[redacted]

Van: [redacted]
Verzonden: maandag 20 april 2020 13:59
Aan: [redacted]
CC: [redacted]
Onderwerp: analyse AVG nav de heer [redacted]
Bijlagen: Analyse klantverzoek AVG-RvB_20200420 (009).DOCX

Hoi [redacted]

Hierbij stuur ik je de notitie concept 1, mbt de AVG vragen van de heer [redacted].
Dit is wat we er van hebben kunnen maken met input van een boel collega's die af en toe zelfs in het weekend hun bijdrage hebben geleverd. Het is een lijvig maar grondig document geworden.
Ik ben benieuwd of dit een goede eerste aanzet is en hoor graag wat jullie verder willen met de analyse.

[redacted]

Analyse afhandeling inzageverzoek AVG

Raad van Bestuur

[redacted]

Van [redacted]

Analyse afhandeling inzageverzoek AVG

Mail klant aan FG

20 april 2020

0.9

Concept

De directeur Klantcontacten a.i. en de regelingdirecteur Zvw verzoeken de RvB akkoord te gaan met de inhoud van dit memo en opdracht te geven om de acties genoemd in het plan van aanpak uit te voeren.

Op 29 maart 2020 ontving de FG een email van een klant waarin deze zijn feedback gaf op de afhandeling van zijn inzageverzoek van 3 januari 2020. De FG heeft de voorzitter van de RvB vervolgens geadviseerd de door de klant genoemde punten te laten analyseren en eventuele aanpassingen aan processen en systemen door te voeren. De voorzitter van de RvB heeft de directeur Klantcontacten a.i. en de voormalig voorzitter van de projectstuurgroep AVG daarop gevraagd om een inhoudelijke analyse van de situatie, de risico's en een plan van aanpak.

In dit memo beschrijven we het proces zoals dat door de AVG wordt voorgeschreven, gevolgd door de daadwerkelijke afhandeling van het verzoek inclusief tijdslijn. Vervolgens gaan we in op de feedback en vragen van de klant. Daarbij beschrijven we per aandachtspunt de uitkomst van de analyse en de vervolgstappen. We eindigen met een tabel waarin we dit overzichtelijk hebben samengevat.

Met dit voorstel beantwoorden we het verzoek van de voorzitter van de Raad van Bestuur. Het plan van aanpak, bestaand uit verschillende acties, is gebaseerd op de analyse van de situatie. Na uitvoering van het plan van aanpak zijn de aandachtspunten die de klant in zijn mail heeft benoemd opgelost.

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) hebben klanten verschillende rechten gekregen om grip te krijgen op de verwerking van hun persoonsgegevens. Het klantverzoek in dit memo betreft het recht van inzage zoals geregeld in artikel 15 van de AVG. Artikel 12 van de AVG stelt dat de verwerkingsverantwoordelijke, in dit geval het CAK, in ieder geval binnen een maand na ontvangst van het verzoek informatie verstrekt over het gevolg dat aan het verzoek is gegeven. De termijn kan indien nodig met twee maanden worden verlengd. Deze verlenging dient binnen een maand na ontvangst van het verzoek aan de klant te worden medegedeeld. De uitvoeringswet AVG stelt dat een schriftelijk beslissing van een bestuursorgaan op een verzoek tot de uitoefening van de in de AVG genoemde klantrechten geldt als een besluit in de

zin van de Algemene wet bestuursrecht (Awb). De klant kan daardoor gebruik maken van verschillende rechtsmiddelen.

Daarnaast stelt de AVG dat de verwerkingsverantwoordelijke met voldoende zekerheid vaststelt dat degene die het verzoek doet daadwerkelijk de betrokkene is. Wij vragen klanten daarom, na het indienen van een verzoek op grond van de AVG, een kopie van het ID-bewijs toe te sturen.

Daadwerkelijke afhandeling verzoek

Klant heeft via het contactformulier op de website een inzageverzoek ingediend. Het KCC ontvangt dit verzoek diezelfde dag, op 3 januari 2020. Op 15 januari ontvangt de klant een reactie met het verzoek meer gegevens aan te leveren omdat de CAK op basis van de gegevens op het formulier de klant niet kon terugvinden in de bronsystemen. Klant heeft hier dezelfde dag op gereageerd. KCC heeft het verzoek vervolgens op 20 februari doorgezet naar de tweede lijn. KCC heeft achterstanden in de verwerking van e-mail waardoor het verzoek ruim een maand is blijven liggen. Vervolgens is het verzoek niet als AVG-verzoek herkend en is niet direct bij het juiste team terecht gekomen. Binnen Klantadvies (KA) is het verzoek ook niet direct als inzageverzoek herkend. Op 28 februari heeft een medewerker van KA de klant een algemeen antwoord toegestuurd, zonder op specifieke gegevens van de klant in te gaan.

Op 6 maart heeft de klant in een reactie aangegeven dat hij de feitelijke informatie die het CAK van hem verwerkt zou willen inzien. Op 19 maart heeft KCC dit verzoek als inzageverzoek herkend en doorgezet naar het juiste team. Op 25 maart heeft een medewerker van KA de klant een beschikking toegestuurd met het antwoord op de vragen van de klant en verschillende schermprints vanuit de bronsystemen.

Feedback en vragen van de klant aan de FG

Op 29 maart 2020 ontvangt de Functionaris Gegevensbescherming (FG) een mail met daarin feedback van de klant op de afhandeling van zijn inzageverzoek. De klant noemt daarin vijf aandachts- en verbeterpunten en stelt twee gerichte vragen over de bewaartermijn en de toepassing daarvan. Op 9 april heeft de FG de twee vragen van de klant via de mail beantwoord.

Hieronder zijn de belangrijkste data van dit proces in een tijdslijn weergegeven

In het vervolg van dit memo beschrijven we per aandachtspunt van de klant de uitkomst van de analyse, inclusief eventuele risico's en de vervolgstappen. Elk punt bevat eerst een analyse en vervolgens de oplossing, uitgeschreven in vervolgstappen en verantwoordelijke. Vervolgens gaan we in op de vragen van de klant. Aan het eind van deze paragraaf hebben we alle informatie samengevat in een tabel.

1. **Geen inzicht in gegevens van 2014 in klantportaal**

De klant heeft het advies gekregen om in te loggen op het klantportaal en heeft dit gedaan. De factuur van 2014 is echter niet terug te vinden in het dossier. De klant adviseert om dit in het privacystatement af te vangen door te benoemen vanaf welk jaar inzage in facturen mogelijk is. In het klantportaal worden beschikkingen en facturen vanaf 1 januari 2016 getoond. De medewerker die het advies gaf, was hier blijkbaar niet van op de hoogte.

Conform suggestie van de klant verdient het aanbeveling om dit op te nemen in het privacy statement. Het TSP zet deze wijziging op haar backlog en stemt dit af met de afdeling Communicatie die verantwoordelijk is voor de inhoud van de website. Afhankelijk van de prioriteiten bij de afdeling, leert de ervaring dat dit een doorlooptijd heeft van gemiddeld twee weken. Daarnaast is het belangrijk dat medewerkers met klantcontact op de hoogte zijn van deze informatie. Dit moet worden toegevoegd aan de Kennisbank. Ook dit punt wordt opgenomen op de backlog van het TSP. Het TSP plant een overleg met redacteuren van de Kennisbank om dit toe te voegen.

2. **Er is geen manier om een aanvraag te doen voor inzage in alle verwerkte gegevens, bij alle formulieren dient een specifieke regeling te worden gekozen**

Klant heeft het advies gekregen een regeling te kiezen en een opmerking toe te voegen dat zijn verzoek betrekking heeft op alle mogelijke regelingen. Op dit moment voorziet de website niet in een webformulier voor inzage of andere AVG gerelateerde verzoeken. Het contactformulier dwingt klanten tot een keuze voor een regeling. Dit wordt ondervangen, zoals aan de klant meegedeeld, door een extra opmerking te plaatsen. Voor de klant is dit geen duidelijke een eenvoudige manier om een verzoek in te dienen.

Daarnaast kan het algemene karakter van het formulier er voor zorgen dat een verzoek niet als AVG-verzoek herkend wordt en niet bij de juiste behandelaar terecht komt. Daarmee lopen we het risico dat we ons niet aan de voorgeschreven reactietermijn (een maand) kunnen houden. De gevolgen daarvan zijn boze of teleurgestelde klanten en mogelijke ingebrekestellingen gevolgd door een dwangsom op grond van de Algemene wet bestuursrecht. Een ander risico is dat klanten gebruikmaken van hun recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Dit zou een onderzoek naar de gang van zaken teweeg kunnen brengen, met een mogelijke sanctie als gevolg.

Het CAK kiest voor regelinggericht werken. Aanpassingen aan het huidige formulier doen afbreuk aan die keuze. Daartegenover staat dat we geen afzonderlijk formulier voor de klantrechten vanuit de AVG hebben. Het CAK heeft in 2019 48 klantverzoeken op basis van de AVG en in 2020 (tot nu toe) 25. De meeste verzoeken worden ingediend via het contactformulier op de website, al dan niet na contact met een medewerker van KCC. Verzoeken komen ook via de post of via de mail bij de FG binnen. Gezien de aantallen en de risico's die het CAK loopt wanneer een verzoek niet direct wordt herkend, is het op zijn minst nuttig een kosten/baten analyse voor het ontwikkelen van een specifiek formulier uit te voeren. Voor het ontwikkelen van een dergelijk formulier zijn we afhankelijk van de prioriteit die het krijgt en wanneer het in de PI-planning wordt meegenomen. Dit zou daarom een langere termijn oplossing zijn.

Op korte termijn kunnen we klanten die eerst telefonisch contact zoeken, vragen een opmerking toe te voegen aan het formulier. Denk aan 'AVG' of 'Privacy' of 'inzageverzoek'. Dit moet worden afgestemd met de redactie van de Kennisbank en alle afdelingen die de contactformulieren indexeren, zodat het bij de juiste afdeling terecht komt. Dit punt is een item voor op de backlog van het TSP. Voor een succesvolle implementatie van dit voorstel is het noodzakelijk dat medewerkers de verzoeken van de klant herkennen als recht op grond van de AVG. Op dat laatste punt komen we verderop in dit memo terug.

3. **Onvoldoende gegevens in het formulier om het dossier van de klant te kunnen vinden**

Het formulier op de website kan gebruikt worden voor algemene vragen en daarom is het BSN geen verplicht veld. Dit was eerder wel het geval, maar het formulier is aangepast op grond van de AVG. Het grootste bezwaar tegen die aanpassing was dat de identificatie van de klant arbeidsintensiever zou kunnen worden en tot meer klantcontact kon leiden op basis van de summiere gegevens op het formulier. Dit is de reden dat de behandelaar de klant om een beschikkings- of factuurkenmerk heeft gevraagd, conform instructie op de kennisbank. Als alternatief is het BSN genoemd. Het CAK gebruikt het BSN als uniek klantnummer, de klant is op basis van het BSN eenvoudig te vinden in de systemen. Het is echter mogelijk om de klant te vinden op basis van andere gegevens of combinaties van gegevens. Als dit niet lukt, biedt het BSN uitkomst. Overigens is de vraag om het BSN conform vastgestelde privacymatrix.

Daarnaast moet het CAK vast kunnen stellen dat het verzoek wordt ingediend door betrokkene zelf, ter bescherming van de klant. Uiteindelijk heeft de klant een kopie van zijn ID-bewijs meegestuurd op aanraden van AP en heeft de behandelaar de klant alsnog gevonden in de systemen. Als het verzoek direct was herkend als AVG-verzoek had de behandelaar direct om een kopie ID-bewijs gevraagd. Herkenning van het verzoek speelt ook hier een grote rol. Bij punt vier gaan we in op de oplossingen voor dit punt.

4. **De reactie is buiten de voorgeschreven termijn verstuurd en het antwoord bestond uit algemene informatie**

Zoals eerder geschreven, noemt de AVG een termijn van een maand en schrijft de verordening voor welke informatie moet worden verstrekt. De termijn is in dit geval ruim overschreden. Zoals in de tijdslijn te zien is, is het verzoek van de klant na meer dan een maand naar de tweede lijn doorgezet. Het KCC kent achterstanden en de medewerkers van KCC en KA herkennen de verzoeken niet altijd als zodanig, waardoor een verzoek op een verkeerde afdeling terecht kan komen. In dit geval heeft de klant op 15 januari op het verzoek om meer gegevens gereageerd en is op 28 februari een reactie door KA verstuurd. Er is geen gebruik gemaakt van de mogelijkheid vanuit de AVG om de klant binnen een maand op de hoogte te stellen van verlenging van de beslistermijn.

Omdat het verzoek niet is herkend als inzageverzoek op grond van de AVG, zijn de eerste behandelaars zich niet bewust geweest van de termijn en van het feit dat de klant een persoonlijk en feitelijk antwoord op zijn verzoek zou moeten krijgen. Toen het verzoek uiteindelijk bij de juiste behandelaar was beland, is het verzoek conform de regels afgehandeld, maar dus ruim buiten de termijn.

De punten 2, 3 en 4 van de klant zijn allen mede veroorzaakt doordat het inzageverzoek niet direct als zodanig is herkend. Er is onvoldoende kennis bij de medewerkers aanwezig om een dergelijk verzoek te herkennen. Dit is door de senior van de afdeling KA als verzoek bij de Privacy Officers neergelegd. Het TSP is bezig met het actualiseren van de e-learning AVG en Datalekken en neemt dit punt mee. De e-

learining, die 25 mei wordt gepubliceerd, zal echter geen gedetailleerde werkinstructie bevatten omdat de e-learning voor het gehele CAK bedoeld is. Daarom moeten er in samenwerking met KA, de quality coaches (QC) van KCC en de afdeling Kwaliteit & Voorlichting aanpassingen worden gedaan aan werkinstructies, de Kennisbanken de coaching op de werkvloer. Wellicht dient dit opgenomen te worden in de training van medewerkers die klantcontact hebben. Dit kan in afstemming met het huidige HR developmentteam worden bepaald. Omdat het TSP de ontwikkeling van de afhandeling van deze klantverzoeken op de backlog heeft staan, kan het TSP hierbij coördineren en meedenken. Deze punten worden als acties toegevoegd aan de backlog.

5. **De gegevens van de klant zijn niet eenmalig gecontroleerd bij het BRP. In de gegevens van de klant staat dat er in 2019 een BRP-mutatie heeft plaatsgevonden** (de mutatie is per telefoon aan de klant meegedeeld en stond niet in de gegevens).
De klant voert aan dat hier niet transparant gehandeld is en dat eer dergelijke mutatie beter toegelicht kan worden. De klant heeft zorg genoten in 2014 en heeft in dat jaar zijn beschikking en factuur ontvangen en de factuur betaald. De gebruikelijke werkwijze is dat een dergelijke klant na twee jaar een einddatum meekrijgt. De klant is dan niet meer 'actief' en de klant dient te worden 'ontvlagd'. Het CAK zou dan geen spontane mutaties meer moeten ontvangen. In dit geval is de klant niet ontvlagd, wat heeft gezorgd voor een mutatie in zijn dossier op basis van een mutatie in de BRP. Het ontvlaggen is geen geautomatiseerde handeling. Het CAK had de mutatie niet mogen ontvangen en verwerkt daarmee persoonsgegevens van de klant zonder doelbinding. Dit is in strijd met de AVG. Dit kan leiden tot een klacht bij de AP en mogelijke sancties.

   Het niet ontvlaggen is het gevolg van een bekend incident. Bij het eenmalig overzetten van personen uit Thinsy naar het Centraal Persoonsregister (CPR) in 2017 zijn personen ontvlagd. De personen hebben echter nooit een einddatum meegekregen, waardoor het ontvlaggen niet gelukt is. Er is een melding ingediend om bij deze klanten alsnog een einddatum te plaatsen. Via een RFU hebben veel klanten alsnog een einddatum meegekregen, maar niet alle. Er is een tweede RFU nodig om alle inactieve klanten een einddatum mee te geven.

   Voor deze klant zal een individuele actie plaatsvinden. De Business Incidentmanager (BIM) heeft het verzoek bij KA uitgezet om deze klant alsnog een einddatum mee te geven en te ontvlaggen. Hiermee voorkomen we mutaties in de toekomst en verkleinen we het risico dat de klant bij een nieuwe verzoek wederom een onrechtmatige mutatie te zien krijgt.

Maak meer gebruik van het klantportaal dan nu het geval is
De klant eindigt zijn aandachtspunten met een algemene opmerking dat het CAK meer gebruik zou moeten maken van het klantportaal. Dit is een veilig middel om klanten inzage te gegeven in de persoonsgegevens die we verwerken en kan officiële klantverzoeken voorkomen.

Analyse en vervolgstappen vragen klant

Vervolgens noemt de klant nog twee 'losse eindjes', die hij formuleert als vragen. Deze vragen zijn op 9 april 2020 door de FG via mail beantwoord. Hieronder volgen de analyse en eventuele vervolgstappen van die vragen.

1. **De klant heeft geen betaalgegevens ontvangen en vraagt zich af of deze gegevens zijn verwijderd voordat de bewaartermijn verstreken is.**

De klant heeft zijn factuur via een acceptgiro betaald. Daarmee is de factuur voldaan en omdat er verder geen zorg meer is aangeleverd voor deze klant waren er verder geen handelingen meer nodig in het dossier. Het rekeningnummer wordt daarom niet vastgelegd in de bronsystemen, er is geen doelbinding voor verwerking van dat gegeven. Daarmee houden we ons aan de AVG. Als een klant via automatische incasso zou betalen, leggen we het rekeningnummer wel bewust vast in de bronsystemen. Alleen dan is het zichtbaar in het klantportaal. In het doorkijkscherm (IEF) naar het financiële systeem van het CAK (OF12) zijn de betaalgegevens echter wel te zien door medewerkers. Daar staat van welk rekeningnummer de betaling is ontvangen. De klant had deze gegevens moeten ontvangen. Het wel of niet hanteren van een bewaartermijn is bij deze vraag niet aan de orde.

De FG heeft bevestigd dat de gegevens van de klant zijn vastgelegd en toegezegd dat deze alsnog naar de klant worden toegestuurd. De BIM heeft KA verzocht de gegevens alsnog naar te klant toe te sturen.

2. **Klant heeft vernomen dat gegevens niet automatisch worden verwijderd na het verstrijken van de bewaartermijn. Slechts op verzoek worden gegevens geanonimiseerd. Is dit de procedure die het CAK hanteert?**
Het CAK is al een lange tijd op zoek naar de juiste bewaartermijnen en een manier om deze te hanteren. Vanuit het AVG-project, in samenwerking met de afdeling Bestuurszaken en de Privacy Officers, zijn verschillende producten opgeleverd om concrete invulling te geven aan de bewaartermijnen. Van automatische vernietiging is geen sprake. In 2019 heeft het project Gestructureerde en Ongestructureerde Persoonsgegevens (GOP) een begin gemaakt met het in bulk vernietigen van gegevens. Het onderwerp is actueel, maar staat in de kinderschoenen.

De Wmo kent een termijn van 15 jaar (artikel 5.3.4 lid 1 Wmo). Alle gegevens ouder dan 15 jaar zijn vernietigd. Deze werkzaamheden moeten periodiek plaatsvinden, zodat het CAK voor de Wmo geen gegevens verwerkt die ouder dan 15 jaar zijn. Automatisch vernietigen heeft de voorkeur. Het CAK heeft dit echter in haar bestaande applicatielandschap niet ingeregeld. Sterker nog, een deel van de applicaties kent niet de mogelijkheid om gegevens te vernietigen. In dat geval worden gegevens gepseudonimiseerd of geanonimiseerd. Pseudonimiseren voldoet echter niet, de gegevens kunnen via een vertaalsleutel nog worden herleid tot een persoon.

Met het uitvoeren van de veranderkalender dient rekening te worden gehouden met deze vereisten. Bij nieuwe applicaties wordt daarom altijd eerst een Privacy Impact Analyse/Assessment (PIA) uitgevoerd. Daarbij wordt standaard opgenomen dat een nieuwe applicatie in staat moet zijn gegevens op bulk en individueel niveau te vernietigen. Uiteraard moet de applicatie ook in staat zijn om aan de andere klantrechten te kunnen voldoen (zoals het inzagerecht). Bewaartermijnen worden ook behandeld tijdens de PIA en worden vastgelegd in het verwerkingenregister. Het is aan de eigenaar van de applicatie om te bepalen of vernietiging geautomatiseerd moet plaatsvinden of handmatig wordt gedaan.

Bij individuele verzoeken wordt per applicatie en per persoonsgegeven vastgesteld wat mogelijk is. Als een klant een gegrond vernietigingsverzoek indient en de gegevens kunnen niet worden vernietigd, dan worden de gegevens daar waar mogelijk geanonimiseerd. Dit wordt als zodanig opgenomen in de beslissing op het verzoek. Voor het anonimiseren is een script ontwikkeld dat zich op dit moment in de testfase bevindt. Het script regelt o.a. het plaatsen van de einddatum, ontvlaggen veranderen van naam en geboortedatum.

1.	Verwezen naar klantportaal, gegevens 2014 niet zichtbaar	Bepaalde gegevens pas zichtbaar vanaf 1-1-2016	Opnemen in privacystatement	TSP + Communicatie
		Onbekend bij medewerkers, onterechte verwijzing	Datum opnemen in Kennisbank	TSP + K&V (redactie Kennisbank)
2.	Contactformulier website voorziet niet in optie alle regelingen of algemeen verzoek	Keuze regelinggericht en gebruik algemeen formulier	Kosten/baten analyse specifiek formulier starten (langere termijn)	TSP + inhoudsdeskundigen
		Verzoek niet herkend als klantrecht AVG	Aanpassen Kennisbank, opmerking op formulier door klant (korte termijn)	TSP + K&V
3.	Identificeren klant niet mogelijk op basis van gegevens contactformulier	Verzoek niet herkend als klantrecht AVG. Verzoek om briefkenmerk of BSN is conform werkinstructie.	Aanpassen Kennisbank en WI, coaches inzetten	TSP + KA + K&V + QC's
4.	Reactie (beslissing) buiten termijn. Antwoord bestond uit algemene informatie.	Verzoek niet herkend als klantrecht AVG.	Aanpassen Kennisbank en WI, coaches inzetten. + Uitzoeken of dit in de training kan worden meegenomen.	TSP + KA + K&V + QC's TSP + HR-D
5.	Mutatie in BRP-gegevens in 2019, terwijl klant na 2014 niet meer actief is.	Geen einddatum waardoor dossier niet ontvlagd is.	Incident met ontvlaggen oplossen. Klant individueel ontvlaggen	IT heeft dit reeds opgepakt Verzoek reeds uitgezet bij KA (door BIM)

1.	Klant heeft geen betaalgegevens ontvangen,	Betaalgegevens zijn vastgelegd en hadden	FG heeft toesturen betaalgegevens toegezegd.	Toesturen betaalgegevens.	Verzoek reeds uitgezet bij KA (door BIM)

	relateert dit aan de bewaartermijn	toegestuurd moeten worden. Bewaartermijn is hier niet aan de orde.			
2.	Gegevens worden na het verstrijken van de bewaartermijn niet automatisch verwijderd, anonimiseren gebeurt alleen op verzoek.	Gegevens worden in huidige databases niet automatisch vernietigd, project GOP heeft eerste bulkvernietiging uitgevoerd.	De FG heeft de bewaartermijn voor de Wmo genoemd en aangegeven dat de gegevens na die termijn vernietigd worden. Indien de klant eerdere vernietiging zou willen, kan hij daartoe een verzoek indienen.	Uitvoeren PIA's bij wijzigingen/nieuwe verwerkingen persoonsgegevens. Klant eerlijk wijzen op onmogelijkheden vernietigen gegevens en alternatieven.	Het vernietigen van gegevens na afloop van de bewaartermijn valt per 1 juni onder de verantwoordelijkheid van de direct reports. KA (gebeurt nu al)

nvt

nvt

nvt

nvt

Dit memo is tot stand gekomen met behulp van input van collega's van de afdelingen KA, IT Frontoffice, Privacy Office, leden van het TSP, de Business Incident Manager (AVG) en de FG.

Mail klant aan FG (geanonimiseerd)

Van: x
Verzonden: zondag 29 maart 2020 11:59
Aan: FG <fg@hetcak.nl>
Onderwerp: feedback en aanvullende vragen AVG inzage

Geachte heer / mevrouw,

Naar aanleiding van informatie van de gemeente Rotterdam dat zij via de BRP informatie hadden gedeeld met het CAK heb ik een inzageverzoek gedaan bij het CAK conform de AVG. Die inzage is inmiddels gegeven (x), maar ik wil graag mijn feedback op het proces met u delen en er zijn nog wat losse eindjes met betrekking tot de informatie die ik heb gekregen.

1. Op https://www.hetcak.nl/uw-privacy staat:
"Ontvangt u Wlz-zorg of ondersteuning vanuit de Wmo? Dan kunt u inloggen op Mijn CAK. Als u bent ingelogd, dan kunt u de belangrijkste gegevens die we van u hebben zelf inzien."
Volgens mij zou het handig zijn om hier een termijn bij te noemen ".. of heeft u die in de afgelopen X jaar ontvangen". Ik werd namelijk door uw medewerkers hiernaar verwezen en heb een account aangemaakt en met DigiD ingelogd, om vervolgens niets te vinden omdat mijn gegevens betrekking hadden op kalenderjaar 2014.

2. Het CAK verwerkt gegevens voor verschillende regelingen en in alle contactkanalen van het CAK wordt hierop voorgesorteerd door gebruikers te dwingen een regeling te kiezen. Maar een inzageverzoek voor alle gegevens heeft betrekking op de *organisatie*, niet op een *regeling*.
Er is geen duidelijke manier om een dergelijke aanvraag in te dienen en uiteindelijk kreeg ik als advies een willekeurige regeling te kiezen en daar bij te zetten dat het om de hele organisatie ging.

3. Nadat ik een inzageverzoek had gedaan kreeg ik als reactie dat er te weinig gegevens bekend waren om mij te vinden en werd mij gevraagd om "het kenmerk van uw laatste beschikking of factuur en uw geboortedatum door te geven. Echter, een AVG inzageverzoek heeft expliciet ook als doel om uit te kunnen vinden *of* er gegevens verwerkt worden, in welk geval er natuurlijk geen beschikking of factuur bekend is.
Als alternatief werd gegevens het invullen van mijn BSN op de website.
Echter, de AP geeft duidelijk aan dat het niet de bedoeling is dat voor een inzageverzoek het BSN verstrekt moet worden. En uiteindelijk bleek dat ook helemaal niet nodig, want ik heb de informatie ook zonder dit te verstrekken gekregen.

4. Vervolgens kreeg ik 1 maand en 25 dagen na mijn verzoek een antwoord.
Dat antwoord was echter gewoon een kopie van de privacy verklaring. Mijn inzageverzoek was geen verzoek om mij de privacy verklaring op te sturen, maar om de feitelijke informatie die het CAK van mij had, waar die informatie vandaan was gekomen

en aan wie die verstrekt was.
Na hier nogmaals om gevraagd te hebben kreeg ik uiteindelijk op 26 maart, 2 maanden en 21 dagen na mijn inzageverzoek, daadwerkelijk inzage.

5. In de beantwoording staat vermeld waar het CAK de verschillende gegevens vandaan heeft: "vervolgens hebben wij uw gegevens gecontroleerd in de Basisregistratie Personen (BPR)".
Wat mij opviel, en bij navraag telefonisch bevestigd heb gekregen, was dat er in de gegevens die ik van jullie kreeg een BRP-mutatie uit 2019 vermeld was. Het CAK heeft dus niet eenmalig in 2014 de gegevens gecontroleerd, maar heeft die tot zeer recent nog geupdate. Dat is niet transparant vermeld in de beantwoording en kan zeker beter toegelicht worden.

Volgens mij had deze hele gang van zaken simpel voorkomen kunnen worden door dossiers *wel* beschikbaar te maken op het webportaal van het CAK.
Aangezien het CAK dat al doet kunnen moeilijk beveiligingsbezwaren tegen zijn. Het enige wat het CAK moet doen is stoppen met het verbergen van dossiers nadat ze gesloten zijn. Hoewel niet iedereen de juiste computervaardigheden en / of een DigiD zal hebben, lijkt mij dat het CAK hiermee het merendeel van de inzage verzoeken zou kunnen opvangen en automatiseren. En het sluit ook netjes aan bij het advies van de AP om waar bestaande authenticatie mogelijkheden zoals een website inlog zijn, deze te hergebruiken voor (authenticatie van) inzage verzoeken.

Tot zover mijn feedback op het inzage proces. Dan zijn er nog wat inhoudelijke losse eindjes.

1. Ik vind het opvallend dat er geen betaalgegevens in het overzicht dat ik heb gekregen staan. Dat zou betekenen dat het CAK bijvoorbeeld gegevens met betrekking tot betaalde acceptgiro's (waarin mijn rekeningnummer staat) korter dan 7 jaar bewaard.
Kunt u bevestigen dat dit inderdaad zo is?

2. Toevalligerwijs kwam telefonisch ter sprake dat het CAK mijn gegevens na het verstrijken van de wettelijke bewaartermijn niet automatisch gaat verwijderen. Het CAK kan mijn gegevens anonimiseren, maar zal dat alleen doen als ik daar een verzoek toe indien.
Kunt u bevestigen dat dit inderdaad de gehanteerde procedure is?

Met vriendelijke groet,

x

Van: [redacted]
Verzonden: maandag 20 april 2020 09:27
Aan: [redacted]; [redacted]; [redacted]
CC: [redacted]
Onderwerp: Fwd: feedback en aanvullende vragen AVG inzage

Beste [redacted], [redacted] en [redacted],

Op 28 maart hebben wij een mail van [redacted] ontvangen waarin hij ons (in zijn visie) wijst op gaten in ons Privacy systeem.
Zijn vragen zijn niet op niveau van een willekeurige klant maar duiden op specialisme.
Ik heb zorg over deze mail want dit kan een journalist zijn en voor je het weet staan we in de krant of op TV. Na enig gegoogel ben ik erachter dat dit een software architect is die diverse bedrijven wijst op " lekken" in hun bedrijf en vervolgens daar mee naar buiten treedt.

[redacted],
Kun je ons informeren hoe je de mail van deze meneer hebt beantwoord en hoe je met hem in gesprek bent gegaan? Loopt dit contact goed? Bewaak jij het contact met deze meneer?

[redacted],
Belangrijk is eerst de uitkomsten van de analyse te ontvangen over de stand van zaken mbt Privacy. Wie van jullie heeft hierin de lead genomen en is ons aanspreekpunt? Zou fijn zijn als we komende week de eerste bevindingen gepresenteerd krijgen. Wat is de status?

Hoor graag vandaag even een korte terugkoppeling.

Hartelijke groet,
[redacted]

Begin doorgestuurd bericht:

> **Van:** [redacted]
> **Datum:** 20 april 2020 om 09:15:26 CEST
> **Aan:** [redacted]
> **Onderwerp: FW: feedback en aanvullende vragen AVG inzage**

> **Van:** [redacted]
> **Verzonden:** dinsdag 7 april 2020 8:57
> **Aan:** [redacted]; [redacted]; [redacted]
> **CC:** [redacted]; [redacted]
> **Onderwerp:** RE: feedback en aanvullende vragen AVG inzage
>
> Hoi,
>
> Even in aanvulling op de vraag van [redacted]: Is er iemand die contact heeft opgenomen met deze meneer, hem heeft verteld wat we met zijn feedback gaan doen en wanneer hij wat terug hoort (en dat in de gaten houdt)?

Gr[redacted]

Van: [redacted]
Verzonden: maandag 6 april 2020 17:39
Aan: [redacted]
[redacted]
CC: [redacted]
[redacted]
Onderwerp: Fwd: feedback en aanvullende vragen AVG inzage

Beste [redacted] en [redacted],

Mag ik jullie vragen (als stuurgroepvoorzitter AVG en als operatie verantwoordelijke) alle punten die de klant noemt uit te laten zoeken en aan te laten passen in de systemen of procedures ingeval juist is wat deze klant stelt?
Graag ontvang ik eerst een inhoudelijke analyse van de situatie en de risico's en een plan van aanpak.

Hartelijke groet,
[redacted]

Begin doorgestuurd bericht:

> **Van:** FG <fg@hetcak.nl>
> **Datum:** 6 april 2020 om 16:52:49 CEST
> **Aan:** [redacted]
> **Kopie:** [redacted]
> **Onderwerp: FW: feedback en aanvullende vragen AVG inzage**
>
> Goedemiddag [redacted],
>
> Onderstaande mail kreeg ik van een klant toegestuurd. Hij snijdt een paar goede punten aan. Mijn advies aan jou is om alle punten uit te laten zoeken en zo nodig aan te laten passen in systemen/procedures. Dit om de compliancy aan de AVG te vergroten want op genoemde punten, als ze waar zijn, lopen wij een risico.
>
> Als je mijn advies op volgt, dan hoor ik graag aan wie je die opdracht verstrekt en van wie ik dus inhoudelijke antwoorden kan verwachten. Dan kan ik vanuit mijn rol een vinger aan de pols houden.
>
> Met vriendelijke groet,
>
> CAK
> [redacted]
> Functionaris Gegevensbescherming (FG)
>
> T [redacted]
> E [redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: zondag 29 maart 2020 11:59
Aan: FG <fg@hetcak.nl>
Onderwerp: feedback en aanvullende vragen AVG inzage

Geachte heer / mevrouw,

Naar aanleiding van informatie van de gemeente Rotterdam dat zij via de BRP informatie hadden gedeeld met het CAK heb ik een inzageverzoek gedaan bij het CAK conform de AVG. Die inzage is inmiddels gegeven (EB-nummer [redacted], kenmerk [redacted], maar ik wil graag mijn feedback op het proces met u delen en er zijn nog wat losse eindjes met betrekking tot de informatie die ik heb gekregen.

1. Op https://www.hetcak.nl/uw-privacy staat:
"Ontvangt u Wlz-zorg of ondersteuning vanuit de Wmo? Dan kunt u inloggen op Mijn CAK. Als u bent ingelogd, dan kunt u de belangrijkste gegevens die we van u hebben zelf inzien."
Volgens mij zou het handig zijn om hier een termijn bij te noemen ".. of heeft u die in de afgelopen X jaar ontvangen". Ik werd namelijk door uw medewerkers hiernaar verwezen en heb een account aangemaakt en met DigiD ingelogd, om vervolgens niets te vinden omdat mijn gegevens betrekking hadden op kalenderjaar 2014.

2. Het CAK verwerkt gegevens voor verschillende regelingen en in alle contactkanalen van het CAK wordt hierop voorgesorteerd door gebruikers te dwingen een regeling te kiezen. Maar een inzageverzoek voor alle gegevens heeft betrekking op de *organisatie*, niet op een *regeling*.
Er is geen duidelijke manier om een dergelijke aanvraag in te dienen en uiteindelijk kreeg ik als advies een willekeurige regeling te kiezen en daar bij te zetten dat het om de hele organisatie ging.

3. Nadat ik een inzageverzoek had gedaan kreeg ik als reactie dat er te weinig gegevens bekend waren om mij te vinden en werd mij gevraagd om "het kenmerk van uw laatste beschikking of factuur en uw geboortedatum door te geven. Echter, een AVG inzageverzoek heeft expliciet ook als doel om uit te kunnen vinden *of* er gegevens verwerkt worden, in welk geval er natuurlijk geen beschikking of factuur bekend is.
Als alternatief werd gegevens het invullen van mijn BSN op de website. Echter, de AP geeft duidelijk aan dat het niet de bedoeling is dat voor een inzageverzoek het BSN verstrekt moet worden. En uiteindelijk bleek dat ook helemaal niet nodig, want ik heb de informatie ook zonder dit te verstrekken gekregen.

4. Vervolgens kreeg ik 1 maand en 25 dagen na mijn verzoek een antwoord. Dat antwoord was echter gewoon een kopie van de privacy verklaring. Mijn inzageverzoek was geen verzoek om mij de privacy verklaring op te sturen, maar om de feitelijke informatie die het CAK van mij had, waar die informatie vandaan was gekomen en aan wie die verstrekt was.
Na hier nogmaals om gevraagd te hebben kreeg ik uiteindelijk op 26 maart, 2 maanden en 21 dagen na mijn inzageverzoek, daadwerkelijk inzage.

5. In de beantwoording staat vermeld waar het CAK de verschillende gegevens vandaan heeft: "vervolgens hebben wij uw gegevens gecontroleerd in de Basisregistratie Personen (BPR)".
Wat mij opviel, en bij navraag telefonisch bevestigd heb gekregen, was dat er in de gegevens die ik van jullie kreeg een BRP-mutatie uit 2019 vermeld was. Het CAK heeft dus niet eenmalig in 2014 de gegevens gecontroleerd, maar heeft die tot zeer recent nog geupdate. Dat is niet transparant vermeld in de beantwoording en kan zeker beter toegelicht worden.

Volgens mij had deze hele gang van zaken simpel voorkomen kunnen worden door dossiers *wel* beschikbaar te maken op het webportaal van het CAK. Aangezien het CAK dat al doet kunnen moeilijk beveiligingsbezwaren tegen zijn. Het enige wat het CAK moet doen is stoppen met het verbergen van dossiers nadat ze gesloten zijn. Hoewel niet iedereen de juiste computervaardigheden en / of een DigiD zal hebben, lijkt mij dat het CAK hiermee het merendeel van de inzage verzoeken zou kunnen opvangen en automatiseren. En het sluit ook netjes aan bij het advies van de AP om waar bestaande authenticatie mogelijkheden zoals een website inlog zijn, deze te hergebruiken voor (authenticatie van) inzage verzoeken.

Tot zover mijn feedback op het inzage proces. Dan zijn er nog wat inhoudelijke losse eindjes.

1. Ik vind het opvallend dat er geen betaalgegevens in het overzicht dat ik heb gekregen staan. Dat zou betekenen dat het CAK bijvoorbeeld gegegevsn met betrekking tot betaalde acceptgiro's (waarin mijn rekeningnummer staat) korter dan 7 jaar bewaard.
Kunt u bevestigen dat dit inderdaad zo is?

2. Toevalligerwijs kwam telefonisch ter sprake dat het CAK mijn gegevens na het verstrijken van de wettelijke bewaartermijn niet automatisch gaat verwijderen. Het CAK kan mijn gegevens anonimiseren, maar zal dat alleen doen als ik daar een verzoek toe indien.
Kunt u bevestigen dat dit inderdaad de gehanteerde procedure is?

Met vriendelijke groet,

[redacted]

[redacted]

Van: [redacted]
Verzonden: dinsdag 21 januari 2020 21:48
Aan: [redacted]; [redacted]
Onderwerp: Onderzoek AP

Goedenavond [redacted] en [redacted],

Even ter jullie informatie:

Naar aanleiding van een onderzoek van de AP naar het al dan niet tijdig melden van vijf specifieke datalekken hebben we op 17 december de gevraagde antwoorden en documenten aan de AP verstuurd.

Gisteren aan het einde van de middag heeft de AP contact met me gezocht omdat de bijlagen door het scannen voor het digitaal indienen niet leesbaar zouden zijn.

Ik heb vanmiddag persoonlijk alsnog de bijlagen in hardcopy bij de AP afgegeven.

Deze mail is er om jullie hierover even te informeren.

Mochten er vragen zijn, dan hoor ik die graag.

Fijne avond!

[redacted]

[redacted]

Van: [redacted]
Verzonden: vrijdag 24 december 2021 16:10
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: acties rondom datalek

Beste collega's,

Ik heb inmiddels gesproken met de voorzitter van het overleg Functionaris Gegevensbescherming Manifestgroep. De problematiek waar wij mee worstelen was voor hem zeer herkenbaar.

Hij heeft hier op twee manieren mee te maken gehad. Zo heeft hij al twee keer in de loonaangifteketen een corrupt bestand gehad. Dat gaat dus van een 3e partij (bijvoorbeeld een verzekeraar) via de belastingdienst naar de organisatie waar hij voor werkt. Die organisatie levert op haar beurt ook weer door met tienduizenden geraakte records én betrokkenen. Daar ben je dus zo een half jaar mee bezig met uitzoeken en herstelacties. En iedereen in de keten moet melden bij de AP en evt. ook bij betrokkenen. Dit probleem is eigenlijk niet oplosbaar: dit is inherent aan de werking van een keten, maar waar mogelijk moet elke organisatie zelf controles op de gegevens uitvoeren.

Een iets kleinschaliger maar wel lastiger voorbeeld dat hij verder noemde zijn ketenpartners die fouten maken: arbodiensten die verkeerde loonheffingsnummers gebruiken voor verzuimmeldingen. Die worden door de organisatie automatisch verwerkt en doorgezet naar de verkeerde werkgever. Ook voor deze situatie geldt dat een organisatie moet melden bij de AP en evt. ook bij betrokkenen en dat intern controles moet worden ingebouwd om de gegevens te controleren. In beide situaties is de organisatie namelijk verwerkingsverantwoordelijk.

In de casus die bij ons speelde geldt dus ook dat we moeten melden bij de AP en dat we intern zo goed mogelijk interne controles moeten inbouwen zoals ook beschreven in de memo aan de RvB. Op het moment dat de AP naar aanleiding van een melding onderzoek komt doen dan kan je in ieder geval aantonen dat je door middel van die interne controles zo goed mogelijk hebt geprobeerd om datalekken te voorkomen.

Met vriendelijke groet,

[redacted]
Adviseur bestuurlijke & juridische zaken CAK
T [redacted]
E [redacted]
Werkdagen: ma, di, wo en do

Van: [redacted]
Verzonden: vrijdag 10 december 2021 20:31
Aan: [redacted]
CC: [redacted]
Onderwerp: acties rondom datalek

Beste Allen,

Het datalek-memo is door de RvB geweest. [redacted] en [redacted], kunnen jullie de melding naar de AP goed onder woorden brengen en deze indienen? [redacted]; als jij met de FG's gesproken hebt, koppel je ons dan terug; daar kunnen we wat van leren! [redacted]; doe jij de evaluatie van het datalek? Verder heb ik nog met [redacted] gesproken; zij zal vanuit WAN de banden aanhalen met de afdeling polis van het UWV om te kijken wat daar te doen is vwb

afstemming, hen bewust maken van de datalekken die ontstaan door de achterstanden en kijken wat we samen op kunnen pakken.

Hgr,

M

[redacted]
Directeur Zvw

M [redacted]
E [redacted]

www.hetcak.nl
Postbus 84015
2508 AA Den Haag

Bezoekadres:
Prinses Beatrixlaan 7 in Den Haag