Gemeente Amsterdam

Rechtmatig gebruik Suwinet

Plan van aanpak 2023

Gemeente Amsterdam
Team Advisering Interne Beheersing
Subsidies, Inkoop en Juridisch Bureau Sociaal

1 Inleiding

Binnen het Cluster Sociaal wordt ten behoeve van het uitvoeren van de Participatiewet gebruik gemaakt van Suwinet-Inkijk en Suwinet DKD-inlezen in het programma RAAK. Vanuit de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi) en aanverwante regelingen zijn strikte regels opgenomen wie, waarom en welke informatie mag raadplegen in Suwinet. De privacygevoelige informatie die is opgenomen in Suwinet mag alleen geraadpleegd worden door daarvoor bevoegde medewerkers en alleen wanneer daarvoor een wettelijke basis is (doelbinding). Wanneer dit niet het geval is, kan een raadpleging als onrechtmatig worden bestempeld.

2 Opdrachtgever

Renger Visser, Directeur Inkomen

3 Onderzoek/ advies vraag

Aan Team Advisering Interne Beheersing is gevraagd maandelijks de raadplegingen in Suwinet te monitoren op mogelijk onrechtmatige raadplegingen.

4 Doel van het onderzoek

Het onderzoek heeft als doel de raadplegingen door de uitvoerende afdelingen te monitoren en onrechtmatige raadplegingen te voorkomen.

5 Scope

De opdracht beperkt zich tot de directies Werk, Participatie en Inkomen, Subsidies Inkoop en Juridisch Bureau Sociaal (waarbij alleen de teams Geschilbeslechting gecontroleerd worden), IV Sociaal en ICT.

Uitgesloten van deze controle zijn de afdelingen Onderwijs en Leerplicht van de directie OJZD en de Jongerenpunten van de afdeling WOJ. Deze afdelingen hebben een aparte suwi-applicatie (RMC) voor raadplegingen ten behoeve van de uitvoering van de Leerplichtwet. Dit onderdeel wordt getoetst door de RMC-coördinator en beleidsadviseur van de afdeling Onderwijs en Leerplicht. De rapportage die daaruit voortvloeit wordt afgestemd en gedeeld met de verantwoordelijke Information Security Officer (ISO).

6 Aanpak onderzoek

Het onderzoek bestaat uit verschillende onderdelen: data-analyse, gericht onderzoek naar autorisaties en raadplegingen en onderzoek logging van DKD-inlezen/RAAK. Hierna wordt

beschreven wat het normenkader is aan de hand waarvan onderzoek plaatsvindt, wat de onderzoekshandelingen per onderdeel zijn en welke vervolgstappen moeten worden genomen.

Normenkader

- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
- Regeling Suwi
- ENSIA
- Factsheet gebruik Suwinet (VNG)
- Handreiking controle op rechtmatig gebruik Suwinet bij onbekende BSN (VNG)
- Baseline Informatiebeveiliging Overheid
- Stedelijk kader informatiebeveiliging Gemeente Amsterdam
- Instructie verantwoord gebruik Suwinet (Gemeente Amsterdam)
- Specifieke privacyverklaring medewerkers aangaande controle rechtmatig gebruik Suwinet

Data-analyse en gericht onderzoek

Maandelijks wordt door het BKWI een bestand beschikbaar gesteld met loggegevens m.b.t. het gebruik van Suwinet-inkijk voor Amsterdamse raadplegingen binnen het Cluster Sociaal. Deze bestanden worden verrijkt met gegevens uit de primaire systemen binnen WPI en het gemeentelijke personeelsadministratie. Door middel van data-analyse wordt een aantal bevindingen geïsoleerd:

A. Bevindingen m.b.t. afwijking t.o.v. de autorisatiematrix

Aan de hand van de autorisatiematrix kan bekeken worden of de raadplegers volgens de matrix op functieniveau toegang mogen hebben tot Suwinet. Als dit niet het geval is wordt de bevinding verzonden naar de Information Security Officer (ISO) en de contactpersoon van de afdeling Beleid en Kwaliteit, team Vakmanschap & Bedrijfsvoering. Zij doen samen een check of de toegekende autorisatie juist is en wat mogelijke vervolgstappen zijn. Indien nodig wordt de autorisatie van de raadpleger ingetrokken.

B. Bevinding die direct uitgezet worden bij leidinggevende

Als na data-analyse blijkt dat een medewerker zichzelf heeft geraadpleegd zal de raadpleging direct worden overgedragen aan de leidinggevende ter beoordeling. Dit gebeurt aan de hand van de Instructie verantwoord gebruik Suwinet. Team AIB vraagt de leidinggevende het gesprek met de medewerker aan te gaan om de reden van raadpleging te achterhalen. De leidinggevende kan in bepaalde gevallen de hulp inroepen van DJZ en/of Bureau Integriteit. De leidinggevende geeft een terugkoppeling aan team AIB. De resultaten worden verwerkt in de kwartaalrapportage.

C. Bevindingen waarbij aanvullend onderzoek moet plaatsvinden

Het komt voor dat gebruikers van Suwinet (ex-)collega's raadplegen. Deze (ex-)collega's kunnen wel of niet voorkomen in de primaire systemen van WPI. De (ex-)collega's of diens (voormalige) partner of huisgenoot hebben bijvoorbeeld een voorziening aangevraagd, in het verleden een uitkering ontvangen, een vordering open staan, zijn onderhoudsplichtig of er loopt een fraudeonderzoek. Bij deze raadplegingen raadpleegt Team AIB de primaire systemen. Wanneer geen logische reden voor raadpleging gevonden wordt, draagt Team AIB de betreffende raadpleging over aan de leidinggevende conform punt B.

D. Bevindingen met hoog risico maar beperkingen voor nader onderzoek
Na de data-analyse blijft een deel van de raadplegingen onverklaard. De geraadpleegde personen komen niet voor in de primaire systemen en de gemeentelijke personeelsadministratie. De namen van deze personen zijn niet bekend. Het gaat hierbij vaak om huisgenoten of familieleden van klanten. Maar het kunnen ook bekende bekenden van suwinetgebruikers zijn, bekende Nederlanders, etc. Team AIB zal door middel van bestandsanalyse bekijken bij welke functiegroepen dit soort raadplegingen het meest voorkomt. Hierbij worden ook geraadpleegde pagina's en gebruikte escape-redenen betrokken. Wanneer een raadpleging vanuit de combinatie van die factoren niet logisch is, kan nader onderzoek gedaan worden conform punt B. Hierbij kan Team AIB gebruik maken van Makelaarsuite. In uitzonderlijke gevallen kan dit uitgezet worden bij Bureau Integriteit Amsterdam (BIA). Zij beschikken over toegang tot Suwinet waardoor meer gegevens van de geraadpleegde persoon achterhaald kunnen worden.

Logging DKD-inlezen/RAAK

Naast Suwinet-Inkijk maakt de gemeente gebruik van de functionaliteit Suwinet-DKD-inlezen. Met DKD-inlezen worden bepaalde gegevens van de bronnen DUO en UWV rechtstreeks ingelezen in het programma RAAK. De gemeente dient maatregelen te nemen op het gebied van het vastleggen van handelingen en gebeurtenissen binnen deze functionaliteit, oftewel logging. Daarnaast moet deze vastgelegde informatie beschermd worden en een analyse ten aanzien van het gebruik plaatsvinden.

Team AIB heeft eind 2022 vastgesteld dat raadplegingen via DKD-Inlezen binnen het programma RAAK op een zodanige wijze worden gelogd dat deze goed herleidbaar zijn. De inhoud van de logbestanden is beveiligd en door medewerkers van de gemeente Amsterdam niet te wijzigen zodat de integriteit daarvan gegarandeerd is. Verder is vastgesteld dat het risico op misbruik zeer beperkt of zelfs verwaarloosbaar is. Team AIB zal dit onderzoek halfjaarlijks uitvoeren, zolang het programma RAAK gebruikt wordt. Actieve controle op de inhoud van de logbestanden zal niet plaatsvinden. Eind 2022 heeft de ENSIA-auditor geoordeeld dat dit onderzoek voldoet.

7 Vastlegging

Per kwartaal zal een rapportage worden opgesteld en aan de opdrachtgever worden aangeboden. Hierin worden de bevindingen gerapporteerd met een verslag van de casussen die zijn uitgezet bij leidinggevenden en de terugkoppeling per casus (indien afgehandeld). De rapportage wordt besproken met de Directieadviseur Inkomen, de contactpersonen bij het team Vakmanschap & Bedrijfsvoering van WPI en de ISO. Deze kunnen zorgdragen voor eventuele organisatie brede communicatie en verantwoording bij de Ensia.

Planning opleveren rapportage rechtmatig gebruik Suwinet 2023	
Kwartaal	**Datum**
Q1	juni/juli 2023
Q2	september 2023 incl logging DKD-inlezen/RAAK
Q3	november 2023
Q4	maart 2023