BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 106

4 februari 2019

Officiële uitgave van de gemeenschappelijke regeling WerkSaam Westfriesland

Informatiebeveiligingsbeleid Suwinet

1. Inleiding

De Westfriese gemeenten hebben de uitvoering van de Participatiewet, IOAW, IOAZ en BBZ overgedragen aan WerkSaam. Voor het juist en rechtmatig uitvoeren van deze taken is het raadplegen van Suwinet een vereiste. Er worden via Suwinet onder meer gegevens van UWV, SVB, gemeenten, BRP, het Handelsregister, de Belastingdienst en de RDW ontsloten voor de uitvoering van de wettelijke taken van onder andere UWV, SVB en gemeenten. Via Suwinet kunnen gegevens worden uitgewisseld van alle burgers in Nederland.
Dit informatiebeveiligingsbeleid Suwinet is gericht op het gebruik van Suwinet-Inkijk en is een aanvulling op het organisatiebrede informatiebeveiligingsbeleid van WerkSaam.

2. ENSIA

Vanaf 2017 is de verantwoording over informatieveiligheid met betrekking tot Suwinet onderdeel van de ENSIA (Eenduidige Normatiek Single Information Audit). Dit is een bredere gemeentelijke verantwoording over informatieveiligheid. Hoewel het raadplegen van Suwinet voor de Participatiewet, IOAW en IOAZ door de Westfriese gemeenten is overgedragen aan WerkSaam, blijven de gemeenten eindverantwoordelijkheid. Daarom moet WerkSaam de gemeenten informeren over de kwaliteit van de informatiebeveiliging. Dit gebeurt via een Third Party Mededeling (TPM), opgesteld door een externe auditor.

3. Gebruikers van Suwinet

Alleen medewerkers in dienst van of werkzaam voor WerkSaam voor wie het raadplegen van Suwinet functioneel noodzakelijk is, krijgen toegang tot Suwinet. Door Suwinet worden op gemeentelijk niveau de volgende functies vereist:

Functioneel beheerder:
De functioneel beheerder voert medewerkers op in Suwinet en autoriseert deze voor de verschillende functionaliteiten van Suwinet, die passen bij de functie(s)/rol(len) van de medewerker. De functies en bijbehorende bevoegdheden zijn opgenomen in een autorisatietabel (zie bijlage 1)

Gebruikers:
De gebruikers raadplegen in Suwinet-Inkijk cliëntgegevens.
Deze gebruikers hebben alleen toegang tot informatie die noodzakelijk is voor het uitvoeren van hun functie/rol (zie de autorisatietabel in bijlage 2). Gebruikers mogen geen informatie raadplegen die niet nodig is voor het uitvoeren van de werkzaamheden.

Functionaris informatiebeveiliging of Security Officer:
- is verantwoordelijk voor het beheer en onderhoud van het informatiebeveiligingsbeleid Suwinet,
- controleert de autorisaties,
- controleert het gebruik van Suwinet aan de hand van de rapportages van het BKWI,
- vraagt specifieke rapportages op als daar aanleiding voor is,
- rapporteert bevindingen rechtstreeks aan het hoogste management.

4. Beveiligingseisen ten aanzien van personeel

Iedere medewerker of ambtenaar in dienst van WerkSaam moet handelen conform de CAR-UWO en de integriteitscode van WerkSaam. Uitsluitend bevoegde personen hebben toegang tot Suwinet-Inkijk en kunnen de gegevens raadplegen. De bevoegdheden van een persoon zijn afgeleid van de taak, functie of verantwoordelijkheid van deze persoon. De leidinggevende van de medewerker vraagt een autorisatie tot Suwinet aan, passend bij de functie/rol.

Een gebruiker die in dienst is van WerkSaam is verplicht om een zorgvuldigheidsverklaring te tekenen (zie bijlage 2) voordat rechten in Suwinet worden toegekend. Hierin wordt aandacht gegeven aan het gebruik van gegevens uit Suwinet. Deze verklaring wordt opgenomen in het personeelsdossier.

5. Bewustwording medewerkers

Om bewustwording te vergroten onder de medewerkers zorgt de Security Officer dat:

het informatiebeveiligingsbeleid onder de aandacht wordt gebracht van de gebruikers,
gebruikers van Suwinet-Inkijk worden geïnformeerd dat het gebruik van Suwinet gegevens wordt vastgelegd en gecontroleerd
elk jaar extra aandacht wordt geschonken aan informatieveiligheid en privacy. Dit kan bestaan uit workshops en/of berichten via mail en intranet.

6. Meldingsplicht

Iedereen moet (vermoedens van) beveiligingsincidenten melden bij de leidinggevende of de Security Officer. De melding wordt onderzocht door het Privacy & Informatieveiligheidsteam (PIT), waar de Security Officer deel van uitmaakt Als uit onderzoek blijkt dat het incident of vermoeden gegrond is, wordt deze direct gerapporteerd aan de directie. Waar nodig meldt het PIT het incident ook aan het AP en de betrokkene zelf. Dit is conform de AVG. Misbruik van Suwinet kan leiden tot ontslag.

7. Logging en rapportages gebruik Suwinet-Inkijk

Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker kan worden nagegaan. De volgende gegevens worden gelogd:
het tijdstip van iedere log-in en log-out en andere actie,
de gebruikersnaam van degene die inlogt/uitlogt,
elk BSN (of andere zoeksleutel) waarvan gegevens worden opgevraagd,
elke actie, zoals de bekeken kolom- of overzichtspagina´s.

Het doel van deze logging is het tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking.

De gebruikers van Suwinet-Inkijk moeten op de hoogte zijn dat over het gebruik gegevens worden verzameld en vastgelegd. De volgende informatie wordt verstrekt aan de medewerkers die (gaan) werken met Suwinet-Inkijk:
het bestaan van de logging,
de (aard van de) gegevens die binnen deze applicatie worden gelogd,
doelen van de logging,
dat de gelogde gegevens niet voor andere doeleinden worden gebruikt,
hoe en door wie de controles op logging worden gedaan.

Controle rapportages
Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft gebruikersrapportages ontwikkeld over het gebruik van Suwinet-Inkijk. Via deze rapportages monitort en controleert de Security Officer het gebruik van Suwinet-Inkijk. Onder monitoren wordt verstaan: signaleren, analyseren, rapporteren en bijsturen. De gebruikersrapportage bevat vier onderdelen: het totale gebruik, het zorgvuldig gebruik, het accountbeheer en het doelmatig gebruik van Suwinet-Inkijk. Deze rapportage bevat geen persoonsgegevens over de medewerker en over de geraadpleegde personen.

Bij vermoedens van ongeoorloofd gebruik, vraagt de Security Officer bij het BKWI een specifieke rapportage op en controleert deze. De resultaten van dit onderzoek worden gerapporteerd aan de desbetreffende teammanager en de directeur.

8. Whitelist

Vanaf november 2018 beperkt WerkSaam de mogelijkheid tot het raadplegen niet-cliënten in Suwinet-Inkijk door te gaan werken met een Whitelist. Cliëntgegevens kunnen daarbij probleemloos geraadpleegd worden (voor de pagina's waar medewerker vanuit de toegekende rol recht op heeft). Niet-cliënten kunnen alleen worden geraadpleegd via een escape-functie, waarbij de medewerker moet opgeven wat de reden is voor het raadplegen. Vanaf het moment dat een medewerker de escape functie toepast voor een BSN, kunnen de gegevens van dat BSN gedurende vier uur worden geraadpleegd.

De aantallen en redenen van de genomen escapes staan in de gebruikersrapportage, waardoor monitoring eenvoudiger is.

Om de Whitelist te vullen logt de functioneel beheerder wekelijks in via Suwinet-Inkijk en upload een lijst met BSN-nummers.

9. Evaluatie en actualisatie beleid

De Security Officer evalueert jaarlijks het informatiebeveiligingsbeleid Suwinet, actualiseert het waar nodig geactualiseerd en laat het beleid opnieuw vaststellen door het Managementteam.

10. Inwerkingtreding en citeertitel
Dit Informatiebeveiligingsbeleid Suwinet treedt in werking op de dag na die van bekendmaking, met terugwerkende kracht tot 1 november 2018.

Dit beleid wordt aangehaald als Informatiebeveiligingsbeleid Suwinet WerkSaam.

Vastgesteld in de vergadering van het dagelijks bestuur van 17 januari 2019,
De voorzitter, D. te Grotenhuis
De directeur, M.J. Dölle