Privacy beleid CAK

Algemene Verordening Gegevensbescherming

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht'

Inhoudsopgave

Inleiding 3

1. Privacy: missie, visie en strategie 4

2. Reikwijdte 5

3. Definities 5

4. Beginselen 6

4.1. Doelbinding 6
4.2. Rechtmatigheid 7
4.3. Behoorlijkheid 9
4.4. Transparantie 10
4.5. Juistheid 10
4.6. Minimale verwerking 12
4.7. Integriteit en vertrouwelijkheid 13
4.8. Opslagbeperking 14
4.9. Verantwoordingsplicht 14

5. AVG-beleid 15

5.1. Rechten van betrokkene 15
5.2. Verwerkingenregister 16
5.3. Verwerkersovereenkomsten 16
5.4. Datalekken 17
5.5. Data Protection Impact Analyses (DPIA) 18
5.6. Privacy by design en default 19
5.7. Gedragscodes en certificering 20
5.8. Doorgifte binnen en buiten de EU 20
5.9. CAK toets kader: NOREA 22

6. Ethisch databeleid en algorithmen. 22

7. Bijlagen 24

Bijlage 1: Stakeholders intern/ extern 24
Bijlage 2: schema's 27
2. Stroomschema meldplicht aan de AP 28
3. Stroomschema meldplicht aan betrokkene 29
Bijlage 3: Schema vertegenwoordiging en bevoegdheden 30
Bijlage 4: RASCI matrix CAK AVG Versie 2.0 2019 (losse bijlage bij het Privacybeleid CAK). 32
Bijlage 5: verplichte inhoud verwerkingenregister 32
RASCI matrix CAK AVG Versie 2.0 2019 (losse bijlage bij het Privacybeleid CAK) 35

Inleiding

De AVG is vanaf 25 mei 2018 van kracht in de EU en is vanaf dat moment ook *het* normenkader voor de bescherming van persoonsgegevens. Daar waar de AVG ruimte biedt, heeft onze nationale wetgever dit nader ingevuld met de Uitvoeringswet AVG (UAVG). Tezamen vormt dit de basis van de *privacywetgeving*.
Dit privacy beleid vormt het kader waaruit de volgende documenten voortvloeien: privacyverklaring, privacy Governance structuur, strategisch informatiebeveiligingsbeleid en het protocol melding en afhandeling datalekken.

Hierbij geldt de AVG als uitgangspunt en is waar nodig toegelicht waarom het CAK gekozen heeft voor een bepaalde beleidsrichting.

1. Privacy: missie, visie en strategie

Het CAK is sinds 2013 een zelfstandig bestuursorgaan (ZBO) met rechtspersoonlijkheid en is in 1968 opgericht als Besloten Vennootschap (BV), te weten een jaar na de inwerkingtreding van de voormalige Algemene Wet Bijzondere Ziektekosten (AWBZ). Het CAK heeft wettelijke taken, maar vervult tegelijk ook een belangrijke maatschappelijke functie. Om het CAK richting te geven in hoe we als ZBO willen zijn, waar we voor staan en welke maatschappelijke rol we willen spelen, is er een visie en missie nodig. Bij elk onderwerp zijn deze facetten bepalend voor de richting die we willen opgaan en zo dus ook voor hoe we tegen privacy aankijken.

VISIE

Iedere burger heeft recht op snelle, foutloze en gemakkelijke dienstverlening door de overheid; het CAK biedt daarbij extra zorg en aandacht voor mensen in kwetsbare situaties.

MISSIE

Het CAK is de klantgerichte publieke dienstverlener die staat voor de zorgvuldige uitvoering van regelingen van de overheid en proactieve communicatie met burgers.

AWARENESS

Aangezien het CAK net zo sterk of zwak is in privacy als de medewerkers, staat en valt alles bij hoe medewerkers van het CAK omgaan met privacy. De afdelingsmanagers dienen te zorgen voor voldoende bewustwording bij de medewerkers op het gebied van privacy. Hierbij dienen zij minimaal op de hoogte te zijn van de privacyregels en de voor hun werkzaamheden relevante bepalingen zodat zij deze in de dagelijkse praktijk kunnen (laten) toepassen.

De verantwoordelijkheid voor bewustwording ligt binnen de diverse clusters. Deze worden hierbij ondersteund vanuit HR en HR-development en CIO-office. Nieuwe medewerkers volgen verplicht de e-learning “De bescherming van persoonsgegevens bij het CAK”.
Op de intranetsite van “privacy en security” is alle relevante informatie m.b.t. het toepassen van de AVG gepubliceerd, inclusief dit privacy-beleid en 6 informatieclips waarin werking en toepassing van de AVG wordt uitgelegd. Deze site is voor alle medewerkers van het CAK, intern en extern, toegankelijk.

PRIVACYBELEID

Het (door)ontwikkelen van privacy en beleid wordt niet alleen gevraagd vanuit de AVG, maar ook gezien de visie en missie van het CAK om in de relatie burger en overheid zorgvuldig, veilig, proportioneel, professioneel, vertrouwelijk, transparant en betrouwbaar om te gaan met het verwerken van persoonsgegevens. Een correcte omgang met privacy is randvoorwaardelijk om de visie en missie op een goede manier voort te brengen.

2. Reikwijdte

De AVG is van toepassing op de verwerkingen van persoonsgegevens van het CAK die voldoen aan één van de volgende voorwaarden:

- Geheel of gedeeltelijk geautomatiseerd.
- Opgenomen in een bestand.
- Bestemd zijn om in een bestand opgenomen te worden.

Het CAK hanteert het uitgangspunt dat zodra op enige manier sprake is van verwerking van persoonsgegevens de privacywetgeving in acht dient te worden genomen.

3. Definities

In artikel 4 van de AVG zijn belangrijke definities gegeven. Hieronder zijn een aantal van de begrippen opgenomen.

PERSOONSGEGEVENS
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat de AVG niet ziet op gegevens van overleden personen of rechtspersonen. Het CAK-beleid is echter dat ook in die situaties behoorlijk wordt omgegaan met persoonsgegevens.

BIJZONDERE PERSOONSGEGEVENS
Persoonsgegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken of de verwerking van genetische/biometrische gegevens of gegevens aangaande gezondheid, seksueel gedrag/geaardheid.

VERWERKING
Het al dan niet geautomatiseerd verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken/wijzigen, opvragen, raadplegen, gebruiken, verstrekken (doorzending), verspreiden, ter beschikking stellen, aligneren/combineren, afschermen, wissen of vernietigen van persoonsgegevens.

BESTAND
Gestructureerd geheel van persoonsgegevens die onder criteria toegankelijk zijn. Niet is vereist dat dit gecentraliseerd is.

VERWERKINGSVERANTWOORDELIJKE
Natuurlijk persoon of rechtspersoon, overheidsinstantie, dienst/orgaan die het doel en de middelen van de verwerking van persoonsgegevens zelfstandig of in samenwerking vaststelt.

VERWERKER
Natuurlijk persoon of rechtspersoon, overheidsinstantie, dienst/orgaan die namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

ONTVANGER
Natuurlijk persoon of rechtspersoon, overheidsinstantie, dienst/orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

BIOMETRISCHE GEGEVENS
Persoonsgegevens als resultaat van specifieke technische verwerking m.b.t. fysieke, fysiologische of gedrag gerelateerde kenmerken op basis waarvan eenduidige identificatie mogelijk is of wordt bevestigd. Denk o.a. aan: gezichtsafbeeldingen, vingerafdrukgegevens, bepaalde wijze van ondertekening, de iris- of netvliesscan en stemherkenning.

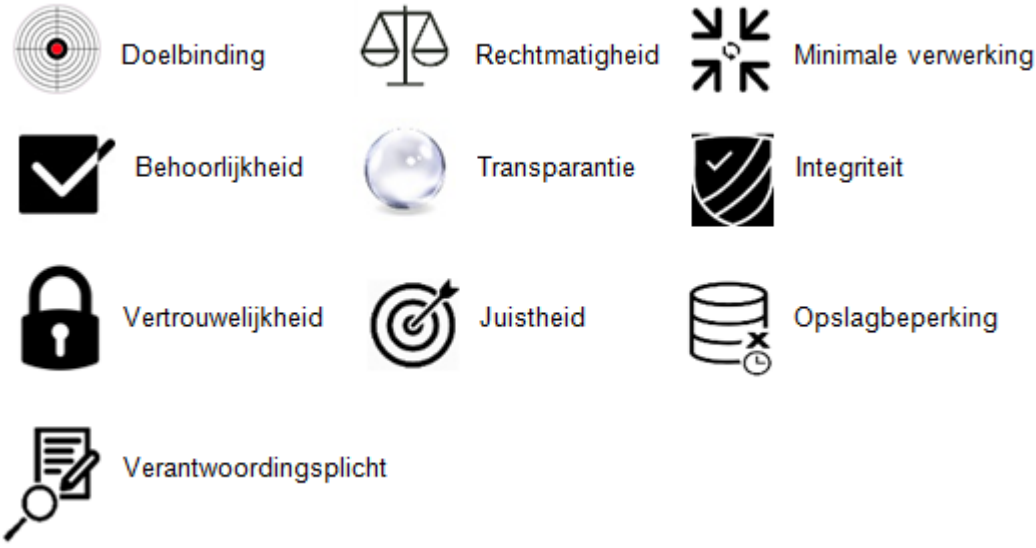
GEZONDHEIDSGEGEVENS
Persoonsgegevens in verband met fysieke/mentale gezondheid, waaronder ook gegevens over verleende gezondheidsdiensten waarmee informatie over de gezondheid wordt gegeven.

GRENSOVERSCHRIJDENDE VERWERKING
Verwerking van persoonsgegevens in verschillende EU-lidstaten of in één EU-lidstaat, maar met wezenlijke gevolgen of waarschijnlijk wezenlijke gevolgen voor betrokkenen in een andere lidstaat.

4. Beginselen

De gehele AVG is opgebouwd uit artikelen die terug te voeren zijn op beginselen. Daarom beginnen we met het behandelen van de beginselen. Voor elk beginsel is hieronder een symbool vastgesteld, zodat dit gemakkelijk toepasbaar is in de interne en externe communicatie om de beginselen aan te duiden.

De verwerking van persoonsgegevens moet voldoen aan de volgende beginselen[1]:



4.1. 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.

Dit betekent dat het CAK voor zijn verwerkingen: het doel specificeert, dit duidelijk omschrijft en legitimeert. In het symbool is dat de rode stip. Zolang het CAK de gegevens verwerkt conform de rode stip, is er doelbinding. Daarbuiten moet opnieuw getoetst worden wat het doel is, hoe dit omschreven

[1] Artikel 5 AVG.

moet worden en wat de legitimiteit van de verwerking is. Specificering (welbepaald), omschrijving (uitdrukkelijk omschreven) en legitimatie (gerechtvaardigd) zijn voorwaardelijk voor de doelbinding.

4.2. Rechtmatigheid

Om te kunnen spreken van een rechtmatige gegevensverwerking is ten minste vereist dat dit gebeurt op basis van één van de AVG-grondslagen[2]. In het onderstaande overzicht is aangegeven welke van toepassing zijn op het CAK.

Grondslag	Toepasselijkheid mogelijk?	Toelichting
Toestemming	Nee [3]	Het CAK valt onder het brede begrip overheid en als ZBO hebben we een relatie burger <-> overheid. In deze ongelijke verhouding is het verwerken van persoonsgegevens op grond van toestemming voor het CAK problematisch. De toestemming moet namelijk vrijelijk gegeven zijn. Daarom kan dit geen grondslag zijn voor het CAK.
Uitvoering overeenkomst	Ja	Denk hierbij aan de arbeidsovereenkomsten en overige (leveranciers)overeenkomsten waarbij sprake is van verwerking van persoonsgegevens.
Wettelijke plicht	Ja	De grondslag kan zijn gelegen in de AVG, andere Unierechtelijke (EU-wetgeving) of lidstaatrechtelijke bepalingen. Een voorbeeld van het laatste zijn de diverse nationale wetten die het CAK uitvoert. Het gaat om specifiek in de wet omschreven verplichtingen waaraan het CAK moet voldoen. Daaruit moet volgen dat het CAK om aan een wettelijke plicht te voldoen persoonsgegevens moet verwerken.
Vitale belangen	Ja	Hierbij kan gedacht worden aan uitzonderlijke situaties waarbij het CAK moreel verplicht is om de vitale belangen te beschermen van de betrokkene/ander natuurlijk persoon. Bijvoorbeeld in geval van een acute medische noodsituatie of andere calamiteit (bijv.: brand).
Taak van algemeen belang/publieke taak	Ja	Vervullen van een taak van algemeen belang of uitoefenen openbaar gezag. Het gaat hier om wettelijke taken.
Behartiging van gerechtvaardigde belangen	Nee	In de AVG is deze grondslag expliciet uitgesloten voor bestuursorganen, zo ook het CAK. Daarom kunnen we ons niet hierop beroepen[4].

[2] Artikel 6 AVG.

[3] In uitzonderlijke gevallen kan het CAK uit hoofde van opdracht door VWS of gerechtelijke uitspraak toch (tijdelijk) aangewezen zijn op deze grondslag. Deze grondslag kan wel van toepassing zijn op secundaire verwerkingen zoals bijvoorbeeld een Klant Tevredenheid Onderzoek.

[4] Uitzondering hierop betreft de dagelijkse bedrijfsvoering, zoals HR en facilities.

Het uitgangspunt is dat bij bestuursorganen de verwerking van persoonsgegevens doorgaans plaatsvindt met een wettelijke grondslag. Voor alle grondslagen geldt dat een beroep daarop door het CAK verantwoord moet kunnen worden. Als er een grondslag is dan is de verwerking in beginsel rechtmatig en is er doelbinding.

Het CAK heeft veelal te maken met bijzondere persoonsgegevens. Vanuit de AVG geldt nadrukkelijk het verbod om bijzondere persoonsgegevens te verwerken, behoudens in de AVG en UAVG opgenomen uitzonderingen.[5] Het CAK zal vanuit zijn wettelijke taken en bedrijfsvoering te maken hebben met het verbod op verwerking op:

- Ras/etniciteit → denk aan land van herkomst en nationaliteit;
- Biometrische gegevens ter identificatie → denk aan stem, vingerafdrukken, beeld (foto's en video's);
- Gezondheid → denk aan zorguren, start- einddatum zorg, zorginstelling, zorgvorm of medische gegevens.

In de UAVG is de uitzondering op de verwerking nader uitgewerkt. Hierbij dient vooropgesteld te worden dat dit onvermiderlijk en noodzakelijk moet zijn. Het verwerken van gegevens met betrekking tot:

- ras en etniciteit mag met het oog op identificatie[6];
- biometrie mag met het oog op authenticatie of beveiligingsdoeleinden[7];
- gezondheid mag voor zover een goede uitvoering van wettelijke voorschriften dit vereist[8].

Het CAK verwerkt alleen gevoelige persoonsgegevens die betrekking hebben op strafrechtelijke vervolgingen en strafbare feiten in de eigen bijdrageregelingen. Er wordt navraag gedaan of iemand in detentie verblijft om eigen bijdragen te kunnen opschorten. Hierbij wordt geen inzicht verkregen in de grond voor de detentie.

Verwerking vindt niet plaats als er een rechterlijke uitspraak of een besluit van een administratieve autoriteit is van een derde land op grond waarvan een verwerkingsverantwoordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken en waarbij dit niet erkend of afdwingbaar is gemaakt dat dit is gebaseerd op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand tussen het verzoekende derde landen en de EU of een lidstaat.

Ander doel (hergebruik)

Uitgangspunt is dat persoonsgegevens niet verwerkt mogen worden voor andere doeleinden. De AVG geeft een mogelijkheid als het nieuwe doel van de verdere verwerking, verenigbaar is met het oorspronkelijke doel. Behoudens enkele uitzonderingen, die niet op het CAK van toepassing zijn, moet het CAK bij de beoordeling of er sprake is van verenigbaarheid onder meer rekening houden met:

1. Ieder verband tussen de twee doeleinden;
2. het kader waarin de initiële verkrijging heeft plaatsgevonden (verhouding betrokkene <-> CAK);
3. de aard van de persoonsgegevens;
4. gevolgen voorgenomen verdere verwerking;

---

[5] Artikelen 9 AVG en paragraaf 3.1 UAVG.

[6] Artikel 25, onderdeel a, UAVG.

[7] Artikel 29 UAVG.

[8] Artikel 30, lid 1, onderdeel a, UAVG.

5. passende waarborgen.

Als deze beoordeling positief is dan mag het CAK de gegevens ook verwerken voor het nieuwe doel. Een voorbeeld is dat het CAK van de burger een rekeningnummer ontvangt om de eigen bijdrage te innen. Strikt genomen zou het CAK dit rekeningnummer niet mogen gebruiken om eigen bedragen op te restitueren, echter het restitueren op hetzelfde rekeningnummer van dezelfde eigen bijdrage is verenigbaar met het oorspronkelijke doel.

Het CAK hanteert als principe dat elke verwerking uitsluitend voor het primaire doel plaatsvindt en dat verdere verwerking niet plaatsvindt, tenzij het oorspronkelijk en het nieuwe doel op slechts één ondergeschikt onderdeel afwijkt (1-5).
Betrokkenen worden altijd vooraf geïnformeerd indien het voornemen bestaat gegevens te verwerken voor andere doelen dan de oorspronkelijke doelen. Betrokkenen hebben het recht toestemming hiervoor te weigeren. Gegeven toestemming kan later op elk moment door betrokkenen worden ingetrokken. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld, omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt.

Voor de door de Autoriteit Persoonsgegevens (AP) uit te voeren taken is het CAK gehouden om de AP persoonsgegevens ter beschikking te stellen, al zijn die gegevens niet voor dat doel verwerkt.[9]

4.3. 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. Dit is een open norm die ingevuld kan worden afhankelijk van de omstandigheden van het geval. De onderdelen waar het CAK zich per definitie aan moet houden, zijn hieronder benoemd.

De algemene beginselen van behoorlijk bestuur

Het CAK is als ZBO gehouden aan de Algemene wet bestuursrecht (Awb) en de beginselen die daaraan ten grondslag liggen. Vertaald naar gegevensverwerkingen dient voor een behoorlijke gegevensverwerking te worden voldaan aan:

- Fair play/onpartijdigheid (artikel 2:4 Awb): de verwerking is eerlijk, betrouwbaar, gelijkwaardig (volgens dezelfde maatstaf) en transparant.
- Zorgvuldigheidsbeginsel (artikel 3:2 Awb): de wijze waarop de verwerking plaatsvindt is zorgvuldig, nauwkeurig en adequaat.
- Motiveringsbeginsel (artikel 3:46 Awb): op heldere, duidelijke en verifieerbare wijze wordt vastgelegd waarom en hoe een verwerking plaatsvindt[10].
- Verbod op misbruik van bevoegdheid/verbod van willekeur (artikel 3:3 Awb): de bevoegdheden tot gegevensverwerking mogen alleen voor dat doel worden gebruikt. Het CAK mag hier niet willekeurig mee omgaan.
- Belangenafwegingsplicht (artikel 3:4 lid 1 Awb): het belang van de gegevensverwerking en het belang van de burger en zijn recht op verbod op gegevensverwerking moeten afgewogen worden.
- Evenredigheidsbeginsel (artikel 3:4 lid 2 Awb): de inbreuk van de gegevensverwerking mag niet onevenredig zwaar wegen tegenover het te dienen doel.

[9] Artikelen 31 en 58 AVG en 5:20 Awb.

[10] Elke verwerking van persoonsgegevens dient in het register van verwerkingen verantwoord te worden.

- Gelijkheidsbeginsel: iedere burger wordt in gelijke situaties met dezelfde mate van gegevensverwerking geconfronteerd.
- Vertrouwensbeginsel: de burger mag erop vertrouwen dat de gegevensverwerking is zoals hierover is gecommuniceerd.
- Rechtszekerheidsbeginsel: de burger mag het CAK houden aan de waarborgen die gegeven zijn vanuit de AVG, de UAVG en het eigen beleid omtrent gegevensverwerkingen.

Andere 'beginselen'

- Hoor en wederhoor (artikelen 7:2 en 9:10 Awb): als een burger bezwaar maakt/klaagt over de gegevensverwerking dan moet het CAK – behoudens in de wet gegeven uitzonderingen – de betrokkene de gelegenheid geven tot een mondelinge toelichting.
- Correcte bejegening: het klachtrecht (artikel 9:1 Awb) veronderstelt dat het CAK de burger correct bejegend. Wat een correcte bejegening is, wordt ingevuld a.d.h.v. de voorgaande beginselen.

Hieruit blijkt dat het CAK reeds op basis van de nationale wetgeving gehouden is aan beginselen die – toegepast op gegevensverwerkingen – vele gelijkenissen vertonen met de beginselen in de AVG.[11]

4.4. 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. De vorm is schriftelijk of digitaal (portaal) of mondeling als de betrokkene daarom verzoekt.[12]

Het CAK stelt ten behoeve hiervan een *privacy statement* beschikbaar via de website. Het privacy statement bevat de informatie aangewezen in artikel 13 en 14 AVG.

Naast de informatie die via het privacy statement al bekend is, moet het CAK ook een kopie van de persoonsgegevens die worden verwerkt, kunnen verstrekken aan de betrokkene (recht van inzage van de betrokkenen). Als het verzoek digitaal is gedaan dan wordt de informatie door het CAK zoveel mogelijk digitaal verstrekt.[13]

Het CAK moet er bij de verstrekking van de persoonsgegevens (het dossier) rekening mee houden dat niet de persoonsgegevens van derden vrijgegeven worden.[14]

4.5. Juistheid

De persoonsgegevens die het CAK verwerkt, dienen juist te zijn en het CAK moet zich ook inspannen om de persoonsgegevens te actualiseren. Hoe ver deze inspanningsplicht reikt, is afhankelijk van de aard van de gegevens, de impact van een eventuele onjuistheid en voor welk doeleinden ze worden gebruikt. De betrokkene heeft hierin ook een rol, namelijk het recht op rectificatie en wissing van gegevens en

[11] Ook de EU-verordeningen 883/2004 en 987/2009 verwijzen in het kader naar privacy naar het Europese en nationale normenkader.

[12] Artikel 12-14 AVG.

[13] Artikel 15 AVG.

[14] Artikel 15, lid 4, AVG. Behoudens gegevens die op basis van een verzoek Wet openbaar bestuur (Wob) verstrekt mogen worden.

beperking van de verwerking.[15] Het CAK dient zich ook in te zetten om dergelijke procedures zo effectief mogelijk te maken.

Onverwijld wissen?

Uitgangspunt is dat persoonsgegevens niet gewist kunnen worden, zolang de noodzakelijkheid er is om een wettelijke plicht na te komen die op het CAK rust.[16] Dit betekent wel dat gegevens die onrechtmatig zijn verwerkt per definitie verwijderd moeten worden evenals gegevens waarvan de door het CAK vastgestelde bewaartermijn verstreken is. Het CAK moet binnen de beschikbare technische middelen maatregelen nemen zodat de gegevens ook bij ontvangers en verwerkers gewist worden.[17] Het CAK borgt dit door eisen te stellen aan de ontvangers voordat ze de gegevens mogen ontvangen.

Op verzoek van de betrokkene worden de hem betreffende persoonsgegevens gewist wanneer een van de volgende gevallen van toepassing is:
a. de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
b. de betrokkene trekt de toestemming waarop de verwerking berust in en er is geen andere rechtsgrond voor de verwerking;
c. de betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking;
d. de persoonsgegevens zijn onrechtmatig verwerkt;
e. de persoonsgegevens moeten worden gewist om te voldoen aan een in het wettelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
f. de persoonsgegevens van kinderen jonger dan 16 jaar zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Beperking van de verwerking

Het beginsel van juistheid van de gegevensverwerking brengt met zich mee dat betrokkene ook beperking van de verwerking kan vragen. Dat kan in de volgende gevallen:

- als de juistheid door de klant is betwist en het CAK controleert het betwiste;
- als de verwerking onrechtmatig is, maar de betrokkene geen wissing maar beperking van de verwerking wenst;
- als niet het CAK de gegevens nog nodig heeft, maar betrokkene zelf voor een rechtszaak;
- als de betrokkene bezwaar heeft gemaakt tegen de verwerking.

De beperking van de verwerking heeft geen betrekking op de opslag van de gegevens. Het gaat erom dat het CAK de gegevens niet meer (verder) verwerkt.[18]

Bezwaar

De AVG geeft het recht van bezwaar tegen de gegevensverwerking, echter hoeft het CAK hieraan geen opvolging te geven als de verwerking is gebaseerd op een wettelijke grondslag.[19]

---

[15] Artikelen 16, 17 en 18 AVG.

[16] Artikel 17, lid 3, onderdeel b, AVG.

[17] Artikel 17, lid 2, AVG.

[18] Artikel 18, lid 2, AVG.

[19] Artikel 21 AVG.

4.6. Minimale verwerking

Uitsluitend die persoonsgegevens mogen verwerkt worden die voldoende zijn om het beoogde doel te bereiken. De persoonsgegevens worden door het CAK veelal verwerkt op grond van een wettelijke grondslag en voor die doeleinden. Dit betekent dat het CAK binnen de doeleinden het moet doen met wat strikt noodzakelijk is om het doel te bereiken. Dit heeft ook impact op de wijze waarop met persoonsgegevens wordt omgegaan in het kader van ontwikkel- en testomgevingen, data warehousing, rapportages etc. Het gebruiken van echte persoonsgegevens hierbij is in strijd met het beginsel van minimale gegevensverwerking (dataminimalisatie). Het CAK moet zorgdragen dat dergelijke systemen en omgevingen (zoveel mogelijk) kunnen werken zonder persoonsgegevens. Het bovenmatig verwerken van persoonsgegevens moet voorkomen worden.

Dit ziet niet alleen op de verwerkingen intern, maar ook op wat het CAK naar buiten communiceert. Als gevolg van het uitvoeren van de wettelijke taken stuurt het CAK namelijk vele uitingen naar burgers of zakelijke partijen (o.a. gemeenten/zorgverleners). De informatie die wij opnemen in de uitingen is ook een wijze van verwerken van persoonsgegevens. Denk hierbij o.a. NAW, geboortedatum, verzekerde-ID, financiële gegevens, zorguren etc. Een aantal van deze gegevens zijn onmisbaar voor de uitvoering en noodzakelijk uit hoofde van het motiveringsbeginsel of de wet. Zo is het vermelden van adresgegevens en naam op uitingen noodzakelijk om onze besluiten op de juiste wijze bekend te maken (3:41 Awb). Het vermelden van inkomens en vermogens is bijvoorbeeld noodzakelijk uit hoofde van motivering (artikel 3:47 Awb) en is voorgeschreven vanuit de Algemene Wet inzake Rijksbelastingen (artikel 21f AWR). Bij minimale verwerking gaat het ook om de frequentie van de verwerking. Bijvoorbeeld dat een bepaald gegeven in beginsel maar één keer voorkomt op een uiting.

Verwerking van persoonsgegevens van minderjarigen

Het CAK is zich er van bewust dat minderjarigen voor de AVG een extra kwetsbare groep vormen.
Het CAK verwerkt gegevens van minderjarigen uitsluitend in de volgende 2 gevallen:

- Gemeenten leveren in het kader van de Wmo personen aan die (nog) niet bijdrage plichtig zijn[20];
- De regeling Wlz.

Communicatie over de minderjarige betrokkene door het CAK geschiedt altijd via de wettelijke vertegenwoordiger van de minderjarige, nooit rechtstreeks met de minderjarige.

Burgerservicenummer (BSN)

Artikel 87 van de AVG vormt samen met artikel 46 van de UAVG de grondslag dat het BSN gehanteerd wordt in Nederland. Voor het CAK is artikel 10 van de Wet algemene bepalingen Burgerservicenummer (Wabb) relevant. Dit geeft de grondslag aan het CAK om bij de uitoefening van de publieke taken het BSN te gebruiken. In diverse materiewetten (Wlz, Wmo 2015 en Zvw) is verder concreter aangegeven wanneer en op welke wijze het CAK het BSN mag gebruiken. Dit ziet voornamelijk op de gegevensuitwisselingen tussen het CAK en derden en de waarborgen daaromtrent. Het BSN dient als authentiek identificatienummer en het gebruik hiervan vergroot de risico's op identiteitsfraude. Bij de gegevensuitwisselingen (bestanden) ter uitvoering van de diverse wettelijke taken is dit evenwel omgeven door eisen aan technische middelen, verificatie en authenticatie. Echter in geval van postverzendingen

[20] Noot S&B: Eerder is de optie besproken dat gemeenten minderjarigen helemaal niet aanleveren. Voortschrijdend inzicht heeft laten zien dat het wenselijker is als het CAK monitort wie meerderjarig worden, zodat zij tijdig kunnen worden geïnformeerd over de gevolgen van dit life event.

ontbreken dergelijke waarborgen. Daarom dient het onderscheid gemaakt te worden tussen elektronische bestands(gegevens)uitwisselingen via beveiligde portalen en andere (analoge) dragers van gegevens (zoals brieven, e-mail, USB-sticks etc. die niet altijd hetzelfde veiligheidsniveau garanderen).

Het CAK neemt in de uitingen het BSN niet op, tenzij daarvoor een expliciete duidelijke wettelijke grondslag is gegeven. Voor de identificatie van de burger en verzending van brieven zijn NAW en geboortedatum afdoende. In geval de wettelijke grondslag gegeven is, is het uitgangspunt van het CAK om de verwerking zo beperkt mogelijk te houden (denk aan minimale frequentie van het vermelden van het BSN).

4.7. Integriteit en vertrouwelijkheid

Bij de verwerking van persoonsgegevens wordt zorggedragen voor passende technische (encryptie en anonimiseren)[21] of organisatorische maatregelen die de beveiliging ervan garandeert.[22] 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.

Een belangrijke rol is hierbij weggelegd voor de Corporate Information Security Officer (CISO). Voor het CAK betekent dit dat elk ICT-systeem moet waarborgen dat de persoonsgegevens veilig verwerkt worden. Met het aansluiten bij de Baseline Informatiebeveiliging Overheid (BIO) voorziet het CAK hierin. De vertrouwelijkheid betekent dat het CAK daarnaast zorgdraagt dat de persoonsgegevens met autorisaties alleen toegankelijk zijn voor die noodzakelijke medewerkers vanwege hun taakstelling. Het CAK hanteert hiervoor het “Need to know and least privileged” principe. Voor beide geldt dat het CAK verantwoordelijk is voor het regulier controleren, up-to-date en op peil houden van de persoonsgegevens en de beveiliging daaromtrent.

Bevoegdheden en middelen

Onderdeel van *integriteit en vertrouwelijkheid* voor het CAK is ook dat persoonsgegevens alleen aan bevoegde personen worden verstrekt of door bevoegde personen worden gewijzigd en dat het verstrekken/ontvangen van persoonsgegevens via beveiligde middelen verloopt. Dit ziet op de uitwisseling van gegevens met derden (o.a. ketenpartners, klanten of wettelijke vertegenwoordigers van klanten). In de bijlage is inzake vertegenwoordiging een overzicht gegeven. Ook het onderling intern verstrekken van persoonsgegevens moet op basis van het *need to know* principe zijn, namelijk alleen als het strikt noodzakelijk is voor de uitvoering van de werkzaamheden. Als het beoogde doel ook zonder verstrekking van persoonsgegevens bereikt kan worden, dan moet de medewerker daar naar handelen. Zo ook als een andere wijze van verstrekken betrouwbaarder is dan dient de medewerker dat middel te gebruiken.

---

[21] Naar aanleiding van het onderzoek door de AP bij de Nederlandse Zorgautoriteit (rapport AP d.d. 13 april 2016, kenmerk: z2015-00355) inzake het verstrekken van weliswaar pseudonimiseerde gegevens vanuit het Diagnose Informatie Systeem (DIS) heeft de AP dit verboden omdat het gaat om bijzondere persoonsgegevens die niet onomkeerbaar geanonimiseerd zijn. Hieraan is het beleid ontleent dat pseudonimisering niet geschikt is voor de verwerkingen die het CAK doet.

[22] Artikel 5, lid 1, onderdeel f, AVG.

Wat betreft middelen moet het CAK ervoor zorgen dat de technische middelen die gekozen worden voldoende beveiligd zijn in relatie tot de te verwerken persoonsgegevens. Dit raakt niet alleen de grootschalige geautomatiseerde bestandsverwerkingen, maar ook de verwerkingen die gaan via portalen, e-mail (Outlook of web-based[23]), cd-rom, USB's etc. Het CAK-beleid is dat externe gegevensdragers niet gebruikt mogen worden in relatie tot persoonsgegevens. Het verwerken van persoonsgegevens met -mail (bijvoorbeeld met Transport Layer Security (TLS)) kan uitsluitend via een beveiligde methode goedgekeurd door de CISO. Als er getwijfeld wordt over de betrouwbaarheid van een emailbericht dan kan dit gemeld worden via de CAK Self Service Portal. Klik in de portal op 'ICT', ga dan naar 'Informatie Beveiliging' en klik op 'Verdachte mail ontvangen'. De opgeslagen mail kun je aan de melding toevoegen.

Voor portalen geldt dat beveiligingscertificaten en inlogmethoden moeten voldoen aan de standaarden van het forum standaardisatie van de Rijksoverheid[24].

De taken en verantwoordelijkheden ten aanzien van privacy zijn vastgelegd in een RASCI matrix die als bijlage bij dit beleid is gevoegd. In deze matrix zijn ook de onderlinge relaties tussen de verschillende verantwoordelijken en verwerkers inzichtelijk gemaakt

4.8. 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).[25] Daarnaast betreft dit ook het vaststellen hoe lang de gegevens bewaard moeten blijven. De bewaartijden zijn vastgelegd in het register van verwerkingen en zijn in lijn gebracht met de bewaartijden welke zijn opgenomen in de selectielijsten[26].

4.9. Verantwoordingsplicht

In de vorige paragrafen zijn diverse beginselen behandeld. Duidelijk is dat voor de naleving 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. Dit hangt ook nadrukkelijk samen met het transparantiebeginsel. Het CAK moet ook zorgdragen voor handhaving om correcte naleving.

In het volgende hoofdstuk worden specifieke onderwerpen in relatie tot de AVG behandeld.

---

[23] Zoals gmail, hotmail en vergelijkbaar. Maar ook ons eigen contactformulier.

[24] https://www.forumstandaardisatie.nl/open-standaarden

[25] Artikel 5, lid 1, onderdeel e, AVG.

[26] De selectielijsten bevatten beschrijvingen van informatieobjecten en hun bewaartijden op grond van de archiefwet. Dit hoeven niet perse persoonsgegevens te zijn.

5. AVG-beleid

In de AVG zijn een aantal concrete materiële onderdelen beschreven waarmee op een bepaald niveau invulling wordt gegeven aan de beginselen. Achtereenvolgens komen rechten van betrokkene, het verwerkingenregister, de verwerkersovereenkomsten, de datalekken, de Data Protectie Impact Analyse (DPIA)[27], privacy by design en default, gedragscodes en certificering en doorgifte van gegevens binnen/buiten de EU aan bod.

5.1. Rechten van betrokkene

De AVG geeft de burger van wie persoonsgegevens worden verwerkt een aantal rechten. Een aantal hiervan zijn in het vorige hoofdstuk al gepasseerd. Voor de volledigheid gaat het om de volgende rechten:

1. Recht op informatie (Artikel 12-14 AVG)
2. Recht op inzage (Artikel 15 AVG);
3. Recht op rectificatie en aanvulling (Artikel 16 AVG);
4. Recht op vergetelheid (Artikel 17 AVG);
5. Recht op beperking van de verwerking (Artikel 18 AVG)
6. Recht op dataportabiliteit (Artikel 20 AVG);
7. Recht om bezwaar te maken (Artikel 21 AVG);
8. Recht op een menselijk blik bij geautomatiseerde besluiten (Artikel 22 AVG);

Al deze rechten zijn niet absoluut. Dit betekent dat om diverse redenen het CAK hier niet altijd rekening mee hoeft te houden. Het CAK faciliteert de betrokkene door op de website uitleg te geven over de procedures en via welke kanalen het verzoek ingediend kan worden. Van belang is dat het CAK de identiteit van de indiener kan vaststellen. De termijn om aan een verzoek van de betrokkene te voldoen is één maand. Als het CAK meer tijd nodig heeft dan kan de termijn met nog twee maanden worden verlengd.[28]

Recht	Van toepassing op CAK?	Recht honoreren, tenzij
1	Ja	betrokkene reeds over de informatie beschikt
2	Ja	geen
3	Ja	betrokkene wordt geïnformeerd over de partijen waar een mededeling van correctie is gedaan.
4	Ja	het verwerken van de rechtmatig verkregen gegevens nog steeds nodig is voor de doeleinden én de bepaalde bewaartermijn[29] nog niet verstreken is.
5	Ja	het verwerken van de rechtmatig verkregen gegevens nog steeds nodig is voor de doeleinden én de bepaalde bewaartermijn nog niet verstreken is. Zie voor de gronden om beperking toe te kennen par. 2.5.2.

[27] Gegevensbeschermingseffectsbeoordeling (GEB)

[28] Artikel 12, lid 3, AVG.

[29] Zoals opgenomen in de selectielijsten.

6	Ja	Dit geldt vooralsnog allen voor de HR-administratie. Niet voor de wettelijke taken.
7	Ja	de verwerking is gebaseerd op een wettelijke grondslag.
8	Ja	

Het overzicht laat zien dat een betrokkene die een recht inroept niet per definitie gelijk krijgt. Op het verzoek neemt het CAK een besluit waartegen bezwaar en beroep openstaat conform de Awb. Daarnaast kan de betrokkene rechtstreeks de AP benaderen om zijn rechten in te laten willigen door het CAK.

De verwerkingsverantwoordelijke reageert op de verzoeken 1 tot en met 8 schriftelijk, telefonisch of elektronisch (email) of middels andere middelen. Indien betrokkene de verzoeken elektronisch bij het CAK indient zal het CAK ook elektronisch reageren De identiteit van de betrokkene wordt conform de bestaande CAK privacy matrix gecontroleerd[30].

Uiteraard kan de betrokkene ook de FG benaderen met klachten of vragen over de gegevensverwerkingen via fg@hetcak.nl. Het CAK-beleid is dat de klachten en bezwaren door de uitvoerende afdelingen zo nodig afgehandeld worden in afstemming met de FG.

5.2. Verwerkingenregister

De AVG vereist dat het CAK een schriftelijk register bijhoudt van de gegevensverwerkingen. Dit mag ook digitaal zijn, zolang het in tekstuele vorm is. Het CAK is verplicht passende en effectieve maatregelen te treffen om te zorgen dat we in lijn met de AVG werken en vervolgens moet het CAK zich daarover kunnen verantwoorden. De aantoonbaarheid begint met het verwerkingenregister. Dit register wordt steeds bijgewerkt als de gegevensverwerking wijzigt of als er sprake is van een nieuwe verwerking.
In artikel 30 van de AVG is duidelijk benoemd wat er in het register opgenomen moet worden[31]. Uiteraard is het register er niet om de persoonsgegevens zelf in op te nemen. Het gaat om een beschrijving van de verwerkingsactiviteiten.

Van belang is dat te allen tijde een bijgewerkt en op te vragen verwerkingenregister beschikbaar is. Indien wijzigingen plaatsvinden in het register dan wordt de eerdere verwerkingsactiviteit gearchiveerd met een einddatum. Het CAK stelt procedureel vast wie verantwoordelijk is voor het bijwerken en hoe controles daarop plaatsvinden. Een kopie van het register is door elke medewerker in te zien. Als de AP het register opvraagt, moet het CAK deze verstrekken. Het verstrekken van het verwerkingenregister aan derden is voorbehouden aan de FG.

5.3. Verwerkersovereenkomsten

De AVG maakt onderscheid in (gezamenlijke) verwerkersverantwoordelijke(n), verwerker(s) en sub-verwerker(s) en ontvanger(s). Het CAK is als uitvoerder van diverse wettelijke regelingen veelal de (gezamenlijke) verwerkingsverantwoordelijke. Het verschil is van belang omdat de laatstgenoemde verantwoordelijk is voor het naleven van de AVG. Om ervoor te zorgen dat het CAK dit ook richting zijn verwerkers borgt, schrijft de AVG voor dat afspraken onderling met een verwerkersovereenkomst worden vastgelegd. Hiermee wordt ondervangen dat het CAK enkel een beroep doet op verwerkers die afdoende

[30] Deze is gepubliceerd op de Dwo van Privacy en Security.

[31] Zie bijlage 5: Verplichte inhoud van het verwerkingenregister.

garanties bieden voor de AVG. Het CAK gebruikt hiervoor het ARVODI/ARBIT Rijksmodel verwerkersovereenkomst. Als de verwerker zelf weer een verwerker wil inschakelen (sub-verwerker) dan kan dit alleen met goedkeuring vooraf van het CAK.

In geval het CAK samen met een derde verwerkingsverantwoordelijke is, dan dragen beide partijen de verantwoordelijkheid om de AVG na te leven. Om de verantwoordelijkheden en verhoudingen tussen het CAK en een medeverantwoordelijke ten aanzien van privacy vast te leggen, wordt dit gedocumenteerd in een afsprakendocumenten (convenant o.i.d.). Hierbij wordt de verwerkersovereenkomst als uitgangspunt gebruikt.

Na het sluiten van de verwerkersovereenkomsten dient geborgd te worden dat het CAK periodiek toetst of de verwerker nog steeds voldoet aan de eisen zoals afgesproken. De bevoegdheid tot ondertekening van de verwerkersovereenkomsten is geregeld in het Besluit mandaat, volmacht en machtiging CAK.

De Verwerkersovereenkomst of de rechtshandeling is in schriftelijke vorm, waaronder elektronische vorm, opgesteld.

5.4. Datalekken

Het CAK is verantwoordelijk om passende technische en organisatorische maatregelen te treffen ter beveiliging van de persoonsgegevens die het CAK onder zich heeft. Het benodigde beveiligingsniveau is afhankelijk van de soort gegevens en het risico dat hiermee gepaard gaat. Als het dan toch misgaat dan moet het CAK binnen 72 uur na ontdekking van een datalek dit melden via het meldloket van de AP.[32] Niet melden is alleen aan de orde als onwaarschijnlijk is dat het lek een risico met zich mee brengt op inbreuken voor de rechten en vrijheden van de betrokkene.[33] Het interne melden van een datalek is een verantwoordelijkheid van elke medewerker (intern en extern) van het CAK. Het melden bij de AP wordt door de datalekkenmanager gedaan. De datalekkenmanager is de contactpersoon als de AP het CAK contacteert inzake een melding.

Als het datalek een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkene dan kan het zijn dat ook de betrokkene direct geïnformeerd moet worden.[34] Dit zal doorgaans via een brief gedaan worden en daarin worden de omschrijving en risico's van het datalek, de maatregelen die genomen worden of zijn en de contactgegevens van de FG opgenomen. De melding blijft achterwege als de maatregelen zodanig zijn dat de persoonsgegevens die met het datalek gemoeid zijn niet meer toegankelijk/begrijpelijk zijn voor onbevoegden, het hoge risico zich niet meer voor zal doen of de mededeling onevenredige inspanningen van het CAK vergt. In dat laatste geval kan een melding op de website (in algemene bewoordingen) volstaan. Bijvoorbeeld: als veel klanten tegelijk geraakt zijn door hetzelfde datalek met dezelfde risico's.

Om dit proces op juiste wijze te borgen heeft het CAK het "Protocol afhandelen datalekken" vastgesteld. De datalekken worden in een register geadministreerd en maandelijks gepubliceerd op de Dwo van Privacy en Security.

---

[32] https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

[33] In de bijlage is een stroomschema van de AP opgenomen.

[34] In de bijlage is een stroomschema van de AP opgenomen.

Wat is een datalek?

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij het CAK, zonder dat dit de bedoeling is van het CAK. Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat er geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarin persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben. [35]

5.5. Data Protection Impact Analyses (DPIA)[36]

Om in een vroeg stadium de privacy risico's in kaart te hebben, schrijft de AVG voor dat het CAK een beoordeling uitvoert om de effecten van de beoogde verwerkingsactiviteiten (of gewijzigde) in kaart te brengen.[37] De FG heeft hierbij een adviserende rol. In de regel geldt dat het CAK te allen tijde een DPIA (ook wel PIA genoemd) uitvoert, omdat het veelal zal gaan om het op grote schaal verwerken van (bijzondere) persoonsgegevens of monitoring, profilering ter besluitvorming, combineren van persoonsgegevens, nieuwe technologische toepassingen in een geautomatiseerde setting met hoog risico.

Nu geeft de AVG de mogelijkheid om af te zien van de DPIA als de verwerking gebaseerd is op een wettelijke plicht of een taak van algemeen belang/publieke taak en zijn grondslag vindt in Unierecht of nationale wetgeving. Dan moet bij het vaststellen van de rechtsgrond door de wetgever wel een DPIA zijn uitgevoerd. Het CAK-beleid is om te allen tijde een DPIA uit te voeren, aangezien de wetgever niet alle uitvoeringsconsequenties kan overzien.

Voor de GEB gelden de volgende kaders:

1. Een DPIA vindt plaats voordat met de betreffende verwerking wordt gestart.
2. Een DPIA wordt na uiterlijk drie jaar herhaald ter evaluatie.
3. Bij het uitvoeren van een DPIA wordt de FG altijd geïnformeerd en gevraagd om advies.
4. De business neemt de maatregelen die volgens de DPIA nodig zijn om de risico's te verkleinen.
5. Het resultaat van de DPIA en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het verwerkingenregister.
6. Indien de business niet in staat is om voldoende maatregelen te treffen om de risico's te beperken, wordt via de FG de AP vooraf geraadpleegd. Zonder positief advies mag het CAK de verwerking niet uitvoeren.[38]
7. DPIA's die binnen het CAK worden uitgevoerd volgen het Rijksmodel.

Overgangsregeling

Voor verwerkingen met een hoog privacy risico die vóór 25 mei 2018 al bestonden, is een GEB na deze datum verplicht indien:

1. de verwerking verandert, bijvoorbeeld door nieuwe technologie of wijziging van doel;
2. het risico verandert;

---

[35] In de bijlage is een stroomschema van de AP opgenomen.

[36] Tegenwoordig wordt meestal weer de oude term, Privacy Impact Assessment (PIA) gebruikt.

[37] Artikel 35 AVG.

[38] Artikel 36 AVG.

3. de omgeving verandert, bijvoorbeeld door maatschappelijke veranderingen.

Het CAK-beleid is om van alle verwerkingen uiterlijk na drie jaar de DPIA uit te voeren of te herhalen ter evaluatie, waardoor binnen deze termijn alle verwerkingen met een hoog privacy-risico aan een DPIA zijn onderworpen.

Het CAK hoeft niet voor elke verwerking afzonderlijk een DPIA uit te voeren. Als de verwerkingen vergelijkbaar zijn en de risico's ook dan is één DPIA voldoende. In de DPIA wordt gemotiveerd aangegeven waarom dit dan zo is. Er is een register waarin de DPIA's worden geadministreerd.

5.6. Privacy by design en default

Privacy by design omvat twee uitgangspunten:
- Verstandig gebruik van persoonsgegevens
- Passende bescherming van persoonsgegevens

Dit betekent dat bij het ontwerpen van producten en/of diensten, het inkopen van systemen en bij de uitvoering van werkzaamheden het CAK de volgende uitganspunten hanteert:

Verstandig gebruik van persoonsgegevens:
- Er worden niet meer gegevens verzameld (uitgevraagd) dan noodzakelijk of juridisch mogelijk.
- Gegevens worden alleen gebruikt waarvoor ze zijn gevraagd.
- Voorkomen wordt dat te veel gegevens worden ontvangen.
- Bij configuratie van systemen wordt altijd voor de privacy vriendelijke variant gekozen (privacy by default).
- De informatie die wij verwerken is correct en up to date.
- Er worden geen onnodige kopieën gemaakt.
- Wat niet meer nodig is, wordt verwijderd. Daarin moet worden voorzien.

Passende bescherming:
- Gegevens worden zo opgeslagen dat voldaan kan worden aan wettelijke kaders van de AVG. Dit betekent vaak gescheiden opslag van verschillende data.
- Toegang tot gegevens is beperkt tot degenen die dit vanuit hun functie nodig hebben (autorisaties).
- Aggregeer gegevens – indien mogelijk – zodat ze niet herleidbaar zijn.
- Logs, audits en rapportages vergroten de aantoonbaarheid.

Als uitgangspunt kiest het CAK voor technische maatregelen om privacy by design te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, wordt gezocht naar organisatorische maatregelen als alternatief voor of als aanvulling op de technische maatregelen.

5.7. Gedragscodes en certificering

In de AVG is de aantoonbaarheid van het voldoen aan de AVG een belangrijke pijler en beginsel (verantwoordingsplicht). Tegelijk biedt de AVG ook handvatten om de aantoonbaarheid te vergroten. Het gaat hierbij dan om het gebruik van gedragscodes[39] en certificering[40]. De AVG moedigt het gebruik hiervan aan.

Gedragscodes

In de Wbp bestonden ook al artikelen die gedragscodes onderschreven. Gedragscodes zijn bedoeld om in samenwerking met andere (gelijksoortige) organisaties (in een branche/sector) tot een concretisering van de AVG te komen, zodat dit kan bijdragen in de juiste toepassing ervan. Op dit moment is er geen algehele gedragscode AVG voor de overheid, maar mocht deze in toekomst er komen dan kan het CAK zich daarbij aansluiten. Het is wel van belang om aan te sluiten bij een gedragscode die door de AP is geaccordeerd en gepubliceerd.[41]

Certificering

Ten opzichte van de Wbp is in de AVG-certificering nieuw. Hiermee kan een organisatie aantonen dat het voldoet aan de AVG. De AP geeft geen certificaten uit. De AP is alleen betrokken bij de beoordeling tot accreditatie. In Nederland is de Raad voor Accreditatie (RvA) aangewezen om te accrediteren en zo dus ook voor de AVG-certificaten. Zij kunnen een organisatie accrediteren om AVG-certificaten uit te geven. Op dit moment zijn er nog geen instellingen geaccrediteerd. Als het zover is dan kan het CAK bij die instelling een certificering aanvragen. Na toekenning betekent dit echter niet dat we hiermee per definitie altijd voldoen aan de AVG. Het ontslaat het CAK niet van de plicht om voortdurend te monitoren of nog steeds aan de AVG wordt voldaan. De certificering is derhalve een momentopname.

5.8. Doorgifte binnen en buiten de EU

Als het CAK vanuit zijn wettelijke taak gegevens moet doorleveren aan andere landen dan wordt voor de AVG onderscheid gemaakt in landen die tot de Economische Europese Ruimte (EER) behoren (EU-landen + Noorwegen, Liechtenstein en IJsland) en daarbuiten. Binnen de EER geldt dat de doorgifte mag zolang wordt voldaan aan de AVG. Doorgifte betekent gegevens sturen of toegang bieden tot de gegevens.

Voor buiten de EER is een adequaatheidsbesluit[42] van de EU-commissie (EC) nodig of als dit er niet is, moeten in (bilaterale) overeenkomsten adequate waarborgen opgenomen worden[43]. Denk hierbij bijvoorbeeld aan Zwitserland. Aangezien ‘het buitenland’ een eigen dynamiek kent, ligt vastleggen van waarborgen grotendeels buiten de invloedssfeer van het CAK. Het CAK zet zich in om waar mogelijk voldoende passende privacy afspraken vast te leggen.

De EC of de AP kunnen standaard contractbepalingen beschikbaar stellen die dan overgenomen kunnen worden. Voor bestaande contracten is van belang dat waar mogelijk aanvullende privacy afspraken

---

[39] Artikel 40 AVG.

[40] Artikel 42 AVG.

[41] Zie https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-gedragscode voor de procedure. Zie als voorbeeld https://wetten.overheid.nl/BWBR0033201/2010-04-26 voor de gedragscode voor financiële instellingen.

[42] Artikel 45 AVG.

[43] Artikel 46 AVG.

worden overeengekomen dan wel bij verlenging privacy bepalingen worden opgenomen. De landen waarvoor adequaatheid besluiten beschikbaar zijn, zijn te raadplegen via de website van de EC.[44]

De mogelijkheden van gedragscodes en certificering[45] of bindende bedrijfsvoorschriften[46] worden voor hier in dit kader buiten beschouwing gelaten. In ieder geval kan in een aantal specifieke situaties toch doorgifte van de persoonsgegevens plaatsvinden. Voor zover relevant voor het CAK zijn dat:

- Doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen.
- Doorgifte is noodzakelijk voor de sluiting of de uitvoering van een overeenkomst in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke of rechtspersoon.
- Doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang.
- Doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
- Doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven.
- Doorgifte is verricht vanuit een bij wet ingesteld register dat bedoeld is om het publiek voor te lichten.

Als op grond hiervan geen doorgifte van gegevens mogelijk is, dan geeft de AVG in artikel 49 nog opties. Doorgifte kan dan alsnog:

- als de gegevens niet herhaaldelijk worden doorgegeven;
- als het slechts om een beperkt aantal betrokkenen gaat;
- als het noodzakelijk is voor de dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke, die niet ondergeschikt zijn aan de belangen, rechten en vrijheden van de betrokkene; en
- wanneer passende waarborgen zijn getroffen.

In dit geval moeten ook de AP en betrokkene geïnformeerd worden.
Doorgifte kan worden beperkt als in de wet- en regelgeving of bepalingen om gewichtige redenen van openbaar belang uitdrukkelijk grenzen worden gesteld aan de doorgifte van specifieke categorieën van persoonsgegevens aan een derde land of een internationale organisatie.

Ten aanzien van de doorgifte van bijzondere persoonsgegevens binnen en buiten de EU geldt dat is verboden, behoudens de volgende uitzonderingen:

a) dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting;
b) de gegevens worden verwerkt door de Autoriteit Persoonsgegevens of een ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht en dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, voor de uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is

---

[44] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_nl#dataprotectionincountriesoutsidetheeu

[45] Artikel 46 AVG.

[46] Artikel 47 AVG.

voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad, of:
c) dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en de Autoriteit Persoonsgegevens ontheffing heeft verleend.

Het CAK verwerkt in de basis persoonsgegevens binnen de EER, ten behoeve van de uitvoer van haar taken. Daarnaast worden er persoonsgegevens verwerkt in landen buiten de EER vanwege ICT-systemen. Dit gebeurt zo min mogelijk. En alleen als er een transfermechanisme is en we hebben beoordeeld dat de doorgifte past binnen de wet- en regelgeving.

5.9. CAK toets kader: NOREA

Het CAK gebruikt een extern erkend toets kader voor de AVG: het Privacy Control Framework (hierna: ‘PCF’) dat is ontwikkeld door NOREA (de Nederlandse beroepsorganisatie van gekwalificeerde IT-auditors / Nederlandse Orde van Register EDP-auditors) NOREA

Het primaire doel van het PCF is het bieden van ondersteuning aan (audit)professionals bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald. Het PCF kan worden gebruikt als startpunt voor privacy audits op maat. Het PCF bevat de voorgeschreven beheersingsdoelstellingen en voorbeelden van maatregelen voor privacy opdrachten op basis van de NOREA Richtlijn 3000.
Het PCF kan daarnaast door entiteiten worden gebruikt om vast te stellen of de maatregelen ten aanzien van privacybescherming adequaat zijn, of om te bepalen in hoeverre de huidige maatregelen dienen te worden aangepast om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG).

6. Ethisch databeleid en algorithmen.

Het gebruik van persoonsgegevens gaat niet alleen over wat wettelijk mag, maar ook over wat vanuit ethisch oogpunt wenselijk is.

Het gebruik van algoritmen speelt een steeds grotere rol bij het uitvoeren van data analyses. Het toepassen van algorithmen biedt grote kansen m.b.t. het verbeteren van de dienstverlening van het CAK. Daarnaast levert gebruik van algorithmen een steeds groter rsico op voor de privacy van onze klanten. Indien onzorgvuldig ontworpen en toegepast kan de impact op de privacy van onze klanten onbedoeld groot zijn. Voor het gebruik van algorithmen volgt het CAK de “Richtlijn algorithmen” opgesteld t.b.v. de toepassing van algorithmen door de Rijksoverheid. Deze richtlijn ziet toe op ontwikkeling en operationele inzet van algorithmen. De richtlijn is vooral gericht op de transparantie en daarmee de uitlegbaarheid van algoritmen, de werking en toepassing daarvan, bedoeld om het inzicht te vergroten alsmede de kwaliteit en betrouwbaarheid van algoritmen te verbeteren. Hiertoe bevat de richtlijn vereisten met betrekking tot:

1. Bewustzijn risico’s;
2. Transparantie & Uitlegbaarheid;
3. Gegevensherkenning;
4. Auditeerbaarheid;
5. Verantwoording;
6. Validatie;
7. Toetsbaarheid;

8. Publieksvoorlichting.

7. Bijlagen

Bijlage 1: Stakeholders intern/ extern

Ter uitvoering van de privacywetgeving zijn er diverse personen/partijen die een rol spelen bij het CAK. Dit worden de stakeholders genoemd. Elke stakeholder heeft een rol met daarbij behorende verantwoordelijkheden. In dit hoofdstuk zijn de interne en externe stakeholders benoemd en welke verantwoordelijken zij hebben. De AVG kent een aantal formele rollen die expliciet zijn benoemd.

1. Verwerkingsverantwoordelijke

Het CAK is de verwerkingsverantwoordelijke en wordt in dezen vertegenwoordigd door de Raad van Bestuur (RvB). Zij dragen een gezamenlijke verantwoordelijkheid voor de naleving van privacy. De RvB bestaat uit drie leden, namelijk de voorzitter/CEO (Chief Executive Officer) en twee andere bestuurders de CFO (Chief Financial Officer) en de COO (Chief Operating Officer).
Intern zijn de afdelingsmanagers (AFDELINGSMANAGERS) verantwoordelijk voor de onder hun regie uitgevoerde verwerkingen.

2. Management en regelingseigenaren

Binnen de clusters zijn de leden van het MT-CAK eindverantwoordelijk voor de naleving van de privacy wetgeving en het uitvoeren van het privacy beleid.
De leden van het MT-CAK leggen verantwoording af aan de raad van Bestuur. De leden van het MT-CAK hebben samen met hun afdelingsmanagers en ook teammanagers een gezamenlijke verantwoordelijkheid in het naleven van de AVG. In de maandrapportage wordt aandacht besteed aan privacy gerelateerde onderwerpen/incidenten. De RvB en de FG worden hierover geïnformeerd.

3. Privacy deskundigen

De regelingen zijn verantwoordelijk voor de eerstelijnstaken m.b.t. privacy. Elke regeling stelt hiertoe per cluster minimaal 1 privacy deskundige aan welke deelneemt aan het privacy gilde.
De belangrijkste taken zijn:

- onderhouden van het register van verwerkingen;
- uitvoeren PIA's, onderhouden PIA register;
- leveren van input t.b.v. EPIC-architecturen;
- creëren van awareness in het cluster.

4. Functionaris Gegevensbescherming (FG)

De AP heeft in het document "Guide Lines FG[47]" o.a. de belangrijkste taken van de FG vastgelegd.

De belangrijkste taken zijn:

- controle op naleving van de AVG.

Activiteiten in dit kader zijn:

- informatie (doen) verzamelen om verwerkingsactiviteiten te identificeren;

[47] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243rev01_nl.pdf

- de naleving van verwerkingsactiviteiten analyseren en controleren;
- de verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen.

- de verwerkingsverantwoordelijke adviseren over het uitvoeren van DPIA's[48];
- samenwerken met de AP en dienen als contactpunt;
- periodiek rapporteren over de status van compliance met de AVG.

Op grond van artikel 37 van de AVG is het CAK gehouden om een FG in te stellen. De FG heeft binnen het CAK een aantal taken. Intern moet de FG toezien op naleving van de AVG en extern is de FG verantwoordelijk voor de samenwerking en de communicatie met de AP[49]. Verder vervult de FG een informerende en adviserende rol binnen de organisatie.[50] De organisatie moet de FG naar behoren en tijdig betrekken als het privacy betreft en hem ondersteunen om de toebedeelde taken aan de FG uit te kunnen voeren (algemene zorgplicht). De FG moet onafhankelijk (zonder instructies) functioneren en doet verslag aan de Voorzitter van de RvB.[51] De FG mag ook nog een andere functie vervullen, echter belangenverstrengeling moet voorkomen worden. Richting de burgers dient de FG als contactpersoon waarbij zij de FG kunnen contacteren voor alle zaken die de verwerking van persoonsgegevens aangaat en de uitoefening van hun rechten. De FG is geen toezichthouder zoals bedoeld in de Awb, de taken en bevoegdheden volgen uit de AVG.

5. Coördinerend Privacy Officer

De Coördinerend Privacy Officer (CPO) is de link naar het lijnmanagement en ondersteunt de privacy deskundigen van de clusters bij organisatie-brede privacyvraagstukken. Verder is de CPO verantwoordelijk voor de algemene kennisoverdracht met betrekking tot privacy en het signaleren en implementeren van organisatie-brede privacyvraagstukken.
De CPO is als stafmedewerker ondergebracht bij de CIO-office.[52] Deze functie ondersteunt de verwerkingsverantwoordelijken middels beleid, preventie, voorlichting, scholing, incidentenaanpak en onderzoek.

Belangrijkste taken zijn:

- het samenwerken met de FG m.b.t. CAK brede privacyvraagstukken;
- het (doen) inrichten en onderhouden van de volgende registers:
  - Verwerkingenregister.
  - Register van uitgevoerde DPIA's.
  - Register van verwerkersovereenkomsten.
  - Functioneel aansturen van de privacy deskundigen in de clusters door het inrichten van een privacy gilde.

6. Corporate Information Security Officer (CISO)

[48] De verwerkingsverantwoordelijke is zelf verantwoordelijk voor het vragen van advies hierover aan de FG.

[49] Artikel 39 AVG.

[50] Bijvoorbeeld inzake de GEB (PIA).

[51] Artikel 38, lid 3, AVG.

[52] De huidige CISO vervult ook de functie van CPO.

Het CAK is verantwoordelijk om passende technische en organisatorische maatregelen te treffen ter beveiliging van de persoonsgegevens die het CAK onder zich heeft. Het CAK beschikt daarom over een Corporate Information Security Officer (CISO) die toeziet op naleving van het informatiebeveiligingsbeleid met betrekking tot alle (persoons)gegevens die het CAK verwerkt. De CISO valt onder de CIO-office.

7. Datalekkenmanager

Het CAK heeft ervoor gekozen een functionaris aan te stellen om het gehele proces rond het melden en afhandelen van datalekken te begeleiden. De datalekkenmanager is gepositioneerd binnen regie Regelingen.
Belangrijkste taken: melden van datalekken bij de AP;
Monitoren van de afhandeling van de datalekken;
Opstellen van periodieke rapportages;
Bijhouden van het datalekkenregister.

8. Autoriteit Persoonsgegevens (AP)

Elke EU-lidstaat moet minstens één onafhankelijke overheidsinstantie aanwijzen als toezichthouder van het naleven van de AVG.[53] In Nederland is het voormalig College Bescherming Persoonsgegevens (CBP) aangewezen als AP. Elk jaar moet de AP een jaarverslag uitbrengen van de uitgevoerde activiteiten. Dit verslag is openbaar en het betekent ook dat als er noemenswaardige incidenten zich voordoen met het CAK, ook wij als organisatie daarin genoemd kunnen worden. De taken en bevoegdheden van de AP zijn te vinden in de artikelen 57 en 58 AVG en afdeling 2 van de UAVG. In de kern komt het neer op toezicht, handhaving, advisering, voorlichting, informatieverstrekking en verantwoording en internationale taken. Voor het CAK zijn het toezicht en de handhaving de belangrijkste. In dat kader kan elke betrokkene een klacht indienen bij de AP.[54] Daarnaast geeft de AVG de AP de mogelijkheid tot het geven van geldboeten tot 20 miljoen. Dit is afhankelijk van de soort overtreding.[55]

9. Ministerie

Het eigenaarschap van het CAK ligt bij het Ministerie van Volksgezondheid, Welzijn en Sport (VWS). Het CAK moet gedurende het jaar VWS informeren over de stand van zaken bij het CAK en zo ook op het gebied van privacy. Zo heeft ook de FG contact met de FG van VWS en informatieverstrekking verloopt via maand-, kwartaal- of jaarrapportages (verantwoording).

[53] Artikelen 51 AVG en 6 UAVG.

[54] Artikel 77 AVG. Zie voor meer informatie https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-indienen-bij-de-ap

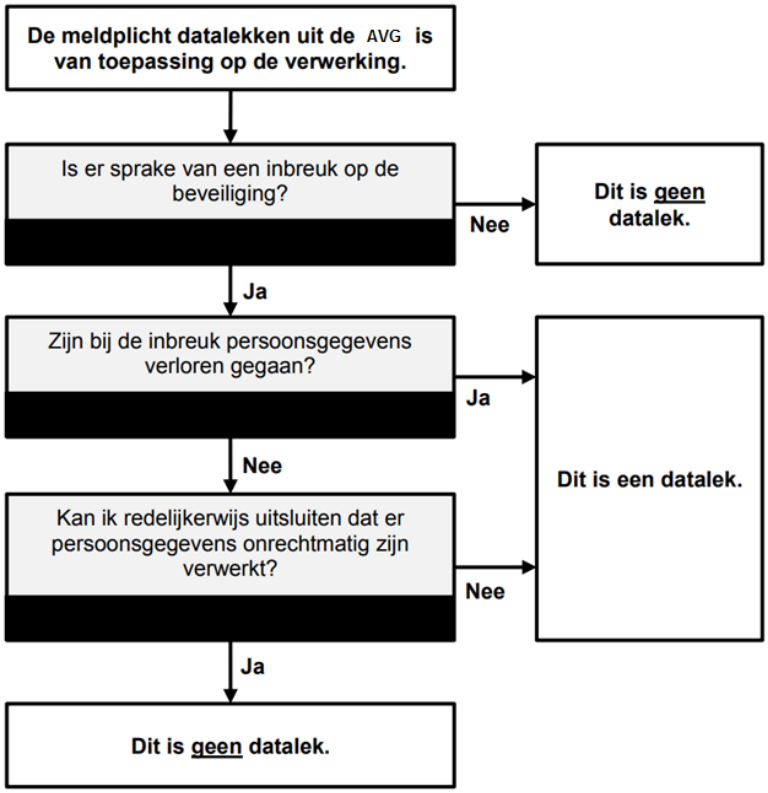
[55] Artikel 83 AVG

Bijlage 2: schema's

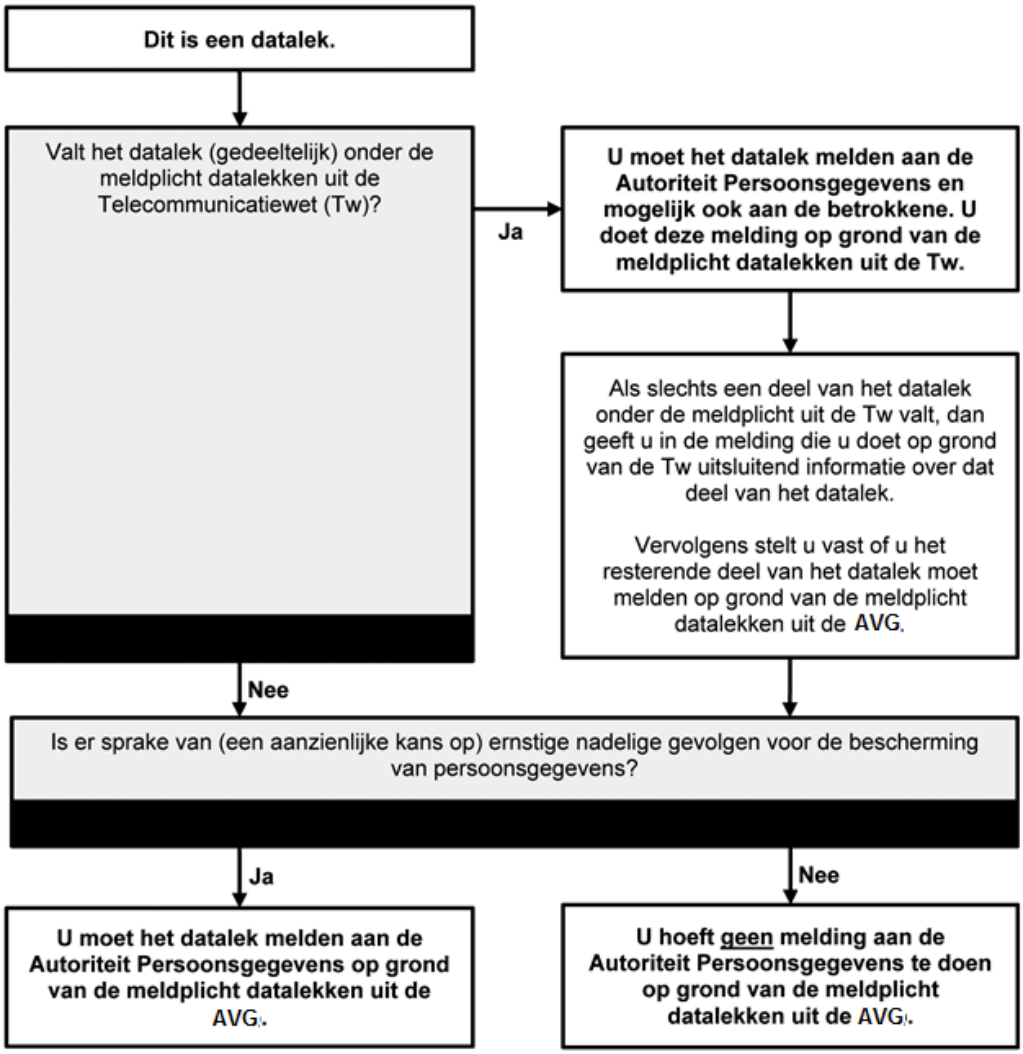
Deze bijlage bevat de volgende schema's:

1. Stroomschema datalek
2. Stroomschema meldplicht aan de AP
3. Stroomschema meldplicht aan de betrokkene

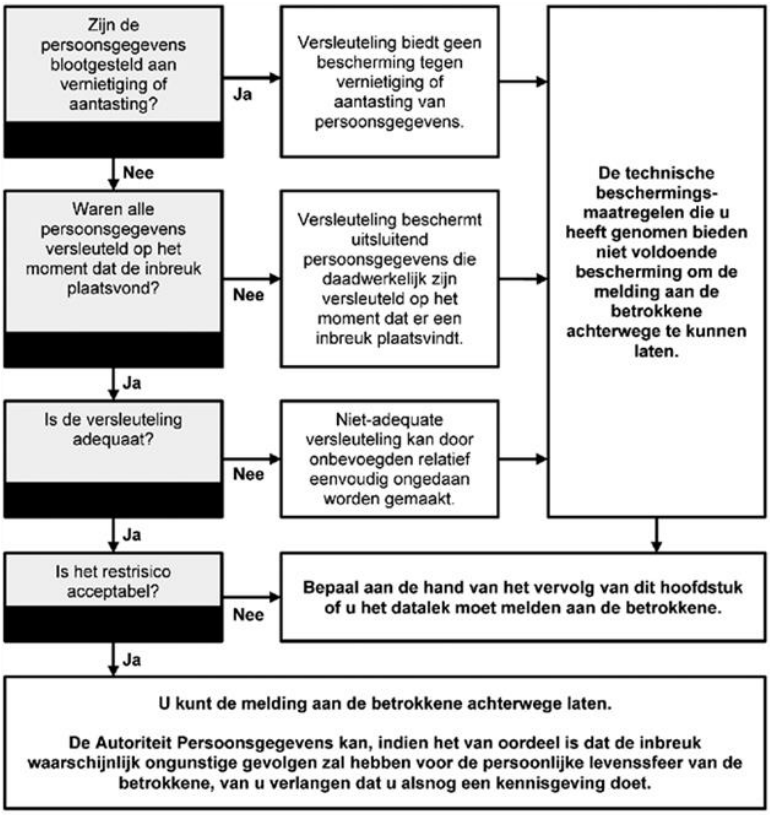
1. Stroomschema datalek



2. Stroomschema meldplicht aan de AP



3. Stroomschema meldplicht aan betrokkene



Bijlage 3: Schema vertegenwoordiging en bevoegdheden

	(Mutatie)verzoek	Curator	Beschermings-bewindvoerder[56]	Zaakwaar-nemer[57]	Erfgenamen	Budgetbeheerder	Mentor	Telefonisch[58]?
1	Aanvraag: bijv. peiljaarverlegging, verdragsbijdrage, subsidie, vrijstelling.	*Ja, raadpleeg register of uitspraak rechtbank*	*Ja, raadpleeg register of uitspraak rechtbank*	*Nee, tenzij gemachtigd*	*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*	*Nee, tenzij gemachtigd. Als gemachtigd dan gelden de regels van de zaakwaarnemer*	*Nee*
2	Openstaand saldo opvragen				*Ja*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Ja*
3	Rekeningnummer wijzigen				*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Nee*
4	AI activeren				*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Nee*
5	Adreswijziging correspondentieadres				*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Nee*
6	Bezwaar maken		*Ja, tenzij het geen financieel onderwerp betreft. Raadpleeg register of uitspraak rechtbank*		*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij gemachtigd*		*Nee*
7	Kopie beschikking aanvragen		*Ja, raadpleeg register of uitspraak rechtbank*		*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Ja*
8	Kopie factuur aanvragen				*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Ja*
9	Overlijden doorgeven				*Ja*	*Nee*		*Nee*
10	Aanvragen betalingsregeling				*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Ja*
11	Uitstel van betaling aanvragen		*Ja, raadpleeg register of uitspraak rechtbank*		*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij budgetovereenkomst dit regelt. Raadpleeg deze.*		*Ja*
12	Huishoudsamenstelling laten aanpassen		*Ja, raadpleeg register of uitspraak rechtbank* [59]		*Ja, mits bewijs van bevoegdheid aanwezig*	*Nee, tenzij gemachtigd*		*Ja*
13	Vragen over (ingediende) declaraties		*Ja, raadpleeg register of uitspraak rechtbank*		*Ja, mits bewijs van bevoegdheid aanwezig*	*n.v.t.*		*Ja*
14	Medicijnen mee op reis verklaring aanvragen	*Ja, wordt altijd gestuurd naar het adres van de aanvrager, tenzij er een begeleidend schrijven is met een ander adres*						*Nee*

[56] De WSNP-bewindvoerder valt hier niet onder, want die zorgt voor afwikkeling van het schuldsaneringstraject. Zijn opdracht is in die zin beperkt en de klant is zelf ook nog handelingsbevoegd. Daarom valt de WSNP-bewindvoerder onder zaakwaarnemer.

[57] Hieronder valt iedere persoon die niet de klant zelf is of onder één van de andere categorieën valt (zo dus ook familie van de klant)

[58] Indien ‘Ja’, dan dienen hiervoor ten minste twee controlevragen gesteld te worden, waarbij de vragen niet beantwoord kunnen worden vanuit een uiting die wij gestuurd hebben.

[59] Is veelal financieel gerelateerd. Bovendien is procedureel afgedekt dat er te allen tijde bewijsstukken nodig zijn, tenzij dit uit de BRP reeds blijkt dat de huishoudsamenstelling niet klopt.

Wat mag de klant nog zelf als de vertegenwoordiger bevoegd is?

Nr.	Curator	Beschermings-bewindvoerder	Zaakwaarnemer	Erfgenamen	Budgetbeheerder
	2, 6[60], 14	**2, 6[61], 7, 8, 12, 13, 14**	**1 t/m 4 6 t/m 14**	**n.v.t.**	**1 t/m 4 6 t/m 14**

Toelichting:

a. Als de klant zelf actie onderneemt, terwijl een derde ook nog bevoegd is, dan is het raadzaam om in geval van curator, (beschermings)bewindvoerder, zaakwaarnemer en budgetbeheerder de wijziging ook naar deze vier categorieën te bevestigen. Daarom is ervoor gekozen om adreswijziging niet toe te staan als één van deze categorieën actief is.

b. Daar waar mutatieverzoeken telefonisch kunnen worden ingediend, betekent dit uiteraard niet dat er geen bewijsstukken nodig zijn. Afhankelijk van het mutatieverzoek onderzoekt de medewerker aan de hand van registraties/ontvangen gegevens/bewijsstukken of de mutatie terecht is.

[60] Nee, tenzij de curator schriftelijk toestemming heeft gegeven aan de klant.

[61] Nee, tenzij de bewindvoerder schriftelijk toestemming heeft gegeven aan de klant.

Bijlage 4: RASCI matrix CAK AVG Versie 5.0 2023 (losse bijlage bij het Privacybeleid CAK).

Bijlage 5: verplichte inhoud verwerkingenregister

Artikel 30
EU-AVG
"Register van de verwerkingsactiviteiten"

=> Grond: 13, 39, 82
=> administrative fine: Art. 83 (4) lit a
1. Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:
=> Artikel: 4
a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
b) de verwerkingsdoeleinden;
c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

2. De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:
a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.
3. Het in de leden 1 en 2 bedoelde register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.
4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de toezichthoudende autoriteit.
5. De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 betreft.
=> Grond: 13