Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport t.b.v. DUO
Beheersing privacyaspecten proces uitwonendencontrole

Definitief

Colofon

Titel	Onderzoeksrapport DUO Beheersing privacyaspecten proces uitwonendencontrole
Uitgebracht aan	Dienst Uitvoering Onderwijs
Datum	14 september 2023
Kenmerk	2023-0000206525

Inlichtingen
Auditdienst Rijk

Inhoud

Verbeteringen noodzakelijk om verdere privacybescherming te borgen

Inleiding

De afdeling Handhaving & Inspectie (H&I) van Dienst Uitvoering Onderwijs (DUO) is verantwoordelijk voor het opsporen van fraude, misbruik en oneigenlijk gebruik van regelingen en tegemoetkomingen van DUO, waaronder de uitwonendenbeurs. DUO wil graag inzicht hebben of bij de hiervoor gebruikte risicoprofielen en de verslaglegging na huisbezoeken de nodige waarborgen zijn getroffen om te voldoen aan privacywetgeving, wat eventuele omissies zijn en welke (mogelijk) aanvullende maatregelen nodig zijn. De Auditdienst Rijk (ADR) is gevraagd hiernaar onderzoek te doen. Het intakegesprek heeft in oktober 2022 plaatsgevonden. Dit heeft geleid tot een opdracht in december 2022.

Voor dit onderzoek is de volgende centrale vraag geformuleerd:
Wordt voldaan aan de gestelde eisen van bescherming van (bijzondere) persoonsgegevens volgens de privacywet- en regelgeving bij de deelprocessen profilering' en 'huisbezoek' van het proces Controle Uitwonendenbeurs?

Hierbij zijn de volgende deelvragen geformuleerd:
1. Hoe verlopen de deelprocessen 'profilering' en 'huisbezoek' van het proces Uitwonendencontrole?
2. Welke risico's op het gebied van privacy zijn te onderkennen bij de deelprocessen 'profilering' en 'huisbezoek'?
3. Welke beheersmaatregelen zijn getroffen om te borgen dat op de juiste wijze met de (bescherming van) persoonsgegevens wordt omgegaan bij het hanteren van het risicoprofiel en het afleggen en vastleggen van huisbezoeken?

Managementsamenvatting

DUO beschikt over een procesbeschrijving voor Controle Uitwonendenbeurs, waaronder profilering en huisbezoek. We hebben vastgesteld dat deze processen tot stand komen met gebruikmaking van onder andere een algoritme, het verrijken van de uitkomsten daarvan met gegevens uit basisregistraties en de uiteindelijk besluitvorming over de te selecteren studenten voor huisbezoek door een bevoegde medewerker, dus met menselijke tussenkomst.

In ons onderzoek hebben wij vastgesteld dat DUO een aantal maatregelen heeft getroffen in het proces Controle Uitwonendenbeurs om de bescherming van persoonsgegevens te borgen. In deze managementsamenvatting benoemen we de onderwerpen die onzes inziens noodzakelijk zijn om met aanvullende maatregelen de privacybescherming verder te borgen. Ook benoemen we een aantal maatregelen die wel zijn getroffen.

1. De taken, bevoegdheden en verantwoordelijkheden van de *privacy*organisatie zijn DUO-breed summier beschreven;
2. Wij hebben een beschreven inrichting van rapportage- en verantwoordingslijnen in opzet aangetroffen;

3. Er is een DUO-breed risicobeheersingskader opgesteld en over het organisatiebrede kwaliteitsmanagementsysteem is in 2023 een ISO-9001:2015 certificaat van goedkeuring afgegeven door Bureau Veritas;
4. De privacyrisico's voor het proces Controle Uitwonendenbeurs zijn niet structureel in kaart gebracht. Hierdoor is er onvoldoende inzicht of het stelsel van getroffen maatregelen toereikend is;
5. Er is geen Data Protection Impact Assessment (DPIA) uitgevoerd, terwijl het proces Controle Uitwonendenbeurs een hoog risico met zich meebrengt en er wel duidelijke procedures voor zijn ingericht. Ook hiervoor geldt dat er onvoldoende inzicht is of het stelsel van getroffen maatregelen toereikend is. DUO had eind 2022 intern het advies gegeven een DPIA op te stellen;
6. We hebben geen informatie aangereikt gekregen waaruit opgemaakt kan worden of en hoe het proces dataminimalisatie is ingericht en wordt nageleefd;
7. Conform het vastgestelde beveiligingsbeleid rapporteert DUO periodiek over de getroffen maatregelen intern en aan de SG van het departement Onderwijs, Cultuur en Wetenschap;
8. Er is geen Informatie- en bronanalyserapport (IBAR) opgesteld waarin wordt beschreven op welke wijze het risicoprofiel en de risicocoderingen zijn ingericht en worden toegepast. Dit maakt het moeilijk verantwoording af te leggen (in het Algoritmeregister);
9. Retentiebeleid is DUO-breed ingericht, maar de uitwerking hiervan is binnen het proces Controle Uitwonende beurs nog niet vastgesteld. Sinds 2011 zijn daar geen retentieactiviteiten ondernomen, te weten verwijderen, vernietigen, anonimiseren;
10. De door DUO gepubliceerde privacyverklaring maakt inzichtelijk voor welke doeleinden DUO persoonsgegevens verwerkt. De rechtmatige grondslag van deze verwerkingen kan herleid worden naar wettelijke bepalingen;
11. Het proces Controle Uitwonenden Beurs is opgenomen in het DUO-brede register van verwerkingsactiviteiten en zal volgens DUO in 2023 in het OCW-brede register van verwerkingsactiviteiten worden opgenomen;
12. Om de juistheid, nauwkeurigheid en volledigheid van de persoonsgegevens te borgen en in het kader van profilering de betrokkene in staat te stellen tussentijds zijn rechten uit te oefenen, dient DUO kwaliteitsmanagement in te richten. We hebben geconstateerd dat er een aantal maatregelen getroffen is, maar dat een beschrijving van het kwaliteitssysteem ontbreekt;
13. Geconstateerd is dat het interne toezicht op de gegevensverwerking ingericht is conform het Three Lines Model. Er is echter gebleken dat er momenteel nog onvoldoende proactieve monitoringsactiviteiten plaatsvinden op de beheersing van privacyrisico's;
14. Binnen DUO is weliswaar een procedure ingericht voor het opstellen van verwerkersovereenkomsten, maar wij hebben vastgesteld dat nog niet voor alle verwerkers uit het proces Controle Uitwonendenbeurs een definitieve verwerkersovereenkomst aanwezig is;
15. Met de privacyverklaring geeft DUO invulling aan de transparantieverplichting in het kader de verwerkingen van persoonsgegevens. Middels de beschikbaar gestelde informatie over de verwerking van persoonsgegevens kan de betrokkenen zijn rechten uitoefenen omtrent inzage, corrigeren, aanvullen en verwijderen. De informatievoorziening behelst echter niet de mogelijkheid om andere rechten, te weten bezwaar met betrekking tot geautomatiseerde besluitvorming en profilering, uit te oefenen. Verder komt uit de informatievoorziening niet naar voren of en op welke manier mogelijk gebruik gemaakt wordt van profilering en/of er sprake is van geautomatiseerde besluitvorming en de gevolgen daarvan.

Leeswijzer

Dit rapport volgt de deelvragen die wij voor dit onderzoek overeen zijn gekomen met de opdrachtgever. Deze zijn opgenomen onder de 'inleiding'.

De eerste deelvraag komt aan bod in hoofdstuk 1, de tweede en derde deelvraag in hoofdstuk 2 en de aanbevelingen worden beschreven in hoofdstuk 3. Tot slot bevat hoofdstuk 4 de verantwoording van het onderzoek.

1 Deelprocessen profilering en huisbezoek

De afdeling H&I van DUO is verantwoordelijk voor het opsporen van fraude, misbruik en oneigenlijk gebruik van regelingen en tegemoetkomingen van DUO. Wij hebben de onderdelen van het proces Controle Uitwonendenbeurs (CUB) en specifiek de deelprocessen 'profilering' en 'huisbezoek' in kaart gebracht.

In dit hoofdstuk wordt antwoord gegeven op deelvraag 1.

Deelvraag 1:
Hoe verlopen de deelprocessen 'profilering' en 'huisbezoek' van het proces Uitwonendencontrole?

Waar wij de term 'profilering' gebruiken, hanteren wij de definitie zoals in artikel 4.4 van de AVG staat beschreven:
"*Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.*"

1.1 Proces Controle Uitwonendenbeurs

DUO beschikt over een procesbeschrijving voor het hoofdproces CUB waarin de deelprocessen 'profilering' en 'huisbezoek' zijn beschreven. In deze paragraaf schetsen we het proces op hoofdlijnen.

Uitwonende studenten worden door een bevoegde medewerker aan de hand van het basisbestand geselecteerd voor huisbezoek. Er zijn vier private partijen gecontracteerd voor het uitvoeren van de huisbezoeken. Op basis van een opgesteld rapport door de private partij beoordeelt DUO handmatig of er sprake is van misbruik. Bij vastgesteld misbruik kunnen de volgende maatregelen worden opgelegd: herziening van de uitwonendenbeurs, beëindigen van het recht op een uitwonendenbeurs en oplegging van een bestuurlijke boete.

In de procesbeschrijving van DUO worden een aantal werkstappen verder uitgewerkt, nl. het toepassen van het risicoprofiel (paragraaf 1.2) en huisbezoek (paragraaf 1.3).

1.2 Toepassen risicoprofiel (profilering)

Uit het SFS-systeem (Studiefinancieringssysteem) wordt door DUO een dump gehaald met een selectie van studenten met een toekenning uitwonendenbeurs plus het woonadres en GBA-adres (Gemeentelijke Basisadministratie). Deze dump wordt met behulp van een query verrijkt met bepaalde kenmerken, zoals correspondentienummer student en ouders, Burgerservicenummer, geslacht en geboortedatum van de student en gegevens van de onderwijsinstelling. Op de met deze gegevens verrijkte dump wordt vervolgens geautomatiseerd het risicoprofiel en de risicocodering toegepast.

Risicoprofiel
Het risicoprofiel is een set van persoonlijke aspecten van een natuurlijk persoon. Het gaat hierbij om de volgende combinaties van volgens DUO objectieve kenmerken van de student:

- Leeftijd;
- Onderwijssoort;
- Afstand woonadres student en ouders op basis van de adressen uit de Basisregistratie Personen (BRP).

Als de student aan bepaalde waardes van deze kenmerken voldoet, is dat volgens DUO een indicatie voor een verhoogde kans op regelovertreding.

Risicocodering
Vervolgens vindt er een risicocodering plaats door de drie kenmerken te scoren / wegen. Het vermenigvuldigen van de gewogen kenmerken van de studenten met een uitwonendenbeurs resulteert in een overzicht gesorteerd op onderwijsniveau en leeftijdscategorie. De studenten met het hoogste risicogetal worden bovenaan de selectielijst, ook wel het basisdocument genoemd, geplaatst. Studenten met een hoog risicogetal maken een grotere kans geselecteerd te worden voor deskresearch.

1.3 Huisbezoek

Selectie
Eerst vindt er sortering van dossiers plaats per regio, gemeente en/of stad. Geselecteerde studenten uit het basisdocument worden via deskresearch handmatig beoordeeld door een bevoegde DUO-medewerker. Handmatig worden aanvullende (persoons)gegevens, zoals locatie onderwijsinstelling, huisgenoten, stageadres, woonoppervlakte en een combinatie ervan, verzameld die bijdragen om een gedegen keuze te kunnen maken of een huisbezoek moet plaatsvinden. Vervolgens worden dossiers toebedeeld aan de private partij werkzaam in een bepaald werkgebied. In het systeem wordt in het basisbestand aangemerkt of een student is geselecteerd, waarbij ook de voortgang wordt aangegeven. Als een student na deskresearch niet is geselecteerd, wordt dit ook met een reden vermeld in het basisbestand.

Wij hebben geconstateerd dat uitwonende studenten binnen het proces CUB niet worden onderworpen aan uitsluitend geautomatiseerde individuele besluitvorming. Er is namelijk sprake van menselijke tussenkomst.

Voor de feitelijke huisbezoeken heeft DUO diverse private partijen ingeschakeld die voor een bepaalde periode zijn aangewezen door de Minister van OCW. Dossiers van geselecteerde studenten worden via het zakelijk portaal van DUO aangeleverd. Voor de externe controleurs van de private partijen zijn richtlijnen opgesteld voor het brengen van huisbezoeken. Deze richtlijnen worden periodiek herzien, bijvoorbeeld naar aanleiding van jurisprudentie en ervaringen van de externe controleurs.

Uitvoering externe controleurs
De voornaamste stappen van de uitvoering van de huisbezoeken door de externe controleurs lopen als volgt:
- Voorbereiden van de huisbezoeken;
- Uitvoering van de huisbezoeken aan de hand van de voor hen geldende richtlijnen (bestaande uit: algemeen, situatie gebonden en vervolgstappen);
- Opstellen van de rapportage, inclusief advies, (vast DUO-format) van het huisbezoek waarbij getoonde ruimte en bezittingen zo uitgebreid mogelijk worden omschreven. Dit wordt, na toestemming van de bewoner, zo mogelijk ondersteund met foto's;

---

is de applicatie waarin de selecties van studenten en hun dossiers die in aanmerking komen voor nader onderzoek op misbruik van de uitwonendenbeurs en de verdere acties naar aanleiding van de controle zijn geregistreerd.

- Vullen van een getuigenverklaring (vast DUO-format), indien een huisbezoek niet mogelijk is. Deze moet objectief en verifieerbaar zijn en daarnaast moet er duidelijk sprake zijn van 'kennis van wetenschap';
- Oplevering van de rapportage met bijlagen; deze worden naar DUO gestuurd via een beveiligd portaal.

Afhandeling
De bevoegde DUO-medewerker beoordeelt het ontvangen rapport met bijlagen en besluit op basis hiervan of er sprake is van misbruik. Als er sprake is van misbruik dan wordt de uitwonendenbeurs omgezet naar een thuiswonendenbeurs. De DUO-medewerker legt een bestuurlijke boete op die geïnd wordt door het Centraal Justitieel Incasso Bureau.

In het volgende hoofdstuk van dit rapport wordt inzicht gegeven in het stelsel van beheersmaatregelen die getroffen zijn in het proces CUB teneinde de privacyrisico's te mitigeren.

2 Getroffen beheersmaatregelen en gesignaleerde privacyrisico's

In dit hoofdstuk geven wij inzicht in het stelsel van beheersmaatregelen die getroffen zijn door afdeling H&I in het proces Controle Uitwonendenbeurs, teneinde de privacyrisico's te mitigeren. Hiermee wordt antwoord gegeven op deelvraag 2 en 3.

Deelvraag 2:
Welke risico's op het gebied van privacy zijn te onderkennen bij de deelprocessen 'profilering' en 'huisbezoek'?

Deelvraag 3:
Welke beheersmaatregelen zijn getroffen om te borgen dat op de juiste wijze met de (bescherming van) persoonsgegevens wordt omgegaan bij het hanteren van het risicoprofiel en het afleggen en vastleggen van huisbezoeken?

De te onderkennen privacyrisico's zijn opgehangen aan criteria opgenomen in de Privacy Baseline (PB) versie 3.3 d.d. 27 oktober 2020 van het Centrum Informatiebeveiliging en Privacybescherming (CIP). In de PB zijn de eisen van de AVG vertaald naar concrete, hanteerbare normen (criteria), die duidelijk maken wat organisaties moeten doen om de privacy van de betrokkenen te waarborgen.

In dit hoofdstuk wordt onder paragraaf 2.1 tot en met 2.11 per criterium aangegeven wat het doel en het bijbehorende risico, volgens de PB, is alsook de aangetroffen maatregelen bij de betreffende criteria.

We geven de aanbevelingen voor verbetering weer per criterium, waar van toepassing. In hoofdstuk 3 geven wij een overkoepelend samenvattend overzicht van onze aanbevelingen.

2.1 B.02 Organieke inbedding

Doel: Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG.

Potentieel risico: Bij het ontbreken van een goede en inzichtelijke taakverdeling en de daarvoor benodigde middelen en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de AVG, de sectorspecifieke wetgeving en het privacybeleid niet effectief worden ingevuld.

2.1.1 *De taken, bevoegdheden en de verantwoordelijkheden van de privacyorganisatie zijn beknopt beschreven*

DUO-breed
DUO volgt het privacybeleid van het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW). Binnen DUO is privacymanagement belegd bij de directies. Wij hebben een Compliance beleid aangetroffen, maar hierin is geen beschrijving opgenomen van de privacyorganisatie met de taken, bevoegdheden en verantwoordelijkheden binnen DUO. Op het intranet van DUO (intranet) is een beknopte beschrijving opgenomen van de rollen en verantwoordelijkheden. Daarnaast hebben wij in het Organisatie & Formatie rapport een beschrijving aangetroffen van de interne beheersing waar

Compliance onderdeel van uit maakt. In paragraaf 2.10 zullen wij hier verder op ingaan.

Sinds september 2002 is binnen DUO een Functionaris Gegevensbescherming (FG) aangesteld. Deze FG ziet erop toe dat de verwerkingen van persoonsgegevens binnen DUO in overeenstemming zijn met de privacywetgeving. De contactgegevens van de FG zijn in de privacyverklaring op de DUO-site aangegeven.

Proces Controle Uitwonendenbeurs
Er is een beschrijving van de verdeling van functionele taken, bevoegdheden en verantwoordelijkheden voor het proces CUB. Dit is afgesproken en vastgelegd in een stroomschema en matrix waarin de onderliggende relaties zijn vastgelegd (onderdeel van privacy kenmerk Principes en Gegevensbescherming door ontwerp e.m.).

2.1.2 *De rapportage- en verantwoordingslijnen privacy zijn beschreven*

DUO beschikt over een overzicht waarin de rapportagelijnen zijn uitgewerkt. Met aanvullende procedures en instructies voor o.a. de handelswijze bij datalekken, opstellen van Data Protection Impact Assessments (DPIA's) en het register van verwerkingsactiviteiten wordt er in opzet invulling gegeven aan de rapportage- en verantwoordingslijnen. Uit de documentatie valt niet altijd op te maken hoe hier verder in de praktijk invulling aan wordt gegeven. DUO heeft in het Compliance beleid de opzet van het Compliancy Management Systeem (CMS) beschreven voor het naleven van wet- en regelgeving, normen, standaarden en richtlijnen. Op welke manier dit tot uiting komt valt niet op te maken uit de ontvangen documentatie.

2.2 B.03 Risicomanagement, Privacy by Design en de DPIA

Doel: Beoordeling van de privacyrisico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht.

Potentieel risico: Privacyrisico's worden niet of niet tijdig gesignaleerd, waardoor de verwerking van de persoonsgegevens niet aan de AVG voldoet en een grote(re) kans loopt op inbreuken op de beveiliging; dit kan leiden tot schade voor natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.

2.2.1 *Privacyrisico's voor proces Controle Uitwonendenbeurs niet structureel in kaart gebracht met risico op niet passende beheersmaatregelen*

DUO-breed
Door DUO is een document "Risicobeheersingskader DUO V1.0 d.d. december 2021 opgesteld. Dit risicobeheersingskader is het raamwerk dat beschrijft op welke wijze het bestuur en het Directieoverleg van DUO de risico's, waaraan DUO bloot staat, in opzet op integrale wijze beheerst. In het document is de toepassing van strategisch- & tactisch risicomanagement en het operationele risicomanagement uitgewerkt. Hierin is de AVG ook meegenomen. Dit kader beschrijft de cyclische risicoanalyse door DUO (opzet).
Voor het organisatiebrede kwaliteitsmanagementsysteem heeft DUO in 2023 een Certificaat van Goedkeuring ISO 9001:2015 ontvangen. Voor het kwaliteitsmanagement specifiek voor de privacy verwijzen we naar hoofdstuk 2.5.

***Aanbeveling**: Breng de privacyrisico's voor het proces Controle Uitwonendenbeurs structureel in kaart en ga aansluitend na of de reeds getroffen beheersmaatregelen passend en toereikend zijn.*

Proces Controle Uitwonendenbeurs
Wij hebben geen vastgesteld privacy risicomanagementprocedure aangetroffen, die toeziet op het cyclisch signaleren van privacyrisico's en het treffen van passende maatregelen, alsook de periodiek evaluatie van de adequaatheid van deze maatregelen.
Jaarlijks stelt de afdeling H&I een controlekalender op. Er vindt dan een inventarisatie plaats van het mogelijke misbruik & oneigenlijk gebruik van de wet- en regelgeving met de bijbehorende risico's. De *privacy* risico's zijn daarbij niet structureel in kaart gebracht.

2.2.2 *DPIA-procedure is ingericht, echter ontbreekt de DPIA-rapportage voor het proces Controle Uitwonendenbeurs*

In het centrale privacybeleid van OCW staat aangegeven dat er voor alle verwerkingen bij diensten, directies, adviesraden en inspecties van OCW een DPIA opgesteld dient te worden. Tevens moeten zij hier procedures voor inrichten. We hebben geconstateerd dat DUO een DPIA-toetsmodel en instructies heeft opgesteld waarin een beslisboom is opgenomen om een risicoanalyse uit te voeren op de verwerkingen. Ook zijn de rollen, taken en bevoegdheden binnen een DPIA-proces beschreven en worden er handreikingen gedaan. We hebben vastgesteld dat de stappen in de DPIA-procedure en adviesformat in opzet borgen dat de vereiste informatieonderdelen behandeld worden, zodat passende maatregelen getroffen kunnen worden. Echter hebben wij hier geen monitoringsactiviteiten in aangetroffen die borgen dat opvolging wordt gegeven aan de te treffen maatregelen.

We hebben geconstateerd dat voor het proces CUB geen DPIA is uitgevoerd ondanks dat dit een verwerking met hoog risico betreft, het heeft immers betrekking op fraudeonderzoeken waar een DPIA-verplichting voor geldt. Door het ontbreken van een DPIA bestaat het risico dat er onvoldoende inzicht is in de mate waarin de getroffen organisatorische en technische beheersmaatregelen passend zijn bij de privacyrisico's die inherent zijn aan het proces CUB.

Eind 2022 is er door de Adviseurs Compliance (AC) van de afdeling Onderwijsvolgers (OVG) aan het Managementteam van OVG het advies gegeven een DPIA voor het proces CUB op te stellen. Dit advies is volgens DUO overgenomen en zou op de planning staan, echter de DPIA is tot op het moment van ons onderzoek niet opgesteld.

Aanbeveling: Voer op korte termijn een DPIA uit op de verwerkingen binnen het proces Controle Uitwonendenbeurs.

2.2.3 *Uitgangspunten voor Privacy by Design beschreven, echter is deze niet aantoonbaar geïmplementeerd*

In het centrale privacybeleid van OCW staat beschreven dat bij het ontwerpen van producten en diensten persoonsgegevens goed moeten worden beschermd, dat niet meer gegevens worden verzameld dan noodzakelijk is voor het doel van de verwerking en dat gegevens niet langer dienen te worden bewaard dan nodig is. Daarnaast neemt OCW technische en organisatorische maatregelen opdat uitsluitend persoonsgegevens worden verwerkt die noodzakelijk zijn. In de handreiking van de DPIA heeft DUO de uitgangspunten van beginselen van privacy by design grafisch uiteengezet.

DUO heeft bij ons aangegeven dat in het proces CUB geen privacy by design is toegepast, omdat hier sprake is van een oud proces en hierbij gebruik wordt gemaakt

van oude systemen. Het anonimiseren van de dossiers zou dan bijvoorbeeld handmatig moeten worden uitgevoerd.
Door DUO is aangegeven dat een oude applicatie is die onderhoud en aanpassing behoeft. moet worden aangepast, omdat een ketenpartner bepaalde systemen aanpast. Dit heeft geen prioriteit, omdat het maar een kleine applicatie is en eigenlijk vervangen moet worden. Door beperkte toegang te verlenen tot wordt de privacy van de opgenomen persoonsgegevens geborgd en is geborgd dat niet te veel medewerkers gegevens kunnen raadplegen, opvoeren, muteren of verwijderen.

2.3 U.01 Doelbinding gegevensverwerking

Doel: 'Doelbinding gegevensverwerking' is het waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden.

Potentieel risico: Het ongeoorloofd en onrechtmatig verzamelen en (verder) verwerken van persoonsgegevens.

2.3.1 Doelbinding is beschreven in de privacyverklaring

In het privacybeleid van OCW zijn AVG-principes beschreven waaronder het principe van grondslag en doelbinding. Beschreven staat dat er enkel persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. In het privacybeleid OCW staat aangegeven dat middels het register van verwerkingsactiviteiten ten behoeve van de verantwoordingsplicht moet worden aangetoond dat voldaan wordt aan de principes rechtmatigheid, transparantie en doelbinding.

DUO heeft op zijn website een privacyverklaring gepubliceerd waarin onder andere beschreven wordt welke persoonsgegevens verwerkt worden en waarvoor (doelen). Eén van de doelen om persoonsgegevens te verwerken is het verstrekken van studiefinanciering.

DUO beschrijft dat zij controles uitvoert om fraude en misbruik te voorkomen en te bestrijden door (persoons)gegevens op juistheid te vergelijken met (persoons)gegevens van bijvoorbeeld de Belastingdienst, de gemeente en onderwijsinstellingen. Bij profilering kunnen (bijzondere) persoonsgegevens worden gebruikt die oorspronkelijk voor een ander doel zijn verzameld. Of deze aanvullende verwerking verenigbaar is met de oorspronkelijke doelen waarvoor de gegevens werden verzameld, hangt onder andere af van welke *informatie* DUO over het gebruik van de gegevens aanvankelijk aan de betrokkene heeft verstrekt. Hier gaat paragraaf 2.7 verder op in.

2.3.2 Rechtmatige grondslag van de verwerking is herleidbaar naar wettelijke verplichting

De grondslag met betrekking tot gegevensverwerking aangaande het proces misbruik Uitwonendenbeurs vloeit voort uit wettelijke basis art. 1.5 WSF 2000, art 9.1a WSF 2000 en art 5.11 AWB. In de Staatscourant zijn de private partijen aangewezen die zijn belast met het toezicht op de naleving van artikel 1.5 van de Wet studiefinanciering 2000.

2.3.3 Uitgangspunt dataminimalisatie niet uitgewerkt

In het centrale Privacybeleid OCW is opgenomen dat om het principe noodzakelijkheid te borgen een proces van dataminimalisatie moet worden ingericht. Dit houdt in dat regelmatig wordt beoordeeld of de verwerking van persoonsgegevens noodzakelijk en minimaal is. We hebben geen informatie aangereikt gekregen waaruit opgemaakt kan

worden hoe de processtap dataminimalisatie is ingericht. Ook is niet bekend of er een leidraad is opgesteld en/of er regelmatig wordt gesproken, beoordeeld en geëvalueerd of de verwerking van gegevens bij het proces CUB noodzakelijk en minimaal is.

Aanbeveling: Werk de uitgangspunten voor dataminimalisatie uit en zie toe op de implementatie daarvan.

2.3.4 Bijzondere persoonsgegevens niet gebruikt bij de totstandkoming basisbestand

Op basis van documentatie maken we op dat er geen gebruik wordt gemaakt van bijzondere categorieën persoonsgegeven bij de totstandkoming van het basisbestand. Wel wordt bij het verrijken van het basisbestand het Burgerservicenummer (BSN) toegevoegd aan de dataset en dit betreft een persoonsgevoelig gegeven. Een gevoelig persoonsgegeven heeft een grotere impact op de privacy en verdient een hogere bescherming. Het is belangrijk dat er extra waarborgen worden getroffen om te garanderen dat ze in overeenstemming met de AVG worden verwerkt. Het basisbestand waarin het BSN is opgenomen wordt geladen in De toegang tot is, op het moment van ons onderzoek, beperkt tot 16 medewerkers.

2.4 U.02 Register van verwerkingsactiviteiten

Doel: Het doel van een 'Register van verwerkingsactiviteiten' is inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de organisatie en bij de instanties die namens de organisatie zorgen voor de verwerking van persoonsgegevens.

Potentieel risico: Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.

2.4.1 Verwerkingsactiviteiten proces Controle Uitwonendenbeurs niet opgenomen in OCW-brede register, wel in DUO-brede register

In het privacybeleid van OCW staat beschreven dat er een OCW-brede register van verwerkingsactiviteiten dient te zijn ten behoeve van de verantwoordingsplicht. Dit register bevat de vereiste informatiebestanddelen die de AVG voorschrijft. DUO maakt momenteel nog niet volledig gebruik van dit register.
De verwerkingen binnen DUO zijn opgenomen in het DUO-brede register van verwerkingsactiviteiten. We hebben geconstateerd dat de verwerkingen van het proces 'H&I In- en uitwonende procedure' (inclusief huisbezoek) hierin zijn opgenomen.

We hebben voor het OCW-brede register van verwerkingsactiviteiten instructies aangetroffen voor het opnemen van nieuwe verwerkingen en het overnemen van bestaande verwerkingen uit het DUO-brede register. Echter is de actualisatie van het OCW-brede register van verwerkingsactiviteiten een aandachtspunt waaraan wordt gewerkt. DUO streeft er naar dat eind 2023 het OCW-brede register van verwerkingsactiviteiten, voor wat betreft de verwerkingen van DUO, gevuld zal zijn.

Aanbeveling: Neem het proces Controle Uitwonendenbeurs op in het OCW-brede register van verwerkingsactiviteiten.

2.5 U.03 Kwaliteitsmanagement

Doel: 'Kwaliteitsmanagement' moet ervoor zorgen dat een gegevensverwerking correct en in overeenstemming met de wens van betrokkenen is.

Potentieel risico: Wanneer de gegevens onjuist of onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene getrokken met negatieve consequenties of naar het oordeel van betrokkene ongewenste verwerking van zijn of haar persoonsgegevens tot gevolg.

2.5.1 *Kwaliteitssysteem voor privacy in het proces Controle Uitwonendenbeurs is niet beschreven, wel zijn er aantoonbaar een aantal maatregelen geïmplementeerd.*

We hebben geen informatie aangetroffen waarin beschreven staat op welke wijze DUO een eenduidig kwaliteitssysteem voor privacy heeft ingericht. Door een dergelijk kwaliteitssysteem dient bewaakt te worden dat in het proces CUB en specifiek voor de stappen binnen de deelprocessen 'profilering' en 'huisbezoek' de betrokkenen de mogelijkheid krijgt zijn gegevens te laten corrigeren en/of de gegevensverwerking te staken. Aangegeven is door DUO dat de kwaliteit tot op afdelingsniveau op een eenduidige wijze wordt bewaakt, inclusief de mogelijkheid persoonsgegevens te (laten) corrigeren (rectificeren, vervolledigen, wissen), te staken en overgedragen te krijgen. DUO heeft een gemeenschappelijke applicatie ingericht voor afhandelen inzage- en verwijderverzoeken. De privacy officers zijn verantwoordelijk voor het opvoeren van nieuwe AVG-verzoeken, de medewerkers van het domein waar de aanvrager een relatie mee heeft handelen de aanvragen af.
Volgens DUO kan het voorkomen dat bij een verzoek tot wissen wordt vergeten de gegevens die op de afdelingsschijf staan ook te wissen.

Aanbeveling: Beschrijf het kwaliteitssysteem om de juistheid, nauwkeurigheid en volledigheid van de persoonsgegevens te borgen en in het kader van profilering de betrokkene in staat te stellen tussentijds zijn rechten uit te oefenen.

We hebben een aantal maatregelen aangetroffen die zich richten op het valideren, aanpassen en bijwerken van persoonsgegevens in de vervolgstappen binnen de genoemde deelprocessen. De vervolgstappen waar hiernaar gerefereerd worden hebben betrekking op de totstandkoming van het basisbestand en de verdere afhandeling daarvan.

Verzamelen van gegevens
DUO geeft aan dat de kwaliteit (juistheid en volledigheid) van de persoonsgegevens in het primaire systeem (SFS-systeem) geborgd wordt doordat de betrokkenen dit voor een groot deel zelf beheren. Dit gebeurt via de webportaal Mijn DUO waar een betrokkenen zelf met gebruik van DigiD of zijn/haar gegevens kan inzien en eventueel kan wijzigen en/of verwijderen. Hiermee wordt de betrokkenen in staat gesteld een deel van hun rechten uit te oefenen. Tevens worden via verscheidene registers gegevens opgehaald en/of gecontroleerd, bijv. via de Basisregistratie Personen (BRP). Vervolgens worden deze gegevens geüpload in het datawarehouse-systeem waar verdere verrijking van de informatie plaatsvindt waaronder met het BSN.

We hebben geen beschrijving aangetroffen van de controles die hierbij uitgevoerd worden teneinde de juistheid van dit tussenbestand te borgen.

Analyseren van gegevens
Aangegeven is dat er geautomatiseerde controles plaatsvinden die de integriteit en actualiteit van het basisbestand borgen. Wanneer er sprake is van afwijkingen ten opzichte van een eerder vastgestelde versie van het basisbestand, dan worden deze afwijkingen opgenomen in een signaallijst en worden deze verder afgehandeld. Dat kan betekenen dat een huisbezoek niet meer uitgevoerd hoeft te worden of een eventuele boete niet wordt gegeven. We hebben geen beschrijving of instructies aangetroffen van deze werkzaamheden.

Opstellen van een risicoprofiel
DUO hanteert een aantal criteria om te komen tot een bepaald risicoprofiel. Deze criteria, afstand woonadres student en ouders, leeftijd student en onderwijssoort, zijn vertaald in een query waarmee het basisbestand wordt gegenereerd. Hieraan worden vervolgens risicocoderingen toegevoegd om te komen tot de te controleren selectie. Van deze handeling / opgestelde query ligt geen beschrijving vast. Er is geen IBAR-document[2] of vergelijkbaar document opgesteld.

Aanbeveling: Laat een IBAR-document opstellen waarin wordt beschreven op welke wijze het risicoprofiel en de risicocoderingen toegepast worden om te komen tot het basisbestand. Zo ontstaat een eenduidig selectieproces waarover zo nodig verantwoording afgelegd kan worden in het Algoritmeregister

Ten tijde van dit onderzoek was DUO nog aan het onderzoeken of zij het gebruikte risicoprofiel en -codering als algoritmes moesten beschouwen. Als we de definitie van de Algemene Rekenkamer volgen gaat het om een algoritme.

Deze definitie luidt als volgt:
Een algoritme is een set van regels en instructies die een computer uitvoert. Algoritmes helpen bijvoorbeeld om problemen te analyseren maar ook om beslissingen te nemen. Zo kan de overheid grote hoeveelheden gegevens (data) combineren en analyseren.

We hebben vastgesteld dat het gebruik van dit algoritme niet staat opgenomen in het Algoritmeregister. De registratie in het Algoritmeregister was nog niet wettelijk verplicht ten tijde van het onderzoek.

Aanbeveling: Neem het toegepaste algoritme op in het Algoritmeregister.

DUO geeft aan dat in het teamoverleg het risicoprofiel wordt besproken en wordt nagegaan of dit nog voldoet aan de eigen risico-inschattingen. In 2022 is het risicoprofiel geëvalueerd naar aanleiding van een praktijkgeval. Als gevolg hiervan is begin 2023 een voorstel ingediend om het risicoprofiel enigszins aan te passen en een nieuw profiel ernaast te maken met maar één indicator, nl. de afstand tussen de adressen van de student, ouders en onderwijsinstelling.

Toepassen van een profiel om een besluit met betrekking tot een persoon te nemen
Het basisbestand is de bron voor de deskresearch voor de medewerkers van H&I.
De controlewerkzaamheden en de vastlegging van aanvullende informatie (bijv. huisgenoten, oppervlakte woning, stageadres) worden in een toelichtingsdocument beschreven. Wij hebben geen leidraad aangetroffen waarin beschreven staat op welke wijze de kwaliteit van deze gegevensverwerking wordt bewaakt. Naast de bespreking in het teamoverleg vindt er naar behoefte ook collegiale controle plaats bij het selecteren van studenten voor een huisbezoek. Wanneer het om bijzondere situaties gaat, wordt met een collega overlegd. Ook wordt af en toe een dossier besproken met een bezwaarmedewerker voordat afhandeling van het dossier plaatsvindt.

Voor de externe controleurs heeft DUO specifieke controlerichtlijnen opgesteld die gehanteerd worden bij het afleggen van huisbezoeken. Deze richtlijnen zijn gebaseerd op eerder opgedane ervaringen met huisbezoeken, aangevuld met recente jurisprudentie. De controlebevindingen na een huisbezoek worden vastgelegd in een rapportage volgens het format van DUO. De schriftelijke toestemming van de student of bewoner maakt hier ook onderdeel van uit. De controleurs geven op basis van de

[2] *Informatie en bronanalyserapport waarin een functionele en technische toelichting in is opgenomen. Alle definities en afspraken, beschrijvingen per veld en de scope van de leveringen zijn erin vastgelegd.*

bevindingen en verklaringen advies aan DUO over de woonsituatie van de student. De inhoud van de rapportage wordt vervolgens beoordeeld door DUO waarna een besluit over het dossier wordt genomen. Alleen bij twijfel vindt er collegiale review plaats van de interpretatie van de resultaten uit het huisbezoek. Wanneer uit de rapportage van het huisbezoek en de interpretatie ervan is gebleken dat de student misbruik heeft gemaakt, zal DUO besluiten tot een herziening van de uitwonendenbeurs en het boetebesluit. DUO geeft aan dat zodra er een besluit genomen is met betrekking tot de herziening en het boetebesluit de student per direct wordt geïnformeerd. Indien er bij de student geen herziening van uitwonend naar inwonend plaats hoeft te vinden, wordt de student hierover niet geïnformeerd. DUO meldt voornemens te zijn dit wel te gaan opnemen in het proces.

Banner in het SFS-systeem
Wanneer er een herziening plaatsvindt, komt in het SFS-systeem een banner bij de student te staan waardoor het principe van 'verantwoord vertrouwen' met betrekking tot de woonsituatie is uitgeschakeld. Wijzigingen in de woonsituatie die betrokkene via MijnDUO doorvoert worden geëffectueerd na controle van een bevoegde medewerker. We hebben geen informatie aangereikt gekregen waaruit blijkt dat de betrokkene hierover wordt geïnformeerd.

DUO stelt dat de banner tot voor kort incidenteel werd verwijderd. In februari 2023 heeft dit voor het laatst plaats gevonden. Sinds februari 2023 is een functionaliteit beschikbaar waarmee periodiek deze banner bij de studenten kan worden verwijderd. DUO geeft aan dat dit proces jaarlijks zal worden uitgevoerd. Wij hebben documentatie aangereikt gekregen waaruit dit blijkt.

2.6 U.04 Beveiligen van de verwerking van persoonsgegevens

Doel: Het doel van 'beveiligen van de verwerking van persoonsgegevens' is persoonsgegevens te beschermen tegen verlies, onbeschikbaarheid, corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

Potentieel risico: Het ongewenst openbaar worden, manipulatie, misbruik en niet beschikbaar zijn van gegevens.

2.6.1 Informatiebeveiligingsbeleid beschreven en rapportagelijnen geïmplementeerd

OCW heeft een Informatiebeveiligingsbeleid d.d. 17 december 2021. Voor alle onderdelen binnen OCW, dus ook voor DUO, is dit beleid leidend. In het beleid is beschreven dat OCW een Basis Beveiligingsniveau 2 (BBN 2) hanteert voor alle informatie(systemen). Indien voor een informatiecomponent of -systeem hogere beveiliging benodigd is, worden op basis van een risicobeoordeling aanvullende beheersingsmaatregelen genomen waar het BBN 2 onvoldoende is. Daarnaast moeten de geïmplementeerde beveiligingsmaatregelen aantoonbaar en controleerbaar zijn. DUO heeft een eigen informatiebeveiligingsbeleid met het uitgangspunt voor de bescherming van Informatiebeveiliging & Privacy (IB&P) op operationeel niveau waar beheersmaatregelen worden geïmplementeerd en nageleefd.

Er wordt op verschillende manieren gerapporteerd over IB&P. Zo is er een jaarlijkse 'rapportage 'IB-beeld', die wordt opgeleverd aan de SG van het ministerie van OCW en zijn er eerstelijns rapportages van het tactisch niveau die worden opgeleverd aan het strategisch niveau. In het beleid staat beschreven dat er jaarlijkse sturing plaatsvindt op de inrichting van de informatiebeveiligingsfunctie middels het jaarplan Informatiebeveiliging dat wordt opgesteld door de CISO.

Binnen DUO dient voor elke applicatie een BIV-classificatie te worden vastgesteld. Dit wordt centraal vastgelegd en gemonitord door de afdeling Compliance (IB). Zij vragen

periodiek na bij de business of de classificatie nog juist is. De lijst met BIV-classificatie is te vinden op het intranet van DUO en wordt jaarlijks aangepast, indien nodig. De BIV-aspecten worden ingeschaald op basis van de niveaus vertrouwelijkheid, integriteit en beschikbaarheid. Het is ons niet duidelijk geworden welke technische- en organisatorische maatregelen er binnen het CUB-proces zijn genomen aan de hand van deze classificering, omdat de link tussen de genoemde classificering en getroffen beheersmaatregelen ontbreekt. Daarom is niet na te gaan of de getroffen maatregelen passend en toereikend zijn. (Zie ook paragraaf 2.2.1.)

Aanbeveling: De BIV-aspecten worden ingeschaald op basis van de niveaus vertrouwelijkheid, integriteit en beschikbaarheid. Leg vast welke maatregelen zijn genomen met betrekking tot de drie genoemde niveaus.

2.6.2 Autorisaties zijn vastgelegd en worden periodiek beoordeeld

OCW heeft een centraal beleid omtrent logische toegangsbeveiliging opgesteld. In het beleid zijn primaire en ondersteunende uitgangspunten opgenomen met betrekking tot de logische toegangsbeveiliging. Binnen het proces CUB is een autorisatiematrix aanwezig waarin de verschillende rollen en bevoegdheden zijn vastgelegd. We hebben informatie aangereikt gekregen waaruit blijkt dat er periodiek beoordeeld wordt of de uitgegeven autorisaties in de systemen van het proces CUB passend en actueel zijn.

2.7 U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens

Doel: Het doel van 'Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens' is om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking, zodat de betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.

Potentieel risico: De organisatie is niet transparant, waardoor de organisatie niet kan verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking, met mogelijk hoge kosten tot gevolg.

2.7.1 Transparantie gebruik persoonsgegevens aanwezig, informatievoorziening profilering ontbreekt

Intern beschikt het ministerie van OCW over een privacybeleid waar DUO gebruik van maakt. In het privacybeleid zijn de AVG-principes beschreven waaronder de principes van rechtmatigheid, behoorlijkheid en transparantie. Beschreven staat dat OCW inzicht geeft in zijn gegevensverwerkingen door deze te publiceren op de website van het ministerie van OCW. Wij hebben echter vastgesteld dat er nog geen verwerkingen van DUO zijn gepubliceerd (zie ook paragraaf 2.4). DUO verwacht de gegevensverwerkingen eind 2023 te hebben geregistreerd in het OCW-brede register van verwerkingsactiviteiten. Vanaf dat moment zullen deze verwerkingen gepubliceerd zijn op de website van het ministerie van OCW.

DUO heeft wel op haar website een privacyverklaring gepubliceerd waarin beschreven wordt welke persoonsgegevens verwerkt worden en waarvoor. Naar deze informatie wordt verwezen wanneer een betrokkene studiefinanciering aanvraagt en daarbij zijn persoonsgegevens deelt. In de privacyverklaring wordt aandacht besteed aan hoe DUO aan persoonsgegevens komt, hoelang ze bewaard en beschermd moeten worden evenals voorwaarden voor de verstrekking van persoonsgegevens aan derden. DUO vermeld in de privacyverklaring dat zij zich bij het uitvoeren van haar wettelijke taken houdt aan de richtlijnen uit de AVG.

DUO beschrijft in de privacyverklaring op haar website dat zij controles uitvoert om fraude en misbruik te voorkomen en te bestrijden door (persoons)gegevens op juistheid te vergelijken met (persoons)gegevens van bijvoorbeeld de Belastingdienst, de gemeente en onderwijsinstellingen. De AVG schrijft voor dat de verwerkingsverantwoordelijke betrokkenen informeren over het bestaan van profilering en de gevolgen daarvan (art. 14 lid 2g AVG). In de privacyverklaring komt niet naar voren of en op welke manier hierbij mogelijk gebruik gemaakt wordt van profilering en/of geautomatiseerde besluitvorming en de gevolgen daarvan.

Aanbeveling: Informeer betrokkenen over of en hoe binnen het proces CUB gebruik gemaakt wordt van profilering en/of geautomatiseerde besluitvorming en de gevolgen daarvan.

Tijdens het uitvoeren van een huisbezoek wordt er informatie over de controle verstrekt middels een flyer. In het kader van privacy en gegevensbescherming staat in de flyer dat huisbezoeken conform de richtlijnen uit de Algemene verordening gegevensbescherming (AVG) worden uitgevoerd. Hierbij wordt verwezen naar de privacyverklaring op de website van DUO.

2.8 U.06 Bewaren van persoonsgegevens

Doel: Het doel van 'Bewaren persoonsgegevens' is te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel.

Potentieel risico: Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.

2.8.1 *Retentieprocedure is DUO-breed ingericht, echter de uitwerking ervan bij het proces Controle Uitwonendenbeurs is nog niet vastgesteld. Sinds 2011 zijn daar geen retentieactiviteiten ondernomen*

In het privacybeleid van OCW staat beschreven dat gegevens niet langer bewaard mogen worden dan nodig is. DUO geeft aan dat voor een aantal verwerkingen de bewaartermijnen vastgelegd zijn in wettelijk vastgesteld selectielijsten (Archiefwet). Voor verwerkingen die niet onder het Archiefwet vallen of waarvoor andere wettelijke bepalingen gelden stelt DUO een termijn vast aan de hand van een nadere analyse. DUO-breed is retentiebeleid vastgesteld in de vorm van diverse kaders zoals de 'Handreiking vernietigen', Procesbeschrijvingen 'selecteren en vernietigen digitale documenten, 'selecteren en vernietigen fysieke documenten op basis van initiatief PADM' en 'archiveren van diverse gegevens bijv e-mail'. Op basis daarvan zijn voor het proces CUB een aantal documenten opgesteld voor het archiveren en schonen van (persoons)gegevens. Deze documenten verkeren nog in de conceptfase. Voor het proces CUB gaat het om het schoningsprotocol, , het Ordeningsplan H&I en het Informatiehuishouding H&I proces MUB.

Aangezien de afdeling H&I voor het proces Uitwonendenbeurs alleen documenten met betrekking tot bewaren en schonen van documenten in conceptfase heeft, mist zij vastgesteld beleid. Hierdoor bestaat het risico dat persoonsgegevens langer bewaard worden dan wettelijk toegestaan is.

We hebben vastgesteld dat DUO sinds 2011 geen retentieactiviteiten (t.w. verwijderen, vernietigen, anonimiseren e.d.) heeft ondernomen binnen het proces CUB. Dit heeft onder andere betrekking op de persoonsgegevens in en de afdelingsschijf. De taken, bevoegdheden en verantwoordelijkheden zijn niet duidelijk belegd. Evenmin vindt er labeling plaats ten aanzien van de vraag wanneer de persoonsgegevens verwijderd dienen te worden. Hierdoor bestaat het risico dat

persoonsgegevens langer worden bewaard dan wettelijk (AVG) noodzakelijk is. Het risico daarvan is dat onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.

Aanbeveling: Werk de retentieprocedure voor het proces Controle Uitwonendenbeurs verder uit en stel de procedure vast; draag zorg voor het periodiek verwijderen, vernietigen of anonimiseren van persoonsgegevens.

2.9 U.07 Doorgifte persoonsgegevens

Doel: Het doel van de vereisten bij 'Doorgifte persoonsgegevens' is te waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid ingeregeld blijft.

Potentieel risico: Als een organisatie niet voldoet aan dit criterium is het niet duidelijk voor de organisatie wat exact wordt verwacht bij het doorgeven van persoonsgegevens waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig verder worden verwerkt en het nemen van verantwoordelijkheid en controle tekortschieten.

2.9.1 Procedure voor het opstellen van verwerkersovereenkomsten ingericht, niet alle verwerkersovereenkomsten zijn opgesteld

In het centrale privacybeleid staat beschreven hoe OCW omgaat met interne en externe verwerkers. Beschreven staat dat met partijen waarmee intern persoonsgegevens worden uitgewisseld afspraken worden gemaakt, waaronder over de beveiliging van de persoonsgegevens. Wanneer een partij namens of in opdracht van OCW verwerkingen verricht, dient hiervoor een verwerkersovereenkomst opgesteld te worden. DUO beschikt over een procedure waarin in opzet het proces (incl. beslisbomen) alsmede de taken, verantwoordelijkheden en bevoegdheden omtrent de totstandkoming van verwerkersafspraken en/of overeenkomsten zijn beschreven.

Binnen het proces CUB wordt gebruikt gemaakt van externe controleurs waarmee DUO persoonsgegevens uitwisselt. Wij hebben geconstateerd dat de uitwisseling van documentatie tussen DUO en de private partijen plaatsvindt via een beveiligd zakelijk portaal. We hebben vastgesteld dat er van de vier private partijen er drie verwerkersovereenkomsten in concept aanwezig zijn. Van één partij is de definitieve versie aangetroffen en is geconstateerd dat onderwerpen hierin in lijn zijn met de CIP Privacy baseline 3.3. Door het ontbreken van verwerkersovereenkomsten waarin een duidelijke omschrijving staat van de taken, bevoegdheden en verantwoordelijkheden bestaat de kans dat persoonsgegevens niet passend worden beschermd.

Aanbeveling: Zorg dat met iedere verwerker een definitief ondertekende verwerkersovereenkomst met de vereiste afspraken is afgesloten.

Teneinde te borgen dat de verwerkers zich aan de gemaakte afspraken omtrent de beschermingsmaatregelen en daarmee de naleving van de privacywetgeving houden, is in de verwerkersovereenkomst opgenomen dat zij tweejaarlijks een rapportage security assessment dienen aan te leveren. De Baseline Informatiebeveiliging Overheid schrijft echter voor dat dit jaarlijks dient plaats te vinden. Deze dient door een onafhankelijk externe deskundige uitgevoerd te worden. Wij hebben vastgesteld dat de private partij, waarmee een verwerkersovereenkomst is opgesteld, het rapport Security Assessment aangeleverd heeft en dat DUO daarmee voldaan heeft aan de

gemaakte afspraken. We hebben niet getoetst of DUO hier follow-up-werkzaamheden op heeft uitgevoerd.

DUO heeft bij ons aangegeven dat er geen doorgifte van persoonsgegevens plaatsvindt met instanties buiten de EU.

2.10 C.01 Intern toezicht

Doel: Het doel van 'Intern toezicht' is het garanderen van een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, het garanderen van naleving van de AVG en van andere wet- en regelgeving betreffende de gegevensbescherming, en het garanderen en aantoonbaar maken van naleving van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens.

Potentieel risico: Als de verwerking van persoonsgegevens niet voldoet aan de AVG, dan zijn de risico's tweeledig: de betrokkene loopt persoonlijke privacyrisico's en de verwerkingsverantwoordelijke wordt geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago als gevolg van communicatieve of handhavende maatregelen van betrokkenen, derden en/of de toezichthoudende autoriteiten.

2.10.1 *Intern toezicht is ingericht; geef meer aandacht aan het proactief invullen van monitoringsactiviteiten die moeten toezien op de beheersing van de privacyrisico's*

Door het nog onvoldoende invullen van de vereiste monitoringsactiviteiten in de verschillende beheersingslijnen is er beperkt inzicht in de adequaatheid van het getroffen stelsel van beheersmaatregelen omtrent het proces CUB. Ook kan niet worden aangetoond dat structureel in het proces voldoende controles plaatsvinden om de naleving van de privacywetgeving te borgen.

Uit de aangereikte documentatie kan worden opgemaakt dat DUO het Three Lines Model hanteert bij de inrichting van haar interne beheersingsmodel teneinde haar doelstellingen te realiseren.

1e line
Om de uniformiteit van het handmatige deel van het proces CUB te waarborgen vindt er collegiale toetsing (4-ogen principe) plaats en indien noodzakelijk navraag bij Bezwaarmedewerkers. We hebben geen cyclische en/of structurele controleactiviteiten aangetroffen met betrekking tot de naleving van *privacy*aspecten binnen het proces CUB.

Voor wat betreft het toezicht op de werkzaamheden van de controleurs van de externe partijen, die de huisbezoeken afleggen, hebben we geconstateerd dat hier enkele beheersmaatregelen zijn getroffen. Jaarlijks vindt er een evaluatie met de private partijen plaats. In documentatie is beschreven dat indien daar aanleiding toe is, de mogelijkheid bestaat voor een tussentijdse evaluatie. DUO heeft richtlijnen opgesteld, waarin ook de omgang met persoonsgegevens beschreven staat, deze worden tenminste een keer per jaar geactualiseerd en aan de private partijen verstrekt. De lopende contracten met de private partijen worden jaarlijks beoordeeld en er wordt ieder jaar een addendum opgesteld.

Het Businessmanagement wordt bij de uitvoering van haar operationele taken omtrent de naleving van de privacyaspecten ondersteund door de Adviseurs Compliance, echter hebben wij geen instructies aangereikt gekregen waaruit blijkt wat deze activiteiten omvatten. Aangegeven is dat de zij met name fungeren als

eerste aanspreekpunt met betrekking tot compliance zaken. Zij voeren geen structurele toetsing- en/of monitoringsactiviteiten uit, die zijn belegd bij de 2e lijn.

2e line
De CIO-office maakt onderdeel uit van de 2e lijn. De 2e beheersingslijn is verder belegd bij de afdeling Compliance. Naast het feit dat zij kaderstellend zijn en als adviseurs fungeren bij DUO-brede en complexe zaken, zijn zij ook verantwoordelijk voor het monitoren en toetsen van de naleving van de privacywetgeving bij de verwerking van persoonsgegevens.

Om de directies te steunen bij de invulling van hun taken en verantwoordelijkheden heeft Compliance een set aan DUO-brede (wettelijke) kaders, regels, richtlijnen, sjablonen en tooling op het gebied van privacy, informatiebeveiliging en archivering & schonen beschikbaar gesteld.

Door DUO is aangegeven dat zij reguliere toetsingsactiviteiten uitvoeren bijv. het reviewen van verwerkersovereenkomsten. Andere toetsingsactiviteiten zijn uitgevoerd naar aanleiding van signalen en casuïstiek.

Door Compliance zijn in 2022 stappen gezet om de monitoringsfunctie verder vorm te geven. Op tactisch en operationeel niveau vinden frequent diverse overleggen plaats waarbij lopende acties en de voortgang van onderwerpen in interne rapportages worden besproken, gemonitord en intern (mondeling) worden afgestemd op het gebied van privacy, informatiebeveiliging, archiefmanagement. Ook worden onderwerpen die op dat moment spelen (ad hoc), in bijv. het CUB-proces, besproken. De monitoringsactiviteiten zijn gericht op het treffen van beheersmaatregelen om aan de AVG te voldoen.
Vanuit deze overleggen wordt input geleverd voor de rapportage op strategisch niveau opgesteld door de chief information officer. DUO heeft aangegeven dat op basis daarvan (bij-)sturing plaatsvindt door het management op strategisch, tactisch en/of operationeel niveau. Wij hebben deze rapportages niet ontvangen.

Wij zien dat de monitoringsactiviteiten vooral een reactieve insteek hebben, terwijl er baat is bij een meer proactieve benadering gezien de complexiteit van de invulling van de privacywetgeving en het belang ervan.

Het is de 2e lijn die de ADR heeft verzocht dit onderzoek uit te voeren. Ze wil inzicht hebben in of wordt voldaan aan de gestelde eisen van bescherming van (bijzondere) persoonsgegevens volgens de privacywet- en regelgeving bij de deelprocessen 'profilering' en 'huisbezoek' van het proces CUB.

3e line
DUO heeft aangegeven een eigen FG te hebben die conform het beleid erop moet toezien dat de verwerkingen van persoonsgegevens binnen DUO in overeenstemming zijn met de privacywetgeving.

Aanbeveling: Zie erop toe dat er op een meer proactieve wijze invulling wordt gegeven aan monitoringsactiviteiten om de privacyrisico's beter te kunnen beheersen.

2.11 C.02 Toegang gegevensverwerking voor betrokkenen

Doel: Het doel van 'Toegang gegevensverwerking voor betrokkene' is om zo nodig transparantie te bieden over de gegevensverwerking, zodat de betrokkene zijn rechten kan uitoefenen en zo de verantwoordelijke kan aanspreken bij onrechtmatigheid van een gegevensverwerking, opdat deze onrechtmatigheid beëindigd wordt.

Potentieel risico: De organisatie is niet transparant, waardoor het inzicht in de rechtmatigheid van organisaties ontbreekt en het vertrouwen in een organisatie verloren gaat.

2.11.1 *Informatievoorziening DUO over de rechten van geautomatiseerde besluitvorming en profilering die betrokken studenten uit kunnen oefenen ontbreekt*

We hebben vastgesteld dat de informatievoorziening aan betrokkenen omtrent de verwerking van persoonsgegevens binnen het proces CUB en met name het profilering aspect beperkt is. Hierdoor kunnen betrokkenen niet adequaat hun rechten uitoefenen.
In het centrale privacybeleid zijn de uitgangspunten en de rechten van betrokkenen beschreven. Hierin staat aangegeven dat betrokkenen het recht hebben op duidelijke informatie over wat er met hun persoonsgegevens wordt gedaan. Daarnaast wordt het recht op inzage, rectificatie, vergetelheid, beperking van verwerking, bezwaar en met betrekking tot geautomatiseerde besluitvorming en profilering beschreven. DUO beschikt over een nader uitgewerkte procedure die ingaat op het recht van inzage en correctie/aanvulling van persoonsgegevens.

DUO heeft op haar website een privacyverklaring gepubliceerd waarin de rechten van betrokkenen worden beschreven. Het gaat hierbij om het recht op inzage corrigeren, aanvullen en verwijderen. Andere rechten, zoals bezwaar met betrekking tot geautomatiseerde besluitvorming en profilering, die wel in het interne centrale privacybeleid worden beschreven, worden niet in de publieke privacyverklaring beschreven.

Betrokkenen kunnen via Mijn DUO hun eigen gegevens inzien en wijzigingen doorvoeren. Daarnaast wordt het recht op inzage en rectificatie ondersteund door modelbrieven en contactgegevens van de privacy officer en FG. Ook kunnen betrokkenen indien gewenst een klacht indienen bij de Autoriteit Persoonsgegevens.

Zoals in paragraaf 2.7 is aangegeven, schrijft de AVG voor dat de verwerkingsverantwoordelijke de betrokkenen dient te informeren over het bestaan van profilering en de gevolgen daarvan (art 14 lig 2g AVG). In de privacyverklaring staat dat betrokkenen bezwaar kunnen maken tegen een formele beslissing van DUO. Er is hierbij geen verwijzing naar mogelijk gebruik van profilering en/of geautomatiseerde besluitvorming en de gevolgen daarvan.

3 Aanbevelingen

3.1 Aanbevelingen

Op basis van de in hoofdstuk 2 beschreven constateringen, doen wij de volgende aanbevelingen:

1. Breng de privacyrisico's voor het proces Controle Uitwonendenbeurs structureel in kaart en ga aansluitend na of de reeds getroffen beheersmaatregelen passend en toereikend zijn (2.2);
2. Voer op korte termijn een DPIA uit op de verwerkingen binnen het proces Controle Uitwonendenbeurs (2.2);
3. Werk de uitgangspunten voor dataminimalisatie uit en zie toe op de implementatie daarvan (2.3);
4. Neem het proces Controle Uitwonendenbeurs op in het OCW-brede register van verwerkingsactiviteiten (2.4);
5. Beschrijf het kwaliteitssysteem om de juistheid, nauwkeurigheid en volledigheid van de persoonsgegevens te borgen en in het kader van profilering de betrokkene in staat te stellen tussentijds zijn rechten uit te oefenen (2.5);
6. Laat een IBAR-document opstellen waarin wordt beschreven op welke wijze het risicoprofiel en de risicocoderingen toegepast worden. Zo ontstaat een eenduidig selectieproces waarover zo nodig verantwoording afgelegd kan worden in het Algoritmeregister (2.5);
7. Neem het toegepaste algoritme op in het Algoritmeregister (niet verplicht ten tijde van onderzoek) (2.5);
8. De BIV-aspecten worden ingeschaald op basis van de niveaus vertrouwelijkheid, integriteit en beschikbaarheid. Leg vast welke maatregelen zijn genomen met betrekking tot de drie genoemde niveaus (2.6);
9. Informeer betrokkenen over of en hoe binnen het proces Controle Uitwonendenbeurs gebruik gemaakt wordt van profilering en/of geautomatiseerde besluitvorming en de gevolgen daarvan (2.7 en 2.11);
10. Werk de retentieprocedure voor het proces Controle Uitwonendenbeurs verder uit, stel deze vast en draag zorg voor het periodiek verwijderen, vernietigen of anonimiseren van persoonsgegevens (2.8);
11. Zorg dat met iedere verwerker een definitief ondertekende verwerkersovereenkomst met de vereiste afspraken is afgesloten (2.9);
12. Zie erop toe dat er op een meer proactieve wijze invulling wordt gegeven aan monitoringsactiviteiten om de privacyrisico's beter te kunnen beheersen (2.10).

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Werkzaamheden
Voor beantwoording van de deelvragen en centrale vraag hebben wij, in de periode januari tot en met mei 2023, documenten bestudeerd, interviews gehouden met diverse betrokkenen bij het proces Controle Uitwonendenbeurs en informatie verkregen uit de Prepared by Client lijst, gebaseerd op het referentiekader (zie bijlage 2), die is uitgezet bij en is ingevuld door de afdeling H&I.

Referentiekader
Voor het referentiekader hebben wij gebruik gemaakt van:

- Algemene Verordening Gegevensbescherming;
- Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Privacy Baseline 3.3 d.d. 27 oktober 2020 van het Centrum Informatiebeveiliging en Privacybescherming.

Het referentiekader is als bijlage 2 opgenomen in het rapport.

Afbakening onderzoek
We hebben niet het gehele proces Controle Uitwonendenbeurs onderzocht. Object van onderzoek zijn de deelprocessen 'profilering' en 'huisbezoek' van het proces Uitwonendencontrole. Het onderzoek geeft inzicht in of relevante beheersmaatregelen over de AVG zijn vastgelegd (opzet) en of de beheersmaatregelen ook zijn toegepast in de praktijk (bestaan). Wij hebben niet getoetst of de gewenste beheersmaatregelen over een bepaalde periode effectief hebben gewerkt (werking). Wij hebben niet onderzocht of de uitkomsten van het proces Controle Uitwonendenbeurs mogelijk onbedoelde en ongewenste uitkomsten heeft in relatie tot de AVG.

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, hoofddirecteur Financiën & Services DUO, 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

Groningen, 14 september 2023

Bijlage 1 Managementreactie DUO

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Controle uitwonenden beurs (CUB): managementreactie op de gedane aanbevelingen in het rapport d.d. 07-09-2023

Eind 2022 heeft DUO u opdracht gegeven om een vraaggestuurd auditonderzoek te doen naar de beheersing van de privacyaspecten rond het proces van de uitwonendencontrole. Dit als onderdeel van onze meerjarige lerende aanpak met betrekking tot het continue verbeterproces rondom de compliancy- en privacyaspecten van onze activiteiten.

Ik wil beginnen met het uitspreken van mijn dank voor het uitgebreide onderzoek dat u verricht heeft en de bijbehorende rapportage en aanbevelingen. Deze aanbevelingen helpen ons een verdere verdiepingsslag te doen op de borging van privacyaspecten van de controle.

Hieronder vindt u onze reactie op de aanbevelingen:

1

Aanbeveling: Breng de privacyrisico's voor het proces Controle Uitwonendenbeurs structureel in kaart en ga aansluitend na of de reeds getroffen beheersmaatregelen passend en toereikend zijn.

Deze aanbeveling wordt overgenomen. Dit vormt onderdeel van de handelingen omtrent de DPIA (zie onder 2). Dit wordt nog dit jaar afgerond.

2

Aanbeveling: Voer op korte termijn een DPIA uit op de verwerkingen binnen het proces Controle Uitwonendenbeurs.

Deze aanbeveling wordt overgenomen. De opdracht voor het opstellen van de DPIA is verstrekt en de DPIA volgens de nieuwe uitgangspunten wordt nog dit jaar afgerond.
Het proces van de uitwonendencontrole wordt momenteel aangepast naar een aselecte steekproef. Daarmee verandert ook de werkwijze. Bij de implementatie van deze nieuwe werkwijze zal de DPIA worden opgesteld.

3

Aanbeveling: Werk de uitgangspunten voor dataminimalisatie uit en zie toe op de implementatie daarvan.

Deze aanbeveling wordt overgenomen. Het uitwerken van de uitgangspunten maakt onderdeel uit van de op te stellen DPIA die nog dit jaar wordt afgerond.
Het proces van de uitwonendencontrole wordt momenteel aangepast naar een aselecte steekproef. Daarmee verandert ook de werkwijze. Bij de implementatie van deze nieuwe werkwijze zal de dataminimalisatie worden toegepast.

Aanbeveling: Neem het proces Controle Uitwonendenbeurs op in het OCW-brede register van verwerkingsactiviteiten.

Aanbeveling: Neem het proces Controle Uitwonendenbeurs op in het OCW-brede register van verwerkingsactiviteiten.

Deze aanbeveling wordt overgenomen. Aan het vullen van het register wordt op dit moment gewerkt. Het proces Controle Uitwonendenbeurs is al opgenomen. De controle en verificatie vindt binnenkort plaats.

5

Aanbeveling: Beschrijf het kwaliteitssysteem om de juistheid, nauwkeurigheid en volledigheid van de persoonsgegevens te borgen en in het kader van profilering de betrokkene in staat te stellen tussentijds zijn rechten uit te oefenen.

Deze aanbeveling wordt overgenomen. Dit wordt meegenomen bij het opstellen van de DPIA en wordt daarmee nog dit jaar afgerond.

6

Aanbeveling: Laat een IBAR-document opstellen waarin wordt beschreven op welke wijze het risicoprofiel en de risicocoderingen toegepast worden om te komen tot het basisbestand. Zo ontstaat een eenduidig selectieproces waarover zo nodig verantwoording afgelegd kan worden in het Algoritmeregister

Deze aanbeveling is reeds overgenomen. Het IBAR document is inmiddels opgesteld.

7

Aanbeveling: Neem het toegepaste algoritme op in het Algoritmeregister.

Deze aanbeveling wordt overgenomen. De uitvoering hiervan zal dit jaar gerealiseerd zijn.

8

Aanbeveling: De BIV-aspecten worden ingeschaald op basis van de niveaus vertrouwelijkheid, integriteit en beschikbaarheid. Leg vast welke maatregelen zijn genomen met betrekking tot de drie genoemde niveaus.

Deze aanbeveling wordt overgenomen en zal dit jaar gerealiseerd zijn.

9

Aanbeveling: Informeer betrokkenen over of en hoe binnen het proces CUB gebruik gemaakt wordt van profilering en/of geautomatiseerde besluitvorming en de gevolgen daarvan.

De privacyverklaring op de DUO-website zal nog dit jaar op dit punt worden aangepast.
Het proces is reeds zo ingericht dat bij huisbezoeken een leaflet wordt achtergelaten waarin staat dat huisbezoeken conform de richtlijnen uit de Algemene verordening gegevensbescherming (AVG) worden uitgevoerd en waarbij wordt verwezen naar de privacyverklaring op de website van DUO.

Daarnaast worden studenten die als gevolg van de controle een sanctie opgelegd krijgen reeds op de hoogte gesteld van de gebruikte middelen bij de totstandkoming van de beoordeling en de bijbehorende gevolgen. Voor studenten bij wie geen sanctie wordt opgelegd zal er vanaf de invoering van de nieuwe werkwijze met de aselecte steekproef voor worden gezorgd dat ook zij op de hoogte gesteld worden van de gebruikte middelen bij de totstandkoming van de beoordeling en de bijbehorende gevolgen.

10

Aanbeveling: Werk de retentieprocedure voor het proces Controle Uitwonendenbeurs verder uit, stel deze vast en draag zorg voor het periodiek verwijderen, vernietigen of anonimiseren van persoonsgegevens.

De aanbeveling wordt overgenomen. DUO-breed is retentiebeleid vastgesteld in de vorm van diverse kaders zoals de 'Handreiking vernietigen', Procesbeschrijvingen 'selecteren en vernietigen digitale documenten', 'selecteren en vernietigen fysieke documenten op basis van initiatief Post, Archief en Documentmanagement (PADM)' en archiveren van diverse gegevens bijv. e-mail'. Op basis daarvan zijn voor het proces Controle Uitwonendenbeurs (CUB) een aantal documenten opgesteld (in concept) voor het archiveren en schonen van (persoons)gegevens. Voor het proces CUB gaat het om het schoningsprotocol, Combuis, Ordeningsplan Handhaving & Inspectie (H&I) en Informatiehuishouding H&I proces CUB.

11

Aanbeveling: Zorg dat met iedere verwerker een definitief ondertekende verwerkersovereenkomst met de vereiste afspraken is afgesloten.

Met iedere verwerker is een contract met een verwerkersovereenkomst opgesteld, inclusief addendum dat op basis van de jaarlijkse rapportage wordt opgesteld. Bij de afhandeling van de verwerkersovereenkomsten en addenda zal meer zorg worden besteed aan de zorgvuldigheid van de administratieve afronding, waaronder het zetten van een handtekening.

12

Aanbeveling: Zie erop toe dat er op een meer proactieve wijze invulling wordt gegeven aan monitoringsactiviteiten om de privacyrisico's beter te kunnen beheersen.

De aanbeveling wordt overgenomen. De ontwikkeling van het monitorings- en toetsingskader zal nog dit jaar worden afgerond. Inrichting zal plaatsvinden vanaf begin 2024.

Bijlage 2 Referentiekader

Het referentiekader is gebaseerd op de Privacy Baseline versie 3.3 d.d. 27 oktober 2020 van het Centrum Informatiebeveiliging en Privacybescherming (CIP). In de Privacy Baseline zijn de eisen van de AVG vertaald naar 13 concrete, hanteerbare criteria die duidelijk maken wat organisaties moeten doen om de privacy van de betrokkenen te waarborgen.

In het referentiekader zijn 11 van de 13 criteria opgenomen. De criteria B.01 Privacybeleid en C.03 Meldplicht datalekken maken geen onderdeel uit van het referentiekader, omdat deze criteria DUO-breed zijn geregeld.

	Te onderzoeken deelprocessen van het proces Uitwonendencontrole
	Risicoprofiel DUO moet maatregelen nemen om te borgen dat op de juiste wijze met de (bescherming van) persoonsgegevens wordt omgegaan bij het hanteren van risicoprofielen. De afdeling Handhaving & Inspectie (H&I) geeft hiermee duidelijkheid over de wijze waarop met betrekking tot het toepassen van het risicoprofiel in het kader van het proces misbruik uitwonden beurs invulling wordt gegeven aan de beginselen van de AVG.
	Huisbezoek DUO moet maatregelen nemen om te borgen dat op de juiste wijze met (de bescherming van) persoonsgegevens wordt omgegaan bij (rapportages van) huisbezoeken. De afdeling H&I geeft hiermee duidelijkheid over de wijze waarop met betrekking tot (de rapportage van) huisbezoeken invulling wordt gegeven aan de beginselen van de AVG.
	Procesbeschrijvingen Zijn er procesbeschrijvingen aanwezig van de deelprocessen 'profilering' en 'huisbezoek'?
	CRITERIA toe te passen op de deelprocessen 'profilering' en 'huisbezoek'
1	**B.02 Organieke inbedding** Zijn de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen door de organisatie vastgelegd en vastgesteld? • De verdeling van taken, bevoegdheden en verantwoordelijkheden is op afdelingsniveau vastgelegd en afgesproken en is vastgelegd in een matrix waarin de onderliggende relaties zijn vastgelegd. (onderdeel van privacy kenmerk Principes en Gegevensbescherming door ontwerp e.m.) • De rapportagelijnen, tussen betrokken verwerkers, verwerkings-verantwoordelijken en de Functionaris Gegevensbescherming, binnen DUO zijn vastgelegd.

	• Ontwikkelingen met betrekking tot 'profilering' en 'huisbezoek' buiten de eigen organisatie, worden actief door de organisatie gevolgd, zodat de impact op de inrichting van de organisatie direct kan worden verwerkt.
2	**B.03 Risicomanagement, Privacy by Design en de DPIA** De verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van de maatregelen. • Is een DPIA uitgevoerd? • Is Privacy by Design toegepast? Bijv. is bij nieuwe "verwerkingen" het systeem zo ingericht dat gegevens kunnen worden geanonimiseerd. Of de logging van verwerkingen. • Zijn privacyrisico's in kaart gebracht?
3	**U.01 Doelbinding gegevensbescherming** De verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven wat de doeleinden en rechtvaardigheidsgronden zijn. De verwerking vindt plaats op basis van een van de in artikel 6 AVG genoemde gronden. • Zijn de doeleinden van de verwerking van een persoonsgegeven bepaald en beschreven? • Zijn de rechtvaardigingsgronden van de verwerking van een persoonsgegeven bepaald en beschreven? • Vindt bovenstaande tijdig plaats, dus voorafgaand aan de verzameling, (verdere) verwerking, profilering of doorgifte van persoonsgegevens. Dit moet gebeuren voor alle verzamelingen, (verdere) verwerkingen, profileringen en doorgiften. **Profilering** Een betrokkene wordt niet onderworpen aan geautomatiseerde individuele besluitvorming zonder menselijke tussenkomst. Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Met het oog op de *transparantieplicht* is minimaal beschreven: o De wijze waarop het profiel wordt opgebouwd, waaronder een beschrijving van het soort persoonsgegevens en de categorieën van betrokkenen; o De wijze waarop betrokkenen worden geïnformeerd over het profileringsproces; o De werking van het gebruikte algoritme en de wijze waarop het algoritme wordt vastgelegd, bijvoorbeeld in een algoritmeregister (indien van toepassing); o Het verder gebruiken van uitkomsten van analyse cq risicoprofielen (indien van toepassing); o De beoordelingscriteria aan de hand waarvan wordt bepaald of een huisbezoek zal plaatsvinden.

	Huisbezoek Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is Betrokkenen worden in eenvoudige en duidelijke taal geïnformeerd over: o Welke gegevens door wie en met welk doel worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt in relatie tot (rapportages van) huisbezoeken; o De beschikkingsprocedure of de procedure m.b.t. het voornemen van een op te leggen boete; o De ontvangers (indien van toepassing).
4	**U. 02 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. • Wordt informatie over de verwerking van persoonsgegevens inclusief, de categorieën die onder uw verantwoordelijkheid worden verwerkt, vastgelegd in het DUO-brede register van verwerkingsactiviteiten? • Wordt informatie over de verwerkingsactiviteiten van verwerkers vastgelegd in het DUO-brede register van verwerkingsactiviteiten? Het register van verwerkingsactiviteiten bevat in relatie tot het proces Controle Uitwonendenbeurs: o Identificatie en classificatie; o De naam en de contactgegevens van de verwerkingsverantwoordelijke; o De verwerkingsdoeleinden; o Bron van de gegevens en de systemen, processen en de organisatie; o De categorieën van betrokkenen; o De categorieën van persoonsgegevens; o De categorieën van ontvangers; o Doorgifte naar derde landen j/n; o Bewaartermijnen; o Een beschrijving van technische en organisatorische beveiligingsmaatregelen.
5	**U.03 Kwaliteitsmanagement** De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht t.b.v. 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. • Rechten van de betrokkenen: wordt de kwaliteit van persoonsgegevens tot op afdelingsniveau op een eenduidige wijze bewaakt, inclusief de mogelijkheid persoonsgegevens te (laten) corrigeren (rectificeren, vervolledigen, wissen), te staken en overgedragen te krijgen. • Worden betrokkenen op een eenduidig manier geïnformeerd over de status van de afhandeling? • Zijn procedures vastgelegd voor het valideren, aanpassen en bijwerken van persoonsgegevens die de juistheid en volledigheid van persoonsgegevens waarborgen?

6	**U.04 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. • Zijn beveiligingsrisico's bepaald en mitigerende maatregelen genomen (technisch en organisatorisch)? Bijv.: registreren van toegang; toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken; pseudonimisering van persoonsgegevens, zodat duidelijk is hoe een veilige verwerking wordt gewaarborgd en hoe de persoonsgegevens onder meer worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. • Is er beveiligingsbeleid opgesteld? • Is er een beveiligingsplan, inclusief taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging?
7	**U.05 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. • Is op een eenduidige wijze bepaald of en wanneer de betrokkene moet worden geïnformeerd? • Is vastgesteld hoe de te verstrekken informatie wordt bepaald (inhoudsvereisten)?
8	**U.06 Bewaren van persoonsgegevens** Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet worden overschreden. • Zijn bewaartermijnen bepaald? • Is bepaald hoe en wanneer persoonsgegevens moeten worden vernietigd?
9	**U.07 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. • Zijn er onderlinge afspraken (eenduidig en uniform) met andere verwerkings-verantwoordelijken en afdoende garanties bij doorgifte aan verwerkers opgesteld (bewerkersovereenkomst)? • Zijn de taken, bevoegdheden en verantwoordelijkheden omtrent de juiste doorgifte vastgelegd en daardoor eenduidig? • Is bepaald of gegevens mogen worden doorgegeven aan andere verwerkingsverantwoordelijken buiten de EU of aan de verwerkers buiten de EU?

	• Vindt er vastlegging van doorgifte plaats? **Huisbezoek** Doorgifte van persoonsgegevens aan derden vindt plaats op basis van voldoende garanties en waarborgen. Met het oog op doorgifte van persoonsgegevens aan partijen die ten behoeve van DUO in het kader van huisbezoeken persoonsgegevens verwerken (Verwerkers) is minimaal beschreven: o De NAW-gegevens van Verwerkers, zoals van sociaal controleurs, softwareleveranciers, hosting providers, etc. (alleen indien zij op enige wijze toegang hebben tot persoonsgegevens); o De Instructies voor Verwerkers (waaronder instructies voor het afleggen van huisbezoeken, het opstellen van rapportages etc.); o De rechten en plichten van DUO en Verwerkers. Deze zijn vastgelegd in een overeenkomst of andere rechtshandeling. De overeenkomst bevat minimaal: ▪ Een algemene beschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en plichten van DUO als verwerkingsverantwoordelijke; ▪ Geheimhoudingsplicht; ▪ Technische en organisatorische beveiligingsmaatregelen; ▪ Subverwerkers; ▪ Verplichtingen Verwerker (meewerken bij het voldoen aan rechten van betrokkenen, melden van datalekken, uitvoeren van een DPIA, meewerken aan audits etc.); ▪ Bewaren en schonen van gegevens. o De procedure die erop toeziet dat bij gewijzigde omstandigheden de Verwerkersovereenkomst wordt aangepast; o De wijze waarop periodiek wordt beoordeeld of Verwerkers-overeenkomsten nog aan de eisen voldoen en de wijze waarop de nakoming van afspraken wordt nagegaan.
10	**C.01 Intern toezicht** Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond. • Is de wijze waarop het toezicht plaatsvindt vastgelegd en eenduidig. • Is toezicht een structureel onderdeel van de processen en vindt dat plaats in een cyclisch proces binnen de afdeling? • Wordt er gereageerd op afwijkingen? • Wordt gerapporteerd of gegevensverwerking rechtmatig plaats vindt? • Is er een functionaris gegevensbescherming aangesteld?
11	**C.02 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. • Is bepaald of de betrokkene toegang krijgt tot de informatie over de verwerking van persoonsgegevens en of er een uitzonderingsgrond geldt? • Is de vorm van verstrekken (bijv. handmatig of via portal) en welke informatie moet worden verstrekt bepaald?

	• Wordt een inzageverzoek van de betrokkene op de juiste wijze afgehandeld en kunnen betrokkenen nagaan welke persoonsgegevens van hen worden verwerkt en op welke manier?

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag