ADVIESNOTA voor burgemeester en wethouders **Openbare besluitenlijst**

Zaaknummer: 53844-2021

Medewerker	:	Jorrit Boxum
Team	:	Werk Inkomen Zorg
Datum	:	1 december 2021
Portefeuillehouder	:	wethouder H. Kamphuis

BIJLAGEN:
☒ Bijlage 0: Beveiligingsplan SUWI
☒ Bijlage 1: Specifiek Suwinet-normenkaders afnemers
☒ Bijlage 2: Benoeming en taakomschrijving Security Officer Suwinet
☒ Bijlage 3: Autorisatiematrix
☒ Bijlage 4: Autorisatieprocedure Suwinet
☒ Bijlage 5: Procedure uitvoeren periodieke controles Suwinet
☒ Bijlage 6: De tien 'gouden' gedragsregels gebruik Suwinet
☒ Bijlage 7: Zorgvuldigheidsverklaring medewerkers

AFSTEMMING MET:

☒ Actief openbaar
☐ Niet actief openbaar
☐ Actief openbaar, eerst contact met steller van deze adviesnota

ONDERWERP
Beveiligingsplan Suwinet 2022-2025

BESLUIT burgemeester en wethouders
Het Beveiligingsplan Suwinet 2022-2025 vast te stellen.

SAMENVATTING
Voor het delen van persoonsgegevens binnen de wettelijke taken op het gebied van werk en inkomen maken gemeenten gebruik van het informatiesysteem Suwinet. Dit biedt een veilige omgeving voor het delen van persoonsgegevens en privacygevoelige informatie tussen organisaties. Zorgvuldig en veilig gebruik van de gegevens moet goed worden geborgd binnen de gemeentelijke organisatie.

Jaarlijks wordt er verantwoording afgelegd over het gebruik van Suwinet op basis van het normenkader, dat is gebaseerd op de BIO-normen (Baseline Informatiebeveiliging Overheid). Hiertoe wordt eens in de vier jaar een Suwinet beveiligingsplan opgesteld. Dit beveiligingsplan beschrijft hoe we in Olst-Wijhe aan deze normen voldoen en hoe we een zorgvuldig en controleerbaar gebruik van Suwinet waarborgen.

In februari 2020 is het strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022 vastgesteld. Dit beveiligingsplan Suwinet past binnen dit strategisch informatiebeveiligingsbeleid.

INLEIDING
Voor een goede uitvoering van de Participatiewet, de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW) en de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) heeft de gemeente gegevens nodig van andere partijen. Bijvoorbeeld bij het vaststellen van het recht op een uitkering. Partijen, waaronder gemeenten, UWV en de Belastingdienst, maken hiervoor gebruik van Suwinet. Dit is een informatiesysteem dat een veilige omgeving biedt voor het delen van gegevens. Het gaat hier om privacygevoelige gegevens, zoals inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, bijstandsuitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering.

Bij behandeling van deze gegevens is zorgvuldigheid en controleerbarheid erg belangrijk. Gemeenten moeten daarom verantwoording afleggen over het gebruik van Suwinet. Dit gebeurt op basis van 14 normen. Deze normen worden afzonderlijk in het beveiligingsplan beschreven, waarbij per norm wordt toegelicht welke beveiligingsmaatregelen worden genomen.

Het laatst vastgestelde beveiligingsplan dateert uit 2019 en had de wettelijk maximale geldigheidsduur tot en met 2021. Het nieuwe beveiligingsplan heeft een looptijd van 2022-2025.

De belangrijkste normen worden hieronder kort toegelicht:

1. Inrichten van een Beveiligingsfunctie Suwinet

De gemeente Olst-Wijhe heeft een Security Officers. Deze functionaris is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document en bevorderen de informatiebeveiliging en de communicatie naar de medewerkers over het gebruik van Suwinet.

2. Scheiding van taken, verantwoordelijkheden en functies

Er is een autorisatiematrix, waarin de scheiding van taken, verantwoordelijkheden en functies staat beschreven. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur, dat de medewerker alleen die gegevens kan raadplegen die van belang zijn voor zijn/haar werkzaamheden.

3. Monitoring, rapportage en controle

Alle handelingen die in Suwinet plaatsvinden worden door het Bureau Keteninformatisering werk en inkomen (BKWI) gelogd, oftewel opgeslagen. Deze informatie wordt maandelijks in een rapportage door BKWI beschikbaar gesteld. Het is de taak van de Security Officer om deze informatie te controleren en te analyseren op het zorgvuldig gebruik van Suwinet. Ook wordt in een controle beoordeeld of alle autorisaties nog overeenkomstig de matrix zijn afgegeven. Signalen van mogelijk onrechtmatig gebruik worden vastgelegd en onderzocht. Ieder half jaar wordt over de uitkomsten van de maandelijkse controles en de eventuele verbeteracties gerapporteerd aan de teamleider Werk, Inkomen en Zorg en de DOWR-brede Chief Information Security Officer (CISO).

4. Verantwoording

Jaarlijks moet door middel van beantwoording van de ENSIA-vragenlijst (in de digitale omgeving van de ENSIA-tool) verantwoord worden hoe de gemeente Olst-Wijhe invulling geeft aan de gestelde normen. Hiermee voldoen we aan de eisen van transparantie. De beheerder (BKWI) kan van de ENSIA-verantwoording/controleverklaring gebruikmaken. Over 2021 is de ENSIA-vragenlijst ingevuld door de Security Officer. Verantwoording aan het college en de gemeenteraad over de normen gebeurt ook via de ENSIA-tool.

Dit beveiligingsplan is gezamenlijk met de gemeenten Deventer en Raalte opgesteld en daar waar nodig gemeentespecifiek gemaakt.

BEOOGD RESULTAAT
Vaststellen van het Beveiligingsplan Suwinet 2022-205, biedt gemeente Olst-Wijhe een duidelijk kader voor een zorgvuldig en controleerbaar gebruik van Suwinet.

KADER
Het Beveiligingsplan Suwinet 2022-2025 kadert binnen de volgende regelingen en wetten:

- Baseline Informatiebeveiliging Overheid (BIO)
- Wet SUWI (Wet Structuurorganisatie Uitvoering Werk en Inkomen)
- Regeling SUWI
- AVG (Algemene Verordening Gegevensbescherming)

Verder wordt het verwerken van persoonsgegevens geregeld in specifieke wetten zoals de Participatiewet.

ARGUMENTEN

1.1 Een vastgesteld Beveiligingsplan Suwinet is voorwaardelijk om aangesloten te kunnen zijn op Suwinet. Deze aansluiting is nodig voor het uitvoeren van wettelijke taken binnen de keten van werk en inkomen. Ook is de aansluiting nodig om het recht op een uitkering binnen de Participatiewet te kunnen vaststellen.

DRAAGVLAK
Omdat Suwinet privacygevoelige gegevens bevat, moeten klanten erop kunnen vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft dan ook al bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Uiteraard zijn er op het gebied van gegevensbeveiliging sindsdien vele (grote) ontwikkelingen geweest. Dit beveiligingsplan dient dan ook als kader waarbinnen we het zorgvuldig gebruik van Suwinet willen borgen.

De Security Officer Suwinet draagt de inhoud van het beveiligingsplan uit aan alle medewerkers die gebruik maken van Suwinet. Dit gebeurt door voorlichting en een-op-eencontact. Dit draagt bij aan draagvlak voor een zorgvuldig gebruik van Suwinet binnen onze gemeente.

DUURZAAMHEID

Niet van toepassing

RISICO'S (financieel/juridisch)

Dit plan draagt bij aan het beperken van risico's in het gebruiken en delen van persoonsgegevens. Aan het plan zelf zijn geen risico's verbonden.

FINANCIËLE CONSEQUENTIES

Niet van toepassing.

AANPAK/UITVOERING

Het beveiligingsplan sluit inhoudelijk nauw aan op het aflopende Suwinet beveiligingsplan 2019-2021. Voor de Security Officer Suwinet blijven taken en verantwoordelijkheden grotendeels hetzelfde. De uitvoering van taken wordt dus voortgezet met een aantal nieuwe accenten en aandachtspunten zoals bijvoorbeeld een periodiek overleg met de Functionaris voor de Gegevensbescherming en CISO in DOWR-verband.

De Security Officer Suwinet draagt de inhoud van het beveiligingsplan uit aan alle medewerkers die gebruik maken van Suwinet. Dit gebeurt door voorlichting en een-op-eencontact.

Het beveiligingsplan wordt gedeeld met de CISO en Functionaris voor de Gegevensbescherming.