Auditdienst Rijk
*Ministerie van Financiën*

# Assurancerapport DUO Self-assessment Suwinet-Inkijk 2021

Definitief, versie 1.0

# Colofon

| | |
|---|---|
| Titel | DUO Self assessment Suwinet Inkijk 2021 |
| Uitgebracht aan | |
| Datum | 11 januari 2023 |
| Kenmerk | 2022 0000321738 |
| Referentienummer | |

*Inlichtingen*
**Auditdienst Rijk**

# Inhoud

# 1 Inleiding

Dienst Uitvoering Onderwijs (DUO) heeft sinds 1 april 2014 via de applicatie 'Suwinet inkijk' inzage in de inkomensgegevens uit de Polisadministratie van het Uitvoeringsinstituut Werknemersverzekeringen (UWV). Deze gegevens gebruikt DUO voor de toetsing van inkomensgegevens van haar Studiefinanciering (SF) klanten. Doel van het gebruik van de gegevens is het voorkomen van onnodige (dubbele) bevraging van burgers en het beperken van het risico op onjuiste beslissingen, wanneer de klanten aan DUO niet voldoende en/of onjuiste informatie verstrekken. Afspraken over de levering en het gebruik van de gegevens zijn vastgelegd in de GeVS (Gezamenlijke elektronische Voorzieningen Suwi) Keten Service Level Agreement. Met ingang van 2020 moeten alle aangesloten organisaties een Self-assessment uitvoeren en vastleggen in een rapport, het transparantierapport, genoemd. Deze verantwoording moet worden beoordeeld door een onafhankelijke EDP auditor en worden voorzien van een zogenoemde getrouwheidsverklaring.
De voor het Self assessment te hanteren normen zijn ontleend aan de BIO. Het ministerie van SZW bepaalt de selectie van normen uit de BIO voor de verantwoording Suwinet (op basis van de SUWI regeling art. 5.2.2. en art. 6.4). Deze selectie is bij het Bureau Keten Informatisering Werk en Inkomen (BKWI) gepubliceerd als de Verantwoordingsrichtlijn Informatiebeveiliging GeVS.
Voor zowel het Self assessment door de deelnemende organisatie als voor de auditor is de onderzoeksaanpak per norm alsmede de rapportage voor deelnemende partijen vastgelegd in "Suwinet guidance", met als handreiking de ENSIA-verantwoording conform de Suwinet guidance". Verder heeft BKWI bepaald dat alle normen even zwaar meetellen in het door de auditor te geven oordeel.

## 1.1 Aanleiding onderzoek, opdracht en opdrachtgever

DUO maakt voor het uitvoeren van enkele specifieke taken gebruik van inkomensgegevens, die door het BKWI worden verstrekt via de applicatie 'Suwinet inkijk. Suwi staat voor Structuur Uitvoeringsorganisatie Werk en Inkomen.
Sinds 2004 wordt jaarlijks de GeVS Keten Service Level Agreement (Keten SLA) opgesteld met de afspraken tussen de partijen die via de GeVS gegevens uitwisselen. DUO is één van deze partijen.
Onderdeel van deze afspraken is dat elke deelnemer, waaronder DUO, jaarlijks een Self assessment Suwinet-Inkijk uitvoert over het afgelopen jaar, in dit geval 2021, en op basis daarvan een transparantierapport opstelt. Dit transparantierapport is de basis voor het al dan niet afgeven door het bestuur van DUO van een In Control Verklaring (ICV) aan de BKWI.
De Auditdienst Rijk (ADR) is gevraagd het Self assessment Suwinet Inkijk van DUO, waarvan de resultaten zijn vastgelegd in het DUO transparantierapport, te beoordelen (zie paragraaf 2.3).

Deze assurance opdracht wordt door de Auditdienst Rijk (ADR) uitgevoerd in opdracht van Hoofddirecteur DUO/Uitvoering. Gedelegeerd opdrachtgever is . Aanspreekpunt is de en daarnaast

Voor Kwaliteitsbeheer & Audit is dit

Opdrachtnemer namens de ADR is

De opdracht wordt uitgevoerd conform het Handboek Auditing Rijksoverheid (HARo) en in overeenstemming met Nederlands recht, waaronder de IIA standaarden. Verder is voor deze opdracht de Audit Charter[1] van de ADR van toepassing.

## 1.2 Doelstelling en onderzoeksvra(a)g(en)

De doelstelling van deze opdracht is het geven van een oordeel over het door DUO opgezette transparantie rapport Self assessment 2021. Dit Self assessment gaat over de opzet, bestaan en werking van de interne beheersingsmaatregelen over de periode 1 januari 2021 tot en met 31 december 2021, die verband houden met de voorwaarden waaronder DUO de gegevens Suwinet Inkijk van het UWV mag ontvangen, gebruiken en bewaren.

De Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2020 spreekt van het afgeven van een getrouwheidsverklaring door een EDP-auditor van NOREA. Dit betekent dat DUO een 3000A verklaring vraagt met een redelijke mate van zekerheid. Aangezien er sprake is van de zogenaamde Suwinet wetgeving is elke vorm van verklaring toegestaan. Het onderzoek is uitgevoerd op basis van de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. (IIA normen).

De te beantwoorden hoofdvraag is:
Is naar het oordeel van de ADR het Self assessment DUO Suwinet Inkijk 2021 uitgevoerd en vastgelegd in het DUO transparantierapport volgens de Verantwoordingsrichtlijn GeVS 2020 en zijn de resultaten per norm juist en volledig weergegeven in het DUO transparantierapport.
Om deze hoofdvraag te beantwoorden moeten de volgende subvragen worden beantwoord:

- Zijn alle vereiste normen uit de Verantwoordingsrichtlijn GeVS 2020 onderzocht.
- Zijn de normen onderzocht zoals aangegeven in de Verantwoordingsrichtlijn GeVS.
- Zijn de resultaten eenduidig vastgelegd en sluit het DUO transparantierapport daarop aan.

Het is niet de intentie dat de ADR zelf onderzoek doet. Wij onderzoeken de uitgevoerde werkzaamheden van DUO op basis waarvan het DUO transparantierapport is opgesteld.

In opdracht van RNE heeft Bedrijfsvoering / Compliance het self assessment uitgevoerd, op basis waarvan het DUO transparantierapport is opgesteld.

[1] http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/fi/organisatie_24/sg_1/auditdienst_rijk/a_organisatie/Audit_charter_ADR_versie_13-04-2016.pdf

## 1.3 Afbakening

Het object van onderzoek is DUO Rapport Self assessment Suwinet Inkijk 2021 (het DUO transparantierapport), versie 2.0, definitief, 21 september 2022, ondertekend door DUO 14 oktober 2022, alsmede de documenten die DUO heeft geraadpleegd voor het self assessment (door DUO beschikbaar gesteld in de samenwerkingsruimte) op basis waarvan het DUO transparantierapport tot stand is gekomen. Nagegaan is of voldaan is aan de Verantwoordingsrichtlijn GeVS 2020. Deze Verantwoordingsrichtlijn beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS. Deze verantwoordingsrichtlijn bevat de gezamenlijke afspraken van de Suwi partijen met betrekking tot de te hanteren normen voor informatiebeveiliging en de wijze waarop partijen verantwoording afleggen over de naleving daarvan.

# 2 Oordeel

## 2.1. Naar ons Oordeel: goedkeurend

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet: Wij zijn van oordeel met een redelijke mate van zekerheid dat het "DUO Rapport Self assessment Suwinet Inkijk 2021 (het DUO-transparantierapport)", versie 2.0, definitief, 21 september 2022, ondertekend door DUO 14 oktober 2022, volgens de Verantwoordingsrichtlijn GeVS 2020 is uitgevoerd en de resultaten per norm juist en volledig (inclusief de tekortkomingen) zijn vastgelegd in het DUO transparantierapport. Het door DUO ondertekende Self-assessment rapport is als bijlage bij het ADR rapport toegevoegd.
De onderbouwing van ons oordeel geven wij weer in de paragraaf 2.2.

## 2.2 Onderbouwing van het goedkeurend oordeel

Ons goedkeurend oordeel hebben we gegeven omdat:

### 2.2.1 *Alle vereiste normen uit de Verantwoordingsrichtlijn GeVS 2020 zijn onderzocht.*

De voor het Self assessment te hanteren normen zijn ontleend aan de BIO. Het ministerie van SZW bepaalt de selectie van normen uit de BIO voor de verantwoording Suwinet Inkijk (op basis van de SUWI regeling art. 5.2.2. en art. 6.4). Deze selectie is bij het BKWI gepubliceerd als de Verantwoordingsrichtlijn Informatiebeveiliging GeVS. In het DUO Self assessment zijn alle aangewezen 12 normen aangetroffen, welke zijn onder te verdelen in de volgende drie onderwerpen:

- Governance: 5.1.1.1, 5.1.2.1, 6.1.1.1, 6.1.1.3, 6.1.2.1, 18.1.4.2
- Awareness: 7.2.2.1
- Autorisaties: 9.2.1.1, 9.2.2.1, 9.2.2.2, 9.2.5.3, 9.2.6.1

### 2.2.2 *De normen zijn door DUO onderzocht zoals aangegeven in de Verantwoordingsrichtlijn GeVS.*

DUO heeft voor het uitvoeren van het Self assessment gebruik gemaakt van de standaard Controleformulieren evidence Suwinet self assessment 2021. Per norm is een standaard Controleformulier opgemaakt.

### 2.2.3 *De resultaten zijn eenduidig vastgelegd en het DUO-transparantierapport sluit daarop aan.*

Object van onderzoek vormt het door DUO opgemaakte "DUO Rapport Self-assessment Suwinet Inkijk 2021 (het DUO transparantierapport)", versie 2.0, definitief, 21 september 2022, ondertekend door DUO 14 oktober 2022 (zie de toegevoegde bijlage aan ons ADR rapport). Wij hebben deze rapportage aangesloten met de corresponderende controleformulieren en de gebruikte info. De door DUO gebruikte info om het self assessment op te stellen is in een samenwerkingsruimte aan ons beschikbaar gesteld.
Per norm hebben wij vastgesteld of aan de norm is voldaan dan wel de tekortkomingen juist en volledig door DUO zijn weergegeven. Bij alle 12 normen van het self assessment is er sprake van juiste en volledige (inclusief de tekortkomingen) weergave in het DUO Rapport Self assessment Suwinet Inkijk 2021 van DUO.

# 3 Verantwoording onderzoek

## 3.1 Werkzaamheden en afbakening

Tijdens het onderzoek hebben wij vastgesteld welke maatregelen en procedures zijn getroffen met betrekking tot de vermelde normen. Hiertoe hebben wij documentatie opgevraagd, zoals autorisatierapportages en loggingrapportages van de gegevensverwerking, bij de afdeling Kwaliteitsbeheer & Audit van DUO, de onderzoekers en opstellers van het transparantierapport. Het is niet de intentie dat de ADR zelf onderzoek doet. Onze bevindingen en rapportage hebben wij voor hoor en wederhoor teruggelegd.

Wij hebben dit onderzoek uitgevoerd op basis van een risicogerichte aanpak. Hierbij hebben wij gekeken per onderdeel/criterium naar het materiële belang en de risico's die door DUO worden gelopen wanneer niet aan de norm wordt voldaan.

## 3.2 Gehanteerde standaard en verantwoordelijkheden

Dit assurance onderzoek is uitgevoerd door de Auditdienst Rijk (ADR) in opdracht van de hoofddirecteur DUO. Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft zekerheid in de vorm van een oordeel.

De verantwoordelijkheid van de opdrachtgever is te zorgen dat:
1) De juiste personen binnen DUO kunnen worden benaderd ten behoeve van het aanleveren van documentatie, het houden van interviews, het reviewen van gespreksverslagen en de hoor/wederhoor van de uiteindelijke bevindingen.
2) Het onderzoeksteam toegang krijgt tot te onderzoeken systemen en de juiste documentatie.
3) Het proces van het opstellen van het DUO self assessment rapport en rapport zelf als zodanig is ingericht dat het DUO self assessment rapport vrij is van afwijkingen van materieel belang als gevolg van fraude of fouten.
4) Voordat het rapport wordt uitgebracht, is de opdrachtgever gevraagd een letter of representation (LOR) te ondertekenen. Hierin is bevestigd dat alle relevante informatie is verschaft.

De taak van de projectleider van ADR is te zorgen dat alle werkzaamheden en het gehanteerde normenkader zijn uitgevoerd conform de opdrachtbevestiging (ons kenmerk: ) en dat de opdracht wordt uitgevoerd conform de bij de ADR geldende kwaliteitsrichtlijnen voor assurance opdrachten zoals opgenomen in het Handboek Auditing Rijksoverheid en dat het (elektronische) dossier conform deze richtlijnen wordt ingericht. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze assurance opdracht.

De ADR is de eigenaar van het audit dossier. ADR kan geen verantwoordelijkheid aanvaarden voor wijzigingen in de door haar geconstateerd feiten en omstandigheden na de datum waarop de desbetreffende werkzaamheden zijn afgerond, tenzij ADR tijdig hiervan op de hoogte is gebracht.

## 3.3 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.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

# 4 Ondertekening

Auditdienst Rijk

# 5 Managementreactie

DUO heeft het Assurancerapport DUO Self assessment Suwinet Inkijk 2021 met belangstelling gelezen en is blij met het goedkeurend oordeel van de Auditdienst Rijk. Het geeft vertrouwen in de wijze waarop DUO het self assessment heeft opgezet, uitgevoerd en haar aanbevelingen heeft weergegeven. De aanbevelingen vanuit onderzoeksrapport self assessment zal DUO het komende jaar oppakken om te komen tot verbeteringen.