C/AK


# DATALEKKENRAPPORT Q1 2023

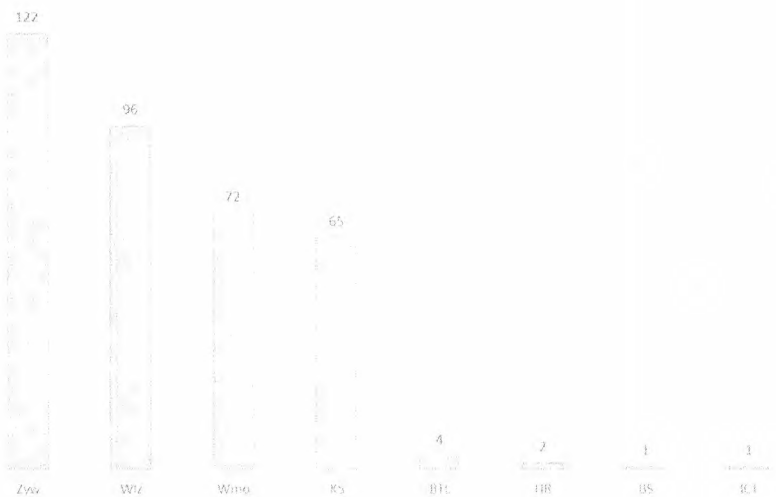
## Het CAK

C/ K

C/A K

# CIJFERS VASTGESTELDE DATALEKKEN

**Vastgestelde datalekken per cluster Q1 2023**




- Dit zijn de vastgestelde datalekken na analyse van de specialisten.
- Er zijn 386 datalekmeldingen in Topdesk ingediend, waarvan 376 daadwerkelijk als datalek zijn vastgesteld.
- Bij het cluster Zvw zijn de meeste datalekken vastgesteld.
- De hoge aantallen van KlantServices wordt voornamelijk veroorzaakt door geopende retourpost van alle regelingen.
- Vanaf 2023 zijn de aantallen geopende retourpost ook bij alle regelingen verwerkt.

C/ K

# CIJFERS GEMELDE DATALEKKEN AP

**Datalek gemeld naar de AP per cluster Q1 2023**


- Er zijn 295 datalekken bij de Autoriteit Persoonsgegevens gemeld.
- 1.369 betrokkenen zijn geïnformeerd.
- De regeling Zvw heeft 1.323 betrokkenen geïnformeerd.
- De meldingen naar de AP zijn lager dan de aantal geraakte personen, omdat sommige datalekken in bulk worden ingediend (retourpost, oud broninhoudersproblematiek).
- De AP is op de hoogte van de totaal aantal geraakte personen.

C/K

# CIJFERS GERAAKTE PERSONEN


- In dit grafiek staan de totaal aantal geraakte personen die bij een datalek zijn betrokken.
- Bij de Wmo is door een menselijke fout 4.253 betrokkenen geraakt.
- Bij de ICT is door een menselijke fout 1.623 betrokkenen geraakt.
- Het hoge aantal bij de ZvW wordt veroorzaakt door het oud broninhoudersproblematiek [redacted].
- Bij de EB regelingen liggen voornamelijk invoerfouten ten grondslag bij datalekken.

C/ K

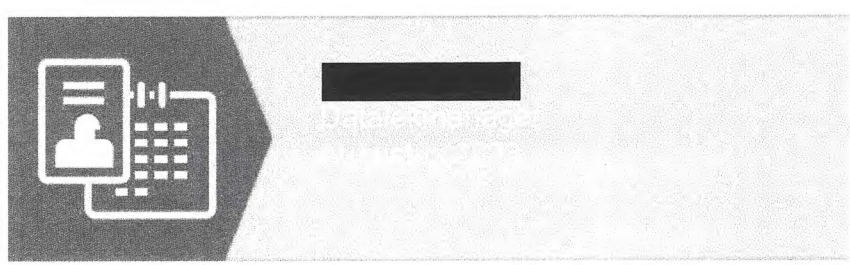
# CIJFERS OORZAKEN DATALEKKEN


- In dit grafiek staan de top 5 oorzaken naar aanleiding van een datalek.
- Momenteel vind geen analyse plaats bij geopende retourpost.
- Het BRP adres is niet actueel. De oorzaak is dat of het CAK onjuiste gegevens hebben of dat de betrokkene niet het juiste adres bij de gemeente heeft aangegeven.
- De technische oorzaak speelt zich voornamelijk af door het oud broninhoudersproblematiek.
- Bij de EB regelingen en Klantservices liggen voornamelijk invoerfouten ten grondslag aan datalekken.


# DATALEKKENRAPPORT Q2 2023

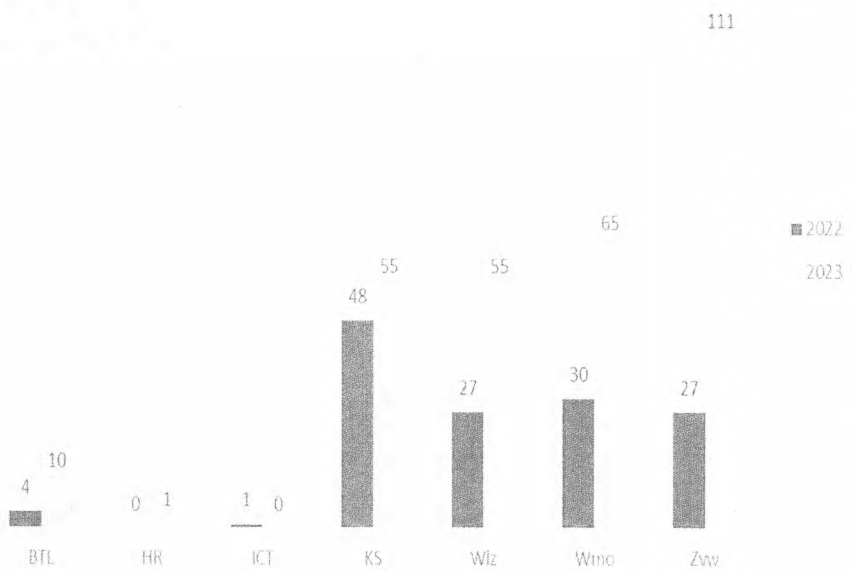
## Het CAK

C/AK



C/AK

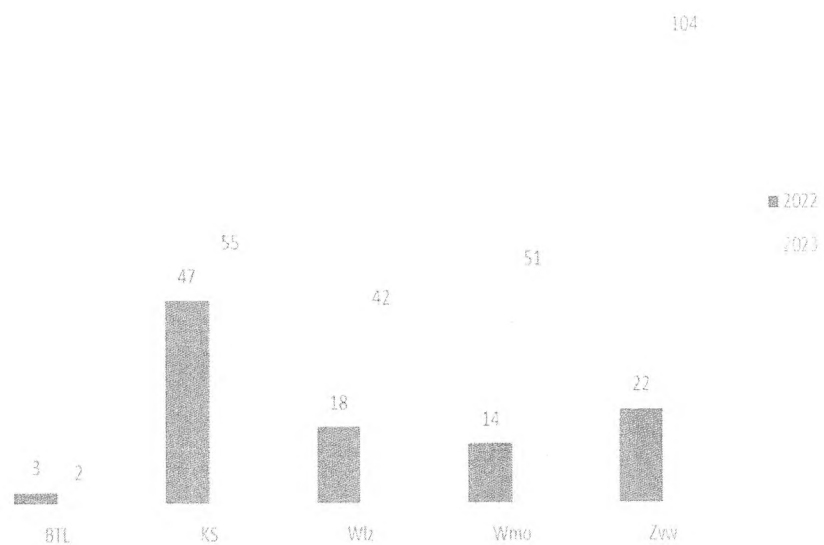
# CIJFERS VASTGESTELDE DATALEKKEN




- Vanaf 2023 zijn de aantallen geopende retourpost bij alle regelingen verwerkt. Hierdoor zijn de cijfers bij de regelingen hoger dan in 2022.
- In Q2 2023 zijn er 142 datalekmeldingen vastgesteld. Ten opzichte van 2022 is dit een stijging van 5 meldingen.
- Bij het cluster Zvw zijn de meeste datalekken vastgesteld. Oorzaak zit in correspondentie versturen naar oud broninhouders.
- De aantallen van Klantservices wordt veroorzaakt door geopende retourpost van alle regelingen.

C/ K

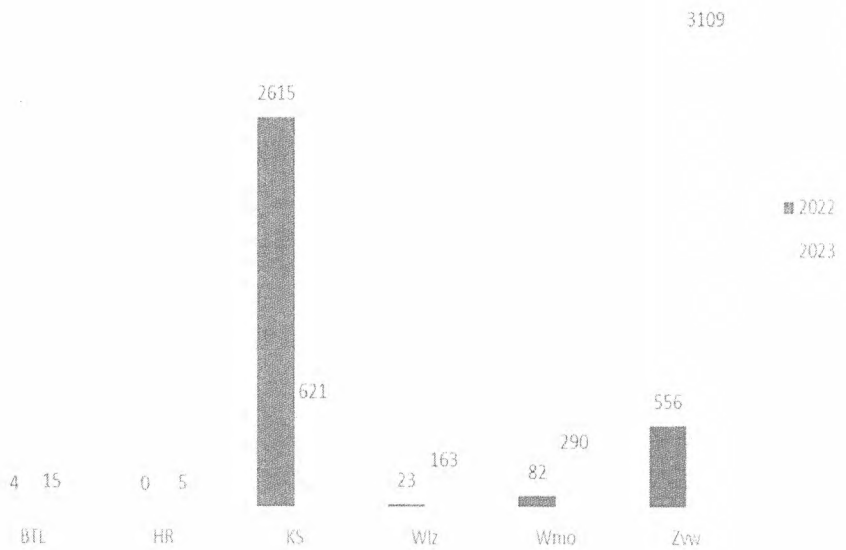
# CIJFERS GEMELDE DATALEKKEN AP




- In Q2 2023 zijn er 99 datalekken bij de Autoriteit Persoonsgegevens gemeld. In 2023 zijn de geopende retourpost bij alle regelingen opgeteld. Hierdoor liggen de cijfers ten opzichte van 2022 hoger.
- In totaal zijn er 1.057 betrokkenen zijn geïnformeerd.
- De meldingen naar de AP zijn lager dan de aantal geraakte klanten, omdat sommige datalekken in bulk worden ingediend (retourpost, oud broninhoudersproblematiek). In 2022 zijn er in totaal 445 betrokkenen geïnformeerd. Van invloed is de oorlog in Oekraïne geweest. De gevluchte personen kwamen in aanmerking voor de regeling Onverzekerden en hierdoor steeg de werkvoorraad dat voorrang had.
- De AP is op de hoogte van de totaal aantal geraakte klanten.

C/A K

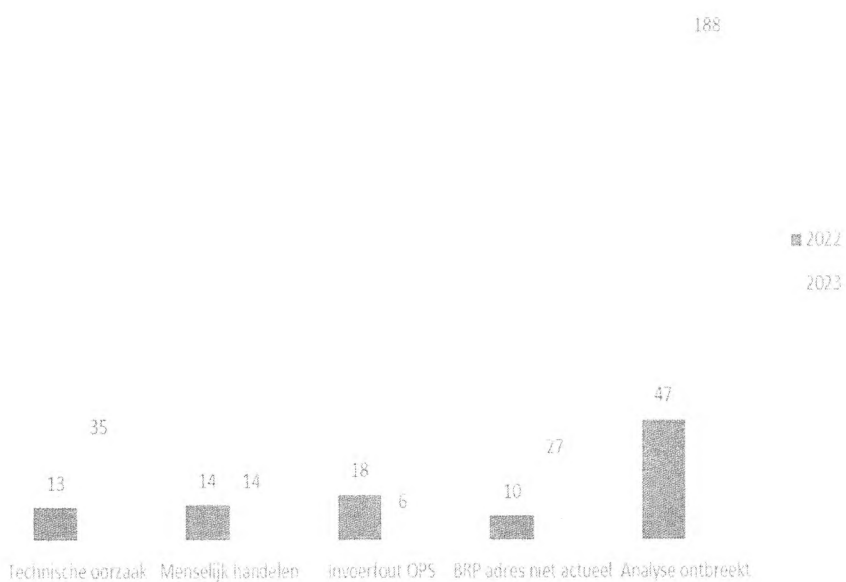
# CIJFERS GERAAKTE KLANTEN




- In dit grafiek staan de totaal aantal geraakte klanten die bij een datalek zijn betrokken.
- Te zien is dat er bij KS een daling van de geraakte klanten te zien. Dit heeft er mee te maken dat er geen groot incident is geweest. Hierdoor zijn er enkel geopende retourpost stukken als datalek geregistreerd.
- Het hoge aantal bij de ZvW wordt veroorzaakt door de oud broninhoudersproblematiek. Daarnaast is er een datalek gemeld waarbij onterecht persoonsgegevens in Azure DevOps worden opgeslagen dat niet de bedoeling is. Hiervoor loopt inmiddels een verbetertraject om alle persoonsgegevens voor de regeling ZvW in ADO te herkennen om ze vervolgens te verwijderen. Dit wordt als testcase gebruikt om het vervolgens voor alle clusters uit te rollen.

C/AK

# CIJFERS OORZAKEN DATALEKKEN

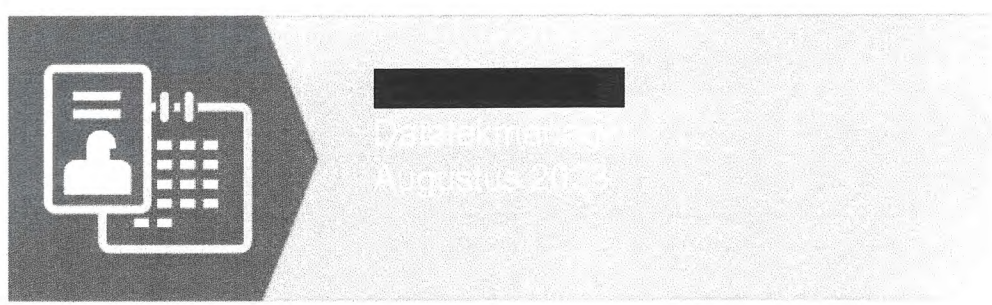



- In dit grafiek staan de top 5 meest voorkomende datalekken naar aanleiding van een melding.
- Geopende retourpost wordt het meest gemeld. Momenteel loopt er een CLV traject om het proces van geopende retourpost aan te passen.
- Het BRP adres is niet actueel. De oorzaak is dat of het CAK onjuiste gegevens heeft of dat de betrokkene niet het juiste adres bij de gemeente heeft aangegeven.
- De technische oorzaak speelt zich voornamelijk af bij het oud broninhoudersproblematiek.
- Om invoerfouten te verminderen wordt bewustwording verhoogd door het MT door toepassing van vier ogen principes. Daarnaast wordt zowel individueel en in teamoverleggen de oorzaken besproken, zodat medewerkers de best practices van elkaar leren.

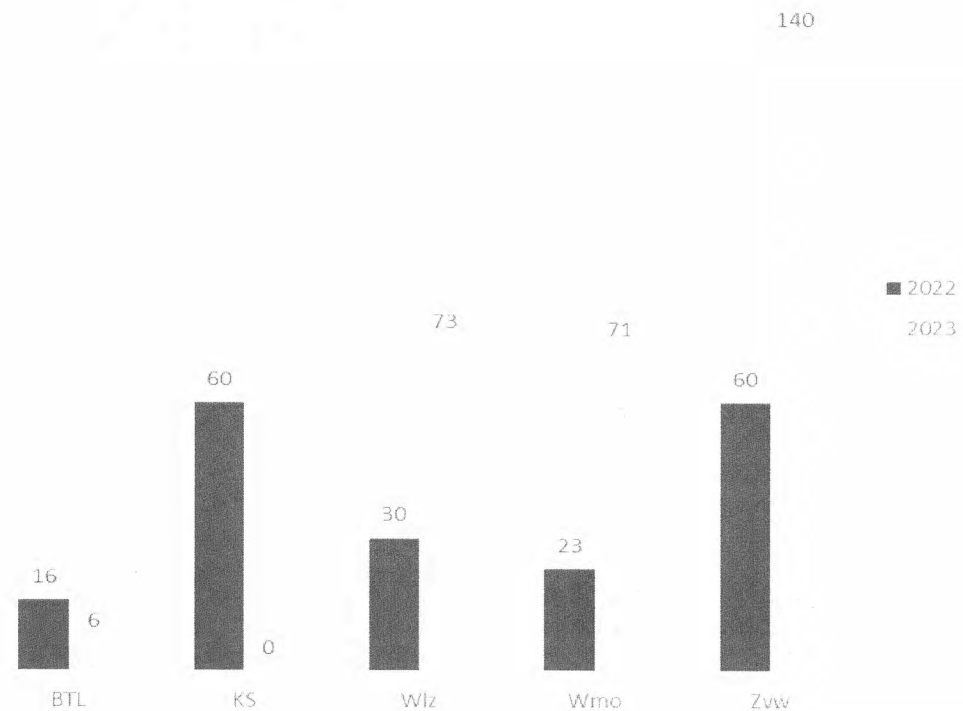

# DATALEKKENRAPPORT Q2 2023

## Het CAK

C/K



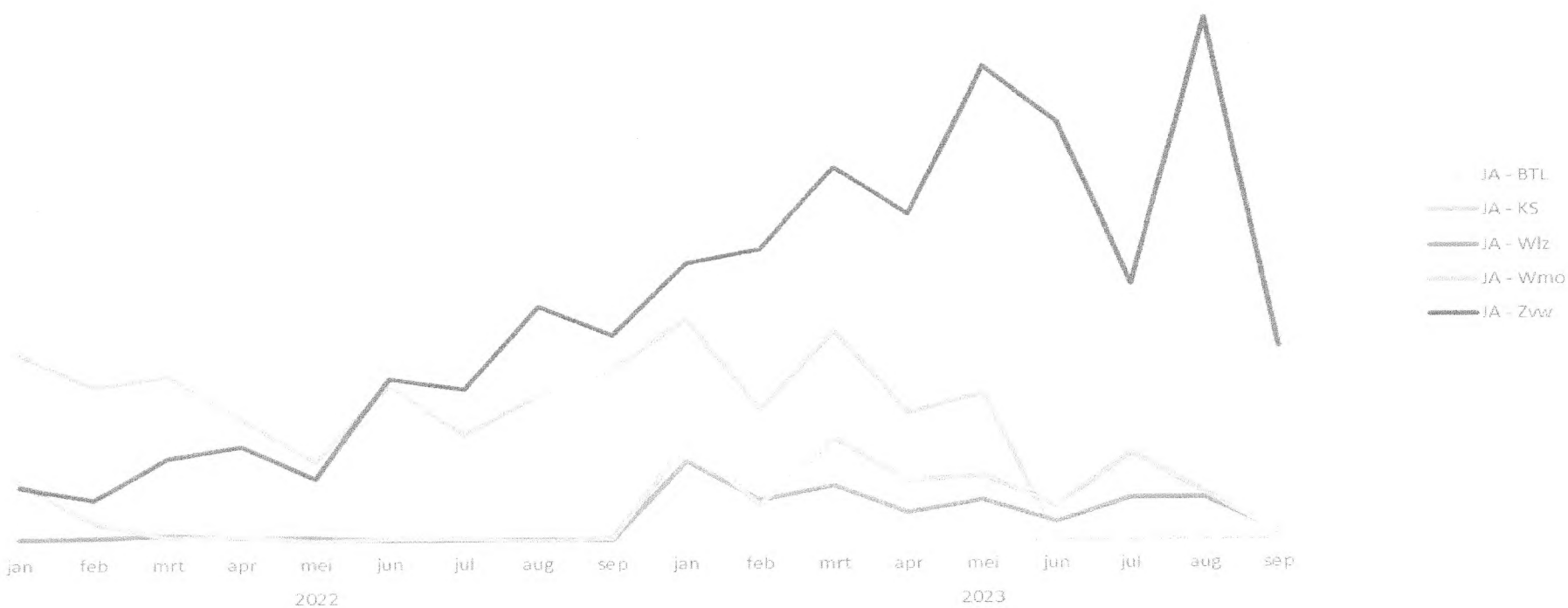
# CIJFERS VASTGESTELDE DATALEKKEN




- Vanaf 2023 zijn de aantallen geopende retourpost bij alle regelingen verwerkt en niet meer bij KS. Hierdoor zijn de cijfers bij de regelingen hoger dan in 2022.
- De oorlog in Oekraïne heeft ook in Q3 2022 een stempel gedrukt op de werkzaamheden en herkennen van datalekken. Sinds de start van de Oekraïne oorlog zijn er 57.000 extra aanvragen bovenop de reguliere werkvoorraad binnengekomen bij de SOV regeling. Deze aanvragen hadden de hoogste prio om te verwerken. In 2023 zijn de aanvragen gestabiliseerd en is er meer aandacht voor het herkennen van datalekken.
- In 2023 is bij de EB regelingen een stijging te waarnemen. Dit heeft er mee te maken dat geopende retourpost vanaf 2023 bij de regelingen zijn genoteerd en niet meer bij Klant Services.

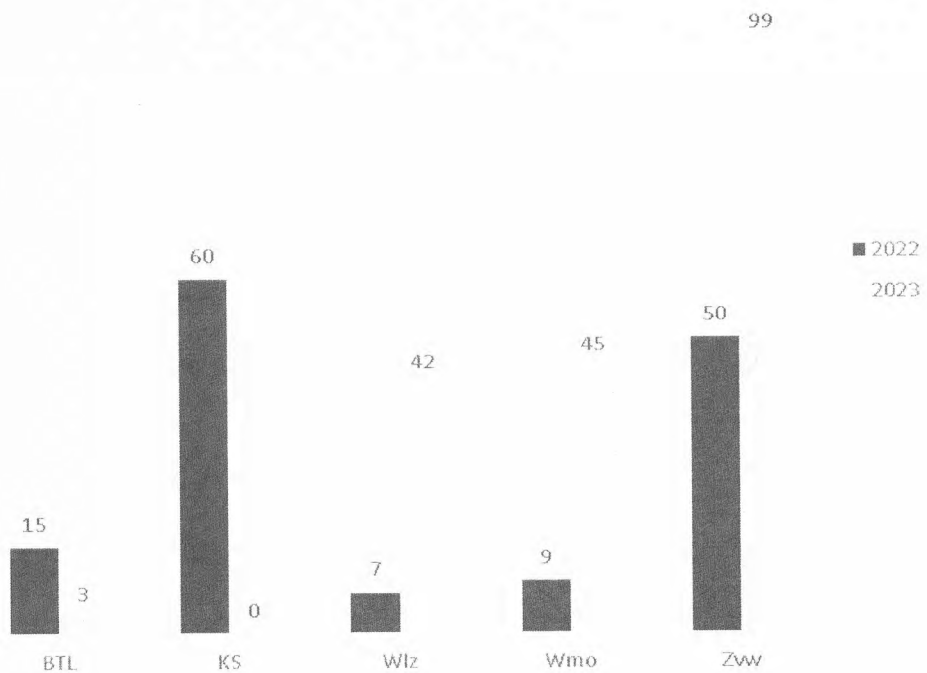
C/ K

# Trend vastgestelde datalekken vanaf 2022



C/ K

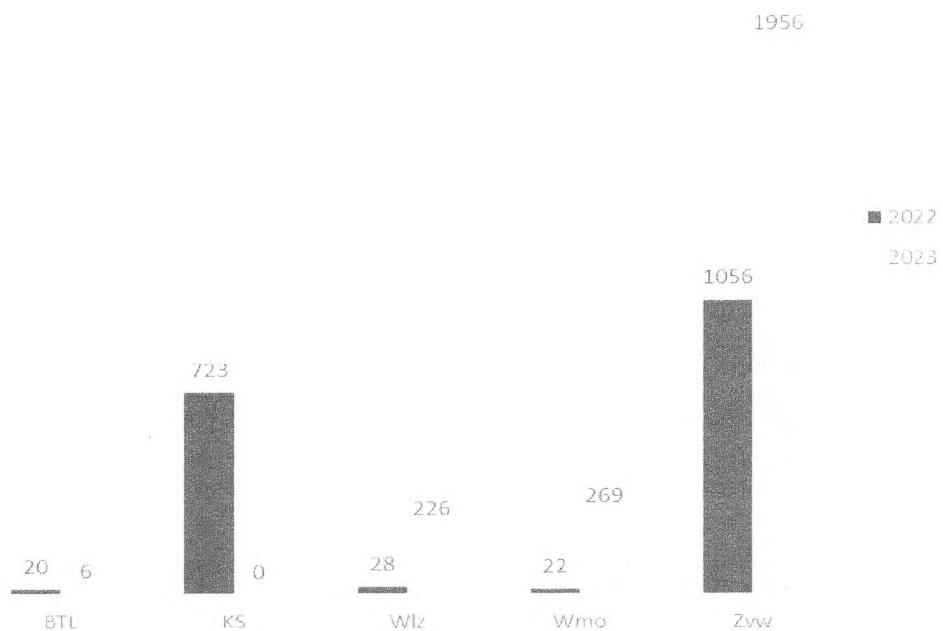
# CIJFERS GEMELDE DATALEKKEN AP




- In Q3 2023 zijn van de 284 datalekken 189 meldingen naar de Autoriteit Persoonsgegevens gemeld. Datalekken die bij een vertrouwelijke partij hebben plaatsgevonden hoeven niet bij de AP te worden gemeld. Een voorbeeld is een factuur wordt verstuurd naar de oude bewindvoerder. De bewindvoerder opent de post en laat aan ons weten dat de betrokken niet meer onder bewind staat.

C/ K

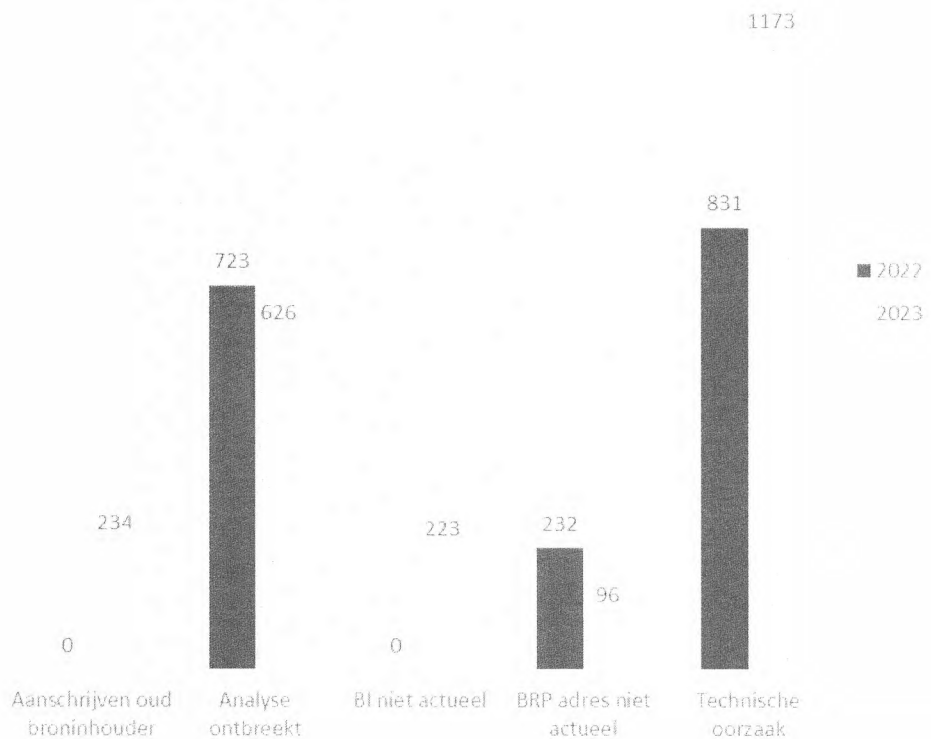
# CIJFERS GERAAKTE KLANTEN




- In dit grafiek staan de totaal aantal geraakte klanten per cluster die bij een datalek zijn betrokken.
- Te zien is dat er in 2023 bij KS geen datalekken hebben plaatsgevonden. Dit komt omdat er geen incident is geweest en dat geopende retourpost bij de regelingen zijn opgeteld.
- Het hoge aantal bij de ZvW wordt veroorzaakt door de oud broninhoudersproblematiek. Inmiddels worden maatregelen genomen om te voorkomen dat de oud broninhouders onterecht worden aangeschreven. Dit staat in ADO geprioriteerd.

C/ K

# CIJFERS OORZAKEN DATALEKKEN




In dit grafiek staan de top 5 meest voorkomende datalekken.

- De technische oorzaak wordt het meest gemeld. Het gaat hier om de oud broninhoudersproblematiek dat buiten de cirkel van invloed van het CAK ligt. De oorzaak ligt in de uitwisseling van verouderde data die door het UWV wordt aangeleverd. Deze issue is sinds 2022 bekend en beschreven in de informerende memo datalekken WAN. Het werk wat daaruit voortkomt bij de regeling Zvw kan niet besteed worden aan hulp voor burgers met een schuldvraag.

- Bij analyse ontbreekt gaat het om geopende retourpost. Inmiddels is het CLV traject bij de EB regelingen afgerond en is er een nieuwe werkwijze. Het CLV traject gaat zich nu richten op ongeopende retourpost om herhaalverkeer te voorkomen.

- Het BRP is niet actueel heeft verschillende oorzaken:
  - Verhuizing en verzenden van uitingen hebben elkaar gekruist..
  - Betrokkene doet geen verhuisaangifte. Een maatregel is een terugmelding naar de gemeente doenvoor het instellen van een onderzoek
  - Betrokkene stuurt om onbekende reden post retour. Maatwerk door team Non Voice wordt geboden..

# Uitstel audit AVG/Privacy

Internal Audit vraagt de RvB akkoord te gaan met het uitstellen van de audit AVG/Privacy 2023.

Raad van Bestuur

[redacted]
Hoofd Internal Audit

Uitstel audit AVG/Privacy

30 oktober 2023

1.0

In het Auditjaarplan 2023 is een AVG/Privacy audit opgenomen. In overleg met de Privacy Officer stellen wij voor deze audit uit te verplaatsen naar eind 2024. In dit memo geven wij een toelichting op de reden van uitstel.

Het uitstellen van deze audit geeft de Privacy Officer de gelegenheid een quick scan te laten uitvoeren naar de implementatie van AVG-Controls. Door het vertrek van een operational auditor en de vacature die hierdoor is ontstaan, gebruikt Internal Audit de vrijgekomen capaciteit voor het uitvoeren van andere onderzoeken in het Auditjaarplan.

De Privacy Officer heeft behoefte aan een quick scan (nul-meting) per regeling (Wmo, Wlz, Zvw, Btl, ICT en Staven) over de status van de implementatie van AVG-controls. Besloten is deze toetsing door een externe partij (Privacy Company) te laten uitvoeren. De planning is deze toetsing in november 2023 te laten plaatsvinden.

De Privacy Company levert een rapport op met een overzicht van de bevindingen en aanbevelingen. De resultaten uit het rapport worden gepresenteerd in het MT CAK en dienen als uitgangspunt voor de verdere implementatie van AVG-controls om privacy risico's te beheersen. De doelstelling van de quick scan overlapt daarmee met de beoogde doelstelling van de geplande audit door Internal Audit. Gezien het specialisme van de externe partij is inzet van Internal Audit op dit moment niet doelmatig.

Internal Audit adviseert daarom om de audit AVG/Privacy uit te stellen tot eind 2024.

Internal Audit communiceert het besluit van de RvB aan de Privacy Officer ([redacted]) en de CIO ([redacted]).

# RASCI matrix CAK AVG Versie 5.0 2023

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

| | | | | | | |
|---|---|---|---|---|---|---|
| Toezicht | | | | | | |
| Er wordt toezicht gehouden. | I | C | | | RSA | C |
| Er is een contactpersoon voor de AP. | I | | | | RSA | |
| Informatiebeveiliging | | | | | | |
| Faciliteert de samenstellling op basis van de BIA/PIA per proces de beheersmaatregelen op het gebied van Informatiebeveiliging en Privacy maatregelen binnen het kader van het beheersraamwerk. | A | | | | A | SC |
| Opstellen en onderhoud privacy statement | | | | | | |

Niet openbaar

# RASCI matrix CAK AVG Versie 5.0 2023

| | | | | | |
|---|---|---|---|---|---|
| Opstellen en onderhoud van het algemene privacystatement op de CAK website. | | I | | | C |
| Opstellen en onderhoud van het regeling specifieke deel van het statement op de website. | AI | CS | | | R |

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

**1. Doelbinding**

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

**2. Rechtmatigheid**

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

**3. Minimale verwerking**

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

**4. Behoorlijkheid**

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

**5. Transparantie**

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

**6. Integriteit en 7. vertrouwelijkheid**

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

**8. Juistheid**

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

**9. Opslagbeperking**

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

**10. Verantwoordingsplicht**

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

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

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

# RASCI uitleg

Dit zijn de rollen binnen de RASCI-matrix:

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

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

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

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

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

NB:

In de kolom "Leden MT-CAK" zijn alle eisen opgenomen met betrekking tot de direct reports.

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

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

| | |
|---|---|
| Organisatieonderdeel | Het CAK |
| Naam hoofd van dienst | [redacted] |
| Naam privacy officer | [redacted] |
| Rapportagedatum | 13-10-2023 |

| Legenda |
|---|
| Volledig |
| Deels |
| Geen |
| Niet van toepassing |

| | KPI | | KPI | Dit houdt in: | Meetwaarde | Toelichting |
|---|---|---|---|---|---|---|
| 1 | Privacy | pag. 7 | De organisatie heeft alle verwerkingen voorzien van tenminste een van de in art 6 van de AVG opgenomen grondslagen en opgenomen in het register van verwerkingen. | *geen verduidelijking noodzakelijk* | Volledig | |
| | | pag. 9 | De organisatie past privacy by design en privacy by default toe bij op te stellen beleid of ontwerp van een nieuw systeem of dienst in een vroeg stadium. Hierin betrekt de organisaties thema's zoals dataminimalisatie, doelbinding, proportionaliteit, subsidiariteit en bewaartermijnen. | De organisatie beschikt over privacy by design beleid en evalueert deze periodiek. Ter uivoering daarvan wordt de privacy officer reeds bij de ontwikkeling en ontwerp van het beleid of systeem betrokken. | Deels | In de basis is er een vastgesteld proces. Verbetering van de betrokkenheid van de privacy officer in een vroeg stadium is onderhanden. |
| | | pag. 20 | De organisatie kan aantonen dat bij nieuwe systemen, beleid en diensten een Quick Scan IB en P en zonodig een PIA is uitgevoerd. | De privacy officer is hierbij actief betrokken dan wel om advies gevraagd voordat deze wordt vastgesteld. | Volledig | Er wordt bij de introductiie van elk nieuw systeem een Business Impact Analyse (BIA) uitgevoerd, waar de punten uit de Quick Scan in zijn opgenomen. De BIA template is recent volledig geupdate.Voor de vaststelling van nieuw beleid en diensten wordt het CIO office standaard geraadpleegd, waar de Privacy Officer onderdeel van is. |
| 2 | Rechten van betrokkenen | pag. 10 | De organisatie beschikt over procedure(s) om de rechten van de betrokkene(n) snel en adequaat af te handelen. | *geen verduidelijking noodzakelijk* | Deels | Er is een protocol beschikbaar. Hiernaast zijn er per regeling ook aparte werkinstructies beschikbaar. Digitalisering van het proces is gepland voor uitvoer in Q4 2023. Daarnaast is er een verdere optimalisatie van het proces bezig om de geconstateerde verbeterpunten nav het recente AP onderzoek in te bedden. |
| | | pag. 10 | De organisatie gebruikt vastgestelde modellen voor afhandeling van AVG verzoeken en bezwaar. | *geen verduidelijking noodzakelijk* | Volledig | Er is een vastgesteld formulier en protocol beschikbaar. Deze worden waar nodig herzien om geconstateerde verbeterpunten door te voeren. |
| | | pag. 10 | De organisatie beoordeelt de ontvangen verzoeken periodiek op vlotte en juiste afhandeling. Zo nodig worden procedures aangepast. | Er wordt aantoonbaar (denk aan een gespreksverslag) periodiek een evaluatie van de afgehandelde AVG-verzoeken ingericht. | Deels | De geplande (Q4 2023) digitalisering van de aanvragen zal zorgen voor een centraal punt van binnenkomst van deze aanvragen en de periodieke overzichten en evaluatie verbeteren. |
| | | pag. 10 | De organisatie informeert betrokkenen op transparante wijze over de verwerking van persoonsgegevens. | Per verwerking is aantoonbaar de informatieplicht in kaart gebracht en daarin worden de toepasselijke wettelijke vereisten (art 13 en 14 van de AVG) meegenomen.(dit kan opgenomen worden in het opmerkingenveld in het | Volledig | Er is een algemene privacyverklaring en per regeling een specifieke verdere toelichting op de CAK-website aanwezig. |
| | | pag. 10 | De organisatie heeft op al haar websites een privacy- en cookieverklaring geplaatst. Deze verklaring is eenvoudig vindbaar, zichtbaar, voldoende specifiek en makkelijk toegankelijk. | *geen verduidelijking noodzakelijk* | Volledig | |
| | | pag. 11 | De organisatie heeft aantoonbaar inzichtelijk gemaakt waar gebruik wordt gemaakt van geautomatiseerde besluitvorming op basis van profilering en op basis van welke grondslag dat gebeurt. | *geen verduidelijking noodzakelijk* | Niet van toepassing | Op de website is hier een passage over opgenomen. Deze zal in Q4 verder uitgebreid worden om de klanten hier meer duidelijkheid over te geven. |
| | | | | Voor alle verwerkingen waarbij sprake is van geautomatiserde besluitvorming op basis van profilering is een PIA uitgevoerd. | | |
| | | | | Alle betrokkenen zijn vooraf aantoonbaar geinformeerd over de geautomatiseerde besluitvorming, de mogelijke gevolgen die dit met zich meebrengt en welke bewaartermijn worden gehanteerd. | | |
| | | | | De organisatie heeft een proces ingericht dat betekenisvolle menselijke tussenkomst in de besluitvorming borgt, en waar de betrokkene een beroep op kan doen. | | |
| | | pag. 12 | Als de organisatie persoonsgegevens verder wil gaan verwerken voor een ander doel dan waarvoor de gegevens zijn verzameld, informeert hij aantoonbaar de betrokkene, voor aanvang van de verdere verwerking, over dat andere doel. | *geen verduidelijking noodzakelijk* | Volledig | Dit vindt ondermeer plaats bij bijv het opnemen vaan telefoongesprekken en klant tevredenheidsonderzoeken. |
| | | pag. 12 | De organisatie heeft in kaart gebracht bij welke verwerkingen sprake is van contact met kinderen en zij heeft voor deze contactmomenten duidelijke, eenvoudige, begrijpelijke en beknopte taal gehanteerd in een toegankelijke vorm voor ouder en kind. | *geen verduidelijking noodzakelijk* | Niet van toepassing | Communicatie verloopt altijd via de wettelijke vertegenwoordiger van de minderjarige. |
| 3 | Privacybeleid | pag. 14 | De organisatie beschikt over privacy beleid welke door of namens de SG is vastgesteld. | *geen verduidelijking noodzakelijk* | Volledig | Het CAK heeft een privacybeleid. Dit is echter niet door of namens de SG vastgesteld omdat het CAK een ZBO is. De RvB stelt dit beleid jaarlijks na de herziening vast. |
| | | pag. 14 | Het privacybeleid wordt minimaal een keer in de drie jaar geëvalueerd en geactualiseerd. Zo nodig wordt het beleid opnieuw vastgesteld. | *geen verduidelijking noodzakelijk* | Volledig | Het beleid wordt jaarlijks herzien en vastgesteld. |
| | | pag. 14 | De organisatie ziet toe op periodieke trainingen van nieuw en bestaand personeel dat betrokkenen is bij de verwerking. | De organisatie kent een opleidingsplan om het kennisniveau van de AVG op peil te houden. | Deels | Momenteel krijgen nieuwe medewerkers een verplichte privacy e-learning aangeboden. Deze is bij de introductie in 2020 aan alle medewerkers aangeboden. Deze training wordt momenteel aangepast en uitgebreid met security elementen en adaptief gemaakt. De planning is dat deze in Q4 wordt vastgesteld zodat vanaf begin 2024 deze aan alle medewerkers jaarlijks verplicht kan worden aangeboden. |
| | | pag. 14 | De organisatie organiseert jaarlijkse een bewustwordingscampagne voor de naleving van de AVG. | De organisatie kent een jaarlijks bewustwordingsplan om de naleving van de AVG te waarborgen en maakt gebruik van meetinstrumenten om het bewustwordingsniveau en de impact van de bewustwordingsmiddelen in kaart te brengen. | Deels | Er is een verplichte onboarding e-learning voor privacy en er worden regelmatig bewustwordings berichten op intranet geplaatst, naast speciifieke privacy thema's die aan het Privacy Gilde (1e lijn) worden aangeboden.De adaptieve e-learning die wordt ontwikkeld is de eerste stap voor een structureel opleidings- en bewustwordingsplan, dat in 2024 verder worden ontwikkeld. |
| 4 | Organisatie van privacy | pag. 15 | De organisatie heeft haar privacy governance in kaart gebracht waarin in ieder geval de verschillende rollen zoals omschreven in hoofdstuk 5 van de Handreiking naleving AVG in zijn opgenomen. Deze governance is kenbaar gemaakt bij de betrokken partijen en vastgesteld door de hoofd van dienst. | De organisatie kent een privacy governance document en actualiseert deze periodiek. Dit kan ook opgenomen zijn in het privacy beleid. | Volledig | Dit is een bijlage bij het privacy beleid. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | pag. 14 | De organisatie heeft een kwaliteitscyclus ingericht voor gegevensbescherming en privacy om de blijvende goede omgang met persoonsgeevens te waarborgen. | *geen verduidelijking noodzakelijk* | Deels | Het Norea Privacy Control Framework is apart opgenomen in een door het CAK ontwikkeld controle dashboard. Uitrol hiervan heeft vertraging opgelopen en is gaande en dit zal in 2024 de basis vormen voor de kwaliteitscyclus. |
| | | pag. 19 | De organisatie toetst haar verwerkers regelmatig op de naleving van de eisen van de AVG | Beschrijf in het veld 'toelichting' op welke wijze en met welke frequentie verwerkers worden getoetst aan naleving van de AVG. Als voorbeeld kan worden gedacht aan het periodiek opvragen van recente audit rapporten of actuele ISO of NEN certificering. | Deels | Deze toetsing is bij een aantal contracten standaard ingebed. Met de inkoop afdeling is hier in 2023 naar gekeken om de bewistwording hieromtrent beter in te bedden in de organisatie. Dit heeft geresulteerd in een aantal stappen die verder worden uitgewerkt om dit jaarlijks onderdeel van de processen te laten zijn. |
| 5 | Register van verwerkingsactiviteiten | pag. 18 | De organisatie houdt een register bij van verwerkingsactiviteiten voor zowel de AVG als de WPG (in haar rol als verwerkingsverantwoordelijk en eventueel ook als verwerker). | WPG is niet eerder uitgevraagd. Geef aan of de organisatie persoonsgegevens onder de WPG verwerkt en op welke wijze wordt voldaan uit de verplichtingen uit de WPG. | Volledig | Het CAK verwerkt persoonsgegevens onder de Wpg (Wet Politiegegevens). Deze (detentie) gegevens zijn onderdeel van een proces of regeling binnen het CAK, waar het CAK een wettelijk verplichte taak uitvoert. De verwerking daarvan is daardoor in overeenstemming met de AVG en de Wpg. Momenteel wordt het proces hieromtrent geoptimaliseerd om te garandern dat de hoeveelheid informatie hieromtrent tot het noodzakelijke minimum beperkt wordt. |
| | | pag. 18 | Per verwerking zijn minimaal de volgende bijlagen opgenomen: PIA's/quickscan IB&P, verwerkersovereenkomsten of afspraken, advies van de FG en andere voor de verwerking relevante documentatie. | *geen verduidelijking noodzakelijk* | Volledig | De documenten zijn beschikbaar, maar niet als bijlage. Registertoool is hier niet geschikt voor. Deze documenten worden op de lokale DWO opgeslagen en zijn voor de complete organisatie inzichtelijk. |
| | | pag. 18 | De organisatie heeft een proces ingericht om de juistheid en de volledigheid van het register te waarborgen en periodiek te controleren. In dit proces is minimaal aandacht voor wijzigende wet- en regelgeving, IT-architectuur, onderkende informatiesystemen bij informatiebeveiliging en het ordeningsplan/selectielijst. | In dit proces is minimaal aandacht voor wijzigende wet- en regelgeving, IT-architectuur, onderkende informatiesystemen bij informatiebeveiliging en het ordeningsplan/selectielijst. | Deels | De kaders hieromtrent zijn beschikbaar. Praktische inbedding in de processen wordt bewerkstelligd en is een continu proces. Icm het verder te implementeren controle dashboard wordt er een hogere borging van de kwaliteit bewerkstelligd. |
| | | | De organisatie heeft in kaart gebracht bij welke verwerkingen sprake is van verwerking van persoonsgegevens waaruit ras of etnische afkomst kan blijken. | *geen verduidelijking noodzakelijk* | Volledig | |
| | | pag. 18 | In het kader van transparantie en het streven naar een open overheid publiceert de Rijksoverheid vastgestelde verwerkingen *in beginsel* op internet. | Beschrijf indien verwerkingen uit het verwerkingenregister niet gepubliceerd worden in het veld toelichting de argumenten om verwerkingen niet te publiceren. | Niet van toepassing | Het CAK is een ZBO. Publicatie van het register is niet verplicht op grond van de AVG. Vanwege de maatschappelijke gevoeligheid van sommige uitvoeringsprocessen is vooralsnog besloten om het register niet te publiceren. |
| 6 | Risicogestuurd beveiligen van persoonsgegevens | pag. 19 | De organisatie heeft per verwerking de noodzakelijke technische en organisatorische maatregelen geidentificeerd en geimplementeerd en neemt de controle op de werking van deze maatregelen op in het periodieke proces van kwaliteitscontrole op het register. | *geen verduidelijking noodzakelijk* | Deels | Verbetering is mogelijk. Managen van risico's en maatregelen neemt vaak veel tijd in beslag, vanwege ondermeer de complexiteit van het systeemlandschap. De onderhanden zijnde professionalisering van de ICT processen en de rationalisatie van het systeemlandschap zullen hier verbetering in gaan brengen. |
| | | pag. 20 | De organisatie beschikt over een procedure meldplicht datalekken. Deze procedure is makkelijk te vinden voor medewerkers. Hierin is opgenomen dat het datalek wordt gerapporteerd aan het juiste managementniveau in de organisatie en in geval politieke- of media gevoelige datalekken en/of er melding bij de AP wordt gedaan, tevens aan de CPO VWS. | *geen verduidelijking noodzakelijk* | Volledig | Melding aan CPO VWS geschiedt door de FG, indien deze dit noodzakelijk acht. |
| | | pag. 20 | De organisatie houdt een register bij van al haar datalekken als verwerker en als verwerkingsverantwoordelijke. | Geef in het veld toelichting aan hoeveel datalekmeldingen de organisatie in 2023 tot heeft geregistreed en hoeveel daarvan aan de AP zijn gemeld. Vermeld daarbij de datum tot wanneer is geteld. | Volledig | Topdeskregistratie. Van januari t/m 30 Sep 2023 zijn er 726 datalekken intern gemeld. Hiervan zijn er 560 naar de AP gemeld. |
| | | pag. 20 | Periodiek, en hoogste jaarlijks, wordt het voorkomen en de afhandeling inclusief registratie van datalekken geanalyseerd. Hierover wordt gerapporteerd aan het management. Zo nodig worden aanvullende maatregelen genomen ter voorkoming van datalekken. | *geen verduidelijking noodzakelijk* | Volledig | Gebeurt 2 wekelijks in overleg FG/Privacy-officer/datalekkenmanager. Ook is er per kwartaal een rapportage over de datalekken vanuit de datalekkenmanager en de Privacy Officer naar de RvB. Daarnaast wordt er jaarlijks een datalekken rapportage over het afgelopen jaar opgesteld en besproken met de RvB. |
| | | pag. 20 | De organisatie voert een PIA uit voor alle verwerkingen die hiervoor in aanmerking komen. Of een PIA is aangewezen wordt bepaald aan de hand van een Quick Scan IB en P. | De definitieve PIA's zijn opgeslagen in het register gegevensverwerking of andere centrale vindplaats. | Deels | Er is in 2022 gestart met de algehele review en updaten van alle PIA's waarbij dat nodig is. Dit proces is gaande. Hierbij wordt wel bij alle PIA's aan de hier aangegeven eisen voldaan. |
| | | | | Iedere PIA is voorzien van een advies van de FG en een beschrijving hoe opvolging is gegeven aan het advies. | | |
| | | | | Elke DPIA is aantoonbaar goedgekeurd door iemand die het formele mandaat heeft om de verwerking vast te stellen en eventuele restrisico's te accepteren. | | |
| | | pag. 20 | Bij de uitvoering van de DPIA zijn minimaal de volgende medewerkers betrokken: (gedelgeeerd) eigenaar van het informatiesysteem of -proces en de gemandateerd medewerker, de medewerker die betrokken is bij de uitvoering van het relevante werkproces, de medewerker met expertise op het gebied van privacy, en, indien relevant, informatiebeveiliging en de betreffende projectleider en -deskundigen. | *geen verduidelijking noodzakelijk* | Volledig | Per PIA wordt vastgesteld welke functionarissen nodig zijn. Dit is beschreven in de procedure. |
| | | pag. 20 | Het inkoopproces is zo ingericht dat bij de inkoop van diensten of systemen waarbij persoonsgegevens worden verwerkt, standaard een PIA wordt overwogen. | *geen verduidelijking noodzakelijk* | Volledig | |
| | | pag. 20 | Er is een procesbeschrijving voor het uitvoeren van PIA's en het opvolgen van uitkomsten. | *geen verduidelijking noodzakelijk* | Deels | Opvolgen van de uitkomsten en de mitigerende acties is de verantwoordelijkheid van de proceseigenaar. Hierop wordt toegezien door de privacy verantwoordelijken, alleen neemt de implementatie van sommige maatregelen soms veel tijd in beslag. |
| 7 | Doorgifte van persoonsgegevens aan derde landen of en internationale organisatie | pag. 15 | De organisatie schakelt alleen verwerkers in indien deze voldoende garanties bieden dat zij aan de wettelijk vereisten voor gegevensbescherming voldoen. | Dit is aantoonbaar ingericht doordat privacy een standaard onderdeel is in het programma van eisen bij een aanbesteding of inkooptraject. | Volledig | |
| | | pag. 15 | Met alle verwerkers binnen de Staat der Nederlanden is een verwerkersafspraak afgesloten. | Daarbij is gebruikgemaakt van het verwerkersafspraakmodel zoals te vinden op het Rijksportaal. | Volledig | |
| | | pag. 15 | Met alle verwerkers buiten de Staat der Nederlanden is een verwerkersovereenkomst afgesloten. | Daarbij is gebruikgemaakt van het Arvodi-model, het Arbit-model of het Ariv-model zoals opgenomen in PIANOo en op rijksportaal gepubliceerd. | Volledig | |
| | | | Met alle gezamenlijk verwerkingsverantwoordelijken is een onderlinge regeling afgesloten. | Daarbij is gebruikgemaakt van het model onderlinge regeling gezamenlijk verwerkingsverantwoordelijken zoals opgenomen in PIANOo en op rijksportaal gepubliceerd. | Volledig | |

| | | | | |
|---|---|---|---|---|
| pag. 22 | Ook bij doorgifte van persoonsgegevens aan een derde land (landen buiten de EEG) of internationale organisaties wordt de privacy en gegevensbescherming gewaarborgd. Hierbij is aandacht voor alle daarbij vereiste waarborgen waaronder doorgifte plaatsvindt zoals adequaatheidsbesluiten, passende waarborgen en, bindende bedrijfsvoorschriften. | Er moet duidelijkheid zijn (register van verwerkingsactiviteiten) welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd. Er wordt rekening gehouden met de consequenties van de actualiteit van wetgevingskaders die op doorgifte kunnen inwerken (denk aan de recente uitspraak over het onrechtmatig zijn van de Privacy Shield overeenkomst in relatie tot gegevensdeling met Amerikaanse bedrijven). | Volledig | |

# Aanbiedingsformulier RvB

Vergaderstukken inclusief dit volledig ingevulde formulier voorlegger indienen op de donderdag uiterlijk 12:00 uur voorafgaand aan de vergadering via: [redacted]
Memo's kunnen uitsluitend worden ingediend door (of na expliciete afstemming met) MT CAK leden.

| | | |
|---|---|---|
| 1 | MT CAK of RvB lid | [redacted] |
| 2 | Titel stuk | Memo uitstel AVG/Privacy |
| 3 | Datum behandeling RvB | 0 7 1 1 2 0 2 3 *DD / MM / JJJJ* |
| 4 | Aard van de behandeling<br>*Vakje aanklikken* | ☐ Ter advisering<br>☑ Ter besluitvorming<br>☐ Ter bespreking<br>☐ Ter kennisname<br>☐ Ter ondertekening<br>☐ Anders: |
| 5 | Vertrouwelijk behandelen | ☐ Ja ☑ Nee |
| 6 | Bespreking in aanwezigheid van<br>*Zorg voor een breed draagvlak en noteer daarom alle relevante MT CAK leden als gast* | ☑ Indiener<br>☐ Andere gasten naast indiener, namelijk: |
| 7 | Eerder behandeld in/met<br>*Gremium of functie noemen* | ☐ Raad van Bestuur<br>Uitkomst behandeling in bovenstaand gremium/met bovengenoemde functie:<br>☐ Overeenstemming *(geen toelichting vereist)*<br>☐ Geen overeenstemming, toelichting: |
| 8 | Korte samenvatting | In het Auditjaarplan 2023 is een AVG/Privacy audit opgenomen. In overleg met de Privacy Officer stelt IA voor deze audit uit te verplaatsen naar eind 2024 omdat er een quick scan wordt uitgevoerd door een externe partij die de doelstelling van de audit overlapt. |
| 9 | Gevraagd besluit<br>*Indien van toepassing. Noteer het besluit* | Internal Audit vraagt de RvB om toestemming om de audit AVG/Privacy uit te stellen tot eind 2024. |

*zo volledig mogelijk.*

10 Communicatie

Internal Audit communiceert het besluit van de RvB aan de Privacy Officer ([redacted]) en de CIO ([redacted]).

11 Betrokkenheid Ondernemingsraad

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

12 Adviezen intern

*Elk besluitmemo moet voorzien zijn van een intern advies. Neem hier kort het advies van alle belanghebbenden op met een beknopte motivatie.*

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

<J>

J Overig, nl

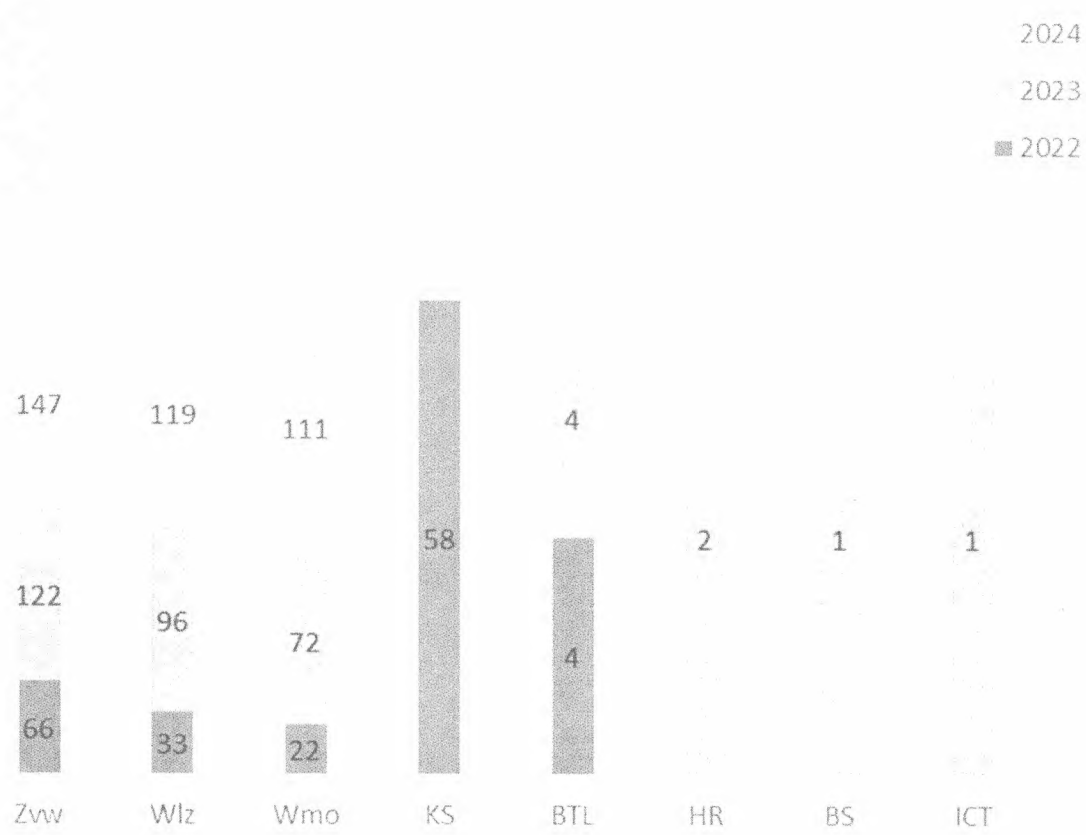
# DATALEKKENRAPPORT
# Q1 2024
## Het CAK

C/AK

[redacted]
Datalekmanager
Mei 2024

C/AK

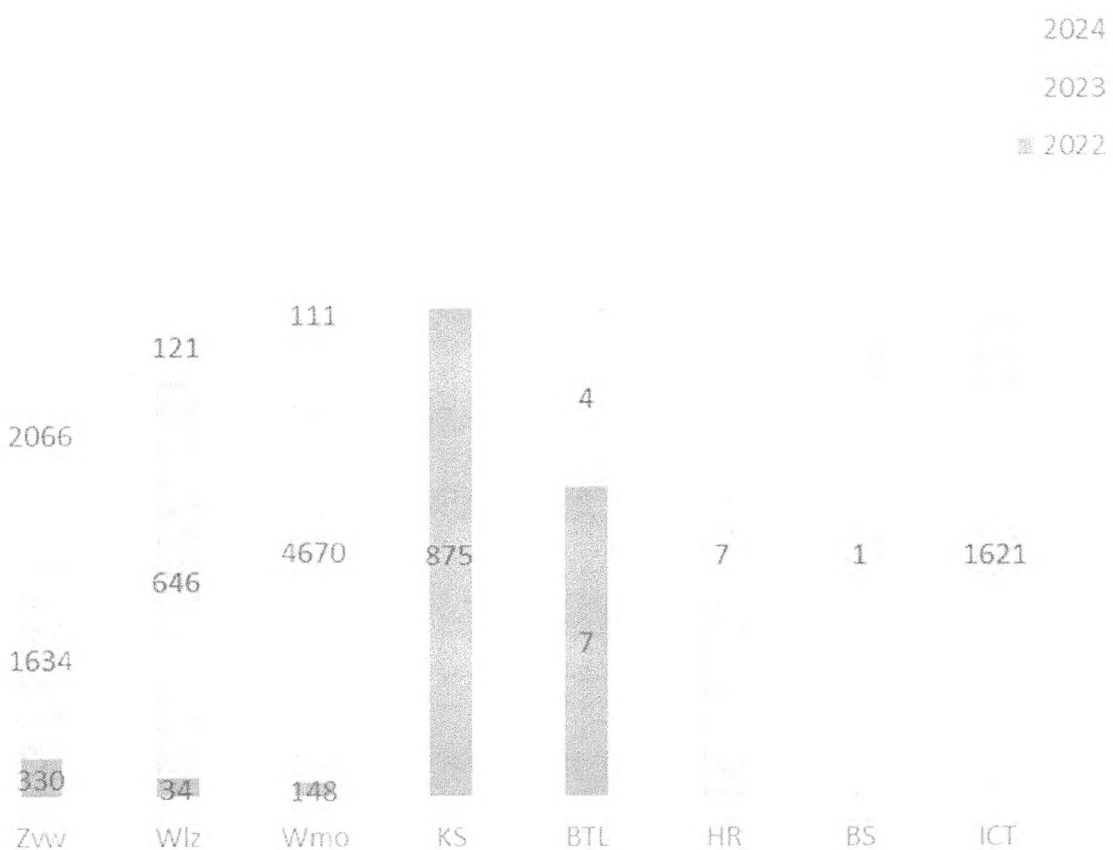
# CIJFERS VASTGESTELDE DATALEKKEN Q1 2024




- In Q1 2024 zijn er in totaal 392 datalekken gemeld.
- Na analyse is gebleken dat er 377 daadwerkelijk als datalek zijn bestempeld.
- Ten opzichte van Q1 2023 is dit een stijging van 21%%. Voornamelijk zijn er bij de Wmo, Wlz en Zvw datalekken gemeld.
- De stijging bij de EB regelingen komt mogelijk door een aantal incidenten waardoor uitingen als geopende retourpost zijn ontvangen.
- Een mogelijke oorzaak voor de stijging bij de Zvw is dat er meer aandacht wordt gegeven voor de oud broninhoudersproblematiek.
- Daarnaast is een mogelijke oorzaak van de stijging dat medewerkers vermoedens van datalekken sneller melden.

C/AK

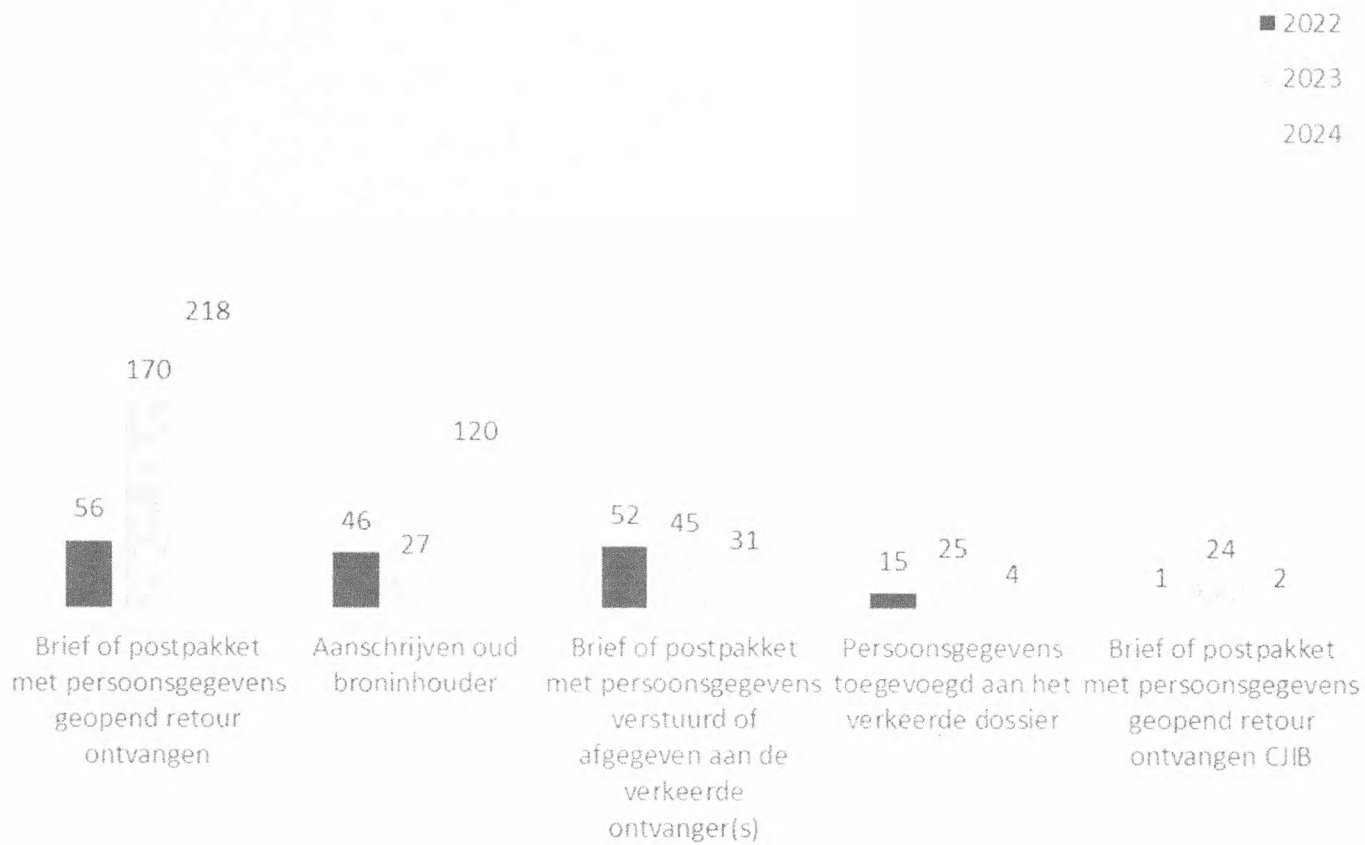
# CIJFERS GERAAKTE KLANTEN Q1 2024




- In dit grafiek staan de totaal aantal geraakte klanten per cluster die bij een datalek zijn betrokken.
- In 2023 zijn een aantal incidenten bij zowel de staven als regelingen geweest. In Q1 2024 zijn de incidenten geminimaliseerd waardoor datalekken zijn verminderd.
- Het hoge aantal bij de Zvw wordt veroorzaakt door de oud broninhoudersproblematiek. Hier is een kanttekening te plaatsen. Er is sprake van een technische uitwisselingsprobleem die verder reikt dan het CAK. Dit is lastig te voorkomen. Inmiddels worden maatregelen genomen om te voorkomen dat de oud broninhouders onterecht worden aangeschreven. Dit staat in ADO geprioriteerd.

CAK

# TOP 5 DATALEKKEN Q1 2024

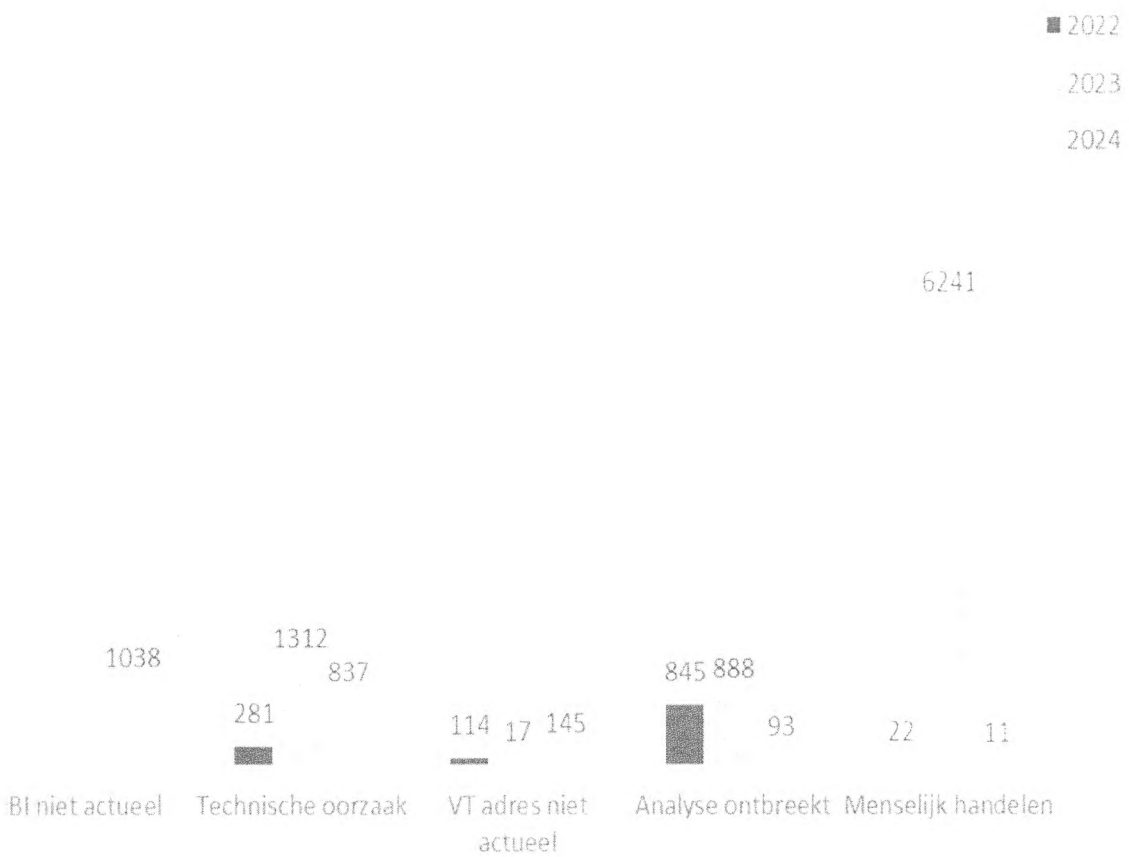



In Q1 2024 zijn de meeste datalekmeldingen binnengekomen die betrekking hebben op geopende retourpost.

Vervolgens is te zien dat de oud broninhouders problematiek veelvuldig worden gemeld.

C/AK

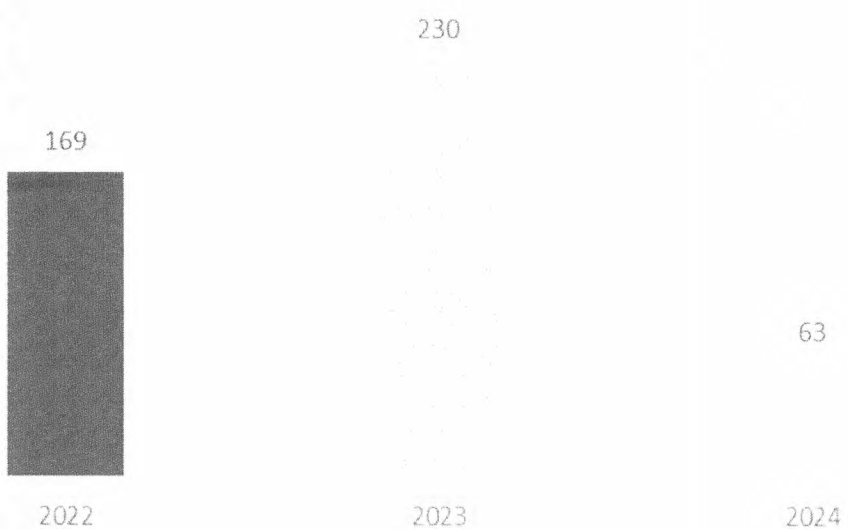
# TOP 5 OORZAKEN DATALEKKEN Q1 2024




- Op klantniveau is af te lezen is dat de grootste groep die geraakt wordt bij de Zvw regeling is.
- Bi niet actueel en technische oorzaak hebben betrekking op de oud broninhoudersproblematiek bij de Zvw. Vanaf september 2023 is hiermee een splitsing gemaakt in de oud broninhoudersproblematiek waarbij aangegeven kan worden waardoor de achterliggende probleem wordt veroorzaakt.
- Inmiddels kan er veel accurater worden aangegeven waarom post retour komt. Momenteel vind geen controle op de actualiteit van correspondentieadressen/ BW adressen plaats. Uitwisseling met het Curatele-Bewindvoerdersregister kan helpen of periodiek controles uitvoeren op de juistheid van correspondentie/ vertegenwoordigersadressen.

C/AK

# CIJFERS GEMELDE DATALEKKEN AP Q1 2024




- In Q1 2024 zijn van de 377 vastgestelde datalekken 63 meldingen naar de Autoriteit Persoonsgegevens gemeld.
- Ten opzichte van 2023 is dit met 73% gedaald. De belangrijkste reden is dat voor geopende retourpost veel beter de impact kan worden ingeschat. Dit zit met name dat onterecht post wordt verzonden naar een vertrouwelijke partij(Bewindvoerder) en de financiële impact lager ligt.
- Opvallend is dat er enkel voor de regeling Zvw datalekken zijn gemeld. Dit komt omdat de impact hoger zijn ingeschat dan bij de overige regelingen.
- De datalekken die voor de Zvw regeling zijn gemeld gaan over de oud broninhoudersproblematiek.

CAK

# OPLOSSINGEN/ ONTWIKKELINGEN DATALEKKEN 2024

In 2024 zijn er een aantal oplossingen geïmplementeerd of zijn teams met oplossingen om datalekken te voorkomen.

- In 10Q Portfolio en ADO zijn diverse initiatieven door de regelingen gepland om vooraf controles op klantgegevens in te bouwen.
- Het least to know principe wordt steeds meer toegepast door uitvoeren van specifieke IT General Controls.
- Datalekken is een onderdeel geworden binnen de IT General Control.
- Er loopt een aanbesteding om de poststroom te uitbesteden.
- Het CAK heeft een gesprek bij de AP naar aanleiding van de datalekken oud broninhoudersproblematiek. De uitkomst wordt in de volgende datalekrapport meegenomen.
- Per 1 maart 2024 is [redacted] privacy adviseur EB. Hiermee is de functie voor datalekmanager als vacature open gesteld.

# Jaarplan Privacy 2024

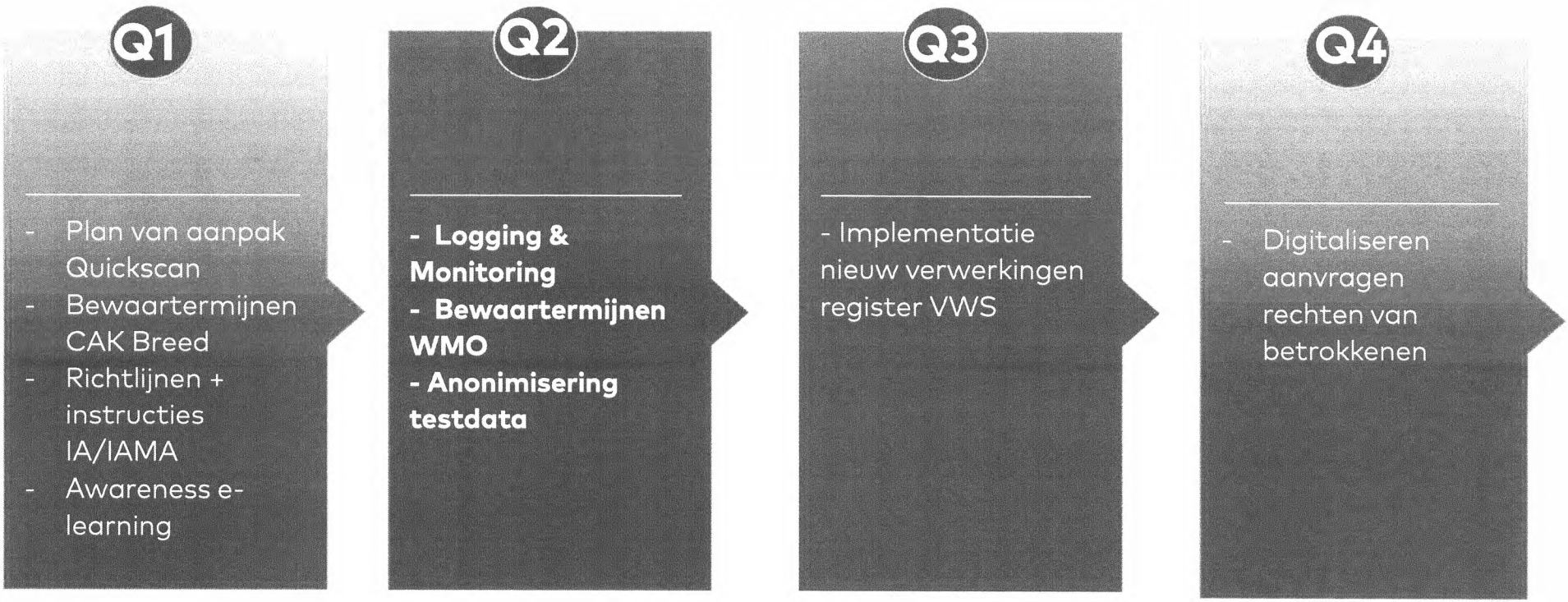
Privacy Officer

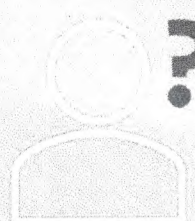
CAK

# Activiteiten

- Plan van aanpak per regeling nav uitkomsten Quickscan Privacy Company
- Bewaartermijnen kaderen CAK breed – beleid/memo/handreiking
- Bewaartermijnen WMO verder inventariseren+uitvoeren
- Anonimisering testdata verder brengen
- Plan van aanpak logging&monitoring op systemen
- Implementatie nieuw verwerkingenregister VWS
- Awareness e-learning implementeren
- Digitaliseren aanvragen rechten van betrokkenen
- Richtlijnen gebruik Algoritmes+AI+Gen AI + introductie IAMA

# Planning


Q1
- Plan van aanpak Quickscan
- Bewaartermijnen CAK Breed
- Richtlijnen + instructies IA/IAMA
- Awareness e-learning
Q2
- Logging & Monitoring
- Bewaartermijnen WMO
- Anonimisering testdata
Q3
- Implementatie nieuw verwerkingen register VWS
Q4
- Digitaliseren aanvragen rechten van betrokkenen



# Heb je een vraag?

CAK

C/AK


# Transitie Privacy

Van centraal geregeld naar regelling

# Inhoud

- Aanleiding voor deze presentatie.
- Privacy in de nieuwe organisatie.
- Aanpak en planning.
- Onzekerheden
- Vragen.

# Aanleiding

- Beëindiging van het AVG project.
  - Inbedding in de lijn van privacy is urgent (want nooit goed ingeregeld).
  - Opgeleverde producten hebben onderhoud nodig en/of moeten verder ontwikkeld worden.

- De organisatie gaat draaien.
  - Vanaf juni 2020 gaan we regeling gericht werken. Een nieuw organisatieontwerp ondersteunt ons hierbij.
  - Privacy draait uiteraard mee!

# Privacy in de nieuwe organisatie

- Compliance met privacy is een verantwoordelijkheid van de Direct Report RvB.
  - Aantoonbaar toepassen van alle van toepassing zijnde privacy principes op de verwerkte persoonsgegevens.
  - Verantwoording over de mate van compliance per Direct Report RvB intern (aan de RvB) en extern (aan het min. van VWS).

- Toepassen 3 lines of defence.
  - 1e lijn werk onder verantwoording van de Direct Report.
  - 2e lijn activiteiten door Risk & Compliance.
  - 3e lijn activiteiten door auditteam / externe toezichthouder.
  - CIO-office stelt kaders en ondersteunt.
  - CIO office is verantwoordelijk voor werking van het privacy stelsel.

# Aanpak draaien

- Direct Reports geven de namen van de medewerkers aan CIO office door.
- CIO office gaat in gesprek met de medewerkers.
- Kick-off privacy gilde.
- Starten met uitvoeren van de draaiing.

# Hulpmiddelen t.b.v. het draaien

- De ”Richtlijn Privacy bij het CAK”.
  - Opgesteld door CIO office als richtinggevend document.
- Backlog TSP
  - Samengesteld door het Tijdelijk samenwerkingsverband Project AVG
- Inrichten “Kris kras groep” privacy over regelingen heen.
  - Geïnitieerd door CIO office.
  - Deelname door alle medewerkers privacy, voorlopig 2 wekelijks.
  - Inbedden van de richtlijn Privacy bij het CAK.
- Opnemen Norea privacy framework in het GRC[1].
  - Het GRC platform verhoogt de grip en ondersteunt de verantwoording.

1. Governance, Risk & Compliance (GRC) tool die inzicht verschaft in de ‘in control status’ van het organisatieonderdeel en het CAK.

# Activiteiten 2020

| Onderwerp | Actie | Verantwoordelijk | Opmerkingen |
|---|---|---|---|
| Resources | Toewijzen medewerkers door Direct Reports | Direct Reports RvB | Elke Direct Report RvB moet vertegenwoordigd zijn. |
| | Individueel vaststellen opleidingsbehoefte | CIO-office | Korte intake door CIO office. |
| | Training basis kennis AVG doorlopen naar behoefte | Medewerker privacy | Springest, AVG en security expert. Elearning. |
| | DPIA training doorlopen | Medewerker privacy | Springest, IMF academy, start 11 juni. 2 daagse training. Afronding uiterlijk 18 juni as. |
| | Mijlpaal: medewerkers beschikbaar en opgeleid | Direct Report RvB / CIO-office | |
| Verwerkingenregister | organisatiestructuur, GAP-analyse IST soll, vaststellen ontbrekende verwerkingen | Medewerker privacy | Na 1 april past de structuur van het huidige register niet meer op de organisatie. |
| | Opvoeren aanvullende verwerkingen | Medewerker privacy | Waar mogelijk kopieerwerk van bestaande verwerkingen en specifiek maken voor de regeling. |
| | Mijlpaal: vaststellen nieuwe verwerkingenregister | CIO-office | |
| | Mijlpaal: afsluiten oude register | CIO-office | Nb: tot de transitie van het oude register is afgerond blijft deze leidend voor evt. controle door de AP. |
| PIA-register | GAP-analyse IST soll | Medewerker privacy | |
| | Inplannen en uitvoeren aanvullende PIA's | Medewerker privacy | Waar mogelijk kunnen bestaande PIA's worden hergebruikt. |
| | Mijlpaal: vaststellen nieuwe PIA register | CIO-office | |
| Leveranciersovereenkomsten | Toewijzing van leveranciers overeenkomsten aan de direct reports | Manager inkoop | Met de evt. hier aan gekoppelde verwerkersovereenkomst(en). |
| | Mijlpaal: Verwerkersovereenkomsten toegewezen aan Direct Report | Manager inkoop | |
| Verantwoording (compliance) | Initiële vulling GRC-tool | Medewerker privacy/CIO-office | |
| | Mijlpaal: start kwartaalrapportage cyclus | Direct Report RvB | Ieder kwartaal 2020 e.v. |
| | Opleveren In control Verklaring AVG. | Direct Report RvB | Nb: format wordt gedurende 2020 bepaald door ministerie van VWS. |
| | Mijlpaal: eerste ICV privacy door het CAK aan VWS opgeleverd. | Direct Report RvB | |
| Inbedden Richtlijn Privacy bij het CAK | Inbrengen in Kris Kras groep | CIO-office | Waarschijnlijk 2 wekelijks overleg over voortgang en knelpunten. |
| | Mijlpaal: Richtlijn is ingebed. | Medewerker privacy | |

# Planning 2020

| Id | | Begindatum | Einddatum | Duur |
|---|---|---|---|---|
| 1 | Toewijzen medewerkers | 2-3-2020 | 30-3-2020 | 4,09w |
| 2 | Vaststellen opleidingsbehoeftes | 2-3-2020 | 15-4-2020 | 6,6w |
| 3 | Basis training doorlopen | 16-4-2020 | 27-4-2020 | 1,42w |
| 4 | Pia training doorlopen | 11-6-2020 | 18-6-2020 | 1,07w |
| 5 | Medewerkers opgeleid | 18-6-2020 | 18-6-2020 | 0w |
| 6 | Mapping verw. register op nieuwe organisatie | 1-4-2020 | 29-4-2020 | 4,09w |
| 7 | Opvoeren aanvullende verwerkingen | 1-4-2020 | 17-6-2020 | 11,2w |
| 8 | Vaststellen nieuwe verw. register | 30-6-2020 | 30-6-2020 | 0w |
| 9 | Mapping PIA register op nieuwe organisatie | 9-4-2020 | 30-4-2020 | 3,2w |
| 10 | Inplannen / uitvoeren aanvullende PIA's | 4-5-2020 | 21-8-2020 | 15w |
| 11 | Vaststellen nieuwe PIA register | 7-9-2020 | 7-9-2020 | 0w |
| 12 | Toewijzen leveranciers overeenkomsten aan direct reports | 2-3-2020 | 28-4-2020 | 7,64w |
| 13 | Optimaliseren datalek proces | 1-4-2020 | 30-10-2020 | 30,6w |
| 14 | Initiele vulling GRC tool | 1-4-2020 | 10-11-2020 | 32w |
| 15 | Start kwartaal rapportcyclus GRC | 1-7-2020 | 1-7-2020 | 0w |
| 16 | Opleveren jaarlijks ICV privacy (concept) | 11-11-2020 | 11-11-2020 | 0w |
| 17 | Inbedden richtlijn privacy | 30-3-2020 | 1-1-2021 | 39,8w |
| 18 | Privacy "in control" | 1-1-2021 | 1-1-2021 | 0w |

Exacte planning is afhankelijk van het moment dat medewerker wordt toegewezen namens het organisatieonderdeel. Uitgangspunt in deze planning is een startdatum van 1 april. Latere toewijzing leidt overeenkomstig tot een verschuiving van de planning voor het betreffende organisatieonderdeel

# Doorkijk naar planning 2021

- Verder van in control naar compliant .
  - O.a. inventariseren legacy issues.
- Start herzien van PIA's uit 2019.
  - Levensduur PIA is 3 jaar.
- GRC wordt leidend in de verantwoording.
  - Realtime inzicht in de mate van compliance.

# Doorkijk planning 2022

- De normale beheers- en onderhoudscyclus
- AVG certificeren??


Wat is een AVG-certificaat?

Hoe kan ik een AVG-certificaat aanvragen?

Als verantwoordelijke of verwerker kunt u een AVG-certificaat aanvragen bij een certificatie-instelling die daarvoor geaccrediteerd is door de Raad voor Accreditatie (RvA).

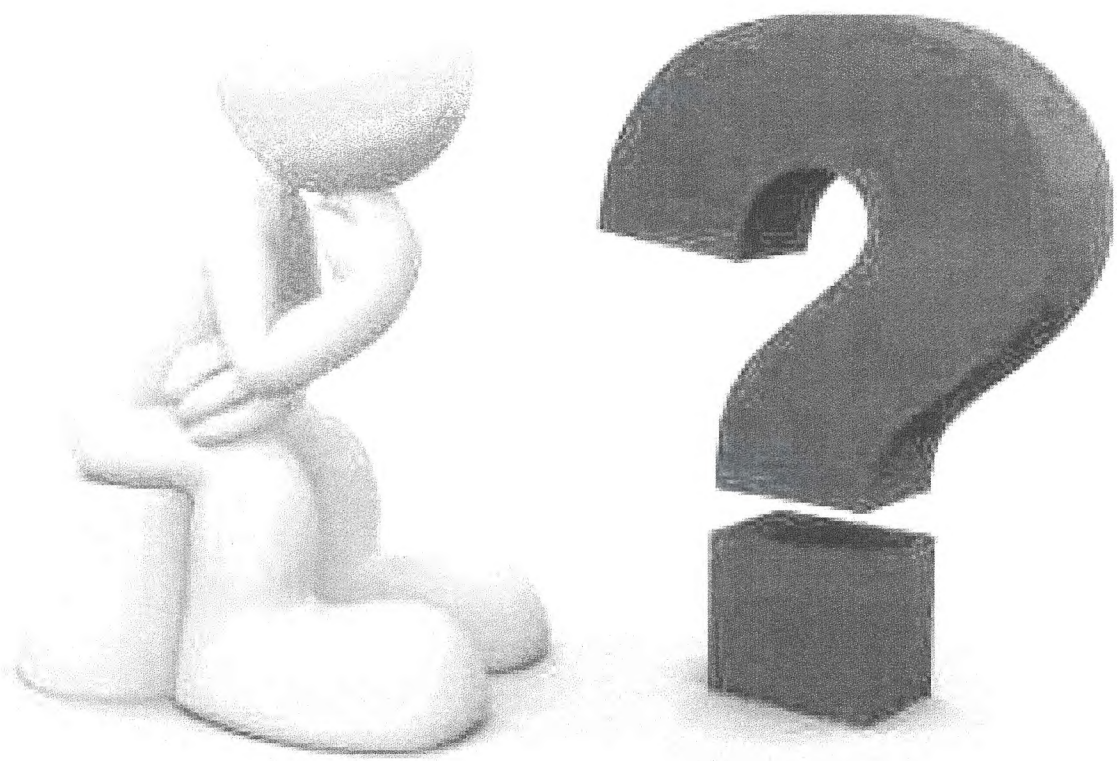
Een certificatie-instelling beoordeelt of uw product, proces of dienst in aanmerking komt voor een AVG-certificaat. Met dit certificaat kunt u aantonen dat u aan bepaalde eisen voldoet volgens de regels van de Algemene verordening gegevensbescherming (AVG).

Op dit moment zijn er in Nederland nog geen geaccrediteerde certificatie-instellingen voor het afgeven van AVG-certificaten in het kader van de verwerking van persoonsgegevens. Zodra de RvA certificatie-instellingen heeft geaccrediteerd om AVG-certificaten te verlenen, vindt u die informatie op onze website en die van de RvA.

# Onzekerheden

- Doorlooptijd van de inrichting van het NOREA privacy framework in het GRC.
- Oplevering van het nieuwe verwerkingen register in het GRC.
- Benodigd aantal uren van medewerkers voor activiteiten m.b.t. het draaien.

# VRAGEN



# Concrete activiteiten medewerkers privacy (niet uitputtend)

- Uitvoeren / onderhouden PIA's
- Adresseren en bewaken privacy risico's (in bijv. PI-planningen)
- Afsluiten verwerkersovereenkomsten
- Registreren / onderhouden verwerkingen
- Toepassen Privacy by Design in PI-planningen
- Bewaken bewaartermijnen persoonsgegevens
- Afhandelen datalekken
- Opleveren evidence in GRC (bestaan)
- (Helpen) beantwoorden specifieke vragen van externe bronnen
- Verantwoorden AVG compliance


# Status Privacy 2023 - ODU

20 april 2023

OPO

C/AK

# Jaarplan 2023 Privacy

| | |
|---|---|
| | Pro-actief verhogen van de P&S kwaliteit voorkomt reactieve P&S incidenten en calamiteiten |
| **Doelstelling** | Privacy & Security by Design implementeren |
| [illegible] | Wendbaar en betrouwbaar |
| [illegible] | Vereenvoudigen ICT |
| [illegible] | Er wordt voldaan aan de P&S Acceptatiecriteria voldaan (of exceptie) |
| [illegible] | Aantal EDU met P&S maatregelen/Aantal Decharge formulieren met P&S maatregelen x 100% |
| [illegible] | > 95% |
| [illegible] | CISO, Privacy Officer |

C/A K

# Jaarplan 2023 Privacy

| CIO Doelstelling | |
|---|---|
| CIO Waarde-propositie | Het nemen van maatregelen ter verhoging van de maturiteit zorgt voor een organisatie waar we steeds meer in control komen op Privacy en Security gebied. |
| **Doelstelling** | Privacy & Security maturiteit verhogen |
| Bijdrage Aan | Wendbaar en betrouwbaar |
| Aanpak | Uitvoeren Roadmap In control |
| KPI | De jaarlijks af te nemen maturiteitsscores via de NBA LIO en het Privacy volwassenheidsassessment dienen progressie te tonen |
| Meetlat | NBA LIO maturity assessment en Privacy Maturiteits assessment |
| Planning Target | 1 volwassenheidspunt hoger tov 2022 op de focusgebieden |
| Verantwoordelijke | CISO, Privacy Officer |

# Jaarplan 2023 Privacy

| | |
|---|---|
| | Een verhoogde P&S awareness verkleint de kans op menselijke fouten met data lekken en/of security incidenten als gevolg |
| **Doelstelling** | Organisatie is P&S aware |
| | Wendbaar en betrouwbaar |
| | Vereenvoudigen ICT |
| | CAK medewerkers hebben awareness programma doorlopen |
| | Aantal mdw. awareness doorlopen / totaal aantal mdw. X 100% |
| | > 90% |
| | CISO, Privacy Officer |

C/A K

# Jaarplan 2023 Privacy

| | |
|---|---|
| **Bijdrage aan CIO Waardeprofielen** | Door klanten tijdig transparantie te bieden omtrent hun persoonsgegevens vergroot het vertrouwen en klanttevredenheid. |
| **Doelstelling** | Rechten van betrokkenen verzoeken worden juist, tijdig en volledig afgehandeld |
| **Bijdrage aan** | In control |
| **Aanpak** | Uitvoeren Roadmap In control |
| **KPI** | Rechten van betrokkenen binnen geldende termijn van 1 maand afgehandeld |
| **Meetlat** | Aantal verzoeken tijdig afgehandeld / totaal aantal verzoeken x 100% |
| **Planning/Target** | 100% |
| **Verantwoordelijke** | CISO & Privacy Officer |

C/AK

# Jaarplan 2023 Privacy – Genomen acties

Privacy by Design – Connectie met diverse gildes → inventarisatie behoeftes

Awareness – Inventarisatie CAK Academy/Opleidingen.nl → Anders extern
Week vd Privacy / Jaarplan Privacy iom communicatie

Maturiteit – Richtlijnen bewaartermijnen / Centralisatie offertes+facturen / Anonimisering testdata / Geupdate verwerkingsregister / PIA's herzien / Beleid logging persoonsgegevens

Rechten van betrokkenen – digitaliseren aanvraagproces via Open CAK

C/AK

Aan
[redacted]

Cc

Van
[redacted]
Functionaris Gegevensbescherming

Onderwerp
Rapportage Functionaris Gegevensbescherming 2e half jaar 2021 en 1e half jaar 2022

Bijlage(n)
-

Datum
4 augustus 2022

Versie
0.1

Status

## Onderwerp

Rapportage Functionaris Gegevensbescherming 2e half jaar 2021 en 1e half jaar 2022

## Inleiding

In deze rapportage deel ik mijn bevindingen met betrekking tot de naleving van de AVG binnen het CAK over de tweede helft van 2021 en de eerste helft van 2022. Ik zal dat doen aan de hand van de volgende toezichtpunten, zoals ook vermeld in het Toezichtplan Functionaris Gegevensbescherming 2021:

1. Beleid.
2. Processen.
3. Organisatorische inbedding.
4. Rechten van betrokkenen.
5. Samenwerking.
6. Beveiliging

Mijn bevindingen zijn mede gebaseerd op de gesprekken die ik heb gevoerd met de Regelingdirecteuren en de collega's die zich binnen het CAK bezighouden met het onderwerp privacy, waaronder de privacy officer en de datalekmanager.

### Beleid

Binnen het CAK bestaan verschillende documenten waarin beleid en richtlijnen staan beschreven met betrekking tot de omgang met persoonsgegevens. Het Privacybeleid CAK en het Privacy Stelsel zijn daar twee voorbeelden van. In mijn rapportage over de eerste helft van 2021 heb ik aangegeven dat deze documenten op sommige punten geactualiseerd en verduidelijkt zouden kunnen worden. Dat is inmiddels gebeurd. Hier blijft echter aandacht voor nodig. Het bestaan van deze documenten wordt kenbaar gemaakt via de eigen intranetsite van privacy en security. De zichtbaarheid en de indeling van deze site is voor verbetering vatbaar. Een logischere en meer toegankelijke indeling vergroot de vindbaarbeid en de praktische toepasbaarheid van de documenten voor de collega's. Dit heeft de aandacht van de privacy officer.

### Processen

De verwerkingen van persoonsgegevens van het CAK dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

In dat kader heeft in de tweede helft van 2021 schoning plaatsgevonden van enkele mappen op de z-schijf en zijn de collega's geattendeerd op het belang van dataminimalisatie en opslagbeperking. De risk officers van de regelingen zullen in 2022 een plan van aanpak opleveren om schoning structureel te borgen in de bedrijfsvoering.

In het informatiebeveiligingsbeleid is vastgelegd dat data uit een productieomgeving niet mogen worden gebruikt in de ontwikkel-, test-, en acceptatieomgeving, tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om niet geanonimiseerde data te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na afloop van het ontwikkelen en testen. Hiervoor is de exceptieprocedure in het leven geroepen. Ten opzichte van de eerste helft van 2021 blijkt dat minder gebruik wordt gemaakt van deze procedure. Dat is een goed signaal dat laat zien dat niet te lichtvaardig (bij herhaling) om een exceptie wordt gevraagd, maar dat methodes ontwikkeld worden om tests uit te voeren zonder data uit een productieomgeving.

Het toetsen van werkprocessen die persoonsgegevens bevatten wordt onder meer gedaan door het uitvoeren van een gegevensbeschermingseffectbeoordeling (PIA). De uitgevoerde PIA's moeten worden geregistreerd in het PIA-register. Voor het uitvoeren van een PIA is een procedure ontwikkeld en beschreven. Deze dateert uit 2020. Mede door signalen uit de organisatie over de bewerkelijkheid van de procedure zal gekeken worden of deze procedure wellicht beter gestroomlijnd/vereenvoudigd kan worden zodat men hier minder tijd aan hoeft te besteden. Dit heeft de aandacht van de privacy officer. Zoals ook reeds gerapporteerd door de privacy officer zit een groot deel van de reeds uitgevoerde PIA's tegen de herzieningsdatum aan. De betreffende clusters maken hier een planning voor. Punt van aandacht blijft daarbij de in de PIA's gesignaleerde risico's en de daarbij voorgestelde mitigerende maatregelen worden onderkend en daadwerkelijk worden uitgevoerd.

### Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen het CAK op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Het toewijzen van taken, verantwoordelijkheden en bevoegdheden is een aandachtspunt. Het privacy beleid en de erbij behorende RACI tabel met taken en verantwoordelijkheden worden jaarlijks vastgesteld door de RvB.

De bemensing van privacy-rollen in de regelingen en staf in het privacygilde blijft een punt van zorg. De collega's die in het gilde zitten moeten in staat worden gesteld om tijd vrij te maken om de privacyrol te kunnen invullen. Ook moeten zijn in de gelegenheid worden gesteld tot het volgen van opleidingen op het gebied van privacy om hun rol nog beter te kunnen vervullen.

Op het gebied van het creëren van bewustzijn valt nog het nodige te winnen. Medewerkers krijgen bij indiensttreding een e-learning over privacy. Daarnaast kunnen zij voor informatie op dit gebied terecht op de intranetsite van privacy en security. Het verdient aanbeveling om onze medewerkers nog actiever bewust te maken van een juiste omgang met persoonsgegevens. Dit kan door het plaatsen van nieuwsberichten op het intranetsite of door het ontwikkelen van opleidingsmateriaal waar ook na indiensttreding aandacht voor is en meer toegespitst is op de specifieke doelgroepen van medewerkers. Het privacygilde kan hierbij ook een rol spelen door het geven van voorlichtingsbijeenkomsten. De privacy officer onderzoekt de mogelijkheden op dit gebied.

### Rechten van betrokkenen

Het CAK dient degene waar de gegevens van verwerkt worden (de betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen genomen

worden om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten, waaronder het inzagerecht controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

In 2022 is de privacymatrix geactualiseerd. Deze matrix geeft handvatten hoe om te gaan met de verschillende informatieverzoeken van klanten of hun vertegenwoordigers met betrekking tot de regelingen en specifiek zijn/haar situatie. Het beantwoorden van deze vragen kan op gespannen voet staan met de privacy regelgeving en dient derhalve zorgvuldig plaats te vinden. Het doel van de privacymatrix is om deze zorgvuldigheid te borgen.

### Samenwerking

Afspraken met betrekking tot de uitwisseling van gegevens tussen partijen moeten in voorkomende gevallen worden vastgelegd in verwerkersovereenkomsten en convenanten. In het verwerkingenregister worden het aantal verwerkingen geregistreerd. Binnen de organisatie ziet men het belang van het opstellen van goede verwerkersovereenkomsten en de registratie daarvan zeker in. Deze activiteiten worden echter nogal eens gezien als lastig en tijdrovend. De privacy officer gaat bekijken of deze procedure wellicht beter gestroomlijnd/vereenvoudigd kan worden.

### Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat het CAK passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.

Incidenten – waaronder inbreuken – op de beveiliging moeten onder omstandigheden gemeld worden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) (meldplicht datalekken). Significante reductie van het aantal datalekken door minder handmatige acties binnen alle regelingen en digitalisering van de uitingenstroom van alle regelingen moet daarbij het streven zijn. Met het aanstellen van een datalekmanager is het proces rondom datalekken verder geperfectioneerd. Bij een aantal datalekken is geconstateerd dat zaken als monitoring en logging nog niet altijd op orde zijn. Deze onderwerpen hebben de aandacht van de privacy officer. Naar aanleiding van een datalek bij het aanschrijven van broninhouders in het kader van de wanbetalersregeling, waarover de RvB ook is geïnformeerd, heeft de directeur Zvw het initiatief genomen om periodiek met de FG en de manager uitvoering regeling Zvw over het onderwerp datalekken te overleggen. Eén van de punten die het resultaat is van die overleggen is dat het onderwerp datalekken veroorzaakt door (verouderde) broninformatie verkregen via ketenpartners besproken gaat worden binnen de Manifestgroep. Het doel hiervan is om ervaringen op dit gebied met elkaar te delen en waar mogelijk met oplossingen te komen.

Onderwerp

Rapportage Functionaris Gegevensbescherming 2023

Aan

[redacted]

Van

[redacted]
Functionaris Gegevensbescherming

Onderwerp

Rapportage Functionaris Gegevensbescherming 2023

Bijlage(n)

-

Datum

1 mei 2024

Versie

1.0

Status

Definitief

## Inleiding

In deze rapportage deel ik conform artikel 38 lid 3 AVG mijn bevindingen met betrekking tot de naleving van de AVG binnen het CAK over het jaar 2023. De vorige rapportage liep van het tweede half jaar 2021 en het eerste half jaar 2022. Na het vertrek van de vorige FG bij het CAK heb ik de functie per 1 januari 2023 overgenomen.

In navolging van de vorige FG en in het belang van de continuïteit volg ik over het rapportagejaar 2023 het rapportageformat dat tot nu toe is gehanteerd. De rapportage is opgesteld aan de hand van de volgende toezichtpunten:

1. Beleid.
2. Processen.
3. Organisatorische inbedding.
4. Rechten van betrokkenen.
5. Samenwerking.
6. Beveiliging.
7. Specifieke aandachtspunten en doorkijk naar 2024.

Het zevende punt heb ik toegevoegd.

Mijn bevindingen zijn gebaseerd op input die ik uit hoofde van mijn functie ontvang, eigen onderzoek, het tweewekelijkse overleg met de privacy officer en de datalekmanager, het maandelijks privacy-securityoverleg, diverse gesprekken met interne stakeholders en externe overleggen op het vlak van privacy.

Bij de volgende rapportage zal ik een ander format gaan gebruiken en wel het format FG Jaarverslag van de VNG dat zich tot een landelijke standaard heeft ontwikkeld. Dit format wordt ook gebruikt door diverse FG's van aan de Manifestgroep deelnemende partijen. Het format biedt een beter handvat om ontwikkelingen op het vlak van privacy te volgen.

### Beleid

Binnen het CAK bestaan verschillende documenten waarin beleid en richtlijnen staan beschreven met betrekking tot de omgang met persoonsgegevens. Het Privacybeleid CAK is daarvan de basis. In de vorige rapportages is door de FG reeds aangegeven dat de actualisering en verduidelijking van dit document een aandachtspunt is. Ik wil daaraan toevoegen dat het Privacybeleid zou moeten worden aangevuld met instrumenten voor terugkoppeling en evaluatie om aan te tonen of het CAK werkelijk compliant is aan privacywetgeving en er een lerend vermogen is. Een werkende PDCA-cyclus zou een belangrijke verbetering opleveren.

In 2023 is gestart met nieuw beleid op het gebied van bewaartermijnen, is besloten de Selectielijst te herzien en is er (concept)archiefbeleid opgesteld. Dit beleid is belangrijk om te bepalen hoe lang dossiers van klanten (met daarin persoonsgegevens) bewaard moeten blijven en op welk moment ze moeten worden vernietigd. Momenteel zijn nog niet alle bewaartermijnen volledig vastgelegd. Daarnaast is er wel een Richtlijn schoning persoonsgegevens maar vernietiging geschiedt nog niet altijd volgens de bewaartermijnen. Bovendien zijn veel IT-systemen binnen het CAK er niet op ontworpen om effectief met vernietiging om te gaan.

Het is positief dat een nieuwe start is gemaakt op het vlak van bewaartermijnen maar er is meer nodig dan beleid dat alle bewaartermijnen bevat. Het verleden heeft geleerd dat het echte probleem zit in de implementatie van het beleid. Het hele project rondom bewaartermijnen ontbreekt het nog aan tijdlijnen en realistische doelstellingen. Het is de bedoeling dat in 2024 SMART-doelen worden geformuleerd zodat hier effectief op kan worden gestuurd.

Het aanpassen van bestaande IT-systemen met functionaliteiten die noodzakelijk zijn vanuit oogpunt van de bescherming van privacy is lastig. Daarom is het belangrijk dat privacy by design een uitgangspunt wordt bij de bouw en aankoop van nieuwe systemen.

### Processen

De verwerkingen van persoonsgegevens van het CAK dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

Het toetsen van werkprocessen die persoonsgegevens bevatten wordt onder meer gedaan door het uitvoeren van een gegevensbeschermingseffectbeoordeling (PIA). De uitgevoerde PIA's moeten worden geregistreerd in het PIA-register. Voor het uitvoeren van een PIA is een procedure ontwikkeld en beschreven.

De kwaliteit van de huidige PIA's is matig, het ontbreekt soms aan een adequate omschrijving van de verwerking en de grondslag van verwerking. Ook zijn niet altijd alle risico's goed in kaart gebracht en gewogen. Bij mitigerende maatregelen is niet altijd duidelijk of deze afdoende zijn en of deze ook daadwerkelijk worden getroffen.

Tot nu toe was het zo dat de FG pas aan het einde, na goedkeuring door de privacy officer en regelingdirecteur, om advies werd gevraagd. Vaak leidde de kwaliteit van de PIA niet tot een direct advies maar tot een reeks aanpassingen in de PIA, waarna de FG pas daarna een goedkeurend advies gaf. Deze werkwijze is recent veranderd door de FG te laten adviseren voordat de PIA al is goedgekeurd. Dit is een verbetering, de FG kan zo eerder in het proces een adviserende rol spelen bij het opstellen van kwalitatief hoogstaande PIA's.

Het format dat het CAK gebruikt is door het CAK zelf ontwikkeld. Ik adviseer om in de toekomst een ander format te gebruiken, bijvoorbeeld het Rijksmodel DPIA. Ook de training van medewerkers voor het uitvoeren van PIA's verdient aandacht. Een goed doorlopen kwalitatief hoogstaande PIA is een belangrijke factor voor de bescherming van privacy.

Het gebruik van standaardinstrumenten en formats verdient in alle gevallen de voorkeur. Het ligt hierbij voor de hand Rijksbrede standaarden te gebruiken. In 2023 heeft het CAK stappen gezet om in 2024 gebruik te gaan maken van een nieuw verwerkingenregister dat VWS-breed zal worden gebruikt. Het gebruik van erkende standaarden zal het ook makkelijker maken het niveau van privacybescherming bij het CAK op een objectieve manier meetbaar te maken.

### Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen het CAK op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Het Privacybeleid belegt de verantwoordelijkheid over verschillende deelaspecten van gegevensbescherming goed binnen het CAK. De eindverantwoordelijkheid ligt bij de Raad van Bestuur van het CAK, die de verantwoordelijkheid delegeert aan de leden van het MT-CAK, die weer delegeren aan de Afdelingsmanagers en eventueel ook Teammanagers. Alle regelingclusters hebben een privacydeskundige aangewezen, die samen het privacygilde vormen. Zij zijn verantwoordelijk voor de privacyadministratie, het uitvoeren van PIA's, het leveren van input over privacy by design en het creëren van awareness rond gegevensbescherming. De privacy officer coördineert activiteiten en adviseert, ook is deze verantwoordelijk voor organisatiebrede taken als het onderhouden van het verwerkingsregister, het bijhouden van uitgevoerde PIA's en afgesloten verwerkersovereenkomsten en voor het aansturen van het privacygilde. Er is een datalekmanager, die is ondergebracht bij een van de Regelingen, die zorgdraagt voor het melden van datalekken bij de AP en voor de interne afhandeling, inclusief het bijhouden van het register van datalekken. Deze inrichting is op zich voldoende. Wel moet het CAK blijven leren van datalekken middels een feedback loop. Hier ligt een duidelijke rol voor het management binnen de regelingclusters.

In de vorige rapportage is vermeld dat de bemensing van privacy-rollen in de regelingen en staf in het privacygilde een punt van zorg blijft. Destijds werd vooral gewezen op het feit dat collega's die in het privacygilde zitten in staat moeten worden gesteld om tijd vrij te maken om de privacyrol te kunnen invullen. Ook moeten zijn in de gelegenheid worden gesteld tot het volgen van opleidingen op het gebied van privacy om hun rol nog beter te kunnen vervullen. Dit blijft een punt van aandacht, zeker bij personele wisselingen.

Het creëren van bewustzijn is een terugkerend aandachtspunt. Medewerkers krijgen bij indiensttreding een e-learning over privacy. Er is een nieuwe e-learning in ontwikkeling op het vlak van privacy en security, die een nieuwe impuls op het vlak van bewustzijn kan geven. Daarnaast kunnen medewerkers voor informatie op dit gebied terecht op de intranetsite. Jaarlijks besteed de privacy officer aanvullend aandacht aan privacy gedurende de privacyweek. Op intranet is ook aandacht besteed aan mijn benoeming tot FG en wat de taken van een FG zijn.

### Rechten van betrokkenen

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

Op 16 december 2022 heeft het CAK een berisping ontvangen van de AP inzake het verwijtbaar te laat reageren op een inzageverzoek van een burger. De AP gaf aan dat uiteindelijk wel aan het inzageverzoek is voldaan en dat de sanctie tot een berisping beperkt blijft omdat sprake is van een kleine inbreuk. De betrokken burger heeft op 22 juli 2023 opnieuw een klacht ingediend n.a.v. de afhandeling van een inzageverzoek. De AP heeft hierop wederom een onderzoek ingesteld. Het gaat om de termijn van beantwoording van het inzageverzoek, de vraag of een dergelijk verzoek telefonisch of schriftelijk dient te geschieden en om de bewaartermijn die van toepassing is. Het CAK heeft vragen van de AP schriftelijk beantwoord. Uiteindelijk leidt deze casus tot een uitnodiging voor een gesprek met de AP op 21 mei 2024, waarbij de afhandeling van inzageverzoeken door het CAK besproken zal worden.

Alhoewel het slechts één casus betreft, is het CAK toch tot de conclusie gekomen dat het proces van afhandeling van inzageverzoeken beter kan. Er zijn ondermeer maatregelen getroffen om tijdlijnen beter te monitoren, andere templates voor afhandelbrieven (de VWS-standaard) te gaan gebruiken en verzoeken om inzage alleen nog maar schriftelijk in behandeling te nemen.

### Samenwerking

Onder het kopje 'Beveiliging' wordt ingegaan op samenwerking in de keten op het vlak van datalekken.

Binnen VWS is er een FG-werkgroep die regelmatig bijeenkomt onder leiding van de FG van VWS. Dit platform is belangrijk om gezamenlijke problemen en nieuwe ontwikkelingen te bespreken. Binnen het VWS concern willen we de bescherming van privacy zoveel mogelijk via Rijksstandaarden inregelen. Het al eerder genoemde verwerkingenregister en het gebruik van gezamenlijke templates voor het afhandelen van inzageverzoeken zijn daarvan voorbeelden. Ik heb zelf ook regelmatig één op één contact met de FG van VWS om onderwerpen af te stemmen.

In 2023 heb ik de FG-werkgroep van de Manifestgroep opnieuw opgericht. Dit is een belangrijk platform voor intercollegiale toetsing en kennisuitwisseling met FG's van soortgelijke organisaties. Dit platform kan ook worden gebruikt om gezamenlijk tot standpuntbepaling te komen ten aanzien van issues waar deelnemers aan de Manifestgroep tegenaan lopen.

### Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat het CAK passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.

Incidenten – waaronder inbreuken – op de beveiliging moeten onder omstandigheden gemeld worden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) (meldplicht datalekken). Significante reductie van het aantal datalekken door minder handmatige acties binnen alle regelingen en digitalisering van de uitingenstroom van alle regelingen moet daarbij het streven zijn. Met het al eerder aanstellen van een datalekmanager is het proces rondom datalekken sterk verbeterd.

Eén onderwerp dat nog steeds op de agenda staat zijn datalekken veroorzaakt door (verouderde) broninformatie verkregen via ketenpartners. Het gaat hierbij niet om fouten in de keten maar om broninformatie die met vertraging wordt geactualiseerd maar wel datalekken tot gevolg heeft. Oplossingen hiervoor zijn niet makkelijk te vinden doordat medewerking van de hele keten noodzakelijk is en dan nog

doorgifte van verouderde informatie niet altijd geheel te voorkomen is. Het idee was dit vraagstuk te agenderen binnen de Manifestgroep. Daartoe is op initiatief van het CAK de FG-werkgroep van de Manifestgroep opnieuw opgericht, in eerste instantie om gezamenlijk met een standpunt naar de Autoriteit Persoonsgegevens (AP) te komen. Hiervoor bestond te weinig animo. Inmiddels is het CAK zelf door de AP uitgenodigd om te komen praten over dit type datalekken. Dit gesprek vindt 14 mei plaats.

### Specifieke aandachtspunten en doorkijk

Mijn belangrijkste constatering over het jaar 2023 is het ontbreken van een geobjectiveerde meting van compliance aan de AVG. Structureel inzicht aan de hand van objectieve meetinstrumenten zijn belangrijk om aantoonbaar aan de AVG te voldoen en een vertrekpunt voor verbetering.

De Privacy Company heeft om bovenstaande reden in opdracht van de CIO in 2023 een Quickscan gegevensbescherming 2023 uitgevoerd. De uitkomsten van deze quickscan worden nog met de RvB gedeeld. Bij het onderzoek is gebruik gemaakt van het meetinstrument van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Het CIP komt voort uit het programma Compacte Rijksdienst en is opgezet door de Belastingdienst, DUO, SVB en UWV. Participanten zijn overheidsinstellingen en marktpartijen doen mee als kennispartners. De CIP meetmethode werkt met volwassenheidsniveaus die aan de hand van objectieve criteria worden bepaald. Het is de belangrijkste standaard waarmee compliance aan de AVG wordt gemeten.

Het rapport van de Privacy Company geeft het CAK inzicht in waar we staan op alle onderdelen van gegevensbescherming en zal aanleiding zijn voor een in 2024 op te stellen plan van aanpak om gegevensbescherming naar een hoger niveau te tillen. Het is een nieuwe start met een solide basis als vetrekpunt.

Voor mij als FG is het rapport en het daaropvolgende plan van aanpak mede de basis voor toezicht in 2024. De rapportage over 2024 zal, met een nieuw format voor rapportage, gebaseerd zijn op de onderdelen die in het rapport zijn genoemd (beleid, procedures, awareness&communicatie, controle&toezicht).

Tot slot. Een FG houdt toezicht op de naleving van de AVG binnen het CAK. De AVG voorziet echter ook een belangrijke adviserende rol bij alle processen waarin persoonsgegevens worden gebruikt. Tot nu toe heeft de nadruk bij het CAK meer op de eerste dan op de tweede rol gelegen. Het verdient aanbeveling de FG meer en eerder bij ontwikkelingen te betrekken in een adviserende rol. Indien dit goed wordt ingericht hoeft dit niet te botsen met de toezichthoudende rol van een FG. Deze rolopvatting vergt wel dat opnieuw wordt bekeken hoe de functie van FG wordt ingevuld. Het zou verstandig zijn als ik in de rol van FG meer ondersteund wordt. Onder meer ook doordat burgers ook steeds vaker de weg naar de FG weten te vinden.