gemeente cuijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Cuijk

Nr. 187977

26 juli 2019

Beveiligingsplan Suwinet

Inleiding

De gemeente heeft een grote rol binnen het "*Sociaal Domein*". Denk hierbij onder andere aan de taken die op basis van de Participatiewet (hierna "P-wet), de Wet inkomens-voorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers ("IOAW") en de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen ("IOAZ") aan de gemeente zijn toegekend. Om deze werkzaamheden goed uit te kunnen voeren, heeft de gemeente gegevens nodig van andere partijen. Het gaat hierbij bijvoorbeeld over het vaststellen van de rechtmatigheid van de uitkering (art. 17 lid 1 en art. 53a lid 1 en 6 P-wet) of het raadplegen van gegevens van een ex-partner voor de vaststelling van de onderhoudsplicht (art. 58-62i P-wet). Daarmee ontstaat een wettelijke grondslag tot het raadplegen van deze gegevens (art. 64 P-wet, art. 44 IOAW en art. 45 IOAZ). In de Wet structuur uitvoeringsorganisatie werk en inkomen ("Wet Suwi") is beschreven (art. 62) dat partijen deze informatie met elkaar uitwisselen via Suwinet.

Suwinet

Suwinet is een systeem, een "*digitale infrastructuur*", waarin gemeenten met andere overheidsinstanties zoals de Belastingdienst, het Bureau Keteninformatisering Werk en Inkomen ("BKWI"), de Dienst Uitvoering Onderwijs (studiefinanciering), het Uitvoeringsinstituut Werknemersverzekeringen (UWV en het UWV WERKbedrijf), de stichting Inlichtingenbureau Gemeenten en de Rijksdienst voor het wegverkeer informatie over burgers delen. Suwinet is tevens het netwerk waarover de klantgegevens voor het Digitaal Klant Dossier ("DKD") worden uitgewisseld.

Suwinet-inkijk is de applicatie die op Suwinet draait. Binnen deze applicatie worden gegevens op basis van het Burgerservicenummer ("BSN") toegankelijk gemaakt voor de daartoe bevoegde medewerkers. Het gaat over privacygevoelige gegevens zoals: inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, uitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. Ook is een Verificatie Informatie Systeem ("VIS module") opgenomen waarmee op basis van legitimatiebewijzen en vreemdelingendocumenten gegevens kunnen worden opgevraagd.

In dit beveiligingsplan wordt beschreven op welke wijze de vertrouwelijkheid van de gegevens uit Suwinet wordt gewaarborgd. Hierbij wordt uitgegaan van de beveiligingsvoorschriften in bijlage XIV van de regeling Suwi maar ook van de Algemene Verordening Gegevensbescherming ("AVG").

Werkorganisatie CGM

De gemeenten Cuijk, Grave en Mill en Sint Hubert maken voor de uitvoering van de genoemde taken gebruik van de medewerkers van de Werkorganisatie CGM. Deze samenwerking is gebaseerd op een gemeenschappelijke regeling. Om die taken goed te kunnen vervullen, maken deze medewerkers gebruik van de gegevens uit Suwinet.

Met ingang van 1 november 2018 worden voor deze bevragingen, met uitzondering van de raadplegingen vanuit Burgerzaken, niet meer de afzonderlijke gemeentelijke aansluitingen gebruikt, maar de nieuwe aansluiting van de Werkorganisatie. Voordeel hiervan is, dat medewerkers maar van één aansluiting gebruik maken. Omdat deze aansluiting wel de mogelijkheid kent dat de medewerker vermeldt voor welke gemeente de bevraging van toepassing is, is een overzicht van raadplegingen per gemeente nog steeds mogelijk.

Hoewel de daadwerkelijke uitvoering van de taken is uitbesteed aan de Werkorganisatie, zijn en blijven de individuele gemeenten verantwoordelijk voor het aantoonbaar voldoen aan de normen van Suwinet. Dit komt onder andere tot uitdrukking in ENSIA.

ENSIA

Met ingang van 2017 maakt de Suwinet verantwoording onderdeel uit van ENSIA (Eenduidige Normatiek Single Information Audit). Met ENSIA verantwoordt de gemeente zich niet alleen aan de betreffende toezichthouders, maar ook aan de gemeenteraad.
ENSIA sluit aan op de gemeentelijke planning en control-cyclus. Voorheen waren er aparte verantwoordingsprocedures voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Met ENSIA is dit nu gebundeld. Dat wil zeggen dat gemeenten in één keer verantwoording afleggen over het gebruik van zes registratiesystemen.

Instructies
Gelet op het feit dat de gemeenten, ondanks dat de feitelijke werkzaamheden worden uitgevoerd door de Werkorganisatie, verantwoordelijk zijn voor het voldoen aan de normen van Suwinet, is dit beveiligingsplan daarom vastgesteld door de drie colleges van de gemeenten die deelnemen aan de Werkorganisatie. In dit plan zijn de "instructies" aan de Werkorganisatie vermeld. De colleges gaan er van uit, dat de Werkorganisatie de werkwijze zo inricht, dat aan de gestelde eisen kan worden voldaan.

Beveiligingsplan Suwinet
Informatiebeveiliging is een aspect dat niet alleen binnen het Sociaal Domein van toepassing is. Het veilig en zorgvuldig omgaan met informatie is een vereiste dat geldt voor de hele organisatie. De wijze waarop informatiebeveiliging, op basis van de BIG, organisatiebreed wordt toegepast, is beschreven in het algemene informatiebeveiligingsbeleid en het privacybeleid.

Ook deze documenten zijn vastgesteld door de colleges en bevatten een "opdracht" voor CGM. Deze algemene beleidsdocumenten gelden dus ook voor de werkzaamheden die met Suwinet worden uitgevoerd. Artikel 6.4 van de Regeling Suwi vereist echter nog een aparte, aanvullende regeling met betrekking tot Suwinet. Dit beveiligingsplan bevat daarom specifiek op Suwinet gerichte regelgeving, voor zover de algemene beleidsdocumenten hierin niet voorzien. Dit plan dient dan ook te worden beschouwd als een specifieke aanvulling op het algemene beveiligingsbeleid en privacyprotocol.

Dit nieuwe beveiligingsplan vervangt het Suwi-inkijkprotocol dat in 2015 is opgesteld.
Het protocol uit 2015 is inmiddels verouderd en, gelet op de looptijd, vervallen.
Het voorliggende beleid voldoet aan de nieuwe wet- en regelgeving zoals het nieuwe Suwinetnormenkader uit 2017. Daarnaast is rekening gehouden met de inwerkingtreding van de AVG op 25 mei 2018.

Wettelijke grondslag
De AVG bepaalt de wijze waarop met persoonsgegevens mag worden omgegaan, het doel waarvoor ze mogen worden verzameld, de wijze waarop ze mogen worden verwerkt en de beveiligingsmaatregelen die moeten worden getroffen. Een gemeente heeft gegevens nodig van andere partijen voor de uitvoering van de P-wet, IOAW, en IOAZ. Daarmee ontstaat een wettelijke grondslag tot het raadplegen van gegevens (art. 64 P-wet, art. 44 IOAW en art. 45 IOAZ). Er worden alleen gegevens uitgewisseld voor zover daar een wettelijke grondslag voor is.

Gebruik Suwinet
Suwinet mag gebruikt worden door:
geautoriseerde medewerkers van gemeenten die belast zijn met uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW en IOAZ. Dit geldt tevens voor ingehuurde capaciteit, bijvoorbeeld een medewerker die wordt ingehuurd via een uitzendbureau. Deze medewerker werkt dan op het kantoor en onder het gezag en toezicht van de desbetreffende gemeente;
niet-Suwipartijen die door middel van een overeenkomst op grond van art. 5.23 van het Besluit Suwi en conform het aansluit protocol (bijlage III Regeling Suwi) een zelfstandige aansluiting hebben op Suwinet:

- belastingdeurwaarders voor het leggen van loonbeslag;[1]

- Regionale Meld- en coördinatiepunten (RMC's) voor hulp aan voortijdige schoolverlaters;[2]
afdelingen burgerzaken voor het bijhouden van de Basis Registratie Personen. Hiervoor is geen overeenkomst (zoals hiervoor bedoeld bij niet-Suwipartijen) nodig. Nadere regels staan in art. 3.3 van de Regeling Suwi;[3]
medewerkers die de inburgering verzorgen mogen via Suwinet gebruik maken van het inburgeringsportaal.

Binnen CGM wordt Suwinet niet gebruikt door belastingdeurwaarders. De gemeente Oss is centrumgemeente ten aanzien van de hulp aan voortijdige schoolverlaters. CGM gebruikt Suwinet daarom niet voor deze doelen, dit beleid is dan ook niet van toepassing op deze situaties. De overige taken worden benoemd in de autorisatiematrix (zie pagina 5).

Verantwoordelijkheid
Binnen de Werkorganisatie CGM dragen de eigenaren van processen en systemen verantwoordelijkheid voor de beveiliging van de informatie die in hun processen en systemen wordt verwerkt en opgeslagen.

1) https://www.bkwi.nl/producten/suwinet-services/suwinet-inkijk/suwinet-inkijk-voor-gemeentelijke-belastingdeurwaarders
2) https://www.bkwi.nl/producten/suwinet-services/suwinet-inkijk/suwinet-inkijk-voor-rmcs
3) https://www.bkwi.nl/producten/suwinet-services/suwinet-inkijk/suwinet-inkijk-voor-burgerzaken

De uitvoering van informatiebeveiliging is, onder leiding van de directeur, een verantwoordelijkheid van het management. Het management is verantwoordelijk voor de kwaliteit van de bedrijfsvoering en informatiebeveiliging geldt als een integraal onderdeel van die bedrijfsvoering. Medewerkers hebben, binnen de bestaande richtlijnen, een eigen verantwoordelijkheid voor de wijze waarop zij met informatie en de beveiliging daarvan omgaan.

Overkoepelend is de CISO (Chief Information Security Officer) verantwoordelijk voor het onderhouden van het gemeentebrede informatiebeveiligingsbeleid. Voor Suwi is een security officer Suwi aangesteld. De security officer Suwi legt verantwoording af aan de teamleider en de afdelingsmanager en informeert het management en de CISO bij geconstateerde gebreken, disproportioneel Suwinet gebruik of een (potentieel) datalek.
De security officer Suwi is aangewezen als gemandateerde voor het opvragen van (specifieke) rapportages.

Proportionaliteit van gegevenslevering
Om de privacy van de burgers van de drie gemeenten te borgen, is het van belang dat proportionele gegevenslevering in acht wordt genomen. Dit betekent, dat niet meer en niet minder persoonsgegevens mogen worden ingezien dan strikt noodzakelijk is voor de uitvoering van de taken in het kader van de P-wet, IOAW en IOAZ. Binnen de Werkorganisatie zijn twee maatregelen getroffen om de proportionaliteit van gegevenslevering te optimaliseren: fijnmazig autoriseren en whitelisting.

Beheer autorisaties
Om de toegang tot Suwinet zo fijnmazig mogelijk in te richten wordt gebruik gemaakt van een autorisatiematrix (zie bijlage 1). Deze matrix is ingericht op basis van "rollen".
Deze rollen zijn samengesteld door het BKWI en bestaan uit een verzameling bronpagina's en overzichtspagina's. Per Suwinetgebruiker is gekeken naar de functieomschrijving en een afweging gemaakt van de noodzakelijke pagina's voor de taakuitvoering. Hierbij zijn proportionaliteit en doelbinding in acht genomen. Deze matrix wordt elke drie maanden door de security officer Suwi herzien en in een gezamenlijk overleg vastgesteld door de betreffende teamleiders en afdelingsmanager.

Wijzigingen in autorisaties worden doorlopend bijgehouden in de autorisatiematrix.
De applicatiebeheerder en security officer Suwi onderhouden de matrix. Een format van de matrix is opgenomen in bijlage 1. De meest actuele versie kan worden opgevraagd bij de security officer Suwi.
Wijzigingen in de autorisaties worden, via de teamleider, doorgegeven aan de security officer Suwi.
De applicatiebeheerder voert de wijziging na toestemming van de security officer Suwi door.

Aanvragen account
De Werkorganisatie kent een procedure voor het in dienst treden van nieuwe medewerkers.
In deze procedure wordt, onder andere, door de leidinggevende bepaald, binnen welke applicaties een nieuwe medewerker toegang en rechten moet krijgen.

Voor het aanvragen van een account voor Suwinet dient aan de volgende voorwaarden te worden voldaan:
- de medewerk(st)er is inhoudelijk op de hoogte van dit beveiligingsplan Suwinet en de binnen de organisatie geldende afspraken inzake het gebruik van Suwinet. Hij/zij is hiervan op de hoogte gesteld in een gesprek met de security officer Suwi;
- de medewerk(st)er heeft de zorgvuldigheidsverklaring van Suwinet gelezen en ondertekend en dit is als PDF toegevoegd bij de aanvraag. Het originele getekende protocol wordt toegevoegd aan het personeelsdossier van de medewerk(st)er.

Pas nadat wordt voldaan aan deze voorwaarden, autoriseert de applicatiebeheerder, na daartoe opdracht te hebben ontvangen van de security officer Suwi, de nieuwe gebruiker.
Bij wijziging van functie (waarbij toegang tot Suwinet in andere vorm of niet meer aan de orde is) of bij uitdiensttreding wordt het account aangepast respectievelijk verwijderd.

Autorisatiematrix
In de autorisatiematrix (zie het format in bijlage 1) wordt beschreven wie in welke hoedanigheid van Suwinet gebruik mag maken. De medewerkers met de volgende functies/taken (hieronder zijn de "rollen" vermeld zoals die door het BKWI gehanteerd worden) zijn geautoriseerd om gebruik te maken van Suwinet-inkijk:
- poortwachter (doel: voeren intakegesprekken, verzorgen participatie-aanvraag, mogelijkheden werkzoekende, onderzoek naar recht op uitkering inzake P-wet, IOAW en IOAZ, rapporteren);
- bestandsbeheerder (doel: onderzoek naar recht op uitkering inzake P-wet, IOAW en IOAZ, rapporteren, handhaven);

- minimabeleid (doel: onderzoek naar recht op uitkering op basis van de PW, rapporteren, handhaven);
- re-integratieconsulent (doel: verzorgen participatie-aanvraag, onderzoek mogelijkheden werkzoekende, rapporteren);
- debiteurenadministratie (doel: onderzoek naar betalingsmogelijkheden en naar draagkracht onderhoudsplichtigen, rapporteren);
- handhaving (doel: onderzoek naar oneigenlijk gebruik en misbruik van uitkeringen inzake P-wet, IOAW en IOAZ, onderzoek naar recht op uitkering inzake P-wet, IOAW en IOAZ, rapporteren en handhaven);
- administratief medewerker (doel: verificatie van de verstrekte gegevens);
- inburgering (doel: onderzoek naar de mate waarin aan de inburgeringsplicht is voldaan, rapporteren);
- burgerzaken (doel: gebruiken adresgegevens UWV voor het bijhouden van adresgegevens in de Basisregistratie Personen (BRP);
- gebruikersbeheer (doel: aanmaken, wijzigen en verwijderen van gebruikersaccounts, downloaden reguliere gebruiksrapportages);
- security officer Suwi (doel: analyseren generieke gebruiksrapportages, aanvragen en analyseren specifieke gebruiksrapportages, signaleren mogelijk onrechtmatig gebruik van Suwinet, bepalen autorisatie per functieprofiel, voorlichting gebruikers over correct gebruik Suwinet).

Whitelist
Organisaties kunnen bij het opvragen van gegevens in Suwinet-Inkijk een "filter" gebruiken dat regelt dat hun medewerkers alleen gegevens kunnen opvragen van de burgers die tot hun werkvoorraad (klantenbestand) behoren. Om de werkvoorraad te vullen en actueel te houden, dient hiervoor een medewerker te worden aangesteld. Vanuit veiligheidsoogpunt dient dit een medewerker te zijn, die niet zelf gegevens opvraagt over burgers.

In april 2017 heeft de Werkorganisatie een whitelist voor Suwinet ingevoerd. De whitelist betreft een filter, welke wordt toegepast op de volledige database met persoonsgegevens. Het filter is op een dusdanige wijze ingericht, dat Suwinetgebruikers van de Werkorganisatie in eerste instantie alleen burgerservicenummers kunnen raadplegen van burgers waarbij een of meerdere van de volgende criteria van toepassing zijn:
- er is sprake van een lopende P-wet, IOAW of IOAZ uitkering van klant of partner;
- er is sprake van een lopende aanvraag op grond van de P-wet, IOAW of IOAZ;
- er is sprake van openstaande vorderingen van klant of partner op grond van de P-wet, IOAW of IOAZ;
- er is sprake van cliënten en partners die als Niet Uitkerings Gerechtigden een re-integratie voorziening krijgen op grond van de P-wet (inclusief cliënten die zijn opgenomen in het doelgroepregister).

Om de whitelist het beoogde doel te laten dienen, is zorgvuldig afgewogen welke medewerkers toegang hebben gekregen tot de whitelist. Dit is vermeld in de autorisatiematrix (zie bijlage 1). De whitelist wordt dagelijks als databestand geüpload op de Suwinetpagina en vervolgens door het BKWI geautomatiseerd verwerkt.

Omdat het soms nodig is om toch informatie op te vragen van burgers waar geen klantrelatie mee bestaat (denk aan taken in het kader van fraudeonderzoek of uitkeringsaanvragen voordat de administratieve verwerking heeft plaatsgevonden), is er een omleiding in de whitelist ingebouwd: de "escapefunctie". Deze escape geeft toegang tot de persoonsgegevens van burgers waar in het kader van de P-wet (nog) geen klantrelatie mee bestaat.

Wanneer de medewerker gebruik maakt van de escapefunctie, wordt gevraagd hiervoor een reden op te geven. De medewerker selecteert één van de vijf beschikbare redenen en klikt vervolgens op doorgaan. Het gebruik van de escape wordt te allen tijde geregistreerd. De vijf redenen waaruit de medewerker kan kiezen zijn:
1. nieuwe klant of aanvraag: wanneer er sprake is van een aanvraag van een nieuwe klant of partner die nog niet is geregistreerd;
2. vaststellen onderhoudsbijdrage: voor verhaalsmedewerkers, bij het vaststellen van de onderhoudsbijdrage bij nieuwe onderhoudsplichtigen;
3. inkomsten van 16 en 17 jarigen: inkomsten van een inwonend kind van 16 of 17 jaar moeten in sommige gevallen met de bijstandsuitkering van de ouders worden verrekend. De hoogte van die inkomsten moet worden achterhaald;
4. bijzonder onderzoek: bij nader onderzoek naar fraude of een sterk vermoeden daarvan;
5. anders: aangeraden is deze optie zo min mogelijk te gebruiken aangezien deze optie weinig inzicht geeft in de reden voor het escapegebruik.

Controle op gebruik Suwi -inkijk

Het BKWI registreert iedere logging en klik binnen Suwinet. De gebruikers van Suwinet-Inkijk zijn hiervan op de hoogte. Bij de aanvraag voor een Suwinet-Inkijk account dienen medewerkers kennis te nemen van dit beveiligingsplan en tekenen zij de zorgvuldigheidsverklaring (zie bijlage 2). Het BKWI heeft rapportages ontwikkeld die inzicht geven in de geregistreerde loggings. Het doel van deze rapportages is het tegengaan en controleren van onrechtmatige of doeloverschrijdende verwerking van persoonsgegevens. Het BKWI levert twee soorten rapportages: generieke gebruiksrapportages en specifieke gebruiksrapportages.

Generieke gebruiksrapportages
De generieke gebruiksrapportages bieden kwantitatieve data over de door Suwinet gebruikers geraadpleegde pagina's binnen Suwinet. Het gaat om algemene statistische gegevens welke niet herleidbaar zijn tot de individuele gebruiker. Iedere maand stelt het BKWI deze rapportages beschikbaar. De rapportages bevatten de data van de afgelopen maand, ten opzichte van de vijf maanden daarvoor. Het totaaloverzicht toont dan ook zes maanden aan gebruikersdata. De security officer Suwi is gemandateerd voor het opvragen van de generieke gebruiksrapportages.

De volgende statistieken worden met deze rapportage inzichtelijk gemaakt:
1. Algemeen:
Totaal gebruik;
2. Zorgvuldig gebruik:
Raadplegingen op zoeksleutel anders dan burgerservicenummer, het percentage raadplegingen buiten kantoortijd, de meest geraadpleegde burgerservicenummers, het hoogste aantal actieve gebruikers dat hetzelfde burgerservicenummer heeft geraadpleegd en het hoogste aantal raadplegingen per actieve gebruiker;
3. Accountbeheer:
De geblokkeerde accounts op de eerste dag van de maand, de ongebruikte accounts, de aangemaakte accounts, de verwijderde accounts en wijzigingsacties op accounts en de verdeling van de rollen;
4. Veilig gebruik:
de verdeling van de raadplegingen over de pagina's, de whitelist escape, verzonden Suwimail, ontvangen Suwimail.

De rapportages zijn door het algemene karakter enkel bruikbaar voor het signaleren van opvallende afwijkingen ten opzichte van de andere maanden. Een dergelijke afwijking kan een signaal zijn dat nader onderzoek wenselijk is.

Specifieke gebruiksrapportages
Bij constatering van afwijkende cijfers in de generieke rapportages kan ervoor gekozen worden vervolgonderzoek uit te voeren. In dat geval vraagt de daartoe gemandateerde medewerker (de security officer Suwi) specifieke rapportages op bij het BKWI. Specifieke rapportages kunnen per item zoals hiervoor beschreven, worden aangevraagd.
De specifieke gebruiksrapportages zijn wel herleidbaar tot de individuele gebruiker.

Indien uit de controle blijkt dat misbruik van persoonsgegevens kan worden geconstateerd, dan informeert de security officer Suwi de betreffende teamleider en de afdelingsmanager.
De teamleider onderneemt actie tot verbetering van gedrag en/of stelt, in overleg met de afdelingsmanager, een procedure in werking voor het treffen van sancties.
De afdelingsmanager informeert, afhankelijk van de situatie, bij ernstig misbruik de betrokken bestuurder(s), de directeur en de CISO. Als er tevens sprake is van een datalek, informeert de leidinggevende de CISO/FG en in het geval van een ernstig datalek meldt de CISO/FG dit lek bij de Autoriteit Persoonsgegevens en eventueel bij de betrokkenen.

De generieke gebruiksrapportages worden eens per kwartaal geanalyseerd door de security officer Suwi. Van deze analyse, inclusief eventueel aangevraagde specifieke rapportages, wordt een kwartaalverslag gemaakt welke wordt verstuurd aan de teamleider, de afdelingsmanager en het kwaliteitsteam. De CISO ontvangt alleen de generieke gebruiksrapportages. Indien de leidinggevenden daartoe aanleiding zien, wordt de CISO geïnformeerd over de analyse en/of de specifieke rapportage.

(Onderzoek naar) misbruik
Bij controle van het gebruik kan er sprake zijn van constateringen die afwijken van het normale gebruiksbeeld. In dat geval wordt er een specifieke rapportage opgevraagd. Indien deze rapportage daartoe aanleiding geeft, stelt de security officer Suwi de teamleider op de hoogte. De teamleider stelt een onderzoek in en betrekt daarbij altijd de afdelingsmanager.

Onderzocht wordt of er sprake was van doelmatig en rechtmatig gebruik van de Suwinet inkijk voorziening. Het kan nodig zijn om met de betrokken medewerker te spreken om dit uiteindelijk vast te stellen. Indien er geen misbruik geconstateerd is, is daarmee het onderzoek ten einde.

Indien er wel misbruik wordt geconstateerd, zal de security officer Suwi een rapportage opstellen waarin deze aard van het misbruik omschreven wordt en deze aan de leidinggevende richten. Er kan sprake zijn van de situatie dat misbruik geconstateerd is en dat de medewerker die hier verantwoordelijk voor is, niet meer bij de organisatie werkzaam is. In die situatie wordt beoordeeld welke stappen ondernomen worden. Hiertoe behoort eventueel ook het inlichten van de nieuwe werkgever.

Er wordt onderscheid gemaakt tussen vermoedelijk en geconstateerd misbruik. Opzettelijk onjuist gebruik wordt aangemerkt als misbruik. Indien er sprake is van (vermoedelijk) misbruik door een medewerker informeert de security officer Suwi de teamleider.
De teamleider heeft een informerend gesprek met de medewerker. Dit gesprek wordt gerapporteerd richting de afdelingsmanager.

Onder ernstig misbruik wordt in ieder geval verstaan het beschikbaar stellen van gegevens van burgers aan derden voor commerciële doeleinden. De security officer Suwi meldt gebleken misbruik aan de teamleider met een advies over de ernst van dit misbruik.
De sanctie wordt afgestemd op de ernst van het misbruik en de omstandigheden. Ernstig misbruik kan leiden tot strafontslag of bij ingeleend personeel tot het onmiddellijk beëindigen van de inleenverhouding en melding aan de uitlener.

Sancties
Een medewerker die de regels onvoldoende naleeft kan daarop worden aangesproken op grond van de Ambtenarenwet of de gedragscode integer handelen. Zowel interne als externe medewerkers tekenen een integriteitsverklaring bij indiensttreding.

Conform de Ambtenarenwet en de CAR/UWO zijn rechtspositionele maatregelen mogelijk. De zwaarte van de sanctie is ter beoordeling van de werkgever. Op basis van hetgeen in de CAR/UWO is beschreven aan disciplinaire maatregelen (van berisping tot ontslag op staande voet) bepaalt de werkgever de zwaarte van de disciplinaire maatregel.
De medewerker wordt hier schriftelijk van in kennis gesteld. Tegen deze beslissing is bezwaar en beroep mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen.

Onjuist gebruik leidt tot een nadere instructie, waarschuwing of sanctie van de betrokken medewerker. Met "*onjuist gebruik*" wordt elk gebruik van Suwi voor eigen doeleinden bedoeld. Het gaat hier dan bijvoorbeeld (de opsomming is niet limitatief bedoeld) om:
1. elk gebruik dat niet ten dienste staat van de uitkeringsverlening;
2. het opvragen van gegevens ten behoeve van derden;
3. het verstrekken van die gegevens aan derden.
Incidentele fouten, zoals het ingeven van een verkeerd burgerservicenummer, worden niet gezien als onjuist gebruik.

Procedures Suwinet-inkijk
Met betrekking tot Suwinet-inkijk zijn door de teamleiders en afdelingsmanager van de afdeling Uitvoering Sociaal Domein, de volgende specifieke procedures afgesproken:

Beheer wachtwoorden: de applicatiebeheerder bepaalt hoe lang een wachtwoord geldig is. De gebruiker moet het toegekende wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord. Het account van Suwinet blokkeert automatisch als het langer dan één kwartaal niet is gebruikt. Zodra een medewerker niet langer gebruikt maakt van Suwinet, zoals bij uitdiensttreding of wijziging van functie, wordt het account verwijderd.

Melden incidenten: beveiligingsincidenten en (mogelijke) datalekken worden gemeld via topdesk. De medewerkers bij de helpdesk informeren de (plaatsvervangend) CISO en de medewerkers van ICT.

Geheimhoudingsplicht: gebruikers van Suwinet-inkijk werken met persoonsgegevens. Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de gegevens, inclusief persoonsgegevens, niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie strikt noodzakelijk is. De persoonsgegevens die via Suwinet inkijk zijn verkregen mogen niet lokaal worden opgeslagen (zoals op de harde schijf of een usb-stick).
Na beëindiging van de werkzaamheden dient te allen tijde te worden uitgelogd.

Kennisnemen van het beveiligingsbeleid Suwinet: dit beveiligingsbeleid Suwinet is van toepassing op alle gebruikers van Suwinet binnen de Werkorganisatie CGM. Het beleid is voor iedereen toegankelijk via Lijn 92 (intranet). De medewerkers worden, hetzij door de teamleider hetzij door de security officer

Suwi, minimaal 2 keer per jaar tijdens een (team)overleg op de hoogte gesteld van de inhoud van het beleid en de noodzaak van het veilig omgaan met Suwinet.

Nieuwe medewerkers worden door de security officer Suwi, bij het ondertekenen van de geheimhoudingsverklaring, gewezen op het beleid met de opdracht er kennis van te nemen. Hierdoor weten medewerkers welk gedrag de organisatie van hen verwacht en weten ze dat er gegevens worden bewaard waarmee hun gedrag (binnen Suwinet) kan worden gecontroleerd.

Bewustwording : organisatiebreed worden verscheidene vormen van bewustwording rondom privacy en informatiebeveiliging toegepast. Daarnaast geldt dat er specifieke Suwinet bewustwordingsacties worden gehouden. Minimaal eens per half jaar of zo vaak als nodig i.v.m. wijzigingen wordt een mail naar de Suwinet gebruikers groep gestuurd. Hierin wordt de gebruikers opnieuw herinnerd aan de afspraken ten aanzien van het gebruik van Suwinet. Daarnaast worden de actuele wijzigingen of andere nieuws rondom Suwinet doorgenomen.

Gegevensverstrekking aan derden via de telefoon : het uitgangspunt is dat medewerkers terughoudend zijn om telefonisch informatie over inwoners te verstrekken. Het voeren van telefoongesprekken brengt namelijk het risico met zich mee dat persoonsgegevens worden verstrekt aan personen die geen recht op deze informatie hebben. In principe wordt er dan ook geen telefonische informatie over inwoners 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 (zoals bijvoorbeeld UWV) 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 indien het een vaste contactpersoon betreft.

Suwinetmail /beveiligd mailen : Suwinetmail is een communicatiefaciliteit in de vorm van een besloten netwerk dat gebruikers van de aangesloten overheidsorganisaties de mogelijkheid biedt om vertrouwelijke informatie met elkaar uit te wisselen. Voor zover voor het uitwisselen van gevoelige gegevens geen gebruik kan worden gemaakt van Suwinetmail (bijvoorbeeld omdat de betreffende instantie hier niet bij aangesloten is), wordt de mail beveiligd verstuurd via Cryptshare. Het wachtwoord dat noodzakelijk is om (de bijlage bij) een e-mail te kunnen openen, wordt op andere wijze dan per e-mail verstuurd.

Clean desk en clear screen policy : 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 moeten zich bij binnenkomst eerst melden bij de receptie. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord), zodra de medewerker de werkplek verlaat.

Vertrouwelijke gegevens in de papierbak : het vernietigen van gevoelige gegevens moet op een veilige manier plaatsvinden. Op verschillende plekken in de organisatie staan papiervernietigers. Het papier wordt door middel van afsluitbare containers, periodiek, door een vernietigingsbedrijf afgevoerd.

Aanspreken van onbekende personen : als een medewerker een voor hem/haar onbekende persoon in het gebouw tegenkomt op een plek waar geen publiek zonder begeleiding mag komen, moet de medewerker deze persoon aanspreken en vragen naar de reden voor de aanwezigheid. Personen die niet bevoegd zijn om zich op deze plek te bevinden, begeleidt de medewerker naar het publieke gedeelte van het gebouw.

Suwinet -Inkijk en inzage door anderen dan gerechtigden
Inzage in Suwinet-Inkijk door derden is niet toegestaan. Op het indienen van een inzage- of correctieverzoek door een client of zijn/haar gemachtigde, zijn art. 15, 16 en 23 van de AVG, art. 41 van de Uitvoeringswet AVG en bijlage 1 van de Regeling Suwi van toepassing.

Frequentie herziening beveiligingsplan Suwinet
Het beveiligingsplan Suwinet wordt periodiek geactualiseerd. Minimaal eens per drie jaar en voor zo ver de landelijke en gemeentelijke ontwikkelingen hierom vragen, zal tussentijdse herziening plaatsvinden. Hierbij valt te denken aan wijzigingen ten aanzien van sociale zekerheid, wetswijzigingen, technische wijzigingen of aanpassingen in de informatiesystemen.

Vastgesteld op 16 april 2019
Burgemeester en wethouders van Cuijk