22
Datalekken bij de AP gemeld (medewerkersgegevens)	2
Datalekmeldingen die na analyse géén datalek blijken te zijn	7
Totaal	**31**
Datalekmeldingen per regeling (december 2019):	
Wmo	14
Wlz	10
Zvw	3
Overig	4
Totaal	**31**

Datalekken die daadwerkelijk bij de AP zijn gemeld (klantgegevens)

Algemene opmerking
Van de **369** datalekken zijn er in totaal **249** bij de Autoriteit Persoonsgegevens gemeld.

Menselijk handelen
Datalekken veroorzaakt door menselijk handelen vormen nog steeds het overgrote deel van het aantal meldingen. Dit komt door de grote hoeveelheid klantcontacten (brieven, e-mails etc.). Menselijke fouten zijn niet helemaal te voorkomen. Een specifieke oplossingsrichting is er dan ook niet. Er kan op individueel niveau wel geleerd worden van gemaakte fouten. Daarnaast moet er continu aandacht zijn voor zorgvuldigheid op de werkplek. Ook moet het onderwerp privacy (met name omgang met persoonsgegevens) blijvend en geïntegreerd in de business op de agenda blijven staan. Dit kan door op enkele momenten in het jaar privacy onder de aandacht van medewerkers te brengen, denk aan berichten op het intranet, e-learnings, casus bespreken op teamniveau. Met betrekking tot de e-learnings datalekken en AVG: deze worden momenteel vernieuwd om het proces van bewustwording actueel te houden. Beiden thema's worden gecombineerd in één e-learning. Alle ervaringen van het afgelopen jaar in kader van de afhandeling van datalekken worden in de e-learning verwerkt. De e-learning is op een nader te bepalen datum beschikbaar in de academie.

Onderstaand een maandelijks overzicht van alle datalekken veroorzaakt door menselijk handelen:

maand	aantallen
juli	32
augustus	33
september	23
oktober	28
november	31
december	14
Totaal	**161**

Een aantal voorbeelden van datalekken veroorzaakt door menselijk handelen zijn (niet limitatief):

- Invoerfouten. Enkele voorbeelden (intern en extern):
  - het invoeren van een postadres (intern);
  - het invoeren van een wettelijk vertegenwoordiger (intern);
  - invoeren van een IBAN in het verkeerde klantdossier (intern);
  - bezorgfouten (extern).

- E-mail naar de verkeerde afzender.
- Persoonsgegeven (veelal BSN) in onderwerp regel van een e-mail

Technische oorzaak/ automatisch proces

Onderstaand een maandelijks overzicht van alle datalekken veroorzaakt door een technische oorzaak/automatisch proces:

maand	aantallen
juli	21
augustus	14
september	15
oktober	14
november	13
december	8
Totaal	**85**

Een aantal datalekken worden veroorzaakt door een technische oorzaak (niet limitatief):

- In het verleden zijn postadressen ingevoerd in Cebes. Dit is destijds gedaan omdat de adreswijzigingen vanuit het BRP niet (tijdig) werden verwerkt. De postadressen zijn naderhand niet

aangepast waardoor zij als leidend adres worden gehanteerd nadat de adreswijziging binnenkomt. Deze gevallen komen nog steeds voor;

- Automatische verwerking adreswijzigingen in Thinsy en Cebes komen niet altijd door in OF. Hierdoor blijven facturen naar een oud adres verstuurd worden. Dit geldt ook voor bijvoorbeeld invoer IBAN of AI in OF. Het oude adres uit OF wordt overgenomen en niet uit Thinsy/Cebes. Ook dit probleem komt regelmatig terug;
- Adreswijzigingen worden niet altijd verwerkt in de bronsystemen. Achteraf vindt er een handmatige synchronisatie plaats. CPR moet in deze gevallen een oplossing bieden.
- Sinds het migratieweekend begin december 2019 (migratie van niet-authentieke klantgegevens uit vijf databases naar één database, de CPR) zijn een aantal facturen naar oude adressen verstuurd. Dit is momenteel in onderzoek en wordt nauwlettend gemonitord op nieuwe gevallen.

Datalekken die daadwerkelijk bij de AP zijn gemeld (medewerkersgegevens)
Het aantal dataleken die betrekking hebben op de persoonsgegevens van medewerkers (intern en extern) zijn ook vermeldenswaardig. De aantallen zijn in deze memo verwerkt.

Datalekken die betrekking hebben op de huishoudsamenstelling
Deze categorie datalekmeldingen ziet op de uitvoeringspraktijk bij het vaststellen van de huishoudsamenstelling in het kader van het innen van de eigen bijdrage Wlz en Wmo. Eerder dit jaar constateerde wij dat er een geleidelijke maandelijkse daling waarneembaar was. Dit heeft te maken met het verwijderen van bepaalde persoonsgegevens van de uitingen. Deze categorie datalekmeldingen komen nagenoeg niet meer voor.

Datalekken met betrekking tot de ex-partnersproblematiek
Deze categorie datalekken heeft betrekking op alle gevallen waarbij het verificatieproces van BRP-gegevens in relatie tot ex-partners foutief verloopt. Mensen die gescheiden waren worden toch aan elkaar gekoppeld in de bronsystemen. Ook in het tweede half jaar van 2019 is het aantal datalekken dat te maken heeft met ex-partnersproblematiek is vrijwel gelijk gebleven.

Datalekmeldingen die na analyse géén datalek blijken te zijn
Van de **369** via de service service portal aangemelde potentiële datalekken bleek in **88** gevallen geen sprake te zijn van een datalek. Een aantal meldingen liggen in de risicosfeer van de klant bijvoorbeeld door het aanleveren van foutieve (adres)gegevens. In een aantal gevallen zijn brieven van overleden klanten naar oude of verkeerde adressen verstuurd (gegevens van overledene zijn geen persoonsgegevens). Ook ongeopende brieven die het CAK retour ontvangt worden niet als datalek geregistreerd. Om 'vervuiling' te voorkomen wordt de categorie 'persoonsgegevens van overleden klanten' opnieuw onder de aandacht gebracht in de nieuwe e-learning.

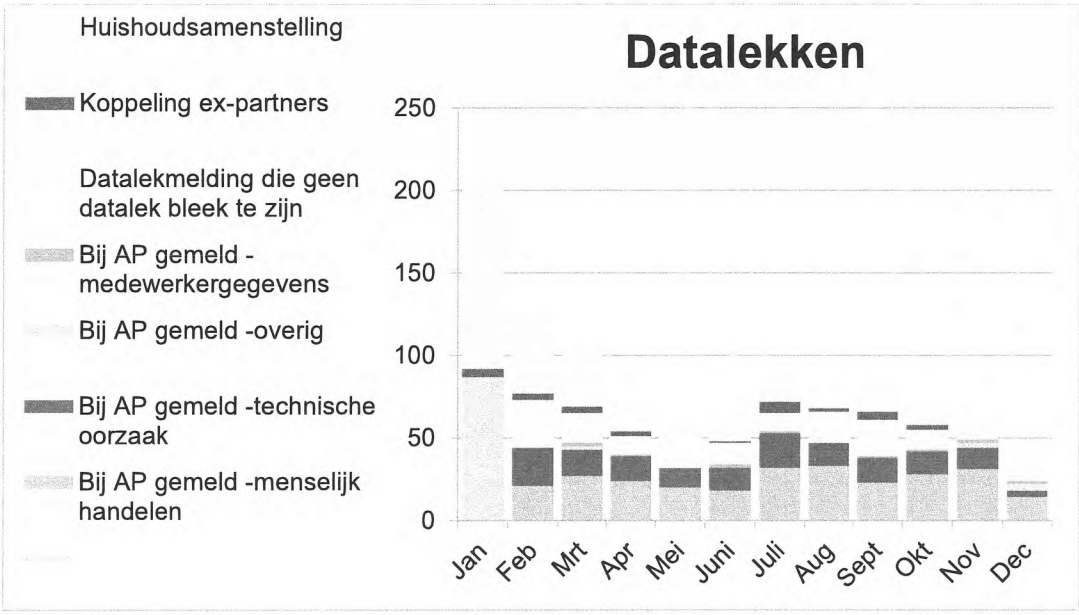
Datalekmeldingen per regeling
Het overgrote deel van alle datalekmeldingen is afkomstig van de Wmo-regeling, direct gevolgd door de Wlz-regeling. Een klein deel van alle datalekmeldingen liggen in het domein Zvw en Buitenland. De exacte aantallen worden in de maandelijkse datalekrapportage opgenomen en zijn in deze memo verwerkt.

Overzicht datalekmeldingen januari tot en met december 2019
Vooraf: Het CAK verstuurt per jaar meer dan 10 miljoen uitingen aan haar klanten. Dit betekent dat er potentieel op jaarbasis veel datalekken kunnen ontstaan. Afgezet tegen dit aantal is het aantal gemelde datalekken relatief laag. In het eerste halfjaar van 2019 ontving de Autoriteit Persoonsgegevens (AP) 11.906 datalekmeldingen. Het gaat om ongeveer 2.000 meldingen per maand. De cijfers van het tweede

https://digitale-werkomgeving/sites/CAK/themasites/Wmo2020/MDM%20Wiki/CPR%20Synchronisatie.aspx

halfjaar zijn nog niet bekend. Bovenstaande geeft een goed beeld van de hoeveelheid gemelde datalekken van het CAK in verhouding tot het totaal aantal bij de AP gemelde datalekken.

Onderstaand overzicht (zie grafiek) geeft een beeld van alle datalekmeldingen van het afgelopen jaar.



Advies FG
Als FG vind ik dit een duidelijk overzicht en analyse. De adviespunten onderschrijf ik. Ik zou daar echter nog enkele adviespunten aan toe willen voegen. Het lijkt er op dat het proces van het afhandelen van datalekken erg gevoelig is omdat slechts één medewerker zich hier mee bezig houdt. Bij ziekte of andere calamiteiten lijkt mij onvoldoende geborgd dat het behandelen van datalekmeldingen doorgang kan vinden. Eerder is toegezegd dat er een structurele oplossing zou worden ingeregeld. Tot op heden is dat nog niet het geval. Ik vraag hier nadrukkelijk de aandacht voor.

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019

Bevindingen FG over 2019

RvB

[redacted]
FG

Bevindingen FG over 2019

geen

29 januari 2020

1.0

Hierbij treft u mijn bevindingen over 2019 aan. Ik heb mijn bevindingen opgesteld aan de hand van een aantal kernpunten uit de AVG. Tot slot ga ik nog kort in op de twee onderzoeken die de AP is gestart.

Er zijn door de organisatie diverse bewustwordingsactiviteiten ondernomen in 2019 waaronder

-Implementatie van een e-learning datalekken en een e-learning AVG voor nieuw personeel.
-Berichten op intranet m.b.t. ontwikkelingen rond de AVG.
-Inrichten van een interne site met de relevante AVG-informatie voor medewerkers

Daarbij zal voor 2020 een nieuwe e-learning worden ontwikkeld, en zal de intranetpagina worden aangepast. Dit zijn goede stappen.

Advies
Gebleken is echter dat de bewustwording voor meer ingewikkelde vraagstukken aandacht behoeft. Er vindt zeer geregeld geen beoordeling plaats van compliancy aan de AVG van (wijzigings)verzoeken die worden uitgevoerd. De eigenaar of opdrachtgever van de data of het proces zou dit standaard mee moeten nemen bij ieder verzoek. In het verlengde daarvan ligt de vraag wie op dit moment verantwoordelijk is voor compliancy aan de AVG. Dat is voor mij niet duidelijk. Daarnaast wordt er veelvuldig gebruik gemaakt van productie data in testomgevingen en worden er door analisten gegevens uit verschillende systemen met elkaar gekoppeld zonder dat gecheckt wordt of die data wel gecombineerd mag worden. Mijn advies is om hier in 2020 aandacht aan te besteden. Met name bij medewerkers bij ICT (privacy by design/default) en analisten.
Draag er zorg voor dat de e-learning verplicht moet worden gedaan en dat aantoonbaar is welke medewerkers hem al hebben gevolgd en welke niet. Een mogelijkheid daarbij zou kunnen zijn om dit onderdeel van de planning en control cyclus te laten zijn.

Het proces hoe betrokkenen hun rechten uit kunnen oefenen is in 2019 verder vorm gegeven
-De klant wordt geïnformeerd via de CAK-website hoe hij zijn rechten kan uitoefenen.

-De frontoffice kan in een voor gedefinieerd web formulier aangeven welke acties intern doorgevoerd moeten worden om aan het klantverzoek te voldoen.
-De back-office voert de acties door.
-Terugkoppeling van het resultaat aan de klant vindt plaats via de front-office.

Advies
Burgers kunnen hun verzoeken ook "verstoppen" in andere documenten zoals bezwaarschriften of naar een ander mailadres binnen het CAK sturen. Maak iedere medewerker alert op dergelijke verzoeken zodat de collega's deze naar het juiste team door kunnen sturen. Zo krijgt de burger snel een reactie op zijn verzoek en loopt het CAK geen risico's met eventuele dwangsommen.
Daarnaast adviseer ik om meer aandacht te besteden aan het IAM beleid zodat duidelijk is wie toegang heeft tot welke data. Dit vergroot het in control zijn op dit onderwerp.

Alle verwerkingen dienen bij de privacy officers te worden gemeld zodat zij deze kunnen verwerken in het verwerkingen register. Dit gebeurt echter lang niet in alle gevallen waardoor met zekerheid is te zeggen dat het verwerkingenregister niet compleet is. Dit is dus het gevolg van het feit dat de organisatie de privacy officers onvoldoende informeert. Dit brengt reële risico's met zich.

Advies
Zorg voor ondertekening van de verwerkingen door de verwerkingsverantwoordelijke. Daarbij zal publicatie van de verwerkingen op de website aan te bevelen zijn (niet verplicht).

In 2019 zijn veel PIA's uitgevoerd. De uitgevoerde PIA's zijn opgenomen in het PIA-register, waarbij een verwijzing is gemaakt naar de verwerkingen uit het verwerkingenregister. De risico's die zijn benoemd in de PIA's zijn opgenomen in het risicoregister.

Advies
Zorg dat bij processen voor bijvoorbeeld nieuwe voor veranderde taken, of andere processen waar privacy gevoelige gegevens een rol spelen goed is geborgd dat er altijd de vraag wordt gesteld of er een PIA dient te worden uitgevoerd.
Bij gebrek aan een duidelijke verantwoordelijke monitoren de privacy officers deze risico's die genoemd zijn in het risicoregister. Het is derhalve van belang dat er een sluitend proces komt zodat er medewerkers daadwerkelijk verantwoordelijk zijn voor de onderkende risico's en dat daarbij de risico's structureel worden gemitigeerd.

Over dit onderwerp is een apart memo opgesteld.

Het proces van het afsluiten van verwerkersovereenkomsten is goed geborgd zodra de afdeling Inkoop betrokken is. Echter, er kunnen ook zaken ingekocht worden zonder dat Inkoop is betrokken. Gebleken is dat dan niet altijd aan de privacy wordt gedacht en er geen verwerkersovereenkomst wordt getekend. Dit

is onwenselijk. Advies is om ook in die gevallen te borgen dat er aan de privacy aspecten wordt gedacht en er dus onder meer een verwerkersovereenkomst wordt gesloten.

Als FG heb ik nu een duidelijk aanspreekpunt in de medewerkers met de rol privacy officer Het is van belang dat ook in de nieuwe organisatie vanaf 1 april 2020 een duidelijk aanspreekpunt komt. Dit om mijn toezichthoudende taak goed uit te kunnen blijven voeren.

De AP heeft in 2019 twee onderzoeken gestart bij het CAK.

Het eerste onderzoek betrof een onderzoek onder meerdere organisaties naar de wijze hoe het datalekmeldingen register vorm is gegeven bij deze organisaties. De AP heeft naar aanleiding van dat onderzoek een algemeen rapport opgesteld met aanwijzingen wat er in het datalekregister vermeld zou moeten worden en op welke wijze. Het CAK heeft zijn datalekregister op deze punten aangepast.

Het tweede onderzoek is de AP in december 2019 gestart en is enkel gericht tegen het CAK. Het betreft een onderzoek naar de vraag waarom een aantal datalekmeldingen niet onverwijld dan wel binnen 72 uur bij de AP zijn gemeld. Het CAK heeft daar op gereageerd en is nu in afwachting van (eventuele) vervolgstappen van de AP.

Voorlegger raad van bestuur

De indiener van het voorstel moet alle velden invullen. Dit pdf bestand graag dezelfde naam geven als het onderwerp hieronder genoemd. Vergaderstukken inclusief voorlegger indienen op donderdag vóór 12:00 uur voorafgaand aan de vergadering bij: [redacted] en [redacted]

Van (direct reports)	FG
Onderwerp	rapportage datalekken Q3 en Q4 2019
Datum	2 7 0 1 2 9 2 9 *DD / MM / JJJJ*
Samenvatting voorstel *Formuleer duidelijk en bondig de aanleiding en samenvatting van het voorstel.*	Als FG houd ik toezicht op de naleving van de AVG door het CAK. Daarnaast probeer ik, daar waar dit geen strijdigheid met mijn toezichthoudende taak oplevert, mee te denken met het compliant zijn aan de AVG. Twee keer per jaar maakt de medewerker die de datalekken behandelt een analyse. Bijgevoegd treffen jullie de analyse van de datalekken over de tweede helft van 2019 aan. Onderaan het document staat mijn advies betreffende de afhandeling van datalekken.
Gevraagd besluit *Welk besluit verwacht je van de raad van bestuur?*	Kennis nemen van de analyse en de adviezen van de FG.
Vervolgproces *Welke vervolgstappen worden genomen na afloop van het besluit van raad van bestuur*	Het niet compliant zijn aan de AVG kan imagoschade, boetes en schadevergoedingen tot gevolg hebben.

Aandachtspunten en risico's

Welke aandachtspunten en risico's voorzie je met het voorstel. Houd met ieder aandachtsgebied rekening.

Algemeen	-
Financieel	-
ICT / Informatie	-
Juridisch	-
HR	-
Medezeggenschap	-
Rechtmatigheid (budget/inhuur/inkoop)	-
Politiek- bestuurlijk	-

Voorlegger raad van bestuur

De indiener van het voorstel moet alle velden invullen. Dit pdf bestand graag dezelfde naam geven als het onderwerp hieronder genoemd. Vergaderstukken inclusief voorlegger indienen op donderdag vóór 12:00 uur voorafgaand aan de vergadering bij: [redacted] en [redacted]

Van (direct reports)	Functionaris Gegevensbescherming (FG)
Onderwerp	rapportage FG over 2019
Datum	2 9 0 1 2 0 2 0 *DD / MM / JJJJ*
Samenvatting voorstel *Formuleer duidelijk en bondig de aanleiding en samenvatting van het voorstel.*	Als FG houd ik toezicht op de naleving van de AVG door het CAK. Daarnaast probeer ik, daar waar dit geen strijdigheid met mijn toezichthoudende taak oplevert, mee te denken met het compliant zijn aan de AVG. Ieder jaar maak ik een rapportage van mijn bevindingen over het afgelopen jaar. Bijgevoegd treffen jullie mijn bevindingen en adviezen als FG over 2019 aan. De analyse van datalekken wordt als aparte memo aan de RvB voorgelegd.
Gevraagd besluit *Welk besluit verwacht je van de raad van bestuur?*	Kennis nemen van de rapportage.
Vervolgproces *Welke vervolgstappen worden genomen na afloop van het besluit van raad van bestuur*	Het niet compliant zijn aan de AVG kan imagoschade, boetes en schadevergoedingen tot gevolg hebben.

Aandachtspunten en risico's

Welke aandachtspunten en risico's voorzie je met het voorstel. Houd met ieder aandachtsgebied rekening.

Algemeen	-
Financieel	-
ICT / Informatie	-
Juridisch	-
HR	-
Medezeggenschap	-
Rechtmatigheid (budget/inhuur/inkoop)	-
Politiek- bestuurlijk	-

Totale standvan zaken 1 november 2020 overall

Onderwerp	KPI cluster rapportage			Cluster Wiz dat. 1 november 2020				Cluster Buitenland 1 november 2020				Services 1 november 2020	
		Status KPI	Opmerkingen	Status KPI	Opmerkingen	Status KPI	Opmerkingen	Status KPI	Opmerkingen	Status KPI	Opmerkingen	Status KPI	Opmerkingen
Verwerkingenregister	Volledigheid van het verwerkingenregister		Alle verwerkingen van het CAK liggen vast, alleen nog niet omgezet naar de nieuwe regeling structuur.		De GAP-analyse is gestart		De GAP-analyse is gestart		Aanpassingen zijn in afrondende fase		Eerste verwerkingen worden opgeleverd.		De GAP-analyse is gestart
Verwerkingenregister	Actualiteit van het verwerkingenregister		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar. Er wordt nog gewerkt met een tool dat fouten vertoont. Medio december 2020 is er en nieuw tool beschikbaar.		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar		Alle registraties van verwerkingen zijn niet ouder dan 2 jaar
Pia register	Volledigheid van het PIA register		Er zijn inmiddels 81 PIA's uitgevoerd en vastgelegd.		GAP-analyse moet nog starten. Kan na bijwerken verwerkingenregister.		GAP-analyse moet nog starten. Kan na bijwerken verwerkingenregister.		GAP-analyse moet nog starten. Kan na bijwerken verwerkingenregister.		GAP-analyse moet nog starten. Kan na bijwerken verwerkingenregister.		GAP-analyse moet nog starten. Kan na bijwerken verwerkingenregister.
PIA register	Actualiteit van het PIA register		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.		Alle geregistreerde PIA's zijn niet ouder dan 3 jaar.
Verwerkersovereenkomsten	Volledigheid van de overeenkomsten		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.		Voor alle bekende verwerkingen zijn overeenkomsten beschikbaar. Inkoop heeft deze toegewezen aan de nieuwe N-1's.
Risico management	Mitigeren van privacy risico's		Risico's liggen vast in een register, opvolging is niet traceerbaar.		Risico's uit PIA's worden niet actief gemanaged.		Risico's uit PIA's worden niet actief gemanaged.		Risico's uit PIA's worden niet actief gemanaged.		Risico's uit PIA's worden niet actief gemanaged.		Risico's uit PIA's worden niet actief gemanaged.
Opleiding	Alle medewerkers zijn opgeleid om met privacy gevoelige informatie om te gaan		Verplichte elearning wordt gevolgd. HR rapporteert aan N-1 voor bewaking.		Bewaking vanuit de lijn vindt plaats		Bewaking vanuit de lijn vindt plaats		Bewaking vanuit de lijn vindt plaats		Bewaking vanuit de lijn vindt plaats		Bewaking vanuit de lijn vindt plaats
Opleiding	Onderhouden van kennis		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.		Middels intranet Adhoc acties. Er is nog geen programma beschikbaar.
Uitvoeringstoetsen	Voldoen aan wet- en regelgeving		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.		Draaiboek uitvoeringstoets is nog onvolledig in opzet. Privacy en security nog niet voldoende ingericht.
Changes	Voldoen aan wet- en regelgeving		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.		Zie mitigeren van privacy risico's. Wordt nog niet actief gemanaged.
Rechten van betrokkenen	Tijdigheid		Werkinstructie is beschikbaar		Gecontroleerd proces		Gecontroleerd proces		Gecontroleerd proces		Procesinrichting onderhanden. Vanuit Wiz wordt meegekeken.		Gecontroleerd proces
Accesmanagement	Personeel heeft toegang tot informatie op basis van need to know		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.
Accesmanagement	Toepassen van de toegangsschema's		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.		Er vinden wel periodieke controles plaats op de belangrijkste systemen op actualiteit (uit dienst e.d). Bij gebrek aan adequate schema's is controle op juistheid maar deels mogelijk.
Logging- en monitoring	Vaststellen van afwijkend gedrag		Er is geen regeling waar dit is ingeregeld.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.		Opgenomen in "input privacy en security OGSM 2021" t.b.v. de cluster jaarplannen.
Dataveiligheid	Testen geschiedt met geanonimiseerde data		Er moet zeer regelmatig met exceptie worden gewerkt. Testdorp wordt aangeschaft, dit moet het probleem definitief oplossen.		Er is vooruitgang geboekt, maar er zijn nog steeds teveel excepties.		Er is vooruitgang geboekt, maar er zijn nog steeds teveel excepties.		Er is vooruitgang geboekt, maar er zijn nog steeds teveel excepties.		Er is vooruitgang geboekt, maar er zijn nog steeds teveel excepties.		Er is vooruitgang geboekt, maar er zijn nog steeds teveel excepties.
Datalekken	Correct melden aan AP		De huidige werkwijze met gecentraliseerde coordinatie door de datalekkenmanager werkt goed. Binnen de regeling clusters (n-2) is discussie of deze afhandeling niet gedecentraliseerd moet worden. Met huidige volwassenheidsniveau komt het proces hier mee in gevaar.		Dreigende decentralisatie van afhandeling kan proces verstoren.		Dreigende decentralisatie van afhandeling kan proces verstoren.		Dreigende decentralisatie van afhandeling kan proces verstoren.		Dreigende decentralisatie van afhandeling kan proces verstoren.		Dreigende decentralisatie van afhandeling kan proces verstoren.
Datalekken	Permanent verbeteren		Er is centraal geen inzicht en overzicht. Staus vaak onbekend.		Er is geen volledige dekking binnen de regelingen.		Er is geen volledige dekking binnen de regelingen.		Er is geen volledige dekking binnen de regelingen.		Er is geen volledige dekking binnen de regelingen.		Er is geen volledige dekking binnen de regelingen.
Datalekken	Opvolging datalekken		Centrale datalekmanager (a.i.) krijgt hierover onvoldoende fedback. Procesinrichting in clusters nog niet in orde.		Datalekmanager krijgt vaak geen feedback. Centraal geen inzicht en overzicht.		Datalekmanager krijgt vaak geen feedback. Centraal geen inzicht en overzicht.		Datalekmanager krijgt vaak geen feedback. Centraal geen inzicht en overzicht.		Datalekmanager krijgt vaak geen feedback. Centraal geen inzicht en overzicht.		Datalekmanager krijgt vaak geen feedback. Centraal geen inzicht en overzicht.

2	Verwerkingenregister	Volledigheid van het verwerkingenregister	100 % van de bekende verwerkingen van persoonsgegevens zijn vastgesteld door de N-1 en opgenomen in het verwerkingen register	Jaarlijkse verklaring van N-1.	Volg deze link voor achtergrondinformatie over het verwerkingenregister.
2	Verwerkingenregister	Actualiteit van het verwerkingenregister	Verwerkingen in het register zijn maximaal 2 jaar geleden beoordeeld op actualiteit	Jaarlijkse verklaring van N-1.	Volg deze link voor achtergrondinformatie over het PIA register.
2	Pia register	Volledigheid van het PIA register	100 % van de uitgevoerde PIA's zijn vastgesteld door de N-1 en opgenomen in het PIA-register. Nog uit te voeren PIA's zijn ingepland met een einddatum maximaal 3 maanden in de toekomst	Jaarlijkse verklaring van N-1.	
2	PIA register	Actualiteit van het PIA register	Ouderdom van de PIA's is maximaal 3 jaar	Jaarlijkse verklaring van N-1.	
2	Verwerkersovereenkomsten	Volledigheid van de overeenkomsten	Voor 100% van de verwerkingen van persoonsgegevens door leveranciers is een verwerkersovereenkomst afgesloten	1) Overzicht via afdeling inkoop (Negometrix) 2) Eigen registratie voor de contracten welke niet via inkoop lopen.	
2	Risico management	Mitigeren van privacy risico's	100% van de (o.a. in PIA's) geïdentificeerde privacy risico's is	Excelsheet uit risico register	Uiterlijk medio 2021 rapportage vanuit GRC. Volg deze link voor de Excel sheet met privacy risico's.
4	Opleiding	Alle medewerkers zijn opgeleid om met privacy gevoelige informatie om te gaan	100 % van de nieuwe medewerkers (in- en externe medewerkers) binnen 4 weken na indiensttreding de elearning AVG en datalekken afgerond	Maandelijks overzicht van de CAK academy	Wordt door HR aan de N-1 verstrekt.
4	Opleiding	Onderhouden van kennis	Ieder medewerker volgt jaarlijks de elearning privacy en datalekken en rond deze af	Maandelijks overzicht van de CAK academy.	
4	Uitvoeringstoetsen	Voldoen aan wet- en regelgeving	In alle uitvoeringstoetsen zijn de privacy aspecten (Risico's en AVG principes) geborgd	Overzicht	
4	Changes	Voldoen aan wet- en regelgeving	Alle van toepassing zijnde privacy risico's zijn geadresseerd in een Pi-planning	Aantoonbaar op back log door productowner	
4	Rechten van betrokkenen	Tijdigheid	100% van de klantverzoeken m.b.t. rechten van betrokkenen zijn binnen de wettelijke termijn afgehandeld	Aantoonbaar door registratie binnen het cluster	
1	Accesmanagement	Personeel heeft toegang tot informatie op basis van need to know	Voor alle rollen is vastgelegd tot welke informatie en informatiesystemen men toegang moet hebben met welke rechten	Door de N-1 vastgestelde schema's zijn beschikbaar	
1	Accesmanagement	Toepassen van de toegangsschema's	3 maandelijks worden er checks gedaan op actualiteit en juistheid van de autorisaties.	Registratie van de gecontroleerde overzichten, traceerbaarheid van de geïnitieerde correcties	
1	Logging- en monitoring	Vaststellen van afwijkend gedrag	Maandelijks worden log gegevens beoordeeld om afwijkend gedrag m.b.t. de verwerking vast te stellen		
4	Dataveiligheid	Testen geschiedt met geanonimiseerde data	Alle OTA-omgevingen bevatten anonieme data. Waar dit niet mogelijk is, is er een door de eigenaar en FG gevalideerde exceptie beschikbaar. Deze 2 onderdelen samen geven een 100% dekking van de OTA.	Overzicht van O, T en A-omgevingen waarin persoonsgegevens voorkomen. Minimaal jaarlijks op te leveren.	Nb: Dit onderwerp is alleen van toepassing op de rapportage van IT.
2	Datalekken	Correct melden aan AP	Alle via het selfserviceportal gemelde datalekken zijn binnen de wettelijke termijn aan AP gemeld.	Rapportage uit Topdesk	
3	Datalekken	Permanent verbeteren	Op alle datalekken is een analyse uitgevoerd om procesoptimalisaties en/of systeem optimalisaties te identificeren.	Rapportage uit Topdesk	
3	Datalekken	Opvolging datalekken	Het cluster heeft van elk datalek op elk moment inzichtelijk wat de status is van de afhandeling / oplossing.	Overzicht uit Topdesk van de op het cluster van toepassing zijnde datalekken.	

Decharge

Project: Algemene verordening gegevensbescherming (AVG)

1.	Managementsamenvatting	3
2.	Wat waren we van plan en wat is daarvan terecht gekomen?	5
3.	Waar zijn we tijdens de uitvoering tegenaan gelopen?	11
4.	Aan wie dragen we wat over?	13
5.	Waarvoor wordt akkoord gevraagd?	17
6.	Akkoordverklaring en decharge	17
7.	Bijlage 1: Rapportage ADO	18
8.	Bijlage 2: Specs. Rapportage	19
9.	Bijlage 3: Opgeleverd voor Agile werkwijze	25
10.	Bijlage 4: Overzicht AVG producten met bron	26
11.	Bijlage 5: Status bevindingen	27
12.	Bijlage 6: Status bevindingen aangevuld met acties Bestuurszaken	28

PROJECT AVG

Wat waren we van plan en wat is daarvan terecht gekomen?

Scope	De origineel gekozen scope van het programma AVG was voldoen aan niveau 3 van het CIP (Centrum Informatiebeveiliging en Privacybescherming). Later heeft het programma zich rechtstreeks gericht op de vereisten vanuit AVG en NOREA (Nederlandse Orde van Register EDP-Auditors). Zie paragraaf 2.1 voor details.
Producten	Aanleggen/actualiseren verwerkingenregister, actualiseren verwerkersovereenkomsten, uitvoeren gegevensbeschermingseffectsbeoordelingen (GEB), bewaar- en vernietigingstermijnen, Privacy By Design, Richtlijn schonen persoonsgegevens, e-learning en awareness communicatie.
Resultaten	86% van de voorgenomen producten (vertaald in pbi's) is opgeleverd. De restpunten worden overgedragen (zie hoofdstuk 4).
Planning	De planning zoals opgegeven in de uitvoeringstoets (UVT) van oktober 2017 (niveau 3 CIP per 25 mei 2018) bleek niet realistisch voor een organisatie met het verwerkingsvolume van het CAK. Ook het realiseren van de run organisatie Privacy heeft langer geduurd dan verwacht. Hierdoor is het borgen van de door het programma opgeleverde producten achter gebleven en heeft het programma veel ondersteuning geleverd aan de run organisatie. Uiteindelijk is d.m.v. een exceptie de einddatum van het programma vastgesteld op 31-12-2019.
Budget	€ 1.193.322,- incl. exceptie. Het project is afgesloten met een positief projectresultaat van € 172.332,-
Resources	Project team: [redacted] Privacy Officers: [redacted]
Kwaliteit	Om de kwaliteit te kunnen waarborgen heeft het projectteam een Definition of Done (opgesteld). De door het project opgeleverde producten zijn o.a. hierdoor van goede kwaliteit. Het projectteam

	heeft bij alle producten gestreefd naar 100%. In een aantal gevallen is deze 100% niet gehaald.
Voldaan aan vereisten vanuit gebruiker	Ja
Voldaan aan acceptatiecriteria (business en ICT)	Ja
Waar zijn we tijdens de uitvoering tegenaan gelopen?	
Risico's	Zie paragraaf 3.1
Issues	Zie paragraaf 3.2
Lessons Learned	Zie paragraaf 3.3
Afhankelijkheden met andere projecten en activiteiten	Project Dataschoning. Zie paragraaf 3.4
Aan wie dragen we wat over?	Gedurende de looptijd van het programma werd de privacy run organisatie aangesterkt naar twee privacy officers. Hierdoor hebben de producten van het project een landingsplaats gehad, maar echte borging in de organisatie is nog niet afgerond. Om deze borging en de restpunten van het project een warme overdracht te geven richting regelingen / de lijn organisatie is het Tijdelijk Samenwerkingsverband Privacy (TSP) opgericht. Voor de details over het TSP, zie hoofdstuk 4.
Back log/restpunten	Zie hoofdstuk 4
Openstaande acties	Er zijn geen openstaande acties

2.1. Scope

Eind 2017 is het project gestart met als doel CIP (Centrum Informatiebeveiliging en Privacybescherming) niveau 3 per 25 mei 2018.

- Deze niveaus hebben betrekking op de mate van borging van privacy in de organisatie en daar was het CAK bij het starten van het project maar deels aan toe.
- De CIP standaard dekte niet 1 op1 de verplichtingen AVG.
- Uitkomsten van het CIP self assessment (in het begin ingezet om voortgang te meten) bleken niet congruent.
- De checklist van het CIP (in 2017 het enig beschikbare standaard) raakte gedurende de looptijd van het project op de achtergrond en NOREA (Nederlandse Orde van Register EDP-Auditors) kwam op als nieuw standaard.

In een besluit aan de RvB is op 14 april 2020 een akkoord gevraagd op de gewijzigde scope.

2.1.1. Producten

Van de rechtstreeks uit AVG en NOREA gedestilleerde producten is een overzicht gemaakt dat vervolgens verdeeld is naar zaken door het programma op te leveren en zaken door de run organisatie op te leveren. De projectproducten zijn vanaf het moment dat we de Agile werkwijze hebben gehanteerd (februari 2019) vertaald naar EPICS, Features en PBI's in de tool ADO (Azure DevOps). Hieronder een overzicht uit ADO met de verschillende productniveaus. Een deel van de producten is niet afgerond, een deel is afgerond maar wordt nog geactualiseerd en een deel is volledig opgeleverd. Voor de producten die nog niet opgeleverd zijn of nog geactualiseerd worden is onder het overzicht een toelichting opgenomen.

Er zijn 3 overzichten opgenomen in de bijlagen:
1. De voortgang van het project in producten en tijd
2. Alle specs en de voortgang daarvan
3. Producten opgeleverd voorafgaand aan de Agile werkwijze

Scope Totaal Aantal EPICS AVG: 8	Aantal EPICS AVG afgerond: 5	Aantal EPICS In Progress: 3	EPIC + Features mee met Decharge	Opmerking
45109 Project VCT (Verwerkingsregister CAK) [redacted] Done 2/2	45109 Project VCT (Verwerkingsregister CAK) [redacted] Done 2/2			EPIC *VCT* Opgeleverd. Zie decharge document voor toelichting van de huidige stand van zaken.
45104 Project PBD (Privacy By Design) [redacted] Done 2/2	45104 Project PBD (Privacy By Design) [redacted] Done 2/2			EPIC *PBD*. Opgeleverd. Zie decharge document voor toelichting van de huidige stand van zaken.
45108 Project APC (Aanpak en Privacy Impact Assessments) [redacted] Done 2/2	45108 Project APC (Aanpak en Privacy Impact Assessments) [redacted] Done 2/2			
50699 Risk Management (BO) [redacted] Done 2/2	50699 Risk Management (BO) [redacted] Done 2/2			
50715 Datamanagement (UO1 en UO3) Done 1/1	50715 Datamanagement (UO1 en UO3) Done 1/1			
45107 Project PKB (Procedures Klantprocessen) [redacted] In Progress 1/2		45107 Project PKB (Procedures Klantprocessen) [redacted] In Progress 1/2	Epic: Project PKB (Procedures Klantprocessen) – In Progress Feature: Frontend - Rechtopvragen ... – Done – 100% Feature: Backend - Procedure uitvoeren klantrechten – In Progress	EPIC *PKB* + Feature ***Backend - Procedure uitvoeren klantrechten***. Zie decharge document voor inhoudelijke toelichting.
45098 Project GOP (Gestructureerde en Ongestructureerde Persoonsgegevens) [redacted] In Progress 1/3		45098 Project GOP (Gestructureerde en Ongestructureerde Persoonsgegevens) [redacted] In Progress 1/3	Epic: Project GOP (Gestructureerde en Ongestructureerde Persoonsgegevens) – In Progress Feature: Vaststellen bewaartermijnen – In Progress Feature: Netwerkscanner (Ongestructureerd digitaal) – In Progress Feature: Datacleaning archief (Gestructureerd fysiek) – Done – 100%	EPIC *GOP* + Features ***Vaststellen Bewaartermijnen & Netwerkscanner***. Zie decharge document voor inhoudelijke toelichting.
48867 AVG Awareness [redacted] In Progress 1/2		48867 AVG Awareness [redacted] In Progress 1/2	Epic: AVG Awareness – In Progress Feature: Nieuwe E-learning opzetten – In Progress Feature: Inrichten DPO – Done – 100%	EPIC *AVG Awareness* + Feature ***Nieuwe E-Learning opzetten***. Zie decharge document voor inhoudelijke toelichting.

Het project heeft in Q4 van 2018 een verwerkingenregister in Excel opgeleverd, bestaande uit losse documenten gebaseerd op de functieprofielen. Vervolgens is besloten dat Excel geen structurele, flexibele en beheerbare oplossing is en is ervoor gekozen om aan te sluiten bij het verwerkingenregister van het Rijk, verkregen via VWS. Deze tool is vanaf eind 2018 gevuld vanuit de aangeleverde Excelregisters. Het overzetten is opgepakt door project en Privacy Office om de business niet nogmaals te belasten. De originele Exceldocumenten zijn toegevoegd aan het register in de tool. Uiteindelijk bleek dat ook deze tool niet de juiste is. Er zitten wat bugs in die met een nieuwe versie zouden moeten worden opgelost, maar er is vanwege voortschrijdend inzicht besloten niet met deze tool verder te gaan. Tijdens het traject van het aankopen van een GRC-tool bleek die ook te kunnen beschikken over een verwerkingenregister die aan een groot deel van de eisen voldoet. Tot er een nieuwe tool is, is besloten de huidige registers te laten accorderen. De coördinatie hiervan ligt bij het Privacy Office. Het CAK voldoet hiermee aan de wettelijke plicht tot het hebben en (kunnen) bijhouden van een register van verwerkingen. Er is nog geen procedure voor het onderhouden van het register, omdat op het moment van decharge nog niet duidelijk is hoe de nieuwe organisatie eruit komt te zien en welke tool we uiteindelijk zullen hanteren. Overigens is de procedure geen product van het project. Toch vragen wij aandacht van de N-1 directeuren en managers voor het vaststellen van een proces rond het toevoegen van nieuwe verwerkingen, aanpassingen bij wijzigingen en actualiseren van het register. Het Tijdelijk Samenwerkingsverband Privacy (TSP) kan bijdragen aan het uitwerken en opstellen van dit proces. Gedurende deze periode worden deze activiteiten via de implementatie portfoliomanagement en het changeprogramma overgeheveld naar de regelingen. Zie hoofdstuk 4 voor meer details.

Momenteel is een pilot gestart voor Privacy by Design, waarbij 'PIA_0214_Uitwisseling UWV nieuw' is geselecteerd als uitgangspunt voor de pilot. Het CAK heeft zich in samenwerking met het UWV tot doel gesteld om naar een webbased uitwisseling te gaan. Het project heeft de organisatie aanbevolen om de pilot voort te zetten met hulp van het TSP en van daaruit de grote lijnen vorm te geven mogelijk met opleidings-/ontwikkelingsmogelijkheden.

Een van de eisen van de AVG is om personen de mogelijkheid te geven om zijn/ haar persoonsgegevens te laten verwijderen. Het project heeft in juni 2019 een voorstel geschreven naar de afdelingsmanager van de Backoffice om dit mogelijk te maken. Hierbij was het van belang om er voor te zorgen dat wat wij aan de klant beloven, namelijk het verwijderen van persoonsgegevens, waargemaakt kan worden. Naast het verwijderen van persoonsgegevens heeft een klant ook het recht zijn of haar data in te zien. Een dergelijk inzageverzoek heeft betrekking op dezelfde data als een verzoek tot verwijdering. In plaats van de data te verwijderen worden kopieën (vaak printscreens) van de data gemaakt, deze worden vervolgens op veilige wijze aan de klant geleverd. Om dit voor elkaar te krijgen was het eerst van belang om de bewaartermijnen vastgesteld te hebben. Met deze vaststelling is het team vervolgens in gesprek gegaan met diverse ontwikkelgroepen. Uiteindelijk is met diverse eindgebruikers een formulier ontwikkeld met als doel via de Self Service Portal (SSP) een melding in te dienen, zodat verwijder en inzageverzoeken gecentraliseerd worden uitgevoerd. Gekozen is om als eerst de draad met CPR door te knippen. Hiermee wordt voorkomen dat de persoon op mijn klantportaal kan inloggen en alle gegevens opnieuw kan binnenhalen. Als dit uitgevoerd is kan het verzoek simultaan naar alle overige ontwikkelgroepen worden verstuurd. De handeling en monitoring dat het volledig verzoek binnen 30 dagen wordt afgehandeld ligt bij het Servicecenter. Het verdient aanbeveling om de werking (bijvoorbeeld d.m.v. een audit) vast te stellen.*

In het kader van het schonen van persoonsgegevens was er behoefte aan duidelijke kaders. Daarom hebben [redacted] (Bestuurszaken), [redacted] (Privacy Office) en [redacted] (Project) met de selectielijsten als uitgangspunt een eerste aanzet gedaan voor een memo met daarin bewaartermijnen. Na verschillende afstemmomenten met de business bleek dat de bewaartermijn voor de WMO niet juist is opgenomen in de selectielijst. In het memo staat wel de juiste termijn en daarom is met Bestuurszaken en Privacy Office afgestemd dat dit memo bekend moet zijn in de organisatie. Hiervoor is het memo aangepast (meer context). Het nieuwe memo moet bekend worden gemaakt in de organisatie. Eind november hebben project en Privacy Office met Communicatie gesproken en dit memo wordt meegenomen in het communicatieplan/-campagne. Het verdient aanbeveling om de werking (bijvoorbeeld d.m.v. een audit) vast te stellen.*

Voor het schonen van persoonsgegevens zijn bewaartermijnen noodzakelijk. Daarnaast heeft het project in samenwerking met Privacy Office een richtlijn schonen persoonsgegevens opgesteld. Deze richtlijn is besproken in de Stuurgroep AVG van 9 december 2019 en is na gevraagde aanpassingen eind januari vastgesteld door middel van een digitale goedkeuringswerkstroom vanuit het projectportaal. De overdracht van het document aan de CIO wordt meegenomen op de backlog die wordt samengesteld door het TSP. Het verdient aanbeveling om de werking (bijvoorbeeld d.m.v. een audit) vast te stellen.*

* Het advies om een audit uit te (laten) voeren op werking van AVG processen, registers, etc… zal worden opgenomen op de backlog van het TSP.

Het deelproject netwerkscanner heeft 6 rapporten afgenomen waarbij de eerste door de projectorganisatie is uitgevoerd en de andere vijf overgedragen worden aan de lijn. Of hier echt sprake is van 'restpunten' is de vraag, maar de 5 resterende rapporten worden bij de decharge overgedragen aan de lijn.
Voor de netwerkscanner wordt op dit moment de laatste hand gelegd aan het eerste rapport. De analyse van dit rapport zal nog niet afgerond zijn ten tijde van de decharge. Deze wordt overgedragen aan het TSP. Op 23 december is de scan succesvol gestart. De verwachting is dat deze begin februari is afgerond. Hierna kunnen de volgende vervolgstappen genomen worden:

- Analyse of scan doet wat is afgesproken – Privacy Officers + Tijdelijk Samenwerkingsverband Privacy
- Uitvoeren wensen en eisen a.d.h.v. resultaten scan – Axians in opdracht van Privacy Officers
- Analyse vooraf opgestelde IT requirements (performance, security, snelheid, etc) – Technisch Projectleider
- Uitvoeren wensen en eisen a.d.h.v. IT analyse – Axians in opdracht van IT
- Uitkomst bespreken met Regeling Directie - Privacy Officers + Tijdelijk Samenwerkingsverband Privacy

In samenwerking met de toenmalige contractpartij E-learning Training is op 1 mei 2018 de eerste e-learning AVG opgeleverd. Deze is opgeleverd aan HR en op de CAK-Academie geplaatst. Helaas bleek dat door een technische onhandigheid niet goed zichtbaar was of een medewerker de training daadwerkelijk had gevolgd en afgerond. Dit is meegenomen als vereiste voor een eventuele volgende versie. In het kader van awareness is besloten een nieuwe versie op te leveren, waarbij de e-learnings AVG en Datalekken worden samengevoegd. Het CAK werkt inmiddels met een nieuw platform en leidt op dit moment een HR-medewerker op om zelf de e-learnings te kunnen ontwikkelen. Het project heeft op basis van de commentaren op de eerste e-learning van AVG en datalekken (helaas niet meer beschikbaar vanwege vernieuwing Academie, dus uit het hoofd), registratie datalekken en eigen ervaringen een eerste aanzet gedaan voor inhoudelijke onderwerpen die meegenomen kunnen worden. Deze eerste verkenning hebben wij gedeeld met de medewerker van HR die zich bezig houdt met het ontwikkelen van de e-learning. De opleiding duurt tot half december en daarna zullen de inhoudsdeskundigen (FG, Privacy Officers, voormalig projectteamleden, functionaris datalekken) gevraagd worden om de inhoud verder uit te werken.

Eind november 2019 heeft het project, samen met Privacy Office en Communicatie afspraken gemaakt over het vervolg van de bewustzijnscampagne informatiebeveiliging & privacy. Daarbij is nagedacht over: de nieuwe e-learning, meer, gerichte aandacht voor privacy op intranet, uitbreiden van de DWO, nieuwsbericht AVG: hoe staat het ermee? (waaronder einde project en successen), communicatie in 2020. Afhankelijk van de nieuwe centrale plek voor Privacy (CIO) communicatieplan overdragen aan verantwoordelijke. Nu belegd bij Privacy Officers.

2.1.2. Resultaten

86% van de voorgenomen producten (vertaald in pbi's) is opgeleverd. De restpunten worden overgedragen (zie hoofdstuk 4).

2.2. Planning

De planning zoals opgegeven in de uitvoeringstoets (UVT) van oktober 2017 (niveau 3 CIP per 25 mei 2018) bleek niet haalbaar:

- Eind 2017 voldeed het CAK niet aan de WBP. Voor de benodigde werkzaamheden om dit gat te dichten is nooit budget aangevraagd, maar de werkzaamheden zijn wel door de projectgroep meegenomen.
- In de UVT werd voorzien in het neerzetten van een privacy run organisatie (3fte) waar de borging van de in de projectorganisatie gemaakte producten plaats zou vinden. Dit is nooit gerealiseerd. Door de beperkte bezetting aan de run kant (lange tijd was het 1 medeweker die de rol van Privacy Officer naast

zijn bestaande functie moest doen) zijn er in de projectorganisatie veel meer uren gemaakt dan verwacht.

- De in de UVT genoemde PM-post voor dataschoning is nooit te gelde gemaakt. De werkzaamheden zijn (deels) wel uitgevoerd.
- Om zover mogelijk te komen met het budget van 1 miljoen is er met een klein team gewerkt. Hierdoor zijn de personeelskosten laag. Omdat het realiseren van producten een bepaalde doorlooptijd heeft (denk bijvoorbeeld aan een aanbestedingstraject) zorgt het vergroten van het team niet per definitie voor versnelling in de realisatie. Hier is dan ook niet voor gekozen.

2.3. Budget

		Dashboard FA
Initieel budget (beschikbaar gekomen eind 2017):	€ 1.000.000	
Exceptie goedgekeurd d.d. 26-6-2019	€ 193.322	
	€ 1.193.322	
Personeelskosten:		
2017 + 2018		€ 446.349
2019 (inclusief extra uitzendkrachten t.b.v. DAC)		€ 435.737
		€ 882.086
Out of pocket kosten 2017+2018+2019:		
Betaald aan opleidingen	€ 5.072	
Betaald aan E-learning AVG	€ 11.435	
Tool GOP	€ 41.371	
White board tekeningen	€ 1.585	
Betaald aan E-learning Datalek	€ 8.228	
HR Recruitment applicatie	€ 1.398	
HR Recruitment applicatie?	€ 2.420	
Aanpassing aan E-learning datalek	€ 2.753	
CIP workshop	€ 1.000	
Factuur change BSN nummer	€ 1.997	
Audit	€ 60.694	
		€ 138.903
Totale uitgaven 2017 + 2018 + 2019:		€ 1.020.989
Projectresultaat:		**€ 172.332**

2.4. Kwaliteit

Om de kwaliteit te kunnen waarborgen heeft het projectteam op aanraden van de scrummaster een Definition of Done (opgesteld). Hieronder de eisen waaraan een afgerond product moet voldoen:

- Er is een spellingscheck gedaan voor de documenten die worden gedeeld met de organisatie
- De documenten zijn gecontroleerd op huisstijl
- De documenten (voor Privacy Office) zijn geaccordeerd/geaccepteerd door Privacy Office
- Er is feedback van eindgebruikers gevraagd op het opgeleverde product

- Eindgebruikers: degene met wie je het product samenstelt en het product uiteindelijk in gebruik gaat nemen.
- Voor het project is het belangrijk om te weten aan wie het product is opgeleverd. Na oplevering moet het product worden opgenomen in het productenoverzicht.
- Bij het afronden van de laatste taak v.d. PBI, moet er aanvullende informatie worden toegevoegd:
  - Aan wie is het overgedragen (daar waar nodig).
  - Link is geplaatst in productenoverzicht (daar waar nodig).

De door het project opgeleverde producten zijn o.a. hierdoor van goede kwaliteit. Het projectteam heeft bij alle producten gestreefd naar 100%. In een aantal gevallen is deze 100% niet gehaald:

- E-learning AVG: onder tijdsdruk is een goede e-learning opgeleverd, maar inhoud en techniek konden beter. Een nieuwe e-learning is in de maak.
- Verwerkingenregister: is vanuit Excel overgezet naar een Rijkstool, maar ook deze heeft niet alle gewenste functionaliteit. Er heeft inmiddels een productpresentatie plaatsgevonden van de firma Yellowtail, leverancier van de GRC-tool. De verwachting is dat het verwerkingenregisteren in Q1 wordt opgenomen in deze tool.

3.1. Risico's

1 Start project	4	5	20 Gesloten	[redacted]	Via de Fg ([redacted]) met de AP communiceren over zaken die wel zijn gelukt en de zaken die meer tijd nodig hebben (Comply or Explain). Stel een planning op om aan te geven wanneer de verwachte realisatie / transitiedatum is. Prioriteiten op basis van risico's.	Verminderen	Productoverzicht voor run en project is opgesteld aan de hand van AVG, Wbp, CIP en overige kaders. Project heeft gewerkt aan de hand van dit overzicht waardoor een degelijke inhaalslag heeft plaatsgevonden.	1-9-2017	25-5-2018	5-12-2019
5 Inzetbaarheid FG	5	3	15 Gesloten	[redacted]	De FG krijgt een operationele assistent toegewezen welke full time inzet wordt. De huidige CISO wil deze taak full time op zich nemen.	Verminderen	FG is voldoende aangehaakt. Restpunt is het adviseren n.a.v. de PIA's. Dit proces loopt.	1-9-2017	25-5-2018	5-12-2019
3 Doorlooptijd implementatie AVG	3	3	9 Gesloten	[redacted]	De directie van het CAK / units moet de urgentie benoemen binnen de domeinen. De units zullen voldoende geschikte capaciteit vrij moeten maken.	Verminderen	Het CAK voldeed op 25 mei niet aan de AVG. Inmiddels zijn veel producten opgeleverd en is er een communicatieplan voor constante [redacted] is nog online en er wordt nagedacht over permanente plekken voor privacy.	1-9-2017	25-5-2018	5-12-2019
2 Fusie met BR (ZINL)	3	2	6 Gesloten	[redacted]	De AVG geldt voor iedereen in de EU. Beide partijen moeten voldoen aan de AVG. Het afstemmen van processen kan ook op een later tijdstip dan 28 mei 2018.	Overdragen	Alle afdelingen van het CAK zijn aangehaakt (denk aan PIA's, BSN van uitingen etc).	1-9-2017	25-5-2018	5-12-2019
6 Afhankelijkheid keten mbt voldoen aan AVG	2	3	6 Gesloten	[redacted]	AVG bespreken en toetsen op de keten.	Verminderen	Ketenstromen zijn in beeld gebracht mede d.m.v. PIA's. Verwerkersovereenkomsten zijn afgesloten en er is een start gemaakt met een proces bij Inkoop. Bij uitvoeringstoetsen wordt privacy meegenomen.	1-9-2017	25-5-2018	5-12-2019
4 Infrastructuur niet gereed voor AVG.	1	3	3 Gesloten	[redacted]	Gebruik de Comply of Explain methode om dit inzichtelijk te maken en de voortgang te monitoren.	Verminderen	Privacy by Design is uitgedacht. Pilot PbD met eerste Product Owner is gestart. Eerste schoning heeft plaatsgevonden. Documenten daaromtrent zijn in ontwikkeling, maar de basis staat. Implementatie van inwilligen individuele klantverzoeken (inzage, verwijderen) werkt aan de voorkant (KA) en in het project is gewerkt aan de ICT-kant. Formulier is opgeleverd, oplossingsgroepen worden nog meegenomen (onderdeel van overdracht na project). 3LOD worden ingericht met organisatiewijzging, evenals de ICT organisatie.	1-9-2017	25-5-2018	5-12-2019
7 Geanonimiseerde databases: i.h.k.v. AVG dient het CAK een volledig overzicht te hebben van aanwezige databases, welke daarvan persoonsgegevens bevatten, of deze geanonimiseerd zijn en zo niet of er een goedgekeurde (tijdelijke) uitzondering ligt.	1	1	1 Gesloten	[redacted]	Deze kennis blijkt niet gecentraliseerd te liggen in de organisatie. IT heeft aangegeven dat de servicedesk niet beschikt over complete, up-to-date, lijst van systemen en systeemeigenaren. De systeemeigenaren worden aangeschreven.	Overdragen	De Configuratiemanager heeft ervoor gezorgd dat er nieuwe CMDB-velden zijn aangemaakt waarin wordt aangegeven of en welke persoonsgegevens aanwezig zijn en of er een exceptie voor is getekend. De nieuwe CMDB is in november opgeleverd. Nu is het zaak om betreffende velden te vullen en de gehele CMDB te fine tunen en correct in te vullen. Wat betreft de velden mbt de persoonsgegevens gaan we ervan uit dat dit in de maand januari volledig is gevuld.	17-9-2019	31-12-2019	5-12-2019
8 Geen privacy office	1	1	1 Gesloten	[redacted]	Privacy office op- en inrichten.	Vermijden	Privacy officers zijn aangesteld. Eind 2019 wordt nagedacht over de inrichting van CIO en de rest van de organisatie. Privacy wordt hierin meegenomen. Tot die tijd zijn de Privacy officers actief.	2-10-2019	31-12-2019	5-12-2019

3.2. Issues

9 Netwerkscanner	Zorg	1 Hoog	[redacted]	Het uitvoeren van de netwerkscan loopt vertraging op. Vanuit AVG is er nu nog 1 blokkerend issue: de Privacy Officer, belast met het raadplegen van de rapportage, mag de inhoud van de documenten (klant- en medewerkergegevens) niet inzien. Er is hier geen sprake van doelbinding. Hij mag slechts zien waar er privacy gevoelige informatie is gevonden (locatie), welke soort het betreft (BSN, telefoonnummer, etc...) en hoeveel er is aangetroffen (aantal 'hits').	Maatregel loopt	Software aanpassing / uitzetten van functionaliteit zodat privacy officer alleen dat kan zien wat hij (vanuit zijn functie en rol) mag zien. Door Axians / Micro Focus	22-10-2019	16-12-2019

3.3. Lessons Learned

Betrokkenheid van de keyplayers, stakeholdersmanagement. Nieuwe mensen binnen het project wegwijs maken binnen het bestaande project. Privacy top of mind krijgen en houden. Successen communiceren.	Korte lijnen binnen het project. B.v. de daily's Open en eerlijkheid loont! Hulpvaardigheid is hoog. Project en privacy	Maak duidelijke afspraken en leg deze vast over rollen, requirements, deliverables, definition of done. Duidelijk opdracht en doelstelling van de stuurgroep. Gedurende het project regelmatig met elkaar checken zitten we nog op de juiste weg. Zorg dat de keuze van de methodiek bij het project passend is. B.v. bij een project met groot business component is Agile niet de juiste methodiek. Audit scherp blijven qua doel en doorlooptijd. Meer handjes is niet per se meer snelheid. PMO als shared service center. E-mail adres is nuttig voor centrale vragen.

3.4. Afhankelijkheden met andere projecten en activiteiten

In eerste instantie had het project dataschoning als product op zich genomen. Omdat dataschoning verder gaat dan de AVG kaders, het gaat niet alleen om persoonsgegevens, is besloten het onderdeel schoning van gestructureerde digitale data 'onder te brengen' in het project dataschoning (DSG). We hebben de projectleider van DSG, vooruitlopend op decharge van dat project later dit jaar, gevraagd een korte samenvatting op te leveren met daarin de producten en resultaten.

Producten

- Daadwerkelijke eerste schoning uitgevoerd voor de eerste schonings slice (Wmo)
- Verwerkingenregister bijgewerkt voor de eerste slice
- Software changes ten behoeve van dataschoning (herhaalbaar bij optreden verjaring)
- Vrijgave en implementatie van de eerste dataschoning slice
- Rapportage van voortgang schoning (performance metrieken / aantallen / volume)
- Leerpuntenlog (ervaringen eerste schoning)
- VTP voor dataschoning voor fase 2

Resultaten

- Software changes ten behoeve van dataschoning (herhaalbaar bij optreden verjaring)
- Daadwerkelijke eerste schoning uitgevoerd t/m 2006 voor de eerste schonings slice AWBZ (Wmo)
- Vrijgave en implementatie van de eerste dataschoning slice
- Rapportage van voortgang schoning (performance metrieken / aantallen / volume)
- Leerpuntenlog (ervaringen eerste schoning)

Niet opgeleverd in deze vorm wegens nieuw inzicht:

- VTP voor dataschoning voor fase 2 (nieuwe termijnen, dus met huidige inzichten niet realistisch)
- Verwerkingenregister bijgewerkt voor de eerste slice (niet nodig, vastgelegd op dwo)

Extra opgeleverd:

- CER-klanten geschoond in WLZ

Gedurende de looptijd van het project werd de privacy run organisatie aangesterkt naar twee privacy officers. Hierdoor hebben de producten van het project een landingsplaats gehad, maar echte borging in de organisatie is nog niet afgerond.

Hierbij gelden de volgende uitgangspunten voor verdere ontwikkeling:
1) N-1 is verantwoordelijk dat zijn/haar organisatieonderdeel aantoonbaar voldoet aan de privacy wet- en regelgeving en het privacy beleid;
2) Het beschikbaar komen van kennis en capaciteit in de lijn is randvoorwaardelijk voor het kunnen nemen van de N-1 verantwoordelijkheid en het in control zijn op het gebied van privacy. Dit is ook in lijn met het transitie plan dat CIO-office heeft opgesteld;
3) CIO-office is kader stellend en ondersteunend .

We kiezen (in overleg met CIO) voor een Tijdelijk Samenwerkingsverband Privacy (TSP). In dit TSP neemt een sponsor van de business (aangesteld door de N-1) deel. Daarmee is er een direct en actief contact met de business. De sponsor is dan de linking pin voor de N-1's en kan hier betrokkenheid creëren.

CIO-office neemt deel aan het TSP in de rol van ondersteuning en kaderstelling, zoals in het transitieplan van CIO-office wordt voorzien.

Het TSP gaat zorg dragen voor:
- Het opstellen van een backlog (things to do lijst) met daarin verwerkt:
    - Openstaande punten vanuit het programma AVG
    - Openstaande bevindingen audit AVG 2019
    - Openstaande punten bij Privacy Officers
    - Openstaande punten bij CISO
- Van de items op deze lijst wordt vervolgens bepaald of:
    - het TSP het item oppakt / afrondt
    - het item overgedragen gaat worden naar de regelingen
    - het item binnen het CIO belegd wordt
    - er een andere actie nodig is dan bovenstaande alternatieven
- Om de overdracht naar de regelingen goed te borgen gaat het TSP gebruik maken van bestaande bewegingen. Zo neemt de CISO de backlog mee als input binnen het portfoliomanagement en is de borging van privacy in de regelingen door de voormalig programmamanager AVG aangemeld bij het changeprogramma ([redacted]). Daar wordt privacy (en security) als milestones en deliverables meegenomen in de diverse domeinen.

In het TSP participeren [redacted], [redacted], [redacted], [redacted] en [redacted].
Nog aan te vullen met de hierboven besproken Business Representative. Regelmatig wordt afgestemd met regelingdirectie.

Uit een eerste backlogsessie is onderstaande (concept) lijst gekomen:

Awareness	Monitoring en naleving
E-learning	Rapportages effectieve werking
Communicatie intranet	Auditing gepland vs ongepland
Communicatie plan	Back en Frontendproces
Strategie CIO	Dataminimalisatie
Richtlijnen (aantoonbaar)bepalen en vaststellen clusters	Privacy by Design
Vaststelling verwerkingsverantwoordelijke	Centrale plek inrichten
Transitieplan opstellen	Vervulling signaalfuncties
Privacyrisico's identificatie proces vastgesteld en vastgelegd	Ongestructureerde data 2.0 vervolg

4.1. Audit AVG 2019

In 2019 is er een audit / nul-meting uitgevoerd op AVG.
Er zijn toen 44 bevindingen gedaan.
In de PowerPoint in bijlage 5 de huidige status per punt.

Status in een paar woorden (nummering gelijk aan PowerPoint):

Norm	**Status**	
1.02	Afgehandeld	1
01.06	Afgehandeld	2
02.06	Is onderhanden bij Bestuurszaken.	3
01.04	Afgehandeld	4
03.01	Afgehandeld	5
01.01	Afgehandeld	6
01.02	Afgehandeld	7
01.03	Afgehandeld	8
01.04	Afgehandeld	9
03.02	Is onderhanden bij Bestuurszaken.	10
04.11	Is onderhanden bij Bestuurszaken.	11
05.02	Is onderhanden bij Bestuurszaken.	12
05.01	Is onderhanden bij Bestuurszaken.	13
05.04	Is onderhanden bij Bestuurszaken.	14
08.01	Afgehandeld	15
02.03 (1)	Kan pas medio 2020 worden gerealiseerd (nieuwe GRC)	16
02.03 (2)	Is onderhanden bij Bestuurszaken.	17
03.01	Deze norm zal na 1 april 2020 per regeling moeten worden beoordeeld op toepasbaarheid en haalbaarheid.	18
03.02	Is onderhanden bij Bestuurszaken.	19
03.04	Is onderhanden bij Bestuurszaken.	20
03.05	Is onderhanden bij Bestuurszaken.	21
03.06	Afgehandeld	22
03.07	Afgehandeld	23
01.04	Kan pas medio 2020 worden gerealiseerd (nieuwe GRC)	24
02.01	Kan pas medio 2020 worden gerealiseerd (nieuwe GRC)	25

01.01	Afgehandeld	26
01.02	Afgehandeld	27
02.04	Afgehandeld	28
01.01	In standaard verwerkingsovereenkomsten. Nog toetsing door FG?	29
02.02	In standaard verwerkingsovereenkomsten. Nog toetsing door FG?	30
02.03	In standaard verwerkingsovereenkomsten. Nog toetsing door FG?	31
04.01	Opnemen in beleid	32
04.02	Opnemen in beleid	33
06.01	Is onderhanden bij Bestuurszaken.	34
06.03	Afgehandeld	35
01.02	Per 1-4-2020 rapportage over naar direct reports	36
02.10	Afgehandeld	37
01.02	Afgehandeld	38
02.01	Afgehandeld	39
02.02	Werkinstructie maken	40
03.01	Werkinstructie maken	41
03.03	Afgehandeld	42
03.04	Afronding eind maart 2020 i.s.m. afdeling communicatie	43
01.04	Afgehandeld	44

Conclusie, van de 44 bevindingen zijn er:
20 afgehandeld
6 die pas later in 2020 kunnen worden opgelost (voor deadlines zie PowerPoint in bijlage 5)
5 waar op dit moment aan gewerkt wordt door TSP
13 in behandeling bij Bestuurszaken. Bestuurszaken heeft aangegeven deze punten voor 1-4-2020 af te ronden.

NOTE PER 8-4-2020 (CD): BESTUURSZAKEN HEEFT INMIDDELS NAAR DE OPENSTAANDE PUNTEN GEKEKEN. AANGEPAST OVERZICHT IN BIJLAGE 6.

4.2. Memo Functionaris Gegevensbescherming

In januari 2020 heeft de FG een memo opgesteld met zijn bevindingen over 2019.
In februari 2020 is in een RvB overleg het volgende afgesproken:
De stuurgroep AVG wordt gevraagd de RvB te adviseren welke punten van de FG rapportage moeten worden overgenomen, waar deze moeten worden belegd.
Dat leidt tot onderstaand overzicht:

Advies FG	Reactie stuurgroep AVG
Er vindt zeer geregeld geen beoordeling plaats van compliancy aan de AVG van (wijzigings)verzoeken die worden uitgevoerd. De eigenaar of opdrachtgever van de data of het proces zou dit standaard mee moeten nemen bij ieder verzoek.	Privacy by design is nog niet helemaal geïmplementeerd. Is één van de moeilijkste processen binnen AVG. Zeker ook om meetbaar te maken dat gemaakte afspraken worden nagekomen. Staat op de backlog van het TSP, maar zal altijd op de privacy agenda moeten blijven staan. Over te nemen door de diverse bedrijfsonderdelen van het CAK.

In het verlengde daarvan ligt de vraag wie op dit moment verantwoordelijk is voor compliancy aan de AVG. Dat is voor mij niet duidelijk. Daarnaast wordt er veelvuldig gebruik gemaakt van productie data in testomgevingen en worden er door analisten gegevens uit verschillende systemen met elkaar gekoppeld zonder dat gecheckt wordt of die data wel gecombineerd mag worden.	De N-1 functionaris is eindverantwoordelijk dat zijn organisatieonderdeel voldoet aan de privacywetgeving en het privacy beleid. Kaders en richtlijnen worden vastgesteld door CIO.
Daarnaast adviseer ik om meer aandacht te besteden aan het IAM beleid zodat duidelijk is wie toegang heeft tot welke data. Dit vergroot het in control zijn op dit onderwerp.	Deze aanbeveling herkennen wij en is in lijn met de bevindingen van de BIO audit: onvoldoende juist en consequent toegepast autorisatiebeleid. Uit handhavingsacties van de privacy toezichthouder blijkt dit ook een belangrijk aandachtsgebied te zijn. Omdat Access Management niet in scope is van het AVG project, zal dit door de lijnorganisatie ism CISO moeten worden opgepakt.
Zorg voor ondertekening van de verwerkingen door de verwerkingsverantwoordelijke. Daarbij zal publicatie van de verwerkingen op de website aan te bevelen zijn (niet verplicht).	Is een activiteit voor de in de verschillende bedrijfsonderdelen te realiseren IBP (informatie beveiliging en privacy) rollen.
Zorg dat bij processen voor bijvoorbeeld nieuwe voor veranderde taken, of andere processen waar privacy gevoelige gegevens een rol spelen goed is geborgd dat er altijd de vraag wordt gesteld of er een PIA dient te worden uitgevoerd. Bij gebrek aan een duidelijke verantwoordelijke monitoren de privacy officers deze risico's die genoemd zijn in het risicoregister. Het is derhalve van belang dat er een sluitend proces komt zodat er medewerkers daadwerkelijk verantwoordelijk zijn voor de onderkende risico's en dat daarbij de risico's structureel worden gemitigeerd.	Voor het eerste gedeelte wordt verwezen naar hetgeen eerder is gesteld inzake privacy by design. Verantwoordelijk voor het monitoren van de risico's zijn de IBP (informatie beveiliging en privacy) rollen.
Het proces van het afsluiten van verwerkersovereenkomsten is goed geborgd zodra de afdeling Inkoop betrokken is. Echter, er kunnen ook zaken ingekocht worden zonder dat Inkoop is betrokken. Gebleken is dat dan niet altijd aan de privacy wordt gedacht en er geen verwerkersovereenkomst wordt getekend. Dit is onwenselijk. Advies is om ook in die gevallen te borgen dat er aan de privacy aspecten wordt gedacht en er dus onder meer een verwerkersovereenkomst wordt gesloten.	Via 'Flits' zal hier vanuit de privacy officers aandacht voor worden gevraagd. Met de komst van P2P (gepland medio 2020) lopen 'kleine aankopen' (<15k) ook via Inkoop.
Als FG heb ik nu een duidelijk aanspreekpunt in de medewerkers met de rol privacy officer. Het is van belang dat ook in de nieuwe organisatie vanaf 1 april 2020 een duidelijk aanspreekpunt komt. Dit om mijn toezichthoudende taak goed uit te kunnen blijven voeren.	De N-1 functionaris is eindverantwoordelijk dat zijn bedrijfsonderdeel voldoet aan privacy wetgeving. In de nieuwe opzet zal dit in de diverse bedrijfsonderdelen operationeel worden ingevuld door de IBP rol. Dit lijkt het meest voor de hand liggende eerste aanspreekpunt. De Privacy Officer die werkzaam is binnen CIO is aanspreekbaar op de kaders en richtlijnen.

C/ K

Met de ondertekening van dit document gaan ondertekenaars akkoord met het beëindigen van het project AVG. Het projectresultaat vloeit terug naar de organisatie.

Interne Opdrachtgever: [redacted]	**Projectmanager:** [redacted]
(handtekening voor akkoord)	(handtekening voor akkoord)
Raad van Bestuur - CFO [redacted]	**CIO** [redacted]
(handtekening voor akkoord)	(handtekening voor akkoord)
Manager Control (voor projectresultaat): [redacted]	
(handtekening voor akkoord)	


2019-04
2019-05
2019-06
2019-07
2019-08
2019-09
2019-10
2019-11
2019-12
Project PKB (Procedures Klantprocessen)
[redacted]
[redacted]
Frontend - Recht op
[redacted]
Backend - Procedure uitvoeren klantrechten
Project PBD (Privacy By Design)
[redacted]
PB&D procedure
Privacy inbedden
Project VCT (Verwerkingsregister CAV 2.0)
[redacted]
Voltooien verwerkingenregister 2.0
PIA's in verwerkingen
Project GOP (Gestructureerde en Ongestructureerde Persoonsgegevens)
Vaststellen bewaartermijnen
Netwerkscanner (Ongestructureerd digitaal)
Dataschoning archief (Gestructureerd fysiek)
Project APC (Aanvullen Privacy Impact Assessments)
[redacted]
PIA's
Procedures
Risk Management (BO3)
[redacted]
[redacted]
Riskmanagement AVG (tijdelijk)
[redacted]
Analyse compliance NOREA
AVG Awareness
[redacted]
Nieuwe e-learning opzetten
[redacted]
Inrichten DWC
Datamanagement (UC1 en UC8)
[redacted]
Dataminimalisatie

C/ K

Project PKB (Procedures Klantprocessen)	**Frontend - Recht op verwijderen, inzage, dataportabiliteit en rectificatie**	**PKB: Proces recht op verwijderen, inzage, dataportabiliteit en rectificatie**	Analyse	Done
			Proces voor KCC opzetten	Done
	Backend - Procedure uitvoeren klantrechten	**PKB: Backend - Procedure uitvoeren klantrechten**	Analyse: Backend - Procedure uitvoeren klantrechten	Done
			Analyse: Backend - Procedure uitvoeren klantrechten deel 2	Done
		Backend procedure klantrechten deel 2: Burgerregelingen WAN, ONV, GEM etc.	Afspraak OHI / Edocs	Done
			Beperking van verwerking - eisen	Done
			Beperking Verwerking Gemoedsbezwaarden	Done
			Analyse Backend proces voor servicedesk	Done
			Gesprek PO's / beheerders / Burgerregeling-guru's	Done
			Inzage verzoek MaxCredible	Done
			Inzageverzoeken B&B BR (ONV,WAN,GEM)	Done
			Inzageverzoeken Gemoedsbezwaarden	Done
			Inzageverzoeken KA BR(ONV,WAN,GEM)	Done
			Inzageverzoeken KCC BR(ONV,WAN,GEM)	Done
			Inzageverzoeken Onverzekerden	Done
			Inzageverzoeken Wanbetalers	Done
			Klantrechten (inzage) WLZ	Done
			Klantverzoeken backend - servicdesk proces	Done
			Klantverzoeken eigen bijdrage regelingen - klantadvies	Done
			Klantverzoeken Schengen	Done
			Klantverzoeken Verseon	Done
			Klantverzoeken buddy	Done
			Klantverzoeken Porta en Ketenportaal	Done
			Planning klantverzoeken 2	Done
			Planning voor klantverzoeken BR1 (Wan,ONV,&GEM)	Done
			Recht op aanpassing gegevens: opvragen procedures	Done
			Verwijderen gegevens WordDocs	Done

C/ K

			Verwijderverzoek B&B / KA (Ultimus & Buddy)	Done
			Verwijderverzoek CPR	Done
			Verwijderverzoek eDOCS	Done
			Verwijderverzoek IEF	Done
			Verwijderverzoek Max credible	Done
			Verwijderverzoek Verint	Done
			Buitenland regelingen	Done
			Cebes - verder aanpak?	Done
			Coordinatie (backend) klantverzoeken via topdesk formulier	Done
			Inzage OF12	Done
			Klantrechten (inzage) WMO	Done
			Klantverzoeken topdesk	Done
			Thinsy - verder aanpak	Done
			Verwijderverzoek Cebes	Done
			Anonimiseren Cebes	Done
			Verwijderverzoek MMS-OHIO	Done
			Verwijderverzoek OF12	Done
			Verwijderverzoeken Thinsy	Done
			Backup bewaartijden uitvragen	Done
			Backups: Procedure en autorisaties	Done
			Dataverwerking inzage- en verwijderverzoeken	Done
			Klantverzoeken buitenbland: status uitzoeken + procedures opzetten	Done
			Topdesk Formulier - Informatie ophalen eindgebruikers	Done
			Topdesk Formulier - afstemmen Joffrey	Done
			Topdesk Formulier - Testen	Done
			Proces voor Servicecenter opzetten	Done
			WMO: Inzage verzoeken laatste updates?	Done
			WLZ inzage verzoeken - laatste updates	Done
			Verwijderverzoek Info Archive	In Progress
			Verwijderen gegevens (Globes en) CODA	In Progress
			Verwijderverzoek OHI	In Progress
			Verwijderverzoek Info Archive	In Progress
			Inhoud e-learning vaststellen	In Progress
			Lijst: Wat komt niet af?	In Progress
			Proces voor IT opzetten	In Progress
			Aandachtspunten WI vanuit audit	In Progress
			Anonimiseren Thinsy	In Progress

C/ K

Project PBD (Privacy By Design)	**P&SbD procedure**	**PBD: Opstellen en implementeren P&SbD procedure**	Analyse: beschikbaar materiaal mbt P&SbD	Done
			Analyse: eerste inventarisatie kennis developmentteams	Done
			Analyse: security maatregelen	Done
			Realisatie: Eerste opzet P&SbD procedure	Done
			Test: voorleggen voorgesteld proces aan product owners	Done
			Implementatie: Privacy en security by design werkwijze	Done
		Inkoop: privacy by design inbedden in Purchase To Pay tool	Realiseren: Inkoop moet privacy by design inbedden in Purchase To Pay tool	Done
	Privacy inbedden	**Privacy inbedden in veranderprocessen**	Implementatie: helpen bij implementatie privacy by design framework	Done
Project VCT (Verwerkingsregister CAK 2.0)	**Voltooien verwerkingenregister 2.0**	**VKC: Voltooien verwerkingenregister 2.0**	Uitsturen mail naar verantwoordenlijken	Done
			Publiceren verwerkingenregister op DWO	Done
			Verwerken reacties verantwoordelijken	Done
			Toevoegen bijlagen	Done
		Verwerkingenregister 2.0	Overzetten OP register naar SAAS	Done
			Verwerkingenregister Invo uitvragen	Done
			Verwerkingenregister FA opnieuw uitvragen	Done
	PIA's in verwerkingsregister	**VCT: PIA's in verwerkingsregister vastleggen**	In PIA register verwijzen naar verwerkingen	Done
Project GOP (Gestructureerde en Ongestructureerde Persoonsgegevens)	**Vaststellen bewaartermijnen**	**VCT/GOP: Per regeling bewaartermijn vaststellen**	Realiseren: concept bewaartermijn per regeling	Done
			Analyse: Afstemmen met Robin Horstkamp	Done
			Realiseren: aanvullen concept bewaartermijnen per regeling	Done
			Realiseren: afstemmen bewaartermijnen met verantwoordelijken	Done
			Realiseren: vaststellen bewaartermijnen	Done
		VCT/GOP: Afspraken vastleggen schonen persoonsgegevens	Realiseren: Implementatie bewaartermijn Wmo Pgb voor schonen OF	Done
			Realiseren: Implementatie bewaartermijn Wmo Pgb voor schonen OF	Done
			Realiseren: Vastgelegde afspraken met IT	Done

			Realiseren: richtlijn schonen persoonsgegevens	In Progress
			Realiseren: Centrale locatie voor data-eigenaren	In Progress
	Netwerkscanner (dataschoning ongestructureerd digitaal)	**GOP/VCT: Voorbereiding Netwerkscanner**	Opstellen beoordelingscriteria van de AVG scantool	Done
			Review beoordelingscriteria AVG scantool	Done
			Intake gesprekken met verschillende partijen	Done
			Versturen nota van inlichtingen	Done
			Bekend maken voorlopige gunning	Done
			Bekend maken definitieve gunning	Done
		GOP: Implementeren Netwerkscanner AVG	Kick Off Meeting CAK	Done
			Kick Off Meeting met Plusine	Done
			Vaststellen wensen en eisen Plusine	Done
			Opleveren wensen + eisen Plusine	Done
			Opstellen Plan van Aanpak (implementatie Netwerkscanner)	Done
			HLD van de oplossing	Done
			Bepaal shares	Done
			Source/destination/poort tbv Firewall	Done
			CAK accounts Axians	Done
			RACI opstellen	Done
			Antivirus Installeren	Done
			Gebruikersrechten/Wie mag wat?	Done
			MS MBSA installeren	Done
			Logfiles scannen beschikbaar stellen	To Do
			Wipe appliance	To Do
Dataschoning archief (Gestructureerd fysiek)	**Dataschoning Archief**		Inventariseren	Done
Project APC (Aanvullen Privacy Impact Assessments)	**PIA's**	**APC: PIA KCC**	Analyse: Voorbereiding PIA KCC	Done
			Analyse / realisatie: PIA sessie KCC	Done
			Realisatie: Uitwerken PIA KCC	Done
		APC: PIA HR 2e spoor	Analyse: voorbereiding PIA 2e spoor	Done
			Analyse: PIA sessie 2e spoor	Done
			Realiseren: Uitwerken PIA HR 2de spoor	Done
		PIA Ketenpartners	Analyse: Voorbereiden PIA Ketenpartners	Done
			Analyse: PIA sessie Ketenpartners	Done
			Realisatie: Uitwerken PIA Ketenpartners	Done
		PIA Bezwaar en beroep	Analyse: voorbereiden PIA B&B	Done
			Analyse: PIA sessie B&B	Done

C/ K

			Realisatie: uitwerken PIA B&B	Done
		PIA Financiele administratie, incasso en excasso	Analyse: Voorbereiden + houden pia institutionele klachten	Done
			Analyse: Voorbereiden + houden pia AWBZ	Done
			Analyse: Voorberiden + houden pia debiteurenbeheer	Done
			Analyse: Voorberiden + houden pia speciaal juridisch beheer	Done
			Analyse: Voorberieden + houden pia voorlichten klant incl webcare	Done
			Realisatie: uitwerken PIA institutionele klachten	Done
			Realisatie: uitwerken PIA AWBZ	Done
			Realisatie: uitwerken PIA debiteurenbeheer	Done
			Realisatie: uitwerken PIA speciaal juridisch beheer	Done
			Realisatie: uitwerken PIA voorlichten klant incl webcare	Done
			Realisatie: uitwerken PIA debiteurenbeheer	Done
			Bijwerken PIA's op DWO	Done
		PIA Klant advies	Analyse: voorbereiden pia complexe klantzaken	Done
			Analyse: Voorbereiden PIA klachten	Done
			Analyse: voorbereiden PIA output management	Done
			Analyse: PIA sessie complexe klantzaken	Done
			Analyse: Voorbereiden PIA klachten	Done
			Analyse: PIA sessie output management	Done
			Realisatie: uitwerrken PIA complexe klantzaken	Done
			Realisatie: uitwerken pia klachten	Done
			Realisatie: uitwerken PIA output management	Done
		PIA Salaris Administratie	Analyse: voorbereiden PIA Collectieve verzekeringen	Done
			Analyse: voorbereiden PIA Leaseauto's	Done
			Analyse: voorbereiden PIA Loonbeslag	Done
			Analyse: PIA sessie Collectieve verzekeringen	Done
			Analyse: PIA sessie Leaseauto's	Done

			Analyse: PIA sessie Loonbeslag	Done
			Realisatie: Uitwerken PIA Collectieve verzekeringen	Done
			Realisatie: Uitwerken PIA leaseauto's	Done
			Realisatie: Uiwerken PIA Loonbeslag	Done
	Procedures	APC: PIA Procedure	Realisatie PIA Procedure	Done
			Zelfscan aanpassen	Done
			Implementatie: Self-Service PIA in werking brengen	Done
		APC: Procedure risico's uit PIA's	Realisatie: Gegevensuitwisseling met brondinhouders benoemen	Done
			Realisatie: invullen risicoregister	Done
Risk Management (BO3)	Riskmanagement AVG (tijdelijk)	Reeds bekende risico's	Analyse van bekende risico's	Done
			Realisatie: documentatie van bekende risico's	Done
			Realisatie: monitoring van bekende risico's	Done
			Overdracht risico's uit PIA's naar lijn	Done
	Analyse compliance NOREA	Analyse compliance NOREA	Analyse: GAP-analyse huidige CAK AVG-documentatie t.o.v. NOREA kader	Done
			Realisatie: Acties bepalen	Done
			Implementatie: Communiceren naar PO	Done
AVG Awareness	Nieuwe e-learning opzetten	Creëer een nieuwe e-learning AVG	Voorbereiding: Afstemmen diverse partijen mbt inhoud	Done
			Monitoren: realiseren nieuwe e-learning AVG	Done
			Inhoud e-learning vaststellen	In Progress
	Inrichten DWO	Inrichting DWO mbt AVG Awareness	Inrichting DWO mbt AVG Awareness	Done
Datamanagement (UO1 en UO3)	Dataminimalisatie	Dataminimalisatie bewerkstelligen	Analyse: Wat kan worden meegenomen in project Data Governance (Wmo2020)	Done
			Overdracht restant OPU	Done
			Samenvatting maken + link accordering SG	Done
Decharge AVG Project		Decharge AVG acties	Opleveren Decharge AVG Project	In Progress

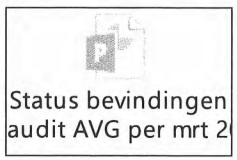
C/ K

Scope Totaal Aantal Producten AVG: 5	Aantal Producten AVG afgerond: 5	Opmerking
Beleid	Privacybeleid vastgesteld en vastgelegd.	Beleid 1.0 is opgeleverd door S&B. Eind 2019 wordt het beleid aangepast n.a.v. de bevindingen vanuit de audit.
Privacy statement	Privacy statement vastgesteld en gepubliceerd.	Privacy statement opgesteld met Communicatie en gepubliceerd op www.hetcak.nl. In oktober geactualiseerd, mede n.a.v. bevindingen uit de audit en klantrechten.
Verwerkersovereenkomsten	Verwerkersovereenkomsten opgesteld	Inzicht in verwerkersovereenkomsten. Met afdeling Inkoop afspraken gemaakt over af te sluiten overeenkomsten.
Uitwisseling van gegevens	Ketenstromen inzichtelijk	Gegevensuitwisseling zijn inzichtelijk gemaakt bij de PIA's.
Overbodige persoonsgegevens van uitingen	Alle uitingen van het CAK bevatten geen onnodige persoonsgegevens meer	Het BSN is van de primaire uitingen verwijderd. Voor de overige uitingen is in de stuurgroep een memo goedgekeurd met het advies dit in de roadmap projecten op te pakken.

Sidenote: Bovenstaande producten zijn door het project opgepakt en afgerond voor de Agile werkwijze is toegepast. Het gaat om de periode 2018 en begin 2019.

C/ K

C/ K



C/ K

Status bevindingen
audit AVG per april

C/ K

Datalekmeldingen Q1 en Q2 2020: feiten en cijfers

RvB

[redacted] (opsteller)

Datalekmeldingen Q1 en Q2 2020

Geen

28-07-2020

1.0

Periodiek geven wij inzicht in alle datalekken binnen het CAK. Deze memo geeft een overzicht van alle datalekmeldingen in Q1 en Q2 2020. Het betreffen voornamelijk datalekken die in de Self Service Portal zijn gemeld. Vanwege het regeling gericht werken bevat deze memo een overzicht van alle meldingen per regeling. Tot slot volgt een overzicht van de belangrijkste oorzaken. Afsluitend volgt een overzicht waarin de gegevens van Q1 en Q2 zijn verwerkt.

In de maanden januari tot en met juni van dit jaar zijn er in totaal **314** datalekken gemeld. Alle binnengekomen meldingen worden beoordeeld op inhoud. Niet alle meldingen zijn namelijk een datalek. Dit neemt niet weg dat er in de meeste gevallen wel sprake is van een incident. Onderstaand overzicht geeft inzage in het aantal datalekmeldingen per maand. De onderverdeling van het aantal datalekmeldingen per regeling weergeven (Wmo, Wlz, Zvw en Buitenland). De categorie 'overig' heeft betrekking op meldingen die niet onder één van de regelingen valt.

Datalekmeldingen per regeling (januari 2020):	
Wmo	22
Wlz	31
Zvw	4
Buitenland	1
Overig	5
totaal	**63**

Datalekmeldingen per regeling (februari 2020):	
Wmo	24
Wlz	34
Zvw	3
Buitenland	4
Overig	4
totaal	**69**

Datalekmeldingen per regeling (maart 2020):	
Wmo	13
Wlz	26
Zvw	4
Buitenland	0
Overig	6
totaal	**49**

Datalekmeldingen per regeling (april 2020):	
Wmo	21
Wlz	18
Zvw	1
Buitenland	2
Overig	1
totaal	**43**

Datalekmeldingen per regeling (mei 2020):	
Wmo	11
Wlz	16
Zvw	2
Buitenland	0
Overig	5
totaal	**34**

Datalekmeldingen per regeling (juni 2020):	
Wmo	33
Wlz	8
Zvw	4
Buitenland	5
Overig	6
totaal	**56**

Datalekken die bij de AP zijn gemeld
Van de **314** interne datalekmeldingen zijn er in totaal **246** datalekken bij de Autoriteit Persoonsgegevens gemeld. Dit is een gemiddelde van 40 meldingen per maand.

Onderstaand overzicht geeft het aantal meldingen per maand:

januari 2020 datalekken bij de AP gemeld	47
februari 2020 datalekken bij de AP gemeld	57
maart 2020 datalekken bij de AP gemeld	44
april 2020 datalekken bij de AP gemeld	35
mei 2020 datalekken bij de AP gemeld	26
juni 2020 datalekken bij de AP gemeld	37

Menselijk handelen
Datalekken veroorzaakt door menselijk handelen vormen nog steeds het overgrote deel van het aantal meldingen. Dit komt door de grote hoeveelheid klantcontacten (brieven, e-mails etc.). Menselijke fouten zijn niet helemaal te voorkomen. Een specifieke oplossingsrichting is er dan ook niet. Er kan op individueel niveau wel geleerd worden van gemaakte fouten. Daarnaast moet er continu aandacht zijn voor zorgvuldigheid op de werkplek.

Onderstaand een maandelijks overzicht van alle datalekken veroorzaakt door menselijk handelen:

maand	**aantallen**
januari	36
februari	43
maart	32
april	28
mei	23
juni	16
totaal	**178**

Een aantal voorbeelden van datalekken veroorzaakt door menselijk handelen zijn (niet limitatief):

- Invoerfouten. Enkele voorbeelden (intern en extern):
  - het invoeren van een postadres (intern);
  - het invoeren van een wettelijk vertegenwoordiger (intern);
  - invoeren van een IBAN in het verkeerde klantdossier (intern);
  - bezorgfouten (extern).
- E-mail naar de verkeerde afzender.

Technische oorzaak/ automatisch proces

Onderstaand een maandelijks overzicht van alle datalekken veroorzaakt door een technische oorzaak/automatisch proces:

maand	aantallen
januari	10
februari	12
maart	9
april	7
mei	2
juni	17
totaal	**57**

Een aantal datalekken worden veroorzaakt door een technische oorzaak (niet limitatief):

- In het verleden zijn postadressen ingevoerd in Cebes. Dit is destijds gedaan omdat de adreswijzigingen vanuit het BRP niet (tijdig) werden verwerkt. De postadressen zijn naderhand niet aangepast waardoor zij als leidend adres worden gehanteerd nadat de adreswijziging binnenkomt. Deze gevallen komen nog steeds voor;
- Automatische verwerking adreswijzigingen in Thinsy en Cebes komen niet altijd door in OF. Hierdoor blijven facturen naar een oud adres verstuurd worden. Dit geldt ook voor bijvoorbeeld invoer IBAN of AI in OF. Het oude adres uit OF wordt overgenomen en niet uit Thinsy/Cebes. Ook dit probleem komt regelmatig terug;
- Adreswijzigingen worden niet altijd verwerkt in de bronsystemen. Achteraf vindt er een handmatige synchronisatie plaats. CPR biedt niet altijd de oplossing althans de gegevens daarin zijn niet altijd up-to-date.

Versturen of afgeven van persoonsgegevens aan verkeerder ontvanger.
In meer dan de helft van de gevallen gaat het datalek om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Bij dit type datalek kan het gaan om een e-mail met daarin gevoelige persoonsgegevens die wordt verzonden naar de verkeerde ontvanger. Bijvoorbeeld door een typefout of omdat er een verkeerd adres bekend is. Daarnaast komt het voor dat personen hun eigen gegevens opvragen bij organisaties maar door een administratieve fout vervolgens ook persoonsgegevens van anderen ontvangen.

https://digitale-werkomgeving/sites/CAK/themasites/Wmo2020/MDM%20Wiki/CPR%20Synchronisatie.aspx

Datalekken met post
In een groot aantal gevallen gaat het om poststukken met gevoelige gegevens die bij de verkeerde persoon terechtkomen en geopend retour worden gestuurd. De onjuiste ontvanger heeft dan kennis kunnen nemen van de inhoud van de brief.

Datalekmeldingen die na beoordeling géén datalek blijken te zijn
Van de **314** via de Service Service Portal aangemelde potentiële datalekken bleek in **71** gevallen geen sprake te zijn van een datalek. Een aantal meldingen liggen in de risicosfeer van de klant bijvoorbeeld door het aanleveren van foutieve (adres)gegevens. In een aantal gevallen zijn brieven van overleden klanten naar oude of verkeerde adressen verstuurd (gegevens van overledene zijn geen persoonsgegevens). Ook ongeopende brieven die het CAK retour ontvangt worden niet als datalek geregistreerd. Om 'vervuiling' te voorkomen wordt de categorie 'persoonsgegevens van overleden klanten' opnieuw onder de aandacht gebracht in de nieuwe e-learning (zie hierna onder awareness).

Overzicht van meldingen die geen datalek blijken te zijn:

januari 2020	
geen datalek	16
februari 2020	
geen datalek	12
maart 2020	
geen datalek	7
april 2020	
geen datalek	8
mei 2020	
geen datalek	9
juni 2020	
geen datalek	19

Datalekmeldingen per regeling
In tegenstelling tot vorig jaar is het overgrote deel van alle datalekmeldingen afkomstig van de Wlz-regeling, direct gevolgd door de Wmo-regeling. Een klein deel van alle datalekmeldingen liggen in het domein Zvw en Buitenland. De exacte aantallen worden in de maandelijkse datalekrapportage opgenomen en zijn in deze memo verwerkt. Dat er bij de ene regeling meer datalekken voorkomen dan bij een andere regeling zegt niet alles. Dat er meldingen binnen komen is een teken dat het op bepaalde onderdelen nog niet helemaal goed gaat. Dit is tegelijkertijd een kans voor de organisatie om met deze signalen (lees: meldingen) aan de slag te gaan. Belangrijk ook is het tijdig melden van datalekken via de SSP. Na ontdekking heeft het CAK 72 uur om melding te doen bij de AP. De meldplicht stelt de AP onder meer in staat om te controleren of er adequaat op de inbreuk is gereageerd, of de inbreuk is beëindigd, of de genomen of aangekondigde beveiligingsmaatregelen voldoende zijn om nieuwe inbreuken te voorkomen, en of de personen die zijn getroffen door het datalek moeten worden geïnformeerd, en zo ja, of de organisatie dat heeft gedaan of nog gaat doen. Met de meldplicht aan de betrokkene is beoogd de betrokkene op de hoogte te stellen van wat er met diens gegevens is gebeurd, en de consequenties die

dat voor zijn belangen heeft. Hierdoor kan de getroffen persoon, voor zover dat mogelijk is, zich tegen de gevolgen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen.

Awareness
De afgelopen jaren is er veel aandacht geweest voor de AVG en zijn door het CAK bewustwordingsmomenten gestart om iedereen scherp te houden. Denk aan e-learnings, kennisbank artikelen voor frontoffice maar ook één-op-één gesprekken in teamverband om zoveel mogelijk fouten te voorkomen. Medewerkers lijken zich mede hierdoor steeds meer bewust te worden van de meldplicht datalekken. Het CAK verstuurt jaarlijks ruim 3 miljoen brieven naar haar klanten. De kans dat daarbij een datalek ontstaat is reëel. Medewerkers wordt gevraagd om ook bij twijfel een melding te doen. De beoordeling vindt plaats door de behandelaar. Ook de FG adviseert om altijd te melden. Liever een melding te veel, dan een datalek niet melden. Na de zomerperiode zal een nieuwe e-learning met betrekking tot de AVG en datalekken worden gepubliceerd. Deze e-learning is verplicht voor nieuwe maar ook voor bestaande medewerkers. Kortom: het onderwerp privacy (met name omgang met persoonsgegevens) moet blijvend en geïntegreerd in de business op de agenda blijven staan.

Datalekken voorkomen
Datalekken helemaal voorkomen is bijna onmogelijk. Je kunt het als organisatie wel proberen te minimaliseren tot een toelaatbaar aantal. Een manier om verbeteringen te realiseren is de werkprocessen onder de loep nemen om er achter te kunnen komen of er efficiënt wordt gewerkt. De AP adviseert ook hoe om te gaan bij een datalek. Actie is vereist om de gevolgen te beperken maar ook om in de toekomst zoveel mogelijk datalekken te voorkomen. Een aantal tips zijn:

1. Zorg voor overzicht op de situatie.
2. Neem onmiddellijk maatregelen om de schade te beperken. En schat de risico's in.
3. Bepaal of u het datalek wel of niet moet melden aan de Autoriteit Persoonsgegevens (AP). Zo ja, doe dit onmiddellijk.
4. Bepaal of u het datalek wel of niet moet melden aan de betrokken personen. Zo ja doe dit zo snel mogelijk.
5. Registreer het datalek in uw datalekregister.

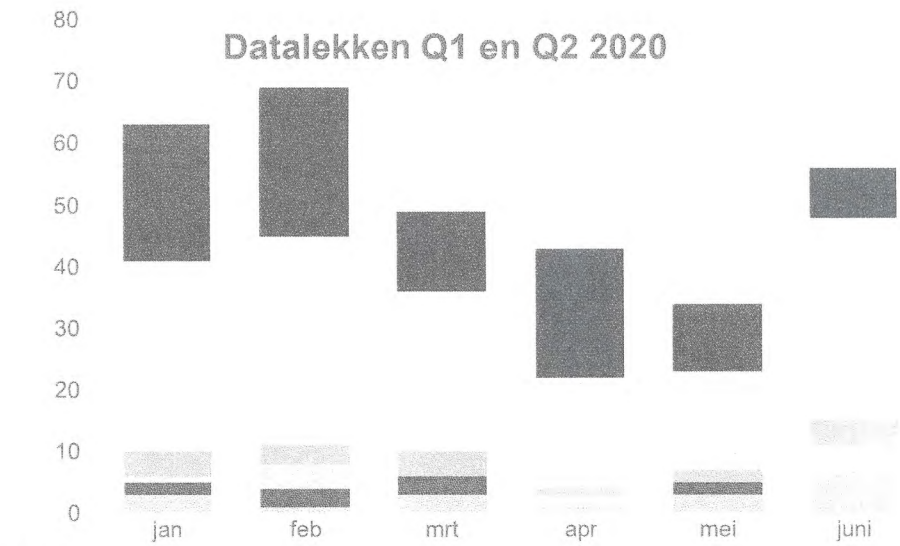
Overzicht datalekmeldingen januari tot en met juni 2020
Het CAK verstuurt per jaar meer dan miljoenen uitingen aan haar klanten. Dit betekent dat er potentieel op jaarbasis veel datalekken kunnen ontstaan. Afgezet tegen dit aantal is het aantal gemelde datalekken relatief laag. In heel 2019 zijn er landelijk ruim 27.000 datalekken bij de Autoriteit Persoonsgegevens (AP) gemeld. Het gaat om ongeveer 2.200 meldingen per maand. Bovenstaande geeft een goed beeld van de hoeveelheid gemelde datalekken van het CAK in verhouding tot het totaal aantal bij de AP gemelde datalekken.

Onderstaand overzicht (zie grafiek) geeft een beeld van alle datalekmeldingen van het afgelopen halfjaar.

https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/acties-bij-datalekken

https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019



	jan	feb	mrt	apr	mei	juni
Wmo	22	24	13	21	11	8
Wlz	31	34	26	18	16	33
Zvw	4	3	4	1	2	4
Btl	1	4	0	2	0	5
Intern	2	3	3	0	2	0
Overig	3	1	3	1	3	6

Reactie rapportage datalekken en voorstellen procesverbeteringen

RvB

[redacted]

[redacted]
Directeur KC ai

Reactie rapportage datalekken en voorstellen procesverbeteringen

Rapportage datalekken Q3 en Q4
Procesprofiel afhandelen datalekken

26-03-2020

1.0

Definitief

De RvB wordt verzocht akkoord te gaan met voorgestelde acties:

- Benoem EB contactpersonen voor het analyseren en afhandelen van datalekken.
- Analyseer de mogelijkheden vanuit Topdesk voor rapportages.
- Maak een volledige procesbeschrijving.

Op 4 februari 2020 heeft de RvB de rapportage van de FG over datalekken van juli t/m december 2019 besproken. De RvB geeft aan blij te zijn met de daling van het aantal meldingen, maar herkent zich niet in de bevinding dat het aantal datalekken relatief laag is en blijft hoge prioriteit vragen ten aanzien van het verder terugbrengen van de datalekken. Aan de directeur Klantcontacten a.i. is gevraagd een reactie op het memo te geven. Daarbij is gevraagd een voorstel voor een meer structurele afhandeling van de datalekken te doen. Dit memo bevat de reactie en een aantal voorstellen. Hierbij houden we rekening met de gewijzigde organisatie per 1 juni 2020.

Het voorstel voor het proces afhandelen datalekken moet leiden tot een meer structurele aanpak van de afhandeling van datalekken, borging van het proces in de nieuwe organisatie en het verminderen van het aantal datalekken.

In het memo 'optimaliseren afhandeling en minimalisering datalekken', in reactie op de vorige halfjaarlijkse rapportage en verschillende vragen van de RvB, was een analyse van de datalekken t/m november 2019 opgenomen. In de halfjaarlijkse rapportage is de maand december daar aan toegevoegd. De conclusie uit de halfjaarlijkse rapportage sluit aan op de conclusie uit het eerdere memo: het aantal meldingen daalt niet sterk meer, maar lijkt zich te stabiliseren. In genoemd memo zijn een aantal reeds geïmplementeerde verbeteringen, aanbevelingen en uit te voeren acties genoemd om het proces te verbeteren en het aantal meldingen te verminderen. In dit memo kijken we terug op de voortgang van die punten en benoemen we de huidige knelpunten in het proces.

Status acties

In het genoemde memo zijn vier acties benoemd: uitkomst scan ongestructureerde data overdragen, IAM inregelen, onderzoek naar datalekken veroorzaakt door menselijk handelen, procesborging in de nieuwe organisatie. De uitkomsten van de datascan worden begin april besproken met het Tijdelijk Samenwerkingsverband Privacy (TSP). Analyse en overdracht kunnen daarna plaatsgevonden. Het TSP heeft inmiddels een backlog opgesteld en houdt de voortgang daarop in ADO bij,

zodat deze en andere punten uit het project kunnen worden overgedragen op het moment dat de organisatie hier klaar voor is. IAM heeft een eigen backlog die wordt gevolgd. Deze voldoet aan de wensen vanuit privacy en security. Om meer aandacht te vragen voor de afhandeling van incidenten, waaronder datalekken, schuiven de regelingsdirecteuren sinds een aantal weken aan bij het wekelijkse business incident overleg. Dat menselijke fouten een belangrijke oorzaak van datalekken zijn, wordt op deze manier regelmatig onder de aandacht gebracht. De vierde actie wordt hieronder verder besproken en uitgewerkt in het procesvoorstel.

Status aanbevelingen Richtlijn voorkomen datalekken

Naast bovenstaande acties zijn de volgende aanbevelingen vanuit de Richtlijn voorkomen datalekken benoemd: Aanstellen privacy experts, structurele bewustwording, volledige implementatie van het proces afhandelen datalekken zoals vastgesteld in het procesprofiel en het borgen van de benodigde resources voor de uitvoering van dit proces.

Volledige implementatie proces afhandelen datalekken

In de nieuwe organisatie zijn de operationele en adviserende werkzaamheden voor informatiebeveiliging en privacy belegd. In de huidige situatie bestaat een dergelijke rol niet. In het procesprofiel staat beschreven dat de medewerker die de datalekmelding registreert, de melding doorzet naar een afdelingsmanager. Die is verantwoordelijk voor de analyse en afhandeling van het datalek. In de nieuwe organisatie zijn de regelingdirecteuren en overige N-1 verantwoordelijk en is het eenvoudiger een verantwoordelijke aan te wijzen. In de huidige praktijk zijn deze lijnen voor de Burgerregelingen, Buitenlandregeling en ICT-services vastgesteld en geïmplementeerd. Voor de EB-regelingen is dit niet geregeld. In veel gevallen wordt een melding niet doorgezet en is er geen sprake van afhandeling waardoor de melding open blijft staan en soortgelijke datalekken kunnen blijven voorkomen. De rapportage laat zien dat juist de EB-regelingen het grootste aandeel in het aantal datalekmeldingen hebben. Het gebrek aan aanspreekpunten, maar vooral ook het gebrek aan analyse kan een oorzaak zijn van de stabilisering van het aantal meldingen. Zonder analyse en afhandeling vindt er geen structurele oplossing plaats en is er geen lerend vermogen voor die datalekken. Dit geldt voor datalekken met zowel een technische, als een menselijke oorzaak.

Structurele bewustwording wordt gerealiseerd door de communicatiecampagne; in januari is bijvoorbeeld een prijsvraag uitgezet. Daarnaast wordt eind mei een nieuwe e-learning opgeleverd waarin opgedane kennis vanuit het datalek proces wordt verwerkt.

Registratie, monitoring en rapportages

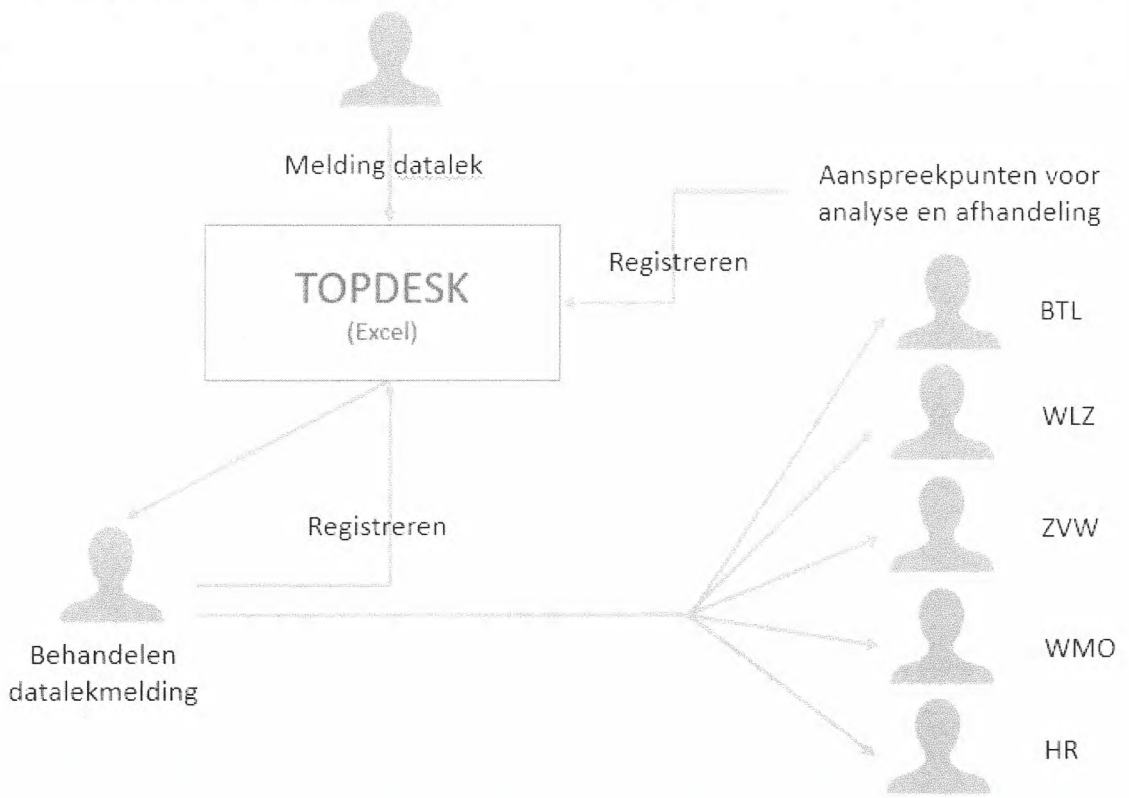
Het Procesprofiel afhandelen datalekken (zie bijlage) beschrijft vastlegging van zowel de melding als de voortgang. Beide vinden plaats, maar niet conform het profiel. Meldingen komen via het SelfServicePortal terecht in Topdesk. Deze applicatie leent zich goed voor het registreren en monitoren van en rapporteren over de voortgang van de afhandeling. ICT incident management en het BRIC-proces maken hier elk op eigen wijze gebruik van. Voor een deel van de meldingen wordt de voortgang in Topdesk geregistreerd. Dit geldt met name voor de meldingen die zijn uitgezet voor analyse en afhandeling. Met de overige meldingen gebeurt na registratie niets. Voor de meldingen die wel zijn uitgezet, volgt niet altijd een terugkoppeling over de afhandeling. Omdat Topdesk niet helemaal aansluit op de wensen vanuit de toezichthouden (AP), worden de datalekken eveneens geregistreerd in Excel. Ook in deze registratie wordt de voortgang niet volledig bijgehouden. Rapportages zijn gelet op bovenstaande slechts beperkt tot

een weergave van de cijfers en een korte analyse van de inhoud van de datalekken zoals getoond in de halfjaarlijkse rapportage van de FG.

Voorstel proces

Het Procesprofiel datalekken beschrijft een duidelijk en compleet proces. Het proces is echter niet volledig geïmplementeerd en de registratie en afhandeling van datalekken is op dit moment niet geborgd. De nieuwe organisatie inrichting vraagt om herijking van het huidige proces en het beleggen van verantwoordelijkheden in de nieuwe structuur. Waar de eindverantwoordelijkheid voorheen binnen de divisie KC is geplaatst, mede vanwege de nadruk op het beschermen van klantgegevens, moet die eigenlijk worden neergelegd op een plaats die regeling- en stafoverstijgend is. De toezichthouder heeft herhaaldelijk aandacht gevraagd voor datalekken van medewerkergegevens en het CAK is hierover eerder al benaderd. Voor de uitvoering verdient het aanbeveling aan te sluiten bij bestaande incidentprocessen. Denk hierbij aan het BRIC-proces of het ICT-incidentmanagementproces. Beide zijn uitgebreid beschreven. De registratie kan in de regelingen worden belegd, maar daarmee is niet duidelijk waar HR-datalekken terecht moeten komen. Daarnaast is regelmatig contact met de AP nodig en verdient het aanbeveling hier een beperkt aantal contactpersonen voor aan te wijzen. Registratie dient daarom plaats te vinden op een centrale plek, maar i.v.m. continuïteit bij verlof en verzuim is de huidige bezetting (1 FTE) onvoldoende. Alle directeuren dienen medewerkers (functies) te benoemen die aanspreekpunt kunnen zijn voor de collega die de datalekken registreert. Die aanspreekpunten nemen de analyse, afhandeling en registratie van de voortgang voor hun rekening. Tussen al deze medewerkers vindt periodiek overleg plaats zodat we een organisatiebreed lerend vermogen hebben.

In grote lijnen ziet het proces er als volgt uit:



C/ K

Acties

Bovenstaande leidt tot de volgende acties:

- Benoem contactpersonen voor het analyseren en afhandelen van datalekken in de EB-regelingen.
- Analyseer de mogelijkheden vanuit Topdesk voor rapportages over de afhandeling van datalekmeldingen, inventariseer de behoefte bij de RvB, N-1, directeur KC a.i. (tot 1 juni) en doe een voorstel voor een rapportage.
- Maak een volledige procesbeschrijving gebaseerd op het huidige procesprofiel, waarbij wordt aangesloten bij soortgelijke processen (BRIC/ICT-incidentmanagement) en voer het proces overeenkomstig uit.

De directeur KC a.i. vraagt de RvB akkoord te gaan met voorgestelde acties ter verbetering en borging van het proces afhandelen datalekken.

Rapportage datalekken Q3 en Q4

Memo datalekken
2019 juli tm december

Procesprofiel afhandelen datalekken

Procesprofiel
Afhandelen Datalekkei

Rapportage status AVG november 2020

Raad van Bestuur

[redacted]

[redacted]
Privacy officer
CIO-office

Status AVG CAK

Stavaza_imp_AVG_okt_2020.xlsx
Taken_IBP_adviseur (003).doc
Memo Datalekken 20200326

10-11-2020

8.0

Vanaf april 2018 is CAK bezig met implementatie van de AVG. Deze rapportage schetst de stand van zaken van de implementatie vanuit perspectief van CIO-office op 2 momenten:

1) Tot 1 juni jl. onder de oude organisatie inrichting
2) Na 1 juni jl. onder de nieuwe, regelingsgerichte, organisatievorm.

De keuze hiervoor is ingegeven omdat de stand van zaken onder de nieuwe organisatievorm een negatiever beeld schetst. Alles wat bereikt is met het implementeren van de AVG op 1juni jl. is nog steeds bruikbaar en waardevol. Alleen de vertaalslag van een generiek ingerichte organisatie naar een regelingsgerichte organisatie vereist deels nog aanpassingen in het tot 1 juni jl. gerealiseerde. Al met al is nog een flinke inspanning van de regeling clusters nodig.

In opdracht van de RvB is medio augustus jl. een set met normen en KPI's opgesteld welke in overleg met de afdeling Control in de cluster rapportages zijn verwerkt. Voor de KPI's in de bijlage (Stavaza_imp_AVG_okt_2020.xlsx) is gebruik gemaakt van de KPI's waarop de clusters zelf voor het eerst over de periode september 2020 hebben gerapporteerd. De normen zijn beschreven in het tabblad "KPI's en normen".

Algemeen

Door de draaiing en de bijbehorende herverdeling van verwerkings-activiteiten over het CAK is er een aanzienlijke inspanning van de regeling clusters nodig om de AVG-componenten (verwerkingenregister, PIA-register, risicoregister) weer in lijn te brengen met de nieuwe organisatie. De RD's is medio augustus jl. verzocht hiervoor met een PvA te komen met een bijbehorende reële planning op basis van een door CIO-office ter beschikking gestelde GAP-analyse. In de week van 10 november is bij de RD's een uitvraag gedaan naar de status van het PvA.

Bemensing

Op 4 september jl. heeft CIO-office het Privacy en Security Gilde opgericht. Deelnemers zijn de security- en privacy specialisten welke door de RD's zijn aangewezen. T.b.v. de werving van geschikte kandidaten is door CIO-office een taakprofiel op gesteld voor een IBP-adviseur (zie bijlage taken IBP_adviseur(003)). Momenteel voldoen slechts 6 van de 16 specialisten volledig aan het profiel. Vanuit het Privacy- en Security gilde wordt het komende halfjaar het kennisniveau van alle specialisten naar het gewenste niveau gebracht. Hiervoor zullen leden van het gilde verplicht trainingen volgen.

Risicomanagement tooling

CAK-breed is risico management nog in ontwikkeling. De organisatie is nog niet gewend consequent risico's te vertalen naar mitigerende maatregelen en deze toe te passen in processen/systemen/keten/PI-planningen. Met de introductie van het GRC moet het beheersen van risico's makkelijker worden. Gepland was het GRC-tool op Q3 2020 operationeel te hebben, maar vanwege prioriteit bij Risk en Compliance is dat nog niet gerealiseerd. De tool is nu gepland medio 2021 operationeel te zijn. Tot die tijd wordt gewerkt met een Excel omgeving.

Datalekken

Procesinrichting

Medio april 2020 heeft de RvB ingestemd met het memo "Datalekken 20200326.DOCX" (zie bijlage datalekken 20200326.doc). De RvB heeft opdracht gegeven aan de toenmalig directeur a.i. KC, in nauwe samenwerking met de RD's, de acties uit de memo uit te voeren. De memo voorziet in een centrale registratie en beoordeling van de datalekken door een datalekkenmanager en decentrale afhandeling en oplossing binnen de regelingsclusters. Tot op heden zijn deze acties niet doorgevoerd. De uitgangspunten uit de memo worden opnieuw ter discussie gesteld v.w.b. de centrale registratie en beoordeling.

Advies: positioneer de huidige datalekmanager bij het cluster services , en maak de manager services verantwoordelijk voor het coördineren van de verdere inrichting. Het betreft hier immers een cluster overstijgend proces.

Gemelde datalekken

Het aantal gemelde datalekken is redelijk stabiel rond de 50-60 datalekken per maand. In de bijlage aan het eind van deze rapportage (Bijlage I) is een overzicht van de Top 5 opgenomen. Sterke reductie van het aantal datalekken is alleen mogelijk door minder handmatige acties binnen alle regelingen en digitalisering van de uitingenstroom van alle regelingen .

Advies: een snelle doorontwikkeling van het klantportaal en/of aansluiting bij "Mijn overheid.nl" zou een goede oplossingsrichting zijn om de digitalisering van de uitingenstroom te versnellen en daarmee het aantal fysiek uitingen van 3 miljoen stuks op jaarbasis terug te brengen.

Dit is besproken in het operationeel overleg in augustus jl. Wegens het niet beschikbaar zijn van uitvoerende medewerkers is met de uitvraag gewacht.

De RD,s hebben late besloten deze functie samen te voegen met de functie van Risk-officer).

Compliance, Risk en Governance.

De medewerker welke deze rol uitvoert doet dit erg goed, maar zonder mandaat en niet centraal gepositioneerd.

Evt. is positionering bij de proces regisseur klantprocessen onder de RD Wmo ook een mogelijk alternatief.

Zie bijlage I: *gemelde datalekken september 2020 per categorie*.

Privacy by design

Elke nieuwe aanbesteding en/of aanschaf wordt voorafgegaan door een Business Impact Analyse (BIA) en indien nodig een Privacy Impact Analyse. Dit is een grote stap vooruit. Het adresseren van privacy risico's en de bijbehorende maatregel in PI-planningen is nog een knelpunt.

Tooling Register van verwerkingen

Het huidige register van verwerkingen is opgenomen in een tool dat door het ministerie van BZK ter beschikking is gesteld. De huidige versie bevat meerder problemen. Aangezien een overeenkomst voor onderhoud en updates te elfder ure door het ministerie is afgeblazen, moest CAK op zoek naar een nieuwe oplossing. Er wordt momenteel hard gewerkt aan de integratie van een registertool in het in 2019 aangeschafte GRC. Na oplevering van het registertool medio december 2020 kunnen de clusters starten met het overzetten van de verwerkingen uit het oude register. Aan het register kunnen per verwerking dan ook de bijbehorende PIA's en verwerkingsovereenkomsten worden gekoppeld. Daarmee volgt CAK de inrichting van het Rijksregister.

Stand van zaken tot 1 juni jl.

Medio april 2020 is decharge verleend op het project AVG. Voor het nawerk van het project is een Tijdelijk Samenwerkingsverband Privacy (TSP) in het leven geroepen, onder voorzitterschap van de directeur ZVW. Het TSP is per 1 juni jl. begonnen met overdracht aan de lijnorganisatie.

Stand van zaken na 1 juni jl.

Het uitgangspunt is dat de clusters per 31 december 2020 inzicht moeten hebben of zij in control zijn m.b.t. de AVG.In control zijn betekent voor 2020:

- Alle KPI's uit de bijlage staan op groen.
- Voor alle KPI's welke op oranje of rood staan is een PVA met een realistische planning beschikbaar om de KPI op groen te krijgen.
- Voor alle KPI's is een norm gedefinieerd. Deze normen worden nog verder verfijnd in afstemming met de leden van het Privacy- en Security Gilde.

Het overzicht met KPI's

Na 1 juni jl. ontstaat een minder rooskleurig beeld door de draaiing van de organisatie en de erbij horende herverdeling van verwerkingsactiviteiten. Hierdoor moeten o.a. het verwerkingenregister en het PIA-register drastisch worden aangepast. De overall status op 1 november jl. is 'rood'. Dit blijkt uit de kolommen per regeling cluster in de bijlage Stavaza_imp_AVG_okt_2020.xlsx. Hier is een analyse opgenomen van de stand van zaken per regeling cluster.
Het cluster buitenland steekt relatief gunstig af. Hier werd al regelingsgericht gewerkt en de benodigde aanpassingen zijn eerder ingezet.

Voor 2020 tot heden ca. 6 aanbestedingen.

Een voorbeeld: voor i juni was er 1 afdeling in- en excasso waarvoor de verwerkingen waren geregistreerd. Dit moet nu specifiek voor elke cluster gebeuren.

Bijlage I: *gemelde datalekken september 2020 per categorie*.

Verkeerd bezorgd door PostnI	5
Verkeerde invoer / selectie adres bij het CAK	19
Systeemfout (synchronisatie systemen)	5
Fouten in BRP adressen	20
Verkeerd verpakt (meerder berichten in 1 enveloppe)	5
Intern delen van informatie	2
Gemeld als datalek maar na analyse geen datalek	3
Totaal gemeld	59 datalekken.

Opvallend: in september 2020 gingen 57 meldingen van de 59 datalekmeldingen over verkeerd bezorgde uitingen door diverse oorzaken. Het CAK verzendt jaarlijks ca. 3 miljoen uitingen. Het verzenden van fysieke uitingen is een belangrijke oorzaak van het totaal aantal datalekken.

Voorlegger raad van bestuur

De indiener van het voorstel moet alle velden invullen. Dit pdf bestand graag dezelfde naam geven als het onderwerp hieronder genoemd. Vergaderstukken inclusief voorlegger indienen op donderdag vóór 12:00 uur voorafgaand aan de vergadering bij: [redacted] en [redacted]

Van (direct reports)	[redacted]
Onderwerp	Decharge project AVG
Datum	0 8 0 4 2 0 2 0 *DD / MM / JJJJ*
Samenvatting voorstel *Formuleer duidelijk en bondig de aanleiding en samenvatting van het voorstel.*	Het lopende project AVG te dechargeren.
Gevraagd besluit *Welk besluit verwacht je van de raad van bestuur?*	Akkoord te gaan met het beëindigen van het project AVG. Het projectresultaat vloeit terug naar de organisatie.
Vervolgproces *Welke vervolgstappen worden genomen na afloop van het besluit van raad van bestuur*	Voortgang AVG borgen in de regelingen / lijn organisatie. CIO begeleidt transitie naar lijn.

Aandachtspunten en risico's

Welke aandachtspunten en risico's voorzie je met het voorstel. Houd met ieder aandachtsgebied rekening.

Algemeen	nvt
Financieel	Er is een positief projectresultaat.
ICT / Informatie	nvt
Juridisch	nvt
HR	nvt
Medezeggenschap	nvt
Rechtmatigheid (budget/inhuur/inkoop)	nvt
Politiek- bestuurlijk	nvt

Voorlegger raad van bestuur

De indiener van het voorstel moet alle velden invullen. Dit pdf bestand graag dezelfde naam geven als het onderwerp hieronder genoemd. Vergaderstukken inclusief voorlegger indienen op donderdag vóór 12:00 uur voorafgaand aan de vergadering bij: [redacted]

Van (direct reports)	[redacted]
Onderwerp	Exceptie AVG
Datum	0 8 0 4 2 0 2 0 *DD / MM / JJJJ*
Samenvatting voorstel *Formuleer duidelijk en bondig de aanleiding en samenvatting van het voorstel.*	Gaandeweg het project AVG is het nodig gebleken de scope van het project aan te passen. Deze aanpassing is op dat moment niet bekrachtigd in een Raad van Bestuur besluit. Dat willen we nu alsnog realiseren.
Gevraagd besluit *Welk besluit verwacht je van de raad van bestuur?*	Wij vragen de Raad van Bestuur akkoord te gaan met de scope aanpassing zoals die in het verleden is doorgevoerd.
Vervolgproces *Welke vervolgstappen worden genomen na afloop van het besluit van raad van bestuur*	Project AVG zal worden gedechargeerd tegen de aangepaste scope.

Aandachtspunten en risico's

Welke aandachtspunten en risico's voorzie je met het voorstel. Houd met ieder aandachtsgebied rekening.

Algemeen	Voortgang AVG geborgd. CIO begeleidt transitie naar lijn.
Financieel	
ICT / Informatie	
Juridisch	
HR	
Medezeggenschap	
Rechtmatigheid (budget/inhuur/inkoop)	
Politiek- bestuurlijk	

Voorlegger raad van bestuur

De indiener van het voorstel moet alle velden invullen. Dit pdf bestand graag dezelfde naam geven als het onderwerp hieronder genoemd. Vergaderstukken inclusief voorlegger indienen op donderdag vóór 12:00 uur voorafgaand aan de vergadering bij: [redacted]

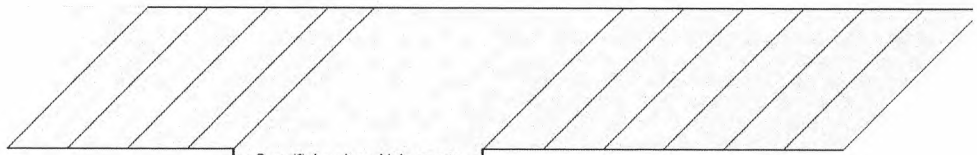
Van (direct reports)	[redacted]
Onderwerp	Reactie rapportage datalekken en voorstellen procesverbeteringen
Datum	2 6 0 3 2 0 2 0 *DD / MM / JJJJ*
Samenvatting voorstel *Formuleer duidelijk en bondig de aanleiding en samenvatting van het voorstel.*	De RvB heeft de directeur KC a.i. gevraagd een reactie te geven op de rapportage datalekken over de tweede helft van 2019. Daarnaast heeft de RvB verzocht een voorstel te doen voor de structurele afhandeling van datalekken, mede gelet op de reorganisatie per 1 juni. Om het gestabiliseerde aantal datalekken af te handelen is concrete invulling van het bestaande proces nodig, waarbij werkzaamheden worden belegd conform de nieuwe structuur van het CAK.
Gevraagd besluit *Welk besluit verwacht je van de raad van bestuur?*	Akkoord op de conclusies in het memo en de daarop gebaseerde voorgestelde acties.
Vervolgproces *Welke vervolgstappen worden genomen na afloop van het besluit van raad van bestuur*	De volgende acties worden uitgevoerd: • Benoem EB contactpersonen voor het analyseren en afhandelen van datalekken. • Analyseer de mogelijkheden vanuit Topdesk voor rapportages. • Maak een volledige procesbeschrijving. Implementatie van de rapportage en het beschreven proces.

Aandachtspunten en risico's

Welke aandachtspunten en risico's voorzie je met het voorstel. Houd met ieder aandachtsgebied rekening.

Algemeen	Verminderde bewustwording datalekken & Focus op RD's ipv alle n-1
Financieel	Zijn er voldoende resources beschikbaar voor structurele inrichting?
ICT / Informatie	IT onvoldoende in staat het proces volledig te ondersteunen
Juridisch	Oorzaken datalekken worden onvoldoende geanalyseerd en opgelost
HR	De functies/rollen in dit proces zijn niet geformaliseerd: geen mandaat
Medezeggenschap	nvt
Rechtmatigheid (budget/inhuur/inkoop)	Bij niet structureel oplossen datalek mogelijk onrechtmatigheid
Politiek- bestuurlijk	Toezichthouder privacy (AP) wordt steeds zichtbaarder

RASCI matrix CAK AVG Versie 3.0 2020



Algemeen					Specifieke eisen N-1 reports							
CAK is AVG compliant.	AI	I	R	C			C	SC				
Een privacybeleid is opgesteld en wordt onderhouden en gecommuniceerd .	A			RS				I				
Het privacy beleid is vastgesteld.	AS	C	I	I			I	I	I	I		I
Er worden voldoende mensen en middelen ter beschikking gesteld.	AS	A						I				
De ter beschikking gestelde middelen en resources worden toegewezen.	I	I	RSA	I			I	C				
Privacy kaders worden gesteld en bewaakt (o.a. privacy by design)			I	RSA			C	C	RI	I		I
Het privacy jaarplan is opgesteld	I	I	RA	C			I	SC	I			
Verwerkingen												
De 10 AVG principes worden toegepast (zie tabblad "de 10 AVG principes").			A	I			C	SC	R			
Alle verwerkingen zijn opgenomen in het verwerkingenregister.			A	I			I	SC	RC			I
Het verwerkingenregister is actueel.			A	I			I	SC	RC			I
PIA												
Per (voorgenomen) regeling / verwerking is vastgesteld of een PIA noodzakelijk is.			A				C	C	RSC			
Pia's zijn uitgevoerd.			A	C			C	SC	RS			
Alle PIA´s zijn opgenomen in een centraal register.			A	I			I	SC	RS			
Alle in het register opgenomen PIA´s zijn actueel.			A	I				SC	RS			
Privacy risico's												
Privacy risico's worden gedidentificeerd d.m.v. PIA's.			A					C	RS			
Voor verwerkingen waar geen PIA voor nodig is worden de Privacy risico's vanuit de verwerking geidentificeerd.			A					C	RS			
Geidentificeerde privacy risico's worden gemitigeerd en bewaakt.			AI		RC			SC	R	R		
Privacy by design (and default)												
Privacy by design (and default) wordt toegepast in systeemontwikkeling.			A					RC	I	RS		
Privacy by design (and default) wordt toegepast in businessprocessen.			A					RC	SA			
Personeel												
Personeel is zich voldoende bewust van de privacy aspecten van de door hen uitgevoerde taken.			A		AC		I	SC	RI			C
Jaarlijks wordt er een awareness programma opgesteld			RC		AS		I	C				
Jaarlijks wordt de opleidingsbehoefte vastgesteld m.b.t. privacy.			R		A		I	C	C			
Externe partijen												
Onderhouden van de aan externe partijen te stellen vereisten.				C		C		SC	A			
Voor de van toepassing zijnde overeenkomsten is een verwerkersovereenkomst opgesteld.			A			R		SC				
De verwerkersovereenkomsten zijn actueel.			A			C		SC	SR			
Controle op naleving			A			I		SC	R			
Datalekken												

Er is een datalekken procedure in werking.			I	C			C	C	C	RA	I
Het datalekken regsiter voldoet aan de aanbevelingen van de AP				C				C		RA	I
Het register wordt maandelijks gepubliceerd op het intranet van het CAK.				C				C		RA	I
Verantwoording											
De RvB wordt periodiek geinformeerd over de werking van het privacy stelsel.				RA				C	I		
De RvB wordt periodiek geinformeerd over de status van de AVG compliance.	I	I	AS	I			I	C			
Toezicht											
Er wordt toezicht gehouden.	I			C			RSA	C			
Er is een contactpersoon voor de AP.	I						RSA				
Informatiebeveiliging											
Faciliteert de samenstellling op basis van de BIA/PIA per proces de beheersmaatregelen op het gebied van Informatiebeveiliging en Privacy maatregelen binnen het kader van het beheersraamwerk.			A				A	SC			
Opstellen en onderhoud privacy statement											
Opstellen en onderhoud van het algemene privacystatement op de CAK website.				I				C			
Opstellen en onderhoud van het regeling specifieke deel van het statement op de website.			AI	CS				R			

Hieronder zijn (beperkt) de 10 AVG principes uit het CAK privacy beleid beschreven.
Een uitgebreide beschrijving is opgenomen in het CAK privacy beleid.

1. Doelbinding

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

2. Rechtmatigheid

Om te kunnen spreken van een rechtmatige gegevensverwerking is ten minste vereist dat dit gebeurt op basis van één van de AVG-grondslagen.

3. Minimale verwerking

Enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld. Uitsluitend die persoonsgegevens mogen verwerkt worden die voldoende zijn om het beoogde doel te bereiken.

4. Behoorlijkheid

Als het CAK voldoet aan de eisen van rechtmatigheid en doelmatigheid dan moet het CAK daarnaast ook
zorgen dat de gegevensverwerking ten aanzien van de betrokkene behoorlijk is. Een beginsel is zorgvuldigheid.

5. Transparantie

Het CAK moet over de verwerking van de persoonsgegevens transparant zijn richting de betrokkenen. Dit transparantiebeginsel ziet op het verstrekken van informatie over de persoonsgegevens (verwerking van) die beknopt, transparant, begrijpelijk, in een gemakkelijk toegankelijke vorm in een duidelijke en eenvoudige taal.

6. Integriteit en 7. vertrouwelijkheid

Bij de verwerking van persoonsgegevens wordt zorggedragen voor passende technische (encryptie en anonimiseren)18 of organisatorische maatregelen die de beveiliging ervan garandeert.19 Met andere woorden: de beveiliging van persoonsgegevens moet op orde zijn. De burger moet erop kunnen vertrouwen dat zijn gegevens beschermd zijn tegen:
-ongeoorloofde/onrechtmatige verwerking;
-verlies;
-vernietiging;
-beschadiging.

8. Juistheid

De persoonsgegevens die het CAK verwerkt, dienen juist te zijn en het CAK moet zich ook inspannen om de persoonsgegevens te actualiseren.

9. Opslagbeperking

De wijze waarop het CAK de persoonsgegevens bewaard, moet zodanig zijn dat zodra de noodzaak vervalt de persoonsgegevens niet meer herleidbaar opgeslagen worden (denk aan anonimiseren of encryptie).

10. Verantwoordingsplicht

Duidelijk is dat voor de naleving van de beginselen het CAK verantwoordelijk is en dat het CAK de nodige inspanningen hiervoor moet verrichten. Dit gaat zover dat het CAK de naleving moet kunnen aantonen.

Degenen van wie persoonsgegevens worden verwerkt (betrokkenen) hebben de volgende rechten:

1. **het recht op informatie**
2. **het recht op inzage**
3. **het recht op rectificatie**
4. **het recht op gegevenswissing (vergetelheid)**
5. **het recht op beperking van de verwerking**
6. **het recht op overdraagbaarheid (dataportabiliteit)**
7. **het recht van bezwaar**
8. **het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profilering**

RASCI uitleg

Dit zijn de rollen binnen de RASCI-matrix:

Responsible: verantwoordelijk voor de uitvoering van een proces of activiteit. Deze persoon legt verantwoording af aan de persoon die accountable is.

Accountable: de eindverantwoordelijke die ook goedkeuring moet geven aan het resultaat.

Support: de persoon die ondersteuning verleent aan het proces of project en de werkzaamheden uitvoert.

Consulted: de persoon die moet worden geraadpleegd, goedkeuring verleent of input levert aan de 'responsible' persoon, voorafgaand aan een stap in het proces.

Informed: degene die geïnformeerd wordt over de beslissingen, de voortgang en de bereikte resultaten, zodat er een volgende stap kan worden gezet.

NB:

In de kolom "N-1" zijn alle eisen opgenomen met betrekking tot de N-1 reports.

Waar voor N-1 functies nog aanvullende eisen zijn geidentificeerd zijn deze opgenomen in de kolom onder de betreffende functie onder de noemer "specifieke eisen N-1 reports".

Uitstel AVG audit

Het CAK heeft het streven om aantoonbaar AVG compliant te zijn conform de NOREA Handreiking Privacy Control Framework (hierna: normenkader). Het CAK is momenteel bezig de nodige stappen te zetten om dit te realiseren.
De afdeling Internal Audit (IA) heeft in 2019 een nulmeting uitgevoerd op de implementatie van het CIP privacy normenkader (het NOREA normenkader was toen nog niet beschikbaar). De afdeling IA is destijds tot de conclusie gekomen dat de organisatie in opzet grote stappen heeft gezet. Implementatie was destijds geen onderdeel van het onderzoek.

Vanaf juni 2020 is de organisatie gekanteld en de AVG dient in deze nieuwe organisatie te worden geïmplementeerd. In het auditplan Q3 Q4 staat een audit gepland op de implementatie. De afdeling IA heeft in samenspraak met de privacy officer besloten in Q4 2020 eerst een vooronderzoek uit te voeren op de actuele status omtrent de AVG compliancy om vast te stellen of de implementatie voldoende gereed is voor een reguliere audit.

De doelstelling van dit onderzoek is inzicht te krijgen in de actuele status van de AVG compliancy. Op basis van de uitkomsten kan de RvB worden geadviseerd over in hoeverre en wanneer een uitgebreide AVG audit effectief is. Hiermee wordt geborgd dat er pas tijd en capaciteit wordt geïnvesteerd (bij zowel de auditee als de auditor) in een uitgebreide audit op het moment dat het object van onderzoek voldoende gereed is.

Het NOREA Privacy Control Framework bestaat uit meerdere onderwerpen. Ieder onderwerp gaat in op specifieke onderdelen van privacy. Voor dit onderzoek is een beperkte scope gehanteerd voor wat betreft deze onderwerpen, namelijk de onderwerpen 'Verwerkingsregister' en 'Rechten van betrokkenen'.

RvB

[redacted] (CIO), [redacted] (Privacy officer), [redacted] (regeling adviseur)

Internal Audit ([redacted], manager Internal Audit, [redacted] en [redacted], Sr. IT Auditor)

Uitstel AVG audit

I – Oordeel per norm

9-12-2020

1.0

Bij het uitvoeren van het onderzoek zijn de onderwerpen 'Verwerkingsregister' en 'Rechten van betrokkenen' getoetst op volledigheid en juistheid van de evaluatie van de NOREA privacy normen door de auditee.

Volledigheid

Er is een vergelijking gemaakt tussen de normen die de auditee heeft voorzien van een evaluatie en de normen die naar de inzichten van IA onderdeel uitmaken van de evaluatie. Er is vastgesteld dat conform de inzichten van IA 28 normen relevant zijn voor de gekozen onderwerpen. Daarentegen is vastgesteld dat de auditee 22 normen heeft meegenomen in de evaluatie . De 28 normen zijn getoetst op juist- en volledigheid van bewijslast. De uitkomsten zijn als volgt:

- ✗ voor zes van de 28 normen is geen evaluatie of bewijslast aangeleverd;
- ✓ voor 22 van de 28 normen is het bewijslast opgeleverd en voorzien van duidelijke begeleiding / omschrijving.

Juistheid

Naast de volledigheid van de evaluatie, is getoetst in hoeverre de aangeleverde bewijslast in voldoende mate de opzet van de beheersmaatregelen aantoont. In totaal is voor 22 normen bewijslast aangeleverd, derhalve zijn 22 normen getoetst op juistheid. De uitkomsten zijn als volgt:

- ✗ voor 11 van de 22 normen is het bewijslast ontoereikend om een voldoende effectieve beheersing in opzet aan te tonen;
- ✓ voor 10 van de 22 normen is het bewijslast toereikend en toont voldoende beheersing aan in opzet.
- ✓ voor 1 van de 22 normen geldt dat deze door NOREA als niet van toepassing is gekenmerkt.

De afdeling IA heeft vastgesteld dat de gehanteerde normen voor het onderwerp 'rechten van betrokkenen' niet volledig is en dat de opzet voor een groot aantal controls/normen nog niet toereikend is of niet aanwezig is. Daarnaast is een juiste en volledige evaluatie door de auditee een belangrijke voorwaarde voor volledige audit. Om een effectieve audit te borgen is het zaak dat het audit object 'audit gereed' is. Gezien de bovenstaande bevindingen adviseren we de RvB in de eerste helft van 2021 opdracht te geven voor wederom een beperkt onderzoek welke, bij positieve resultaten, kan worden omgezet naar een volledige audit.

We hebben van de auditee vernomen dat de werkzaamheden om de NOREA AVG normen in het Governance, Risk en Compliance (GRC) tool Key Control Dashboard (KCD) te vullen, in december 2020 gaan starten. De auditee heeft de verwachting uitgesproken de eerste AVG compliancy rapportage rond eind Q1 2021 te kunnen verkrijgen uit KCD. Het doel bij het vullen van de NOREA AVG normen in KCD is het juist beleggen van de verantwoordelijkheden en het tijdig verkrijgen van benodigd bewijslast. Dankzij de automatiseringsfuncties van KCD worden de verantwoordelijken periodiek geattendeerd op de door hen uit te voeren controles. Daarnaast fungeert KCD als centrale opslaglocatie voor alle bewijslast. IA zal de juiste- en volledige omschrijving van de bewijslast vereisten per norm binnen KCD meenemen in het vervolgonderzoek.

Zie de tabel in bijlage I voor een specificatie van deze normen en het oordeel van IA per norm.

Onderwerp: Rechten van betrokkenen

Selectie Control PCF	Oordeel
CFR01	Geen evaluatie ontvangen bij initiële audit uitvraag.
CFR02	Geen evaluatie ontvangen bij initiële audit uitvraag.
CFR03	Geen evaluatie ontvangen bij initiële audit uitvraag.
CFR04	Geen evaluatie ontvangen bij initiële audit uitvraag.
URE02	✓
PST01	Geen evaluatie ontvangen bij initiële audit uitvraag.
PST02	Geen evaluatie ontvangen bij initiële audit uitvraag.
DAR01	✗
DAR03	✓
DAR04	✓
DCR01	✗
DCR03	✓
DCR04	✗
DDR01	✗
DDR02	✗
DDR04	✓
DPR01	✗
DPR02	✗
DPR04	✗

Onderwerp: Verwerkingsregister

Selectie Control PCF	Oordeel
RRE01	✓
RRE02	N.v.t.
RRE03	✗
RRE04	✓
RRE05	✓
PDI01	✗
PDI02	✓
PDI03	✓
PDI04	✗