

Beveiligingsplan Suwinet 2024 - 2026

Domein Samenleving,

Gemeente Dalfsen
Februari 2024

Inhoud

1. Inleiding	3
2. Kader voor het Suwinet beveiligingsplan.....	3
3.1 Gebruikers van Suwinet-Inkijk	4
3.2 Functie raadplegen	4
3.3 Logging rapportages.....	5
4. Algemene gedragsregels ter beveiliging van de persoonsgegevens	6
Bijlage 1 Protocol	10
Bijlage 2 Zorgvuldigheidsverklaring	11

1. Inleiding

Suwinet-Inkijk biedt overheidsorganisaties de mogelijkheid om gegevens van burgers, die bij andere overheidsorganisaties of basisregistraties zijn opgeslagen, te raadplegen in een web toepassing.

De volgende organisaties en basisregistraties wisselen gegevens met elkaar uit: UWV, gemeente GSD, Sociale Verzekeringsbank(SVB), gemeente BRP, Dienst Wegverkeer(RDW), Dienst Uitvoering Onderwijs(DUO), Kamer van Koophandel(KvK), Kadaster, Belastingdienst, Bureau Krediet Registratie(BKR).

Door Suwinet-Inkijk worden gegevens op basis van Burger Service Nummer (BSN) toegankelijk gemaakt voor de bevoegde medewerkers.

Het gaat om privacygevoelige gegevens zoals arbeidsverleden, loon, uitkeringen, opleiding en bevolkingsgegevens van burgers. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Om de SUWI keten effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat “hun” gegevens door de partners in de Suwiketen op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage I van de regeling Suwi.

Als gevolg van de regeling Suwi is elke gemeente verplicht te beschikken over een actueel informatiebeveiligingsplan. In de Algemene Verordening Gegevensbescherming (AVG) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan. Ook staat hierin welke beveiligingsmaatregelen er moeten worden getroffen.

Het beveiligingsplan is geen statisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en het domein Samenleving zijn voortdurend in ontwikkeling, onder andere door gewijzigde of vernieuwde inzichten en wetgeving of aanpassingen in de informatiesystemen. Het beveiligingsplan wordt periodiek (jaarlijks) beoordeeld op actualiteit.

Sinds augustus 2013 hebben de medewerkers van Burgerzaken in principe toegang tot Suwinet-Inkijk. De gegevens die opgevraagd kunnen worden blijven beperkt tot de adresgegevens zoals deze door het UWV worden aangeleverd. Deze gegevens kan de medewerkers helpen bij ‘adresonderzoeken’, dat zijn die situaties waarin onduidelijkheid bestaat waar de burger woont. In Dalfsen is deze bevoegdheid niet verleend, omdat er geen aanleiding toe is gezien. Dit kan mogelijkwijze in de toekomst veranderen. In dat geval wordt dit vastgelegd in het beveiligingsplan Suwinet.

In dit beveiligingsplan zal eerst het kader voor het beveiligingsplan geschetst worden. Vervolgens wordt ingegaan op de bevoegdheden van gebruikers en aangegeven in welke situaties Suwinet-Inkijk gebruikt mag worden. Verder worden de algemene gedragsregels ter beveiliging van de persoonsgegevens beschreven waar medewerkers van het domein zich aan dienen te houden.

2. Kader voor het Suwinet beveiligingsplan

Het Bureau Keteninformatisering Werk en Inkomen ondersteunt de gemeenten en stelt diverse voorbeelden via hun website beschikbaar. De gehanteerde plannen zijn veelal informatiebeveiligingsplannen die van toepassing zijn op de gehele organisatie. Onderwerpen zijn bijvoorbeeld:

- fysieke toegangsbeveiliging gebouwen
- fysieke toegangsbeveiliging dossiers
- fysieke toegangsbeveiliging tot computerapparatuur

- beveiliging van digitaal opgeslagen gegevens
- beveiliging van (digitale) communicatiekanalen
- back-ups van gegevens
- integriteitbeleid gemeente
- calamiteitenplan
- waarborgen continuïteit (noodstroom e.d.)
- periodieke testen en evaluatie van bovengenoemde zaken.

De gemeente Dalfsen heeft voor de gehele gemeentelijke organisatie regels vastgesteld voor de beveiliging van gegevens. Zie hiervoor het gemeente breed informatiebeveiligingsbeleid 2021 gemeente Dalfsen. Dit beleid vormt het vertrekpunt van alle procedures en richtlijnen gebaseerd op de Baseline informatieveiligheid Gemeenten (ISO-normen 27001 en 27002). Daarnaast zijn in het informatiebeveiligingsplan alle aanvullende procedures opgenomen, dit plan wordt elk jaar geëvalueerd en minimaal 1x in de 4 jaar opnieuw vastgesteld.

Het gemeente breed informatiebeveiligingsbeleid 2021 vormt het vertrekpunt voor het specifieke beveiligingsplan van het domein zoals bedoeld in artikel 6.4. van de regeling SUWI. De gemeente Dalfsen gaat ervan uit dat het voldoende is om voor de medewerkers van het domein Samenleving gebruikersnormen voor het gebruik van Suwinet-Inkijk op te stellen.

3.1 Gebruikers van Suwinet-Inkijk

De volgende functies zijn geautoriseerd om gebruik te maken van Suwinet-Inkijk:

- applicatiebeheerder verzorgt autorisatie voor Suwinet-Inkijk binnen het pakket
- security officer vraagt periodieke en specifieke rapportage op en mag raadplegen om de rapportages te kunnen beoordelen.
- kwaliteitsmedewerker mag raadplegen
- consulenten Werk en Inkomen (inclusief uitvoering Bbz en inburgering) mogen raadplegen
- consulenten bijzondere bijstand mogen raadplegen
- consulenten schuldhelpverlening mogen raadplegen
- administratief medewerkers verzorgen standaard uitdraaien voor de consulenten en mogen raadplegen
- medewerkers terugvordering en verhaal mogen raadplegen
- stagiaires mogen beperkt raadplegen

De concernmanager is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk.

3.2 Functie raadplegen

Hierboven is benoemd wie Suwinet-Inkijk mogen raadplegen. In deze paragraaf wordt aangegeven wanneer dat mag. Wordt Suwinet- om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik. Over het algemeen geldt dat slechts mag worden geraadpleegd, indien die stap binnen het werkproces expliciet is beschreven.

Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet-Inkijk dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen.

De applicatiebeheerder ontvangt periodieke overzichten van het BKWI. Daarnaast beheerst de applicatiebeheerder de autorisaties en meldt hij deze mutaties (via de mail) aan de security officer.

De security officer controleert handhaving van dit beveiligingsplan door (specifieke) rapportages bij het BKWI op te vragen en te analyseren. Daarnaast houdt de security officer de mutaties in het autorisatieoverzicht bij.

Consulenten Werk en Inkomen mogen raadplegen bij het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussentijdse onderzoeken voor zover het de Participatiewet, IOAW en IOAZ of een door de eenheid daarvan afgeleide uitgevoerde regeling betreft.

De consulent die is belast met inburgering kan ook deze betreffende pagina's raadplegen. Het raadplegen van Suwinet-Inkijk bij aanvragen wordt met een afschrift in het dossier vastgelegd.

Consulenten schuldhelpverlening mogen raadplegen bij aanvragen en bij het opstellen van een plan van aanpak voor zover het de Wet gemeentelijke schuldhelpverlening betreft. Het raadplegen van Suwinet-Inkijk wordt met een afschrift in het dossier vastgelegd.

Consulenten bijzondere bijstand mogen raadplegen bij het behandelen van de aanvragen bijzondere bijstand of rechtmatigheidsonderzoeken en tussentijdse onderzoeken voor zover het de Participatiewet of een afgeleide uitgevoerde regeling betreft. Het raadplegen van Suwinet-Inkijk bij aanvragen wordt met een afschrift in het dossier vastgelegd.

Medewerkers die verantwoordelijk zijn voor incasso, terugvordering en verhaal mogen raadplegen bij onderzoeken die samenhangen met verhaal op onderhoudsplichtigen of vorderingen. Dit bijvoorbeeld ter vaststelling van woonplaats, medebewoners, draagkracht, inkomen of werkgever.

De administratief medewerker mag raadplegen om standaard uitdraaien voor het onderzoek van de consulenten Werk en Inkomen te maken. Zij zijn ook bevoegd dit te doen bij de verwerking van meldingen van het inlichtingen bureau.

Kwaliteitsmedewerkers mogen raadplegen om besluiten te kunnen toetsen.

Stagiaires mogen raadplegen, maar beperkt binnen die rollen die gekoppeld zijn aan de stage werkzaamheden.

De medewerkers van de unit Burgerzaken hebben op dit moment geen toestemming om de gegevens uit Suwinet-Inkijk te raadplegen om adresonderzoeken te behandelen.

Raadplegen van Suwinet-Inkijk in andere situaties wordt gemotiveerd in de rapportage.

Een BSN raadplegen van een cliënt die onbekend is in GWS in verband met een rechtmatigheids- en/of fraudeonderzoek wordt door de medewerker zelf geregistreerd als deze informatie noodzakelijk is voor de vaststelling van een onderhoudsbijdrage of terugvordering. Dit wordt in de rapportage vastgelegd of door de uitdraai Suwinet-Inkijk als bijlage in het dossier op te nemen.

3.3 Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet-Inkijk.

Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van de gemeente kan worden nagegaan. Iedere klik wordt door het BKWI vastgelegd.

Het doel van deze logging is tweeledig:

1. Tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking;
2. Wetenschappelijke en/of statistische doeleinden.

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd. Met toegang tot Suwinet-Inkijk krijgen medewerkers het protocol 'Suwinet-Inkijk' (bijlage 1) uitgereikt en tekenen zij de 'zorgvuldigheidsverklaring medewerkers' (bijlage 2).

Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. De medewerkers zijn op de hoogte van de volgende informatie:

- Het bestaan van de logging-gegevens;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd;
- Misbruik leidt tot zware sancties;
- Doelen van de logging;
- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doeloverschrijdend gebruik van het Suwinet-Inkijk wordt geconstateerd;
- Dat bij bovenstaande constatering dit door de concernmanager wordt gecommuniceerd met de betreffende medewerker(s).

In het kader van functiescheiding is het beheer voor het gebruik van Suwinet-Inkijk neergelegd bij de applicatiebeheerder van domein Samenleving. Deze is uitvoerend verantwoordelijk voor het beheren van de accounts.

Het BKWI levert twee soorten rapportages. Een periodiek rapport gaat automatisch naar de applicatiebeheerder. De specifieke rapportages kunnen worden opgevraagd door de applicatiebeheerder en de security-officer.

De security-officer vraagt minstens twee keer per jaar specifieke rapportages op en analyseert de login- gegevens om te bezien of de gemeente aan de gemaakte afspraken voldoet. De resultaten hiervan worden gerapporteerd aan de manager van het domein Samenleving.

4. Algemene gedragsregels ter beveiliging van de persoonsgegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Zoals bijvoorbeeld de Algemene Verordening Gegevensbescherming (AVG), het informatiebeveiligingsbeleid 2021 gemeente Dalfsen en het privacybeleid gemeente Dalfsen. Daaruit zijn gedragsregels afgeleid die gelden voor de medewerkers van domein Samenleving.

1. Beheren van wachtwoorden

De gebruiker moet het door de applicatiebeheerder uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord. Het wachtwoord bestaat uit minimaal 8 tekens waaronder een cijfer, een letter en een bijzonder teken. Het wachtwoord moet eens per 8 weken worden gewijzigd. Het gewijzigde wachtwoord mag niet overeenkomen met 1 van de vorige 10 gekozen wachtwoorden. Zodra een medewerker de gemeente verlaat, wordt het account verwijderd door de applicatiebeheerder.

Wanneer het account langere periode niet wordt gebruikt wordt deze automatisch geblokkeerd.

2. Melden van beveiligingsincidenten en datalekken

Het is verplicht dat beveiligingsincidenten direct worden gemeld bij de CISO. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak. Datalekken (het lekken van persoonsgegevens) moet direct gemeld worden bij de privacybeheerder.

3. Geheimhoudingsplicht

Binnen het domein wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Algemene verordening gegevensverwerking (AVG), het informatiebeveiligingsbeleid 2021 gemeente Dalfsen en het privacybeleid gemeente Dalfsen. In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

4. Gedragscode internet- en e-mailgebruik

De gemeente hanteert een protocol voor gebruik van email en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels met betrekking tot de controle op het gebruik van e-mail en internet. Het protocol is te vinden op het gemeentelijke intranet. In 2018 wordt ook een protocol informatiegebruik vastgesteld. Dit protocol is nu nog in ontwikkeling.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen domein Samenleving geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is van toepassing op iedereen binnen het domein die gebruik maakt van Suwinet-Inkijk. Bestaande gebruikers zijn op de hoogte; nieuwe gebruikers worden op de hoogte gesteld. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Jaarlijks wordt dit onderwerp geagendeerd voor het teamoverleg.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen.

Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben.

In principe wordt er dan ook geen telefonische informatie over cliënten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging.

Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven als er een vaste contactpersoon aan de lijn is.

7. Clean desk en clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven.

Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers.

Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord), zodra de medewerker de werkplek verlaat. Na enkele minuten vergrendeld het werkstation automatisch en dient de medewerker met een wachtwoord zelf opnieuw in te loggen.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens, waaronder persoonsgegevens, is erg belangrijk binnen de eenheid. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Binnen de gemeente is geregeld hoe vertrouwelijke stukken worden verzameld en vernietigd en iedereen is daarvan op de hoogte.

Er staan op de eenheid speciale containers waarin het te vernietigen materiaal wordt verzameld. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een prullenbak of een bak die bestemd is voor oud papier.

9. Aanspreken van onbekende personen

In het geval dat een medewerker van de eenheid een voor hem/haar onbekende persoon in de gang van de eenheid tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet.

Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hun beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naar toe te begeleiden.

10. De dagelijkse werkzaamheden vs. Informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen een eenheid waar de medewerkers veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerking van hun gegevens.

Reden waarom in het werkoverleg geregeld aandacht voor dit onderwerp dient te zijn.

11. Sancties

Als een medewerker de regels overtreedt, dan spreekt de eenheidsmanager hem daarop aan. Er zijn rechtspositionele maatregelen mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen.

Verantwoording

Dit beveiligingsplan vormt een bijlage bij het Interne controleplan. De controle op gebruik van Suwinet wordt gewaarborgd door de controles die in het IC-plan staan beschreven. Tevens is dit beveiligingsplan geborgd in het gemeente brede beveiligingsplan. Bij het opstellen van de IC-rapportage wordt eveneens gerapporteerd over het proces van opvragen cq controleren van login gegevens.

Bijlage 1 protocol

PROTOCOL

Met betrekking tot het gebruik van gegevens van Suwinet-Inkijk

Ter ondersteuning van de uitvoering van de Participatiewet is de gemeente Dalfsen aangesloten op het besloten Suwi-netwerk. Hiermee is het mogelijk om gegevens uit te wisselen met bijvoorbeeld de belastingdienst, DUO, UWV, RDW en andere gemeenten.

Op de gegevens van Suwinet-Inkijk zijn de bepalingen van de Algemene Verordening Gegevensbescherming en van de Wet Suwi van toepassing. Hierdoor zijn aan het gebruik van de applicatie Suwinet-Inkijk en aan overige webapplicaties die Suwi-gegevens inlezen regels verbonden.

Voor de gemeente Dalfsen luiden die regels als volgt:

1. De manager van het domein Samenleving wijst een medewerker functioneel beheer aan als applicatiebeheerder voor het gebruik van Suwinet-Inkijk, alsmede medewerkers die worden geautoriseerd om gegevens uit dit systeem te raadplegen.
2. Elke medewerker die geautoriseerd wordt voor het raadplegen van gegevens via Suwinet-Inkijk, wordt gerechtigd en beperkt tot het inwinnen van die informatie die nodig is om de opgedragen taken te verrichten zoals rechtmatigheids- of fraudeonderzoeken.
3. De geautoriseerde medewerker heeft toegang tot Suwinet-Inkijk door middel van een toegangscode. Het gebruik van het account en wachtwoord is strikt persoonlijk.
4. Het gebruik van Suwinet-Inkijk (elke muisklik) wordt vastgelegd en gecontroleerd.
5. Van de personen die niet voorkomen in het klantvolgsysteem en waarvoor Suwinet-Inkijk is geraadpleegd, houdt de medewerker afzonderlijk een eigen registratie in een Word- of Excelbestand bij. In dit overzicht is minimaal de BSN, naam en datum en reden opvraag vermeld.
6. Bij vermoeden van onrechtmatig gebruik of misbruik van de Suwinet-Inkijk gegevens vindt een onderzoek plaats. Bij vaststelling van onrechtmatig handelen of van misbruik zullen passende maatregelen worden getroffen.

Doel: verantwoording controle

Het management benoemt een security-officer die de taak heeft te bevorderen en te controleren dat de beveiliging van het Suwinet op orde is. Dit doet de security-officer door rapportages uit het audit logging systeem te analyseren.

De security-officer controleert twee maal per jaar het gebruik van de gegevens van Suwinet-Inkijk en rapporteert zijn bevinden aan de manager van het Domein Samenleving.

Indien sprake is van kennelijk onjuist gebruik van de gegevens van Suwinet-Inkijk hoort de manager de betreffende medewerker en neemt zo nodig maatregelen.

Bijlage 2 Zorgvuldigheidsverklaring

Zorgvuldigheidsverklaring medewerkers

Ondergetekende,

Naam: _____

Functie: _____

Team: _____

belooft/verklaart dat hij/zij:

er van op de hoogte is dat de privacy wet- en regelgeving beoogt een zorgvuldige omgang met persoonsgegevens te beschermen en dat deze wet- en regelgeving het gebruik van persoonsgegevens - in de ruimste zin van het woord - verbindt aan regels.

Zorgvuldig zal omgaan met de (persoons)gegevens en de inhoud van de documenten die hij/zij bij de uitvoering van de werkzaamheden in Suwi-verband mag inzien en zich daarbij houdt aan de werkinstructies zoals opgenomen in de functionele beschrijvingen van Suwinet-Inkijk en Suwinet-Mail.

Concreet betekent dit onder meer dat hij/zij:

- niet meer of vaker (persoons)gegevens raadpleegt dan strikt noodzakelijk is;
- een eigen registratie bijhoudt van personen die niet voorkomen in een werkproces of module fraude en doel van opvraging;
- (persoons)gegevens niet aan onbevoegden verstrekt;
- het Suwi-account (en wachtwoord) zorgvuldig hanteert en niet aan anderen ter beschikking stelt.

Kennis heeft genomen van de regels die gelden voor het zorgvuldig omgaan met persoonsgegevens.

Kennis heeft genomen van de algemene gedragsregels ter beveiliging van de persoonsgegevens en het beveiligingsplan Suwinet.

Gedurende de duur van zijn/haar inzet voor werkzaamheden in Suwi-verband enkel die (persoons)gegevens gebruikt, die van belang zijn voor het nastreven van het doel van Suwinet.

Alle medewerking zal geven aan het naleven van de privacywet- en regelgeving door de gemeente waar hij/zij werkzaam is.

Gedurende de duur van zijn/haar inzet voor de werkzaamheden in Suwi-verband en ook na beëindiging van deze werkzaamheden, [tegenover derden] geheimhouding zal betrachten met betrekking tot alle (persoons)gegevens waarvan hij/zij bij de uitvoering van de deze werkzaamheden kennis neemt.

Bekend is met het gegeven dat in het kader van interne controle alle BSN's die zijn geraadpleegd via Suwinet-Inkijk opgevraagd worden en dat deze worden gekoppeld aan de werkprocessen of de module fraude.

Bekend is met het gegeven dat bij het vermoeden van onrechtmatig gebruik of misbruik een intern onderzoek wordt gestart en dan bij vaststelling passende maatregelen kunnen worden opgelegd.

Datum:

Handtekening medewerker:

