Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport Naleving AVG bij afhandeling Kinderopvangtoeslagenaffaire

Definitief

Colofon

Titel	Naleving AVG bij afhandeling Kinderopvangtoeslagenaffaire
Uitgebracht aan	Functionaris Gegevensbescherming DUO
Datum	11 oktober 2022
Kenmerk	2022-0000237641

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding

Op 19 januari 2021 heeft het kabinet toegezegd om de schulden van gedupeerden van de Kinderopvangtoeslagaffaire (KOT) kwijt te schelden. DUO heeft naar aanleiding van dit besluit de opdracht gekregen de invordering van schulden van mogelijk gedupeerde ouders te pauzeren en van gedupeerde ouders kwijt te schelden. De Functionaris Gegevensbescherming (FG) heeft de ADR gevraagd onderzoek te doen naar de wijze waarop uitvoering is gegeven aan de AVG-vereisten. Het doel van het onderzoek is inzicht geven op welke wijze invulling is gegeven aan de met de opdrachtgever overeengekomen onderwerpen van de Algemene Verordening Gegevensbescherming (AVG) in het proces "kwijtschelden van schulden van gedupeerden van de kinderopvangtoeslagenaffaire". Dit inzicht wil de opdrachtgever gebruiken om te bepalen of het proces voldoet aan de AVG en waar mogelijk nog risico's zitten.

Voor dit onderzoek is de volgende centrale vraag geformuleerd:

Op welke wijze is invulling gegeven aan de AVG in het proces "kwijtschelden van schulden van gedupeerden van de Kinderopvangtoeslagenaffaire" en welke risico's worden eventueel gelopen met betrekking tot de naleving van de AVG?

Hoofdboodschap: DUO heeft geen DPIA opgesteld voor de uitvoering van de KOT-regeling, wel is invulling gegeven aan verschillende AVG-onderwerpen bij de uitvoering van de regeling maar is op bepaalde aspecten verbetering mogelijk

DUO heeft voor de uitvoering van de KOT-regeling geen Data Protection Impact Assessment[1] (DPIA) opgesteld. De keuze om geen DPIA uit te voeren is niet gemotiveerd vastgelegd. Aangegeven is dat de uitvoering van de KOT-regeling onder hoge tijdsdruk plaatsvond en het DPIA-proces vertragend kan werken.

Ondanks dat geen DPIA is uitgevoerd is aan meerdere onderwerpen wel uitvoering gegeven. Het rapport geeft hier in hoofdstuk 2 nader inzicht in. Daarbij hebben wij per onderwerp een feitelijke uiteenzetting gegeven op basis van onze bevindingen vanuit interviews, documenten en deelwaarnemingen.

Op basis van ons onderzoek komen wij tot een aantal mogelijke risico's. Dit betreffen aanknopingspunten die DUO in overweging kan nemen om het proces verder te verbeteren. Het gaat om de volgende punten die in hoofdstuk 3 nader zijn toegelicht:

- Zorg voor gestructureerde vastlegging van afwegingen en risico's;
- Zorg voor een sluitende cyclus waar het gaat om de opvolging van adviezen van compliance;
- Maak afspraken over de uitvoering van controles door uitvoerders KOT-proces en laat rapporteren over de uitkomsten;
- Wees scherp op de toegang tot en het gebruik van de beveiligde KOT-map en omgang met KOT-bestanden intern;
- Maak zorgvuldige afwegingen met het oog op bewaren en vernietigen van KOT-informatie.

[1] De DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Leeswijzer

De structuur van het rapport volgt de deelvragen die wij voor dit onderzoek overeen zijn gekomen met de opdrachtgever. De deelvragen zijn:

1. Hoe is het Data Protection Impact Assessment (DPIA)-proces vormgegeven?
2. Zijn de uitkomsten van de DPIA meegenomen in het proces "kwijtschelden van schulden van gedupeerden van de kinderopvangtoeslagenaffaire"?
3. Op welke wijze is in het proces "kwijtschelden van schulden van gedupeerden van de kinderopvangtoeslagenaffaire" invulling gegeven aan de overige overeengekomen onderwerpen uit de AVG (privacy baseline CIP)?
4. Welke risico's kunnen worden geduid als het gaat om naleving van de AVG?

De eerste twee deelvragen komen aan bod in hoofdstuk 1, de derde deelvraag in hoofdstuk 2 en de vierde deelvraag over risico's behandelen wij in hoofdstuk 3. Tot slot bevat hoofdstuk 4 de verantwoording van het onderzoek.

1 DUO heeft geen uitvoering gegeven aan het DPIA-proces voor de KOT-regeling

Dit hoofdstuk gaat in op de eerste twee deelvragen.

1. *Hoe is het Data Protection Impact Assessment (DPIA)-proces vormgegeven?*
2. *Zijn de uitkomsten van de DPIA meegenomen in het proces "kwijtschelden van schulden van gedupeerden van de kinderopvangtoeslagenaffaire"?*

Aangezien uit ons onderzoek naar voren komt dat het DPIA-proces niet is vormgegeven voor de uitvoering van de KOT-regeling bij DUO, zijn beide vragen in feite beantwoord. In overleg met de opdrachtgever hebben wij wel besloten nog enige toelichting hierbij te geven en ook na te gaan of onderwerpen van de DPIA eventueel op andere wijze zijn meegenomen.

1.1 Een gemotiveerd besluit om geen DPIA uit te voeren is niet vastgelegd

DUO heeft geen DPIA opgesteld voor het KOT-proces. Wij hebben geen documentatie aangetroffen waarin gemotiveerd is opgenomen waarom de DPIA niet is opgesteld voor dit proces.
Wel is aangegeven dat het DPIA-proces vertragend kan werken en daarom mogelijk niet is uitgevoerd. De KOT-regeling stond onder hoge politieke druk en moest zo spoedig mogelijk worden vormgegeven, zodat de invordering van schulden kon worden gepauzeerd en schulden van gedupeerden kon worden kwijtgescholden. Ook is opgemerkt dat meerdere onderwerpen Rijksbreed zijn vormgegeven, zoals de grondslag voor uitwisseling van gegevens. Daardoor was volgens DUO de noodzaak minder groot een DPIA op te stellen bij DUO voor het KOT-proces.

1.2 Meerdere onderwerpen van de DPIA zijn wel op andere wijze vormgegeven

Tijdens interviews is wel verwezen naar het convenant tussen DUO en de Belastingdienst (BD) van 18 december 2020 voor de reguliere gegevensuitwisseling met de BD. Dit convenant is niet aangevuld met de gegevensuitwisseling voor uitvoering van de KOT-regeling. Hiervoor is een apart document met Technische Afspraken en Procedures opgesteld tussen DUO en de Belastingdienst (UHT), het TAP-document. In het TAP-document is ook aandacht voor een aantal AVG-aspecten. De eerste definitieve versie is van 22 juli 2021, meerdere gegevensuitwisselingen hadden toen al plaatsgevonden. De eerste conceptversie zou volgens dit document dateren van 11 februari 2021.

In het volgende hoofdstuk gaan wij nader in op de vraag hoe DUO invulling heeft gegeven aan verschillende onderwerpen opgenomen in de DPIA met betrekking tot de AVG bij uitvoering van de KOT-regeling.

2 Bevindingen over AVG-onderwerpen

In dit hoofdstuk gaan wij in op de derde deelvraag van het onderzoek.
Op welke wijze is in het proces "kwijtschelden van schulden van gedupeerden van de kinderopvangtoeslagenaffaire" invulling gegeven aan de overige overeengekomen onderwerpen uit de AVG?

Hierna geven wij bevindingen over de volgende onderwerpen/normen, die zijn overgenomen uit de privacy baseline van het CIP:

- B.02 Organieke inbedding
- B.03 Risicomanagement, Privacy by Design en de DPIA
- U.01 Doelbinding gegevensbescherming
- U.02 Register van verwerkingsactiviteiten
- U.03 Kwaliteitsmanagement
- U.04 Beveiligen van de verwerking van persoonsgegevens
- U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens
- U.06 Bewaren van persoonsgegevens
- U.07 Doorgifte persoonsgegevens
- C.01 Intern toezicht
- C.02 Toegang gegevensverwerking voor betrokkenen
- C.03 Meldplicht datalekken

Elk onderwerp is opgenomen in een afzonderlijke paragraaf en start met een korte beschrijving van de norm, zoals is verwoord in het kader van de CIP. Vervolgens hebben wij per norm de bevindingen uiteengezet.

De focus van ons onderzoek is in grotere mate gericht op het domein van Onderwijsvolgers (OVG). In beperkte mate geven wij ook inzicht in het domein van Inburgering. Waar dit van toepassing is, zal Inburgering specifiek worden benoemd.

2.1 Organieke inbedding

Om inzicht te geven in de organieke inbedding hebben wij onderzoek gedaan of de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen door de organisatie zijn vastgelegd en vastgesteld.

Hierna volgen onze bevindingen.

2.1.1 Niet alle KOT-specifieke taken, verantwoordelijkheden en bevoegdheden zijn vastgelegd en vastgesteld

DUO heeft voor de uitvoering van de KOT-regeling geen specifiek document opgesteld waarin de taken, verantwoordelijkheden en bevoegdheden zijn vastgesteld voor de uitvoering ervan. Dit heeft ook te maken met het feit dat de uitvoering grotendeels binnen de bestaande organisatie plaatsvindt, met de reguliere taken, bevoegdheden en verantwoordelijken. De aanleiding voor stopzetten van inning of kwijtschelden van schulden is anders, maar aangegeven is dat de processen niet nieuw zijn. Intern heeft DUO voor het KOT-proces voor OVG een coördinator KOT aangesteld. Inburgering beschikt niet over een coördinator, deze taak maakt deel uit van het takenpakket van de verantwoordelijke manager. Het verschil tussen OVG en Inburgering heeft te maken met de omvang van de populatie.

Nadat bekend was geworden dat publieke schulden van KOT-gedupeerden kwijtgescholden zouden worden is bij DUO een kernteam ingericht. In dit kernteam komen vertegenwoordigers van verschillende betrokken afdelingen veelvuldig bijeen

om zaken af te stemmen en de voortgang te bewaken. Een vertegenwoordiger van Inburgering maakte ook deel uit van het kernteam.
Naast het kernteam is ook een uitvoeringsteam ingericht. Hierin komen medewerkers van verschillende betrokken afdelingen wekelijks bijeen om casuïstiek over het KOT-proces te bespreken. De overleggen worden voorgezeten door de coördinator KOT. De product owner schuift soms aan en wordt geïnformeerd door de coördinator KOT indien nodig.

Voor de uitvoering van de KOT-regeling is een TAP-document opgesteld, waarin afspraken zijn opgenomen over de uitwisseling van informatie tussen de Belastingdienst (BD) en DUO. Het gaat daarbij om lijsten met zelfmelders die de BD naar DUO stuurt, een vraagbestand van DUO met de zelfmelders die een schuld hebben bij DUO en een antwoordbestand met de status van zelfmelders (gedupeerd en niet-gedupeerd of nog in onderzoek). Deze informatie wordt binnen DUO verrijkt en verspreid via verschillende schakels naar verschillende afdelingen ter verwerking. Daarbij wordt gebruik gemaakt van een beveiligde KOT-map op de L-schijf van het DUO-netwerk, deze map is alleen toegankelijk voor de daartoe geautoriseerde personen. De werkwijze aangaande de bestanden van de BD en afgeleiden daarvan in de mappenstructuur hangt veelal op medewerkers. Niet beschreven is wie welke taken, verantwoordelijkheden en bevoegdheden heeft als het gaat om verwerking van bestanden in de diverse mappen, waaronder de KOT-map op L-schijf. Ook ontbreekt een beschrijving van wie welke controles vanuit zijn functie zou moeten uitvoeren voor een juiste, volledige en tijdige verwerking van de KOT-regeling. Voor het daadwerkelijk stopzetten, kwijtschelden en herstarten van inning hebben wij wel procesbeschrijvingen en/of werkinstructies gezien, waaronder ook de geautomatiseerde bulkverwerkingen in het Studiefinancieringssysteem (SFS).

2.1.2 *DUO beschikt over diverse middelen om te voldoen aan de privacy vereisten*

DUO heeft een afdeling Compliance ingericht. Deze afdeling stelt kaders, adviseert, monitort en toetst de business op het gebied van privacy, informatiebeveiliging en archiefmanagement. De functies die onder deze afdeling vallen zijn: centrale privacy officer (CPO), privacy officers (PO), een WOO-functionaris, bedrijfsjuristen en een centrale klachtenfunctionaris. Daarnaast beschikt DUO over Adviseurs Compliance per directie die de business op dezelfde gebieden adviseren en begeleiden. Tot slot beschikt DUO over een Functionaris Gegevensbescherming (FG), deze heeft een toezichthoudende rol.

Naast de compliance gerelateerde functies beschikt DUO ook over de wiki en een kennisbank. Deze bevatten diverse procesbeschrijvingen en werkinstructies die hulp kunnen bieden om zo goed mogelijk met privacygevoelige zaken om te gaan. DUO geeft awarenesstrainingen aan nieuwe medewerkers en managers om het bewustzijn met betrekking tot onder andere privacy te vergroten. Maatwerk voor afdelingen behoort ook tot de mogelijkheden.
Verder heeft DUO een privacyverklaring waarin staat voor welke doelen persoonsgegevens worden verwerkt en om welke gegevens het gaat. De persoonsgegevens worden gebruikt om taken uit te voeren die in de wet zijn vastgelegd. DUO geeft aan dat ze persoonsgegevens zorgvuldig verwerkt in overeenstemming met de geldende wet- en regelgeving.
De privacyverklaring van DUO kan wijzigen als nieuwe ontwikkelingen daartoe aanleiding geven. Het kwijtschelden van schulden in het kader van de kinderopvangtoeslagenaffaire is niet in de privacyverklaring opgenomen.

2.1.3 *DUO heeft KOT specifieke rapportages, AGV-onderwerpen komen daarin niet terug*

Voor de uitvoering van het KOT-proces maakt DUO in geval van OVG gebruik van verschillende rapportages. De rapportages bevatten algemene informatie over de uitvoering van de KOT-regeling, zoals aantallen zelfmelders per systeem, verhoudingen en gemiddelde schulden per systeem, aantallen verzonden brieven, bedragen die zijn kwijtgescholden. Rapporten bevatten ook informatie over bedragen en uren te gebruiken door de lijn en IT. Het gaat niet om informatie over de naleving van de AVG.

2.2 Risicomanagement, Privacy by Design en de DPIA

De verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacy risico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van de maatregelen.

In deze paragraaf geven wij inzicht in de wijze waarop uitvoering is gegeven aan risicomanagement en privacy bij design voor uitvoering van de KOT-regeling.

2.2.1 *DUO heeft aandacht voor Privacy by Design, ontvangen gegevens van de BD is veelal conform afspraken (TAP), niet alle gegevens zijn aantoonbaar gebruikt*

Uit ons onderzoek komt naar voren dat aandacht is geweest voor dataminimalisatie. In het TAP-document is gemotiveerd waarom is gekozen voor de gegevensuitwisseling via bruto lijsten met zelfmelders en via vraag- en antwoordbestanden tussen de BD en DUO. Ook is nagedacht over welke informatie nodig is voor het doel. In het Tap-document is het volgende opgenomen: "Om te voldoen aan het beginsel van proportionaliteit is onderzocht of voor dit doel noodzakelijk is om gegevens te verstrekken en of deze gegevensverstrekking plaats zou kunnen vinden met minder gegevens dan reeds verstrekt zijn. Gebleken is dat, om vast te stellen of de populatie schuldenaars van het DUO getroffenen van de Toeslagenaffaire bevat, het noodzakelijk is een bestandvergelijking te maken tussen de partijen. Aangezien Belastingdienst/Toeslagen beschikt over de volledige populatie van zelfmelders en deze informatie reeds beschikbaar heeft voor zijn processen, is gekozen om deze gegevensset te verstrekken en niet de populatie schuldenaars van DUO aan de Belastingdienst/Toeslagen te verstrekken. Deze verstrekking bestaat alleen uit gegevens die noodzakelijk zijn om het doel te bereiken."
Ook in interviews is aangegeven dat is nagedacht over welke gegevens nodig zijn en hoe zorgvuldig met gegevens om moet worden gegaan.
Uit onze waarneming is naar voren gekomen dat de ontvangen bestanden van de BD conform het TAP-document zijn, maar dat DUO meerdere ontvangen gegevens van de ontvangen bestanden (nog) niet heeft gebruikt. De bruto-lijsten (zelfmelders) en het antwoordbestand van de BD bevatten gegevens als geboortedatum, voorletters, voorvoegsels en de naam. Aangegeven is dat de BD deze persoonsgegevens altijd toevoegt in het kader van de "vergewisplicht". Zo kan DUO controleren op onbedoelde persoonsverwisseling. Deze controle is niet (aantoonbaar) uitgevoerd. Verder is een kolom met een indicatie 'bezwaar' aan het antwoordbestand toegevoegd. Dit aanvullende gegeven is ook opgenomen in de geactualiseerde versie van het TAP-document van 17 maart 2022.

2.2.2 *Aangegeven is dat geen risicoanalyse is uitgevoerd, wel is aandacht geweest voor verschillende AVG-onderwerpen*

DUO heeft geen specifieke risicoanalyse opgesteld voor het KOT-proces en de privacy risico's zijn niet expliciet in beeld gebracht. Aangegeven is dat gezien de doelgroep van de KOT-regeling betrokkenen bij de uitvoering van de regeling wel meer aandacht hebben voor privacy risico's. Deze doelgroep moest goed en snel worden geholpen. De hoge tijdsdruk zorgde ervoor dat mogelijk minder aandacht is geweest voor het opstellen van een risicoanalyse.
Bepaalde DPIA-onderwerpen zijn volgens geïnterviewden in het kernteam besproken en/of uitgewerkt, zoals gegevensverwerking, doelbinding, betrokken partijen, rechtsgrond, noodzaak en beveiliging. In de notulen van het kernteam zien wij geen

duidelijke uitwerkingen terug van overwegingen omtrent risico's en te treffen maatregelen. Wel hebben wij een aantal onderwerpen teruggezien in mailberichten van verantwoordelijken met onder andere de adviseur compliance (AC) en (centrale) privacy officer (CPO/ PO).

De business heeft bij de inrichting van het KOT-proces (in de beginfase) regelmatig contact gehad met de CPO, PO), en AC over diverse privacyaspecten zoals: grondslag verwerking, beveiligde map op het DUO-netwerk, beveiligde overdracht van data tussen DUO-BD, DUO-deurwaarder, dataminimalisatie, kenmerk "hersteloperatie KOT" in een notitieveld van systemen. Dit kenmerk is in SFS tegenwoordig weergegeven middels een banner. Ook is advies gegeven door de compliance-medewerkers over uiteenlopende onderwerpen. Aangegeven is dat de terugkoppeling over de opvolging van adviezen niet altijd plaatsvindt en voor verbetering vatbaar is.

2.3 Doelbinding gegevensbescherming

De verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven wat de doeleinden en rechtvaardigheidsgronden zijn.

Hierna geven wij inzicht in de grondslag voor gegevensverstrekking.

2.3.1 De grondslag zou zijn gelegen in het kabinetsbesluit en de AWIR

De grondslag voor de gegevensverstrekking met betrekking tot (mogelijk) KOT-gedupeerden zou zijn gelegen in de taakstelling van de BD. Met de inwerkingtreding van hoofdstuk vijf van de Algemene wet inkomensafhankelijke regelingen (AWIR) behoort het volledige herstel voor gedupeerden van de kinderopvangtoeslagenaffaire tot een wettelijke taak van de BD. Op basis van het kabinetsbesluit en deze taakstelling is de gegevensverstrekking in de ogen van de BD gelegitimeerd en is er sprake van een noodzaak tot verstrekking van deze gegevens. Het pauzeren van publieke schulden, in relatie tot hoofdstuk vijf van de AWIR, wordt door de BD gezien als het verenigbaar gebruiken van deze gegevens. DUO steunt deze grondslag.

Verder steunt DUO op de "Beleidsregel kwijtschelding studieschulden gedupeerden kinderopvangtoeslagproblematiek" van OCW voor OVG en "Verzamelwetsvoorstel hersteloperatie toeslagen" van SZW voor Inburgering. OCW heeft middels twee aparte opdrachtbrieven aan DUO aangegeven dat schulden van mogelijk gedupeerden gepauzeerd mogen worden en schulden van gedupeerden kwijtgescholden. Voor inburgering heeft DUO van SZW ook een opdrachtbrief ontvangen.
Aangegeven is dat de BD contact heeft gehad met de Autoriteit Persoonsgegevens (AP) in verband met het delen van persoonsgegevens. De AP zou toestemming hebben gegeven om persoonsgegevens te delen voor de uitvoeringen van de KOT-regeling. Wij hebben kennisgenomen van een uitgave van de Uitvoeringsorganisatie Herstel Toeslagen[2] waarin is vermeld dat de AP goedkeuring heeft gegeven.

Ondanks voorgenoemde zijn niet alle geïnterviewden even gecharmeerd van de grondslag voor verwerking persoonsgegeven bij DUO voor de uitvoering van de KOT-regeling. Aan de andere kant bestaat wel begrip gezien de noodzaak om betrokkenen te helpen en de hoge tijdsdruk waaronder de uitvoering van het herstelproces KOT moest plaatsvinden.

[2] "2-wekelijkse update Schuldenproblematiek dd 16-2-2021", een uitgave van de Uitvoeringsorganisatie Herstel Toeslagen (UHT)

2.3.2 *Grondslag eenmalige levering DUO-zelfmelders aan BD niet aanwezig*

Mogelijk KOT-gedupeerden moeten zich melden bij de BD. In het begin (januari 2021) hebben mogelijk gedupeerden zich echter ook gemeld bij DUO. Gegevens van deze zelfmelders zijn door DUO doorgegeven aan de BD. Aangegeven is dat de eerdergenoemde grondslag niet van toepassing is op de eenmalige levering van de circa 120 DUO-zelfmelders aan de BD. Op ambtelijk niveau is formeel afgesproken dat DUO eenmalig de gegevens van deze zelfmelders mag delen met de BD, zodat de BD contact met hen kan opnemen en zij opgenomen kunnen worden in het gehele proces voor compensatie in het kader van de kinderopvangtoeslagenaffaire. De afspraken zijn vastgelegd in een brief[3] van de directeur-generaal DUO aan de directeur Uitvoeringsorganisatie Herstel Toeslagen bij Belastingdienst.

2.4 Register van verwerkingsactiviteiten

De verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over hun gegevensverwerkingen in een register vastgelegd; het register biedt een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.

Hierna volgt onze bevinding over de wijze waarop DUO uitvoering heeft gegeven aan het verwerkingenregister.

2.4.1 *DUO beschikt over een centraal verwerkingsregister, KOT is daarin niet apart opgenomen*

DUO beschikt over een centraal verwerkingsregister. Het register bevat informatie over persoonsgegevens die DUO verwerkt voor diverse (hoofd)processen in verschillende applicaties. Aangegeven is dat het KOT-proces niet apart in het verwerkingsregister is opgenomen, omdat verwerkingen op hoofdproces en applicatieniveau moeten worden vastgelegd. De verwerking van persoonsgegevens voor de KOT-regeling zou vallen onder de applicatie SFS (en andere OVG-applicaties), SAP (Inburgering) en hoofdprocessen van OVG en Inburgering.
Een compliance-medewerker gaf aan de voorkeur te hebben om deze specifieke verwerking toch apart op te nemen in het verwerkingsregister. Als reden is aangegeven dat het niet een reguliere verwerking is (op grond van de WSF2000), maar een verwerking voor een specifieke doelgroep die voortvloeit uit een nieuwe opdracht/regelgeving.

Het centrale verwerkingsregister van DUO hebben wij voor SFS geanalyseerd en bevat de vereisten (onderwerpen) conform de AVG. Wel blijkt uit een notitie in het register bij het proces SFS – Incasso en invordering schulden dat voor bepaalde onderwerpen nog aanvulling nodig is en nog een check op de lijst met betrokkenen en gegevens moet worden uitgevoerd.

[3] Brief DG DUO: "Overdragen zelfmelders toeslagenaffaire door DUO aan Belastingdienst", 24 maart 2021, kenmerk HD.021.038.

2.5 Kwaliteitsmanagement

De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht voor de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit op verzoek van betrokkene gebeurt, wordt deze over de status van de afhandeling geïnformeerd.

De bevindingen hierna gaan in op de wijze waarop inzage en correctie van persoonsgegevens is vormgegeven en hoe de juistheid van gegevens wordt bewaakt.

2.5.1 *Inzage of correctie van persoonsgegevens is DUO-breed geregeld*

Waar het gaat om de rechten van betrokkenen, is dit onderwerp DUO-breed geregeld. DUO beschikt over een procesbeschrijving voor afhandeling van verzoeken om inzage of correctie van persoonsgegevens. Ook bevat de privacyverklaring van DUO informatie over omgang met persoonsgegevens en hoe verzoeken om inzage of correctie in te dienen.

2.5.2 *DUO beschikt over meerdere instrumenten om de juistheid van persoonsgegevens te borgen*

Voor de juistheid van persoonsgegeven als onderdeel van kwaliteitsmanagement is deels het DUO-brede proces van toepassing. Zo bevat de privacyverklaring van DUO informatie over omgang met persoonsgegevens en hoe verzoeken om inzage of correctie in te dienen.
Specifiek voor de KOT-regeling deelt de BD bestanden met DUO, waarin bepaalde persoonsgegevens zijn geleverd voor controles gericht op onbedoelde persoonsverwisselingen. Deze controle heeft DUO (nog) niet uitgevoerd, zoals eerder benoemd in paragraaf 2.2. Daarbij hebben wij in paragraaf 2.1.1 opgemerkt dat wij geen afspraken hebben gezien over wie welke controles uitvoert.

Doordat betrokkenen zijn geïnformeerd indien sprake is geweest van stopzetten innen, kwijtschelden van schulden of herstarten van inning aan de hand van speciaal daarvoor opgestelde brieven, kunnen betrokkenen reageren indien sprake is van een onjuiste verwerking. Specifiek voor KOT kunnen betrokkenen bijvoorbeeld contact opnemen met het KOT-loket. Voorgaande draagt daarmee ook bij aan de juistheid van persoonsgegevens of juiste verwerking van gegevens.

2.6 Beveiligen van de verwerking van persoonsgegevens

De verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen om een verwerking van persoonsgegevens op een passend niveau te beveiligen.

Hierna geven wij inzicht in verschillende maatregelen.

2.6.1 *Diverse maatregelen zijn getroffen voor beveiligen van de verwerking*

DUO beschikt over beleid voor informatiebeveiliging. Voor dit onderzoek is de focus meer gericht op de specifieke onderwerpen die als gevolg van de KOT-regeling zijn ingericht. Zoals eerder aangegeven heeft DUO geen risicoanalyse uitgevoerd voor KOT. Wel is volgens diverse geïnterviewden gesproken over risico's in het proces en hoe deze gemitigeerd kunnen worden. Bij de inrichting van het KOT-proces heeft de business (OVG) regelmatig contact gehad met de CPO, PO, en AC over diverse privacyaspecten zoals: grondslag verwerking, beveiligde map op DUO-netwerk, beveiligde overdracht van data tussen BD en DUO en tussen DUO en deurwaarders. Een aantal beveiligingsmaatregelen zijn getroffen om risico's op het gebied van privacy te mitigeren.

Ter plaatse hebben wij inzage gekregen in de map op de L-schijf en van een willekeurige gegevenslevering van de BD gezien, dat deze is voorzien van een wachtwoord. Alleen personen die het wachtwoord hebben ontvangen, kunnen het betreffende bestand openen.

Voor verwerking van de lijsten van de BD maakt DUO voor OVG gebruik van een KOT-map op de L-schijf. Dit is een beveiligde map op het DUO-netwerk, waarvan is aangegeven dat een beperkt aantal medewerkers toegang tot deze map heeft (circa 52 geautoriseerde medewerkers). Het is de bedoeling dat de KOT-bestanden via deze map worden gedeeld en bewaard.
Uit interviews en waarnemingen komt naar voren dat niet iedereen die toegang heeft tot de map op de L-schijf hier ook gebruik van maakt. Ook komt het voor dat kopieën of afgeleiden van de Excelbestanden intern op een afdelingsschijf worden opgeslagen. Specifiek voor Inburgering is het gebruik van een beveiligde KOT-map ons niet bekend. Wel komt uit een interview naar voren dat bij Inburgering Excelbestanden intern per mail worden gedeeld voor de uitvoering van de KOT-regeling.

Communicatie over het pauzeren, kwijtschelden, of herstarten van zaken met externe partijen, zoals het CJIB en de voormalige DUO-deurwaarders, kennen ook maatregelen. De communicatie over (mogelijk) gedupeerden met het CJIB verloopt via het reguliere berichtenverkeer (toegankelijk middels een token) waarbij bepaalde codes worden gebruikt. Daarnaast ontvangt het CJIB voor de volledigheid een lijst met zelfmelders en gedupeerden of niet-gedupeerden via het zakelijk portaal.
Verder worden bestanden versleuteld verstuurd via de mail naar deurwaarders, waarbij het bijbehorende wachtwoord via een ander kanaal, namelijk een SMS-bericht, wordt verstuurd. Wij hebben inzage gekregen in een gegevenslevering en gezien dat deze werkwijze is toegepast.
In geval van Inburgering ontvangen deurwaarders per dossier een mail met daarin een verzoek voor pauzeren, kwijtschelden of herstarten van zaken.

2.7 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens

De verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.

Hierna geven wij inzicht in de wijze waarop DUO betrokkenen informeert.

2.7.1 DUO informeert betrokkenen via standaardbrieven op vastgestelde momenten

DUO informeert betrokkenen middels standaardbrieven over de voortgang van het proces op het moment dat DUO de informatie van de BD heeft verwerkt. Deze informatie kan aanleiding zijn om de inning van schulden te pauzeren, inning te herstarten of schulden kwijt te schelden. Uit de notulen van het kernteam blijkt dat veelvuldig aandacht is geweest voor het informeren van betrokkenen middels brieven over de voortgang van het KOT-proces.
Tussen ontvangst van informatie van de BD en de verwerking ervan binnen DUO kan enige tijd zitten. OVG en Inburgering sturen vanuit hun eigen domein allebei brieven naar betrokkenen. Bij OVG hebben wij 13 zaken ingezien en vastgesteld dat naar betrokkenen brieven zijn verstuurd in geval van pauzeren en kwijtschelden of herstarten[4]. Voor Inburgering hebben wij 1 zaak bekeken en ook vastgesteld dat de brief over het pauzeren van de invordering en in dit geval het kwijtschelden van de schuld van een gedupeerde heeft plaatsgevonden.

[4] Bij 2 zaken was sprake van een niet-gedupeerde, bij 9 zaken van een gedupeerde, de overige 2 zaken waren nog in onderzoek en was een brief voor herstart of kwijtschelding nog niet van toepassing.

Via een speciaal opgetuigd Loket (apart telefoonnummer en emailadres) kunnen (mogelijk) gedupeerden contact opnemen met DUO (in beginsel bedoeld voor OVG klanten en niet voor Inburgering). De telefonisten zijn geïnstrueerd over hoe ze de betrokkenen te woord dienen te staan. De KOT-doelgroep wordt daarbij met voorrang behandeld. Verder geldt specifiek voor SFS dat betrokkenen inzage hebben via mijn DUO in de schuldenstand in het SFS-systeem en voor Inburgering is inzage in schulden mogelijk via Mijn Inburgering.

De gegevens van mogelijk gedupeerden die zich bij DUO hebben gemeld (DUO-zelfmelders), maar niet voorkwamen op de aangeleverde lijsten van de BD zijn naar de BD gestuurd. Deze zelfmelders zijn achteraf via een brief geïnformeerd dat de gegevens met de BD zijn gedeeld. Aangegeven is dat 8 DUO-zelfmelders niet terug zijn geleverd via de antwoordbestanden van de BD. Mogelijk is geen opvolging gegeven aan de afspraak*: "Mochten er mensen zijn in deze groep die niet in aanmerking komen of willen komen voor compensatie en daarmee voor kwijtschelding van de publieke schulden, dan zal DUO ook van de Belastingdienst te horen krijgen dat zij niet behoren tot de groep van gedupeerden. De invordering van de schulden kan dan hervat worden."*
Aangegeven is dat de invorderingen van deze personen voor een jaar was gepauzeerd en inmiddels zijn hervat en dat DUO voornemens is deze klanten nog een maal per brief te berichten.

2.8 Bewaren van persoonsgegevens

Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.

Hierna volgen bevindingen over het bewaren en het vernietigen van KOT-gegevens.

2.8.1 Bewaartermijnen zijn voor KOT-specifieke informatie nog niet duidelijk

De algemene bewaartermijnen zijn vastgelegd in het document *"Generieke selectielijst Onderwijs, Cultuur en Wetenschap"* van 8 juni 2018. Deze selectielijst is ook van toepassing op DUO. Voor het bewaren van gegevens van het KOT-proces zijn geen afwijkende bewaartermijnen bepaald. Afspraken over omgang met bewaartermijnen en vernietiging van KOT-specifieke informatie in de primaire systemen en in de mappen zijn nog niet gemaakt.
Aangegeven is dat informatie over de Kinderopvangtoeslagenaffaire mogelijk als "hotspot"-informatie wordt gekwalificeerd. Daarom behandelt DUO KOT-informatie al als ware het hotspot-informatie. Hiertoe zijn afspraken opgenomen in een document genaamd *"Richtlijn archiveren afhandeling affaire Kinderopvangtoeslag"*. Specifiek is in dit document opgenomen dat het bij hotspot-informatie niet gaat om de operationele informatie en wat er per klant is gedaan aan afhandeling. Het gaat meer om informatie, die kan worden gezien als richtinggevend, besluitvormend, evaluerend, koersbepalend in de context van de KOT.

2.8.2 DUO beschikt over een vernietigingsprotocol, mogelijk niet actueel

Na het verstrijken van de bewaartermijn moeten de gegevens worden vernietigd. Aan de hand de bewaartermijnen die zijn vastgesteld in *"Generieke Selectielijst OCW"* kan worden vastgesteld wanneer gegevens moeten worden vernietigd. DUO beschikt over een vernietigingsprotocol dat dient als handreiking om een zorgvuldige vernietiging van gegevens te realiseren. Ook is verwezen naar het proces *"Selecteren en Vernietigen"*, dit document hebben wij niet aangetroffen op het Rijksportaal van DUO. Over het hoe en wanneer gegevens inzake de KOT-regeling moet worden vernietigd zijn nog geen afspraken gemaakt. Van belang is dat DUO daarbij onderscheid maakt tussen eventuele gegevens aangaande individuen voor uitvoering van de KOT-regeling en de mogelijke hotspot-informatie (bestuurlijke informatie aangaande doelgroepen). Specifieke KOT-informatie voor individuele doeleinden betreft onder

andere het kenmerk hersteloperatie KOT in primaire systemen, maar ook de bestanden van de BD en afgeleiden daarvan op de L-schijf en in mailboxen. Twee geïnterviewden betrokken bij de uitvoering hebben wel aangegeven bestanden te verwijderen uit de mailbox zodra lijsten zijn afgewerkt.

2.9 Doorgifte persoonsgegevens

Bij doorgifte aan een andere (externe) verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er voldoende garanties. Bij doorgifte naar buiten de EU zijn aanvullende eisen gesteld.

Wij hebben voor deze norm uiteindelijk vooral de focus gelegd op informatiedeling tussen DUO en het CJIB en voormalige DUO-deurwaarders (LAVG). Aandachtspunt daarbij is of DUO wegens de KOT-regeling andere informatie deelt, dan al gebruikelijk is in het reguliere proces. De bestaande afspraken tussen DUO en CJIB en DUO en voormalige DUO-deurwaarders, hebben wij niet bekeken voor dit onderzoek.

2.9.1 *Doorgifte persoonsgegevens aan CJIB en DUO-deurwaarders kent voor uitvoering van de KOT-regeling een aantal aanvullende afspraken*

DUO heeft in geval van deurwaarders en schuldsanering te maken met externe partijen. De invordering van schulden via de deurwaarder moeten worden gepauzeerd of worden stopgezet indien schulden moeten worden kwijtgescholden. Aangegeven is dat dit bestaande processen zijn.
Wij hebben een opdrachtbrief ontvangen waarin afspraken zijn opgenomen met het CJIB, deze zien voornamelijk toe op de praktische uitvoeringen van de KOT-regeling waaronder wie communiceert met de doelgroep. Voor de voormalige DUO-deurwaarders hebben wij geen opdrachtbrief ontvangen, maar wel een mail met daarin een vooraankondiging van de uitvoering van KOT-regeling.

2.9.2 *Van doorgifte van gegevens aan verwerkers buiten de EU zou geen sprake zijn*

Aangegeven is dat geen doorgifte plaatsvindt van persoonsgegevens met andere verwerkingsverantwoordelijken of verwerkers buiten de EU. DUO heeft alleen te maken met Nederlandse verwerkers en verwerkingsverantwoordelijken.

2.9.3 *Doorgifte van KOT-gegevens is herleidbaar aan de hand van codes en KOT-notitie*

Uit onze waarneming komt naar voren dat delen van informatie met het CJIB via het digitale berichtenverkeer verloopt. Dit geldt ook voor de uitvoering van de KOT-regeling. Vastlegging van doorgifte is daarmee terug te zien in het systeem mede aan de hand van codes en een KOT-notitie.
Het delen van informatie met voormalige DUO-deurwaarders is ook herleidbaar in het systeem op basis van codes en notities. De uitwisseling van informatie verloopt echter per mail, zoals eerder aangegeven. Tijdens onze waarneming hebben wij ook notities aangetroffen in het systeem DWT en gezien dat codes zijn toegepast.

2.10 Intern toezicht

Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.

Wij geven hierna inzicht in de rapportages en wijze van evaluatie.

2.10.1 *Wij hebben geen rapportages aangetroffen over de rechtmatigheid van de gegevensverwerking.*

Wij hebben geen rapportages gezien waarmee de rechtmatigheid van de gegevensverwerking van KOT-gegevens is aangetoond. Voor een ander doel, namelijk financiële rechtmatigheid, heeft de afdeling Procescontrol eind 2021 wel een controle uitgevoerd gericht op het kwijtschelden van schulden in het kader van de KOT-regeling. Daarbij is aan de hand van een deelwaarneming voor 24 zaken nagegaan of de kwijtschelding rekenkundig juist is en is toegekend aan de rechtmatig gedupeerde

en of de schulden t/m 31 december 2020 per gedupeerde volledig zijn verwerkt in de OVG-systemen. De bevindingen van Procescontrol zijn meegenomen in de maandelijkse rapportage van 2021 (november/december) en vanaf 2022 zullen bevindingen structureel onderdeel uitmaken van de reguliere viermaands rapportage OVG.

Waar het gaat om intern toezicht beschikt DUO ook over Privacy Functionarissen. Aangegeven is dat geen toets is uitgevoerd gericht op de naleving van de AVG met betrekking tot het KOT-proces.

2.10.2 *Reageren op afwijkingen en evaluatie vindt onder andere plaats in het kernteam*

Bij aanvang van de uitvoering van de KOT-regeling vond dagelijks overleg plaats over het KOT-proces. DUO heeft daartoe twee overlegvormen ingericht voor KOT: kernteamoverleg en uitvoeringsteamoverleg. Tegenwoordig vindt nog wekelijks afstemming plaats over het KOT-proces. Uit notulen maken wij op dat regelmatig casuïstiek voorbij is gekomen vanuit de uitvoering. Dit zorgt ervoor dat knelpunten gesignaleerd en geadresseerd kunnen worden. Ook is het voornemen om 1 à 2 keer per jaar een brede evaluatie plaats te laten vinden met de kernteamleden. Deze brede evaluatie heeft tot nu toe een keer plaatsgevonden en lijkt op basis van notulen vooral gericht te zijn geweest op de samenwerking.

2.10.3 *Is er een functionaris gegevensbescherming (FG) aangesteld*

DUO heeft een onafhankelijke, interne toezichthouder aangesteld. Deze Functionaris voor de Gegevensbescherming ziet erop toe dat de verwerkingen van persoonsgegevens binnen DUO in overeenstemming zijn met de wet.

2.11 Toegang gegevensverwerking voor betrokkenen

De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.

Hierna geven wij inzicht in toegang tot de gegevensverwerkingen voor uitvoering van de KOT-regeling voor betrokkenen.

2.11.1 *Informatie over verwerking van persoonsgegeven vindt plaats middels brieven op vastgestelde momenten en via Mijn DUO of Mijn Inburgering*

Op de website van DUO staat een privacyverklaring waarin is aangegeven met welk doel DUO persoonsgegevens verwerkt. Deze verklaring bevat geen nadere informatie over de verwerking van gegevens voor de uitvoering van de KOT-regeling. DUO informeert betrokkenen wel via standaardbrieven indien de inning wordt gepauzeerd, hervat of schulden worden kwijtgescholden op basis van informatie van de BD. DUO verstuurt deze brieven op het moment dat DUO de informatie vanuit de BD heeft verwerkt.

Verder hebben betrokkenen de mogelijkheid om in geval van studiefinanciering via Mijn DUO inzage te krijgen hun (persoons)gegevens, die bekend zijn bij DUO. Voor Inburgering is inzage mogelijk via Mijn Inburgering. Tot slot beschikt DUO over een loket voor de doelgroep waar betrokkenen per telefoon of mail informatie kunnen opvragen aangaande OVG. Inburgering maakt geen gebruik van een KOT-loket, gezien het geringe aantal mogelijk KOT-gedupeerden, en gebruikt de reguliere kanalen.

2.12 Meldplicht datalekken

De verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.

Hierna geven wij inzicht in de wijze waarop melding van datalekken is vormgegeven en welke maatregelen DUO kent ter voorkoming van datalekken.

2.12.1 *Centraal datalekregister bevat melding van mogelijke datalekken*

DUO beschikt over één centraal datalekregister. (Vermoedelijke) datalekken moeten worden gemeld bij de afdeling Compliance en worden daar geregistreerd en beheerd. De verantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk en informeert de betrokkene, tenzij hiervoor een uitzondering geldt. Waar het gaat om verwerking van KOT-gegevens, zijn intern twee datalekken gemeld. Wij hebben afschriften ontvangen van de meldingen, waaruit blijkt dat deze meldingen zijn geregistreerd in Topdesk. Het verantwoordelijk managent is geïnformeerd en ook de Adviseur Compliance en de Privacy Officer. De datalekken zijn niet gemeld bij de Autoriteit Persoonsgegevens, dit was volgens de behandeld privacy officer niet nodig.

2.12.2 *Diverse middelen zijn voorhanden om een mogelijk datalek te onderzoeken*

Om de gegevens goed te beschermen beschikt DUO over verschillende functionarissen zoals eerder genoemd in paragraaf 2.1.2. Zo adviseren de CPO en de PO-ers op alle gebieden aan zowel medewerkers als aan het management met betrekking tot de bescherming van persoonsgegevens. De AC werkt binnen een directie en adviseert en ondersteunt op operationeel en strategisch niveau binnen haar of zijn directie met betrekking tot vraagstukken op de gebieden Privacy, Informatiebeveiliging en Archiefmanagement. De FG houdt toezicht op de juiste verwerking van persoonsgegevens door DUO en is adviseur voor het bestuur over tactische en strategische zaken. Met betrekking tot de melding van datalekken en de afhandeling ervan zijn diverse procesbeschrijvingen opgesteld en is op de site van DUO informatie opgenomen.
De AC van OVG is betrokken geweest bij het KOT-proces, die van Inburgering niet.

2.12.3 *DUO beschikt over diverse maatregelen ter voorkoming van datalekken*

DUO heeft diverse maatregelen getroffen en hulpmiddelen beschikbaar gesteld om datalekken te voorkomen. Zo zijn er stukken opgesteld met betrekking tot autorisatiebeheer en autorisatiebeleid, clear desk beleid, verwerkersovereenkomst, DPIA of een compliance formulier. Ook worden awarenesstrainingen (op maat) gegeven en wordt maandelijks gerapporteerd op directieniveau over aangetroffen datalekken. Dit alles om het risico op een datalek te voorkomen en indien van toepassing zorgvuldig af te handelen.

3 Risico's en verbetermogelijkheden

Het laatste hoofdstuk gaat in op welke risico's kunnen worden geduid als het gaat om naleving van de AVG. Wij hebben in het vorige hoofdstuk inzicht gegeven in de wijze waarop DUO invulling heeft gegeven aan onderwerpen van de privacy baseline van het CIP. Dit is de basis geweest voor onze analyse om te komen tot risico's die eventueel worden gelopen in het KOT-proces op het gebied van privacy. De eventuele risico's geven DUO handvatten om het proces verder te verbeteren om te kunnen voldoen aan de AVG. Het is uiteindelijk aan de opdrachtgever/DUO een afweging te maken of en wat te doen met onderstaande punten.

3.1 Zorg voor gestructureerde vastlegging van afwegingen en risico's

Uit ons onderzoek komt naar voren dat geen DPIA is opgesteld. De afweging voor deze keuze is niet gemotiveerd vastgelegd. Wij hebben wel vernomen dat afwegingen zijn gemaakt over de wijze waarop risico's te adresseren. De vastlegging van risico's en getroffen maatregelen zijn beperkt inzichtelijk. Dit maakt het moeilijker om opvolging van risico en maatregelen te monitoren.

3.2 Zorg voor een sluitende cyclus bij opvolging van adviezen compliance

Uit ons onderzoek komt naar voren dat niet altijd duidelijk is voor functionarissen met een advies/compliance rol of en welke opvolging is gegeven aan adviezen. Belangrijk is dat de opvolging van gegeven adviezen bewaakt wordt. Belangrijk is goede afspraken te maken over de wijze waarop DUO hier invulling aan wil geven. Dit betekent ook escaleren indien opvolging uitblijft. Belangrijk is dat op het juiste niveau bewuste afwegingen worden gemaakt en vervolgens worden teruggekoppeld richting de adviseur of de compliance-functionaris.

3.3 Maak afspraken over de uitvoering van controles en rapporteer over de uitkomsten

Afspraken over wie welke controles uitvoert met het oog op een juiste, tijdige en volledige verwerking van persoonsgegevens en wanneer zijn niet vastgelegd. Het risico is dat controles niet uitgevoerd worden of mogelijk dubbel. Besteed daarbij ook aandacht aan de aantoonbaarheid van uitgevoerde controles en op welke wijze uitkomsten moeten worden gerapporteerd.

Voor het KOT-proces maakt DUO gebruik van meerdere Excelbestanden en deze bestanden zijn vatbaarder voor onbedoelde mutaties. Ons advies zou zijn ook eenvoudige controles in te bouwen, zodat eventuele onbedoelde omissies tijdig worden gesignaleerd. Denk aan gebruik van hashtotalen (de som van ID-nummers en artikelnummers), waarmee vergelijking tussen bestanden gemaakt kan worden.

3.4 Wees scherp op het gebruik van de KOT-map en omgang met KOT-bestanden intern

Uit het onderzoek komt naar voren dat niet alle personen met toegang tot de beveiligde KOT-map op de L-schijf, hier gebruik van maken. Ook komt het voor dat lijstwerk of afgeleiden daarvan opgeslagen worden in decentrale mappen buiten de KOT-map. Verder worden bestanden soms intern per mail doorgezet naar collega's voor verdere verwerking. Voorgenoemden werkwijzen en omgang met bestanden maakt dat minder grip is op verspreiding van KOT-gegevens binnen DUO. Het risico is dat meer personen toegang hebben tot de informatie dan wenselijk.

Breng het belang van het gebruik van de beveiligde KOT-map op de L-schijf opnieuw onder de aandacht. Maak duidelijke afspraken over het gebruik hiervan en het gebruik van decentrale afdelingsmappen en mail.

3.5 Maak zorgvuldige afwegingen met het oog op bewaren en vernietigen van KOT-informatie

Waar het gaat om de bewaartermijnen van persoonsgegevens, dan is informatie opgeslagen in de KOT-map, de afdelingsmappen en mailboxen een belangrijk punt van aandacht. Dit naast de KOT-informatie in de reguliere primaire systemen. Hoewel DUO beschikt over de Generieke Selectielijsten van OCW met bewaartermijnen, is het gezien de KOT-affaire belangrijk te bepalen of deze affaire al dan niet van invloed is op de huidige bewaartermijnen. Deze afweging hebben wij nog niet teruggezien.

Tijdens interviews is verder aangegeven dat de indicatie KOT in de primaire systemen eenvoudig kan worden verwijderd. Indien deze indicatie wordt verwijderd is het van belang om na te gaan of dit geen afbreuk doet aan de herleidbaarheid van doorgifte van gegevens aan bijvoorbeeld deurwaarders en met het oog op verantwoording.

Verder ontvangt DUO brutolijsten met zelfmelders van de BD. Deze lijsten zijn nog niet verwijderd. Onduidelijk is op basis van welke grondslag deze informatie bewaard blijft en voor welke termijn. Wel merken wij op dat de lijsten zijn voorzien van een wachtwoord en alleen toegankelijk zijn voor personen die het wachtwoord hebben ontvangen van de BD.

Tot slot hebben wij gezien dat DUO beschikt over een vernietigingsprotocol. In dit protocol wordt verwezen naar het proces "*Selecteren en Vernietigen*", echter hebben wij dit proces niet terug kunnen vinden op het Rijksportaal van DUO. Mogelijk dat de informatie nog niet actueel is, wat van invloed kan zijn op een zorgvuldige vernietiging van informatie.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Werkzaamheden
Voor beantwoording van de deelvragen en centrale vraag hebben wij documenten bestudeerd en interviews afgenomen van diverse betrokkenen bij de uitvoering van de KOT-regeling bij DUO. Ook hebben wij een dossieronderzoek uitgevoerd en een waarneming ter plaatse verricht om inzicht te krijgen in werkwijze aangaande de KOT-map en informatie die DUO vastlegt met betrekking tot de uitvoering van KOT-processen.

Als referentiekader hebben wij gebruik gemaakt van de privacy baseline van het CIP (Centrum Informatiebeveiliging en Privacybescherming). De onderwerpen uit deze baseline komen terug in hoofdstuk 2. Het rapport is afgestemd met de verantwoordelijk managers van OVG en R&E. Vervolgens is het rapport voorgelegd aan de opdrachtgever en definitief gemaakt.

Afbakening onderzoek
Het object van onderzoek is het proces "kwijtschelden van schulden van gedupeerden van de kinderopvang-toeslagenaffaire". Daarbij is het onderzoek gericht op de naleving van de AVG. Relevante gegevens in het kader van de AVG voor dit proces zijn onder andere de opgestelde lijsten met (mogelijk) gedupeerden van de BD, informatiedeling met de deurwaarders en interne DUO-registraties.
Het onderzoek geeft inzicht in of relevante beheersmaatregelen aangaande de AVG zijn vastgelegd (opzet) en of de beheersmaatregelen ook worden toegepast in de praktijk (bestaan). Wij hebben niet getoetst of de gewenste beheersmaatregelen over een bepaalde periode effectief hebben gewerkt (werking).

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

4.3 Verspreiding rapport

De opdrachtgever, , is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

5 Ondertekening

Den Haag, 11 oktober 2022

Projectleider
Auditdienst Rijk

Bijlage 1: managementreactie OVG

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Directie
Onderwijsvolgers
Afdeling
-
Contactpersoon

Datum
5 september 2022
Bijlagen
-

memo

Managementreactie: onderzoeksrapport Naleving AVG bij afhandeling Kinderopvangtoeslagenaffaire

Beste

Om te beginnen dank ik u voor de oplevering van de resultaten van uw onderzoek naar de naleving van de AVG bij de afhandeling van de Kinderopvang-toeslagenaffaire. In het onderzoek heeft u gekeken naar de wijze waarop invulling wordt gegeven aan de AVG in het proces "kwijtschelden van schulden van gedupeerden van de Kinderopvangtoeslagenaffaire" en welke risico's daarbij eventueel zijn gelopen met betrekking tot de naleving van de AVG. In dit memo gaan we in op uw bevindingen en aanbevelingen.

Het pauzeren van het innen van schulden bij gemelde gedupeerden van de KOT en het kwijtschelden van de schulden bij daadwerkelijk gedupeerden is onder hoge druk ontwikkeld. DUO heeft deze activiteiten met zeer betrokken, bevlogen en verantwoordelijke medewerkers in korte tijd opgezet en stapsgewijs uitgebouwd. Er is een sterke drang om dit goed uit te voeren. De verbeterpunten zijn met dankbaarheid in ontvangst genomen en zullen bijdragen aan de kwaliteit van de uitvoering.

De constatering dat DUO voor de uitvoering van de KOT-regeling geen DPIA heeft opgesteld is correct. Voor de regeling voor het kwijtschelden van de studieschulden is een apart document met Technische Afspraken en Procedures opgesteld tussen DUO en de Belastingdienst (UHT), het TAP-document. In het TAP-document is ook aandacht voor een aantal AVG-aspecten zoals de grondslag voor uitwisseling van gegevens. Daarcoor was volgens DUO de noodzaak minder groot een DPIA op te stellen bij DUO voor het KOT-proces. De gesprekken rondom dit thema zijn gevoerd in het kernteam voor de KOT, maar hadden beter gemotiveerd vastgelegd moeten worden. Ondanks dat geen DPIA is uitgevoerd is aan meerdere onderwerpen wel uitvoering gegeven. Op basis van ons onderzoek komt u tot een aantal mogelijke risico's en verbeterpunten. Hieronder wordt per punt uit hoofdstuk 3 van uw onderzoek onze reactie gegeven:

3.1 Zorg voor gestructureerde vastlegging van afwegingen en risico's
Dit verbeterpunt wordt overgenomen. Er wordt aan verslaglegging gedaan van de overleggen. De verslagen zijn kort en bondig (op afsprakenniveau). Hierdoor zijn overwegingen en geconstateerde risico's minder goed vastgelegd. Dit is een aandachtspunt voor de toekomst.

Pagina 1 van 2

3.2 Zorg voor een sluitende cyclus waar het gaat om de opvolging van adviezen van compliance;
Dit punt wordt overgenomen. Hier wordt opgemerkt dat direct bij de start van de activiteiten compliancy officers actief betrokken zijn geweest om samen met de kernteam leden de eerste opzet van de werkwijzen op te zetten. Hun input is onderdeel van de reguliere werkwijzen geworden en dat is tijdens de veelvuldige opstartbijeenkomsten ook besproken. Later in het traject is de directe betrokkenheid van de compliancy officer bij deze overleggen afgenomen. Op dat moment had de cyclus anders ingericht moeten worden.

3.3 Maak afspraken over de uitvoering van controles door uitvoerders KOT-proces en laat rapporteren over de uitkomsten;
Dit punt wordt overgenomen. DUO heeft na de eerste opstartfase een coördinator aangesteld die verantwoordelijk is voor de administratie van de gegevensuitwisselingen met de UHT, de verdeling van de te verrichten kwijtscheldingen en het vastleggen hiervan. Bij aanvang was dit proces relatief eenvoudig en overzichtelijk. Inmiddels is er echter sprake van een veelvoud aan lijsten en bestanden waardoor de complexiteit is toegenomen. Op dit moment worden de stappen ondernomen die onbedoelde omissies gaan voorkomen. Bij veel van de kwijtscheldingen wordt gebruik gemaakt van al langer bestaande transacties, (systeem)processen en controles. DUO zal de controles evalueren en extra aandacht besteden aan het vastleggen van de afspraken en de resultaten van de controles.

3.4 Wees scherp op de toegang tot en het gebruik van de beveiligde KOT-map en omgang met KOT-bestanden intern;
Dit punt wordt overgenomen. Er is bij aanvang afgesproken alleen de beveiligde KOT-map op de L-schijf te gebruiken en dat de toegang hiertoe beperkt moet zijn. De toegang tot deze map wordt geëvalueerd en waar nodig aangepast. Decentraal opslaan van gegevens of delen van gegevens buiten deze map is niet toegestaan. Het nakomen van deze afspraken zal opnieuw onder de aandacht gebracht worden.

3.5 Maak zorgvuldige afwegingen met het oog op bewaren en vernietigen van KOT-informatie
Dit advies wordt overgenomen. DUO zal i.o.m. haar compliancy officers het protocol hiervoor ontwikkelen.
In de primaire systemen kunnen gegevens eenvoudig verwijderd worden. Hetzelfde geldt voor de gegevens in de beveiligde map. De indicaties worden verwijderd zodat dit geen afbreuk doet aan de verantwoording die DUO moet afleggen over de verrichte activiteiten (compliancy en accountability). Daarbij houden we uiteraard ook rekening met de bestaande wet- en regelgeving m.b.t. het schonen van gegevens van (oud) studenten.

Met vriendelijke groeten,
Directeur Onderwijsvolgers

Bijlage 2: managementreactie R&E

Aan: Auditor Sector Operational Audit
Van: directeur Registers & Examens (R&E)

Directie
Registers & Examens
Afdeling
M&O
Contactpersoon

Datum
13 september 2022
Bijlagen
geen

memo Managementreactie op Onderzoeksrapport KOT AVG DUO

Beste

Het MT-R&E heeft kennis genomen van het Onderzoeksrapport KOT AVG DUO en de vermelde bevindingen en conclusies.

Algemeen.
Zoals in het rapport aangegeven moet de wijze waarop invulling is gegeven aan de taakuitvoering gezien worden in het licht van de maatschappelijke, bestuurlijke en politieke druk om snel en adequaat te acteren richting de betrokken burgers. De signalering dat een DPIA ontbreekt is in dat kader verklaarbaar, maar is gelijk ook een terecht aandachtspunt voor de toekomst. Zo zou achteraf geconstateerd kunnen worden dat in deze een paralleltraject een optie was geweest.

Niet tegenstaande het gegeven dat vanuit de directie RenE/Examens/Inburgering van meet af aan nauwe samenwerking heeft plaatsgevonden met het DUO brede project, moet ook het volgende opgemerkt worden.
Anders dan voor OVG geldt voor Inburgering dat het om een beperkt aantal burgers gaat én dat noodzakelijke procedures en bijbehorende rollen/verantwoordelijkheden reeds vergaand ingericht waren. Datzelfde geldt voor de afstemmingslijnen met de opdrachtgever (SZW, directie SenI) en de (reguliere) verantwoordingsrapportages.

Specifiek.
Hieronder treft u een reactie aan op de benoemde aanbevelingen.

- Aanbeveling 3.1
  Onder verwijzing naar het hierboven gestelde worden uw bevindingen en uw aanbeveling onderschreven. N.a.v. de aanbeveling zullen, voor zover nog relevant voor de verdere afronding, risico's en getroffen maatregelen eenduidig worden vastgelegd.

- Aanbeveling 3.2
  Niet tegenstaande dat de afstemming met Compliance standaard onderdeel uitmaakt van de ingerichte procedures binnen mijn directie, onderschrijf ik het aangeven belang om functionarissen met een advies/compliance rol te informeren over of en welke opvolging is gegeven aan adviezen.
  In dat kader heb ik inmiddels gevraagd om, in nauw overleg met Compliance, te bezien welke nadere afspraken in dit kader wenselijk of nodig zijn.

- Aanbeveling 3.3
  Zoals hierboven, onder algemeen, aangegeven geldt enerzijds dat sprake is van een zeer beperkte doelgroep ('taakuitvoering Inburgering') en die doelgroep anderzijds geen relatie heeft met andere onderdelen van DUO op dit onderwerp.

  In algemene zin kan ik de aanbeveling en de voorgestelde maatregel volgen, maar heb mijn aarzeling bij het door u in deze beoogde effect voor deze doelgroep.

Pagina 1 van 2

In dat kader wacht ik de meer DUO brede ontwikkelingen ten aanzien van dit punt af met de opmerking dat hieraan alsdan, uiteraard, volledige medewerking verleend zal worden.

- Aanbeveling 3.4
  N.a.v. de aanbevelingen is een Samenwerkruimte ingericht met de naam Kinderopvangtoeslag Inburgering. Deze sterk beveiligde ruimte wordt alleen door direct bij het KOT-proces betrokkenen gebruikt. Het beheer van deze ruimte (inclusief toegangsrechten verlenen en intrekken) ligt bij [redacted] (manager DPD-RNE-EMS2). Over het gebruik van de Samenwerkruimte zijn werkafspraken gemaakt. Bestanden met gegevens worden alleen nog (rechtstreeks) in deze ruimte geplaatst. Er gaan geen gegevens meer rond via mail of andere kanalen.

  Vóór het gebruik van deze Samenwerkruimte werden bestanden op verschillende plaatsen door betrokkenen bewaard, deze zijn d.m.v. een schoningsactie verwijderd.

Met vriendelijke groeten,

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00