Gemeente Heerlen

GEMEENTEBLAD

Officiële uitgave van de gemeente Heerlen

Nr. 262373

12 oktober

2020

Gemeente Heerlen - Informatiebeveiligingsbeleid Suwinet gemeente Heerlen

Het college van burgemeester en wethouders van de gemeente Heerlen

OVERWEGING
gelet op het bepaalde in Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI);
mede gelet op het Besluit Suwi en op de Regeling SUWI;
mede gelet op het bepaalde in de Wet eenmalige gegevensuitvraag werk en inkomen (WEU);
mede gelet op het bepaalde in de Wet Regionale Meld- en Coördinatiefunctie (Wet RMC);
mede gelet op de Algemene verordening gegevensbescherming (AVG);
mede gelet op de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);
mede gelet op het bepaald in de Baseline Informatiebeveiliging Overheid (BIO);

BESLUIT
vast te stellen het navolgende: Informatiebeveiligingsbeleid Suwinet gemeente Heerlen

Beleidsinhoud
De gemeente deelt op basis van de Wet SUWI persoonlijke informatie van inwoners met een aantal organisaties. Het gaat om informatie over arbeidsverleden, loon, uitkeringen en opleiding. Het is natuurlijk heel belangrijk dat het delen van deze informatie zorgvuldig gebeurt. Daarvoor heeft de gemeente Heerlen het beveiligingsbeleid Suwinet vastgesteld, dit naast het informatiebeveiligingsplan Suwinet en het informatiebeveiligingsbeheer Suwinet.
Het informatiebeveiligingsbeleid Suwinet zegt wat over de interne organisatie, waaronder:

- Governance: relevante functies met hun taken en verantwoordelijkheden zoals bijvoorbeeld de beveiligingsfunctie
- Aansluitbeleid: de randvoorwaarden voor aansluiting op de Gemeenschappelijke elektronische Voorziening Suwi (GeVS, ook wel Suwinet genoemd). Het aansluitbeleid betreft het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens.

Het informatiebeveiligingsplan Suwinet wordt jaarlijks of vaker, wanneer daar aanleiding toe is, geactualiseerd. Het informatiebeveiligingsplan bevat verbetervoorstellen op basis van evaluaties.
Het informatiebeveiligingsbeheer Suwinet behelst een ingerichte beheersorganisatie waarin beheerprocessen en evaluatieactiviteiten zijn vormgegeven. Bijvoorbeeld:

- Evaluatie van het aansluitbeleid
- Logging en rapportage
- Autorisatiebeleid.

Daarnaast is sanctiebeleid bij oneigenlijk gebruik van Suwinet opgesteld.

Hoofdstuk 1 - Algemeen

Inleiding en het belang van dit beleid

Het Uitvoeringsinstituut werknemersverzekeringen (UWV), de Sociale verzekeringsbank (SVB) en de colleges van burgemeester en wethouders werken samen bij de uitvoering van taken op grond van de Wet SUWI, de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (Wet IOAW), de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (Wet IOAZ) en de Wet gemeentelijke schuldhulpverlening met het oog op een doeltreffende en klantgerichte uitoefening van die taken (Wet SUWI artikel 9). Met het oog op de dienstverlening met betrekking tot deze wetten werken het UWV en de colleges van burgemeester en wethouders ook samen ten aanzien van de registratie van werkzoekenden en vacatures met behulp van de elektronische voorzieningen, bedoeld in artikel 62, tweede lid van de Wet SUWI. Ook werken zij in regio's samen bij de dienstverlening aan werkgevers en het verrichten van taken met betrekking tot de regionale arbeidsmarkt (wet SUWI artikel 10). Het UWV, de SVB en de colleges van burgemeester en wethouders verstrekken elkaar uit eigen beweging en op verzoek, kosteloos, alle gegevens en inlichtingen die noodzakelijk zijn voor de uitvoering van de taken die bij of krachtens de Wet SUWI of enige andere wet aan het UWV, de SVB en bij of krachtens de Participatiewet, de Wet IOAW, de Wet IOAZ, de Wet gemeentelijke schuldhulpverlening of bij of krachtens andere wetten aan de colleges van burgemeester en wethouders zijn opgedragen, voor zover dit voortvloeit uit de samenwerking (Wet SUWI artikel 62 lid 1).
Bij de gegevensverwerking voor de uitvoering van de diensten en taken zijn het UWV en de colleges van burgemeester en wethouders gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 van de Algemene verordening gegevensbescherming voor de verwerking van gegevens voor de

uitvoering van taken ten aanzien van dezelfde uitkeringsgerechtigde of werkzoekende (Wet SUWI artikel 62 lid 3). Deze verantwoordelijkheid stelt eisen aan de interne organisatie en het aansluitbeleid van de gemeente Heerlen.

Wat is Suwinet?

De Gemeenschappelijke elektronische Voorziening Suwi (GeVS, ook wel Suwinet genoemd), is een digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat, de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld voor zover daar een wettelijke grondslag voor is. De gegevens die getoond worden zijn vastgelegd in de wettelijke taak die de afnemende organisatie uitvoert en bepaalt welke gegevens van welke burgers mogen worden geraadpleegd. Het betreffen gegevens over onder meer uitkeringen, werk, re-integratie en opleidingen.
Via Suwinet Services kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen. Suwinet Services zijn primair bedoeld voor UWV, SVB en de gemeentelijke sociale diensten (GSD), maar inmiddels maken ook veel andere overheidsorganisaties gebruik van deze services. Door gegevens binnen de overheid te delen, kunnen burgers sneller en beter worden geholpen en hoeven zij geen gegevens te verstrekken.
Via Suwinet Services wordt de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) aangeboden, hieronder vallen de volgende producten en diensten:

- Suwinet-Inkijk biedt overheidsorganisaties de mogelijkheid om gegevens van burgers, die bij diverse andere overheidsorganisaties of basisregistraties zijn opgeslagen, te raadplegen in een beveiligde webtoepassing.
- Suwinet-Inlezen biedt overheidsorganisaties de mogelijkheid om gegevens van burgers, die bij diverse andere overheidsorganisaties of basisregistraties zijn opgeslagen in hun bedrijfsapplicatie in te lezen en voor in te vullen in e-formulieren.
- Suwinet-Mijn gegevens biedt overheidsorganisaties de mogelijkheid om geregistreerde gegevens van burgers over werk, uitkeringen en re-integratie, die bekend zijn bij de overheid, digitaal in te zien.
- Suwinet-Correctie biedt, aan zowel de burger als overheidsprofessional, de mogelijkheid om onjuistheden in de vastgelegde gegevens te melden aan de bron van dit gegeven.
- Suwinet-Mail stelt aangesloten partijen (zoals UWV, SVB en GSD) in staat mail te versturen via de besloten Suwinet-Infrastructuur.
- Suwinet-Meldingen wordt gebruikt om informatie over te dragen tussen burgers en overheidsorganisaties en tussen overheidsorganisaties onderling.
- Suwinet-Autorisatie is de gebruikersadministratie van Suwinet-Inkijk waarmee de aangesloten organisaties hun medewerkers kunnen autoriseren voor Suwinet-Inkijk. Suwinet-Autorisatie kan ook dienen als autorisatieservice voor applicaties van andere SUWI-partijen.
- Suwinet-Infrastructuur is het besloten netwerk Suwinet en de centrale omgeving waar alle Suwinet servers staan. Op Suwinet zijn diverse overheidsorganisaties aangesloten. Via dit besloten netwerk worden gegevens van burgers en organisaties veilig uitgewisseld.

Het via Suwinet uitwisselen van gegevens tussen gemeenten, SVB, UWV en andere bronnen is om meerdere reden noodzakelijk. Allereerst om burgers beter te kunnen helpen en ten tweede om fraude of misbruik te voorkomen.
De persoonsgegevens die via Suwinet worden uitgewisseld zijn zeer privacygevoelig. Daarom is het van belang dat gebruikers zorgvuldig met de gegevens die via het systeem worden uitgewisseld omgaan.

Wie mag Suwinet gebruiken?

- Geautoriseerde medewerkers bij de (I)GSD van gemeenten die belast zijn met de uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW en IOAZ. Dit geldt ook voor ingehuurde externe capaciteit; deze medewerkers werken immers onder gezag en toezicht van de desbetreffende gemeente.
- Niet-Suwinetpartijen die middels een overeenkomst op grond van artikel 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;
- RMC's (Regionale Meld- en Coördinatiepunten) voor hulp aan voortijdig schoolverlaters;
- Afdelingen Burgerzaken voor het bijhouden van de BRP (Basis Registratie Personen). Hiervoor is geen overeenkomst nodig. Nadere regels staan in artikel 3.3 van de Regeling SUWI.
- Medewerkers die de inburgering verzorgen mogen via Suwinet gebruik maken van het inburgeringsportaal.

Waarom Suwinet?

De verplichting tot eenmalige gegevensuitvraag in de SUWI-keten is vastgelegd in de Wet eenmalige gegevensuitvraag werk en inkomen (WEU). De genoemde wet stelt de burger in plaats van de uitvoerende ketenpartners (UWV, SVB en gemeenten) centraal in de dienstverlening. Hiertoe is voor de uitvoerende organisaties bij de door hen uitgevoerde wetten rond werk en inkomen in de wet een verbod op dubbele gegevensuitvraag in de SUWI-keten vastgelegd. Het verbod op dubbele gegevensuitvraag geldt voor een set gegevens die in lagere regelgeving is geconcretiseerd. De ketenpartners mogen de betreffende gegevens (waarover zij al beschikken) niet opnieuw uitvragen, maar moeten deze via elektronische voorzieningen uit (basis)registraties hergebruiken. Hiertoe verplicht de WEU de ketenorganisaties ook om gezamenlijk zorg te dragen voor de instandhouding van gezamenlijke elektronische voorzieningen (GeVs) waarmee zij elkaar gegevens verstrekken of inzage bieden in elkaars gegevens. Uiteindelijk moet de WEU leiden tot een zogenaamde omgekeerde intake: niet de klant is de primaire bron van informatie, maar de overheid zelf.

Van wie is Suwinet?

Het Ministerie van Sociale Zaken en Werkgelegenheid is verantwoordelijk voor de vaststelling van de Wet Suwi. Hierin is vastgelegd dat de Suwipartijen UWV, SVB en gemeenten gezamenlijk een voorziening voor digitaal gegevensverkeer in stand dienen te houden. Tevens regelt de wet SUWI de kaders hiervoor. Suwinet is de verantwoordelijkheid van de Suwipartijen UWV, SVB en de gemeenten. Het Bureau Keteninformatisering Werk en Inkomen (BKWI) is in de wet aangewezen als de beheerder van Suwinet.

Organisatie GeVS

De Gezamenlijke elektronische Voorzieningen Suwi (GeVS) zijn voorzieningen waarin drie type partijen participeren: Bronhouders, Beheerders van de centrale (BKWI) en decentrale (Inlichtingenbureau (IB)) omgeving en Afnemers.

- Bronhouders – Bronhouders zijn de partijen die - ten behoeve van Afnemers – authentieke gegevens beschikbaar stellen aan de Beheerders via de centrale omgeving. De bronhouders vormen de zogeheten leveranciers van gegevens, zoals UWV, SVB en de Gemeenten, BRP, RDW, Kadaster, HR (KvK).
- Beheerders – Er zijn drie landelijke beheerders: het BKWI, het Inlichtingen bureau en het UWV.
    - Beheerder van de centrale omgeving (BKWI) is de partij die - conform de ketenafspraken en –standaarden zorg draagt voor het beschikbaar stellen van de centrale omgeving Suwi en voor de transformatie, autorisatie, transport en verdere routering van gegevens/berichten. Hiertoe stelt de Beheerder van de centrale omgeving instrumenten, zoals applicaties beschikbaar. De Beheerder van de centrale omgeving is BKWI.
    - Inlichtingenbureau (IB) is de beheerder van de decentrale gemeentelijke omgeving die conform ketenafspraken en standaarden zorg draagt voor het beschikbaar stellen van de decentrale omgeving voor gemeenten en voor de transformatie, autorisatie, transport en verdere routering van gegevens/ berichten van en naar gemeenten. Hiertoe stelt de Beheerder van de decentrale omgeving instrumenten (voorzieningen en applicaties) beschikbaar.
    - UWV is de decentrale beheerder voor Sonar (klantvolgsysteem, communicatie via de Werkmap), voor WBS (vacatureregistratie, matching en CRM-werkgever), voor Beheermodule werk.nl (inzicht in cv's op werk.nl), en voor GIP (Gemeente Informatie Portaal: informatiekanaal van UWV met onder andere nieuws, release-informatie, ondersteunende documentatie en sturingsinformatie).

- Afnemers - Afnemers zijn de partijen die via de GeVS - voor hun bedrijfsvoering en uitvoering van hun wettelijke taken - gegevens betrekken uit gegevensbronnen van bronhouder.

De Bronhouders stellen beleidsvoorwaarden aangaande het beschikbaar stellen van hun gegevens en maken afspraken met de Afnemers en Beheerders welke gegevens voor wettelijke taken en onder welke voorwaarden zij beschikbaar stellen. Dit wordt door Bronhouders met Afnemers en/of Beheerders geformaliseerd in een overeenkomst (waarin de te leveren gegevens worden beschreven) om invulling te geven aan proportionaliteit en doelbinding.
In dit kader is van belang dat partijen voor de GeVS - als onderdeel van het beveiligingsbeleid – elk een specifiek eigen aansluitbeleid formuleren. Dit aansluitbeleid is de vertaling van het 'GeVS aansluitvoorwaarden' en gericht op de bescherming van de GeVS, beperkt tot de eigen organisatie, de eigen delen van de GeVS en de via de GeVS beschikbaar gestelde gegevens.
Het is gewenst dat de organisatie vanuit haar ICT omgeving adequate beveiligingsmaatregelen treft ten aanzien van de GeVS treft en dat zij deze ook aantoonbaar transparant maakt.

De Beheerder, Afnemers en Bronhouders

Op advies van Beheerder van het centraal deel en Suwipartijen stellen de betrokken partijen vast of een afnemer aangesloten mag worden (en voldoet aan eisen van SZW en bronhouders).

Vervolgens sluit Beheerder de Afnemer aan en waarbij door zowel Beheerders als Afnemer activiteiten verrichten, zoals: aanvragen van lijnen, parameterinstellingen/configuraties, rapportages, berichten uitwisselen.

Communicatie over proportionaliteit

Medewerkers moeten uiteraard op de hoogte worden gebracht van eventuele wijzigingen. Het is de bedoeling dat de medewerker alleen de gegevens opvraagt die nodig zijn voor de uitvoering van zijn taak. Een medewerker die enkel voertuiggegevens nodig heeft, kan volstaan met raadpleging van de bronpagina RDW en hoeft geen overzichtspagina handhaving te gebruiken, waar de voertuiggegevens naast vele andere gegevens worden getoond. De verandering in het beperken van het gebruiken van overzichtspagina's betekent dat medewerkers zich bewust moeten worden dat 'less' in veel gevallen 'more' is. Voorlichting en continue in gesprek blijven is daarom essentieel. In het Informatiebeveiligingsplan Suwinet worden jaarlijks concrete acties inzake voorlichting en bewustwording opgenomen.
In de toekomst wordt het mogelijk dat burgers (met gebruik van hun DigID) zelf kunnen inzien welke organisatie uit welke bron gegevens van hen heeft opgevraagd. Als er dan steeds grote overzichtspagina's zijn opgevraagd is het niet uit te leggen dat een medewerker bijvoorbeeld inkomensgegevens heeft opgevraagd terwijl alleen geverifieerd moest worden of een auto op naam van de klant staat.

Periodieke DPIA Suwinet

De Suwinet gegevensverwerking heeft een aantal risico-kenmerken die maken dat voor deze gegevensverwerking een Data Protection Impact Assessment (DPIA) moet worden uitgevoerd, dit conform artikel 35 van de AVG:

- Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn (zoals Suwi);
- De verwerking bevat gegevens over kwetsbare personen. Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Kwetsbare personen zijn onder andere kinderen jonger dan 16 jaar, mensen in de schuldhulp of personen die aanspraak maken op de Wmo.
- De verwerking kan mogelijk leiden tot de blokkering van een recht, dienst of contract van betrokkenen. Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht (zoals het recht op een uitkering of een Wmo voorziening) niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

Omdat de omgeving verandert, het risico verandert, of de verwerking verandert, raadt de Autoriteit Persoonsgegevens aan om bij risico volle gegevensverwerkingen periodiek, bijvoorbeeld een keer per 3 jaar, een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd.
Deze gegevensverwerking is risicovol, dus driejaarlijks zal een DPIA worden uitgevoerd, voor het eerst in het jaar 2020.
Voor de volledigheid: De BIO gaat in per 1-1-2020 en treedt niet in de plaats van een Data Protection Impact Assessment (DPIA). Een DPIA gaat namelijk over veel meer dan alleen de beveiliging van persoonsgegevens, zoals het vraagstuk van rechtmatigheid van verwerking.

De ENSIA-verantwoordingssystematiek

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.
De ENSIA-verantwoordingssystematiek sluit aan op de Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen SUWI (GeVS). De gemeente Heerlen volgt de ENSIA-verantwoordingssystematiek en voldoet dus automatisch aan deze Verantwoordingsrichtlijn GeVS. In 2020 verandert de Verantwoordingsrichtlijn, omdat dan de Baseline Informatiebeveiliging Overheid (BIO) van kracht wordt. De Specifieke SUWI-Normenkaders zijn dan niet meer geldig, en is alleen de ENSIA nog van toepassing. De ENSIA-verantwoordingssystematiek zal hierop worden aangepast.
Voor de RMC-rol (regionale rol inzake vroegtijdig schoolverlaters) is een TPM-verklaring (third party memorandum) vanuit de gemeente Heerlen aan de andere regiogemeenten niet verplicht voor de ENSIA-verantwoording. Een Third Party Memorandum (TPM) is een verklaring die wordt afgegeven door een onafhankelijke auditpartij. De verklaring heeft betrekking tot de kwaliteit van de ICT-dienstverlening en beheersing van een organisatie.
De gemeente Heerlen voert RMC-taken uit, en de gemeente Heerlen legt verantwoording af over het gebruik van Suwinet-Inkijk bij RMC-taken, dit verloopt via de reguliere ENSIA verantwoording.

Hoofdstuk 2 – De Governance-structuur

Generieke verdeling taken / verantwoordelijkheden

1. Het college van burgemeester en wethouders is bestuurlijk eindverantwoordelijk voor de informatieveiligheid van haar organisatie. Middels de jaarlijkse collegeverklaring geeft het college aan in hoeverre de gemeente Heerlen voldoet aan de voor Suwinet (en DigiD) geselecteerde informatiebeveiligingsnormen.
2. Binnen het college zijn drie portefeuillehouders direct betrokken bij Suwinet: de wethouder onderwijs (RMC en VSV), de wethouder Participatie (GSD), en de wethouder Informatievoorziening (informatiebeveiligingsbeleid).
3. De Secretaris/algemeen directeur van een organisatie is ambtelijk eindverantwoordelijk voor de integrale beveiliging en de inrichting en werking van de beveiligingsorganisatie. In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligingskaders in zijn organisatie, dus ook voor een juiste toepassing van dit informatiebeveiligingsbeleid Suwinet.
4. Elke domeinmanager is verantwoordelijk voor het correct gebruik en beveiliging van de binnen de zijn of haar domein gebruikte Suwinet services. Deze domeinmanagers dragen gezamenlijk zorg voor een driejaarlijkse uitvoering van de DPIA Suwinet.
5. Elke teamleider is verantwoordelijk voor de uitvoering en naleving van de informatiebeveiliging Suwinet binnen zijn of haar team. De teamleider is verantwoordelijk voor het aanvragen of afmelden van autorisatie tot Suwinet; het functieprofiel van de betreffende medewerkers is hierbij bepalend.
6. Iedere Suwinet geautoriseerde medewerker is zelf verantwoordelijk voor ordentelijk wachtwoordbeheer, het melden van beveiligingsincidenten, het melden van inbreuken op de privacy (datalekken), het vertrouwelijk omgaan met persoonsgegevens (oa clean desk en clear screen). Ook ondertekent iedere geautoriseerde medewerker tweejaarlijks de Verklaring zorgvuldig gebruik Suwinet, zoals opgenomen in de bijlage van dit beleid; deze verklaring wordt opgenomen in het Personeelsdossier van de betreffend medewerker.
7. De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De teamleiders zijn verantwoordelijk voor het aanleveren van alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.
8. Het eerste aanspreekpunt voor geautoriseerde Suwinet medewerkers bij (technische) problemen is belegd bij het team Functioneel Beheer. Ook het uitvoeren van autorisatieverzoeken Suwinet, of het afmelden ervan is een taak voor team Functioneel Beheer.
9. De netwerkbeheerder Parkstad-IT (PIT) beheert de technische aansluiting op het landelijke netwerk.
10. De serverbeheer Parkstad-IT (PIT) beheert de interne Suwinet-mail adressenlijst.
11. De Information Security Officer (ISO) tbv Suwinet beheert en beheerst beveiligingsprocedures en – maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet in overeenstemming is met de wettelijke eisen en het gevoerde beleid. Hieronder vallen ook het informatiebeveiligingsbeleid Suwinet, het informatiebeveiligingsplan Suwinet, het informatiebeveiligingsbeheer Suwinet, en het sanctiebeleid bij oneigenlijk gebruik Suwinet.
12. De privacy officer tbv Suwinet ondersteunt de gemeentelijke organisatie bij privacyvraagstukken (zoals rondom artikel 24, 25 en 26 van de AVG), bij het opstellen van een DPIA Suwinet (artikel 35 van de AVG), bij het opnemen van de gegevensverwerking in het verwerkingsregister (artikel 30 van de AVG), en bij inbreuken in de privacy (datalekken) (artikel 33 van de AVG). Ook vraagt de privacy officer tbv Suwinet maandelijks de (logging)-gegevens op over het gebruik van Suwinet-Inkijk, en verzorgt de beoordeling en rapportage.
13. Melding van een inbreuk in verband met persoonsgegevens (artikel 33 van de AVG) worden conform het daar voor geldende protocol afgehandeld.
14. Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie in Suwinet, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC door of namens de Chief Information Security Officer (CISO).
15. De functionaris gegevensbescherming houdt oa toezicht op de gegevensverwerking, op de DPIA, op het verwerkingsregister.
16. De CISO houdt overzicht en toezicht over de concernbrede informatiebeveiliging, en specifiek op het aansluitbeleid Suwinet.
17. Elke hier genoemde functionaris levert, voorzover noodzakelijk, verbetervoorstellen voor het informatiebeveiligingsplan Suwinet.

De gemeentelijke sociale dienst van de gemeente Heerlen

De gemeente Heerlen voert de Participatie-wet zelf uit (taken rondom rechtmatigheid, handhaving, reintegratie, fraudeonderzoek en terugvordering en verhaal).
Suwinet vervult binnen de keten Werk en Inkomen een essentiële functie in de informatievoorziening voor de uitvoer van de wettelijke taken. Onder andere:

- Aanvragen inkomen, Participatiewet, loaw, loaz, Wgs, verhaal, bezwaar en beslag;
- Heronderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken);
- Debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen, werkgever etc;
- Verwerking, controle van de maandelijkse mutatieformulieren en in die gevallen ter beoordeling van de consulent/medewerker. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage van de consulent die belast is met de taken die vallen onder de voor gebruik van Suwinet toegestane wetgeving.
- De Wet gemeentelijke schuldhulpverlening is een Suwi taak. Het is echter nog niet mogelijk om Suwinet voor dit doel te raadplegen omdat een AMvB op grond van de Wet gemeentelijke schuldhulpverlening ontbreekt (2019).

Deze wettelijke taken worden binnen domein Inwoners uitgevoerd door de volgende teams:
- Team Inkomen: hier zijn de taken van de consulenten inkomen geïntegreerd. De 'poort' voor allerlei vragen over het sociaal domein is in dit team ondergebracht.
- Team Administratie: omvat de uitkeringsadministratie en voert daarnaast diverse administratieve werkzaamheden uit voor de processen Inkomen, Schuldhulpverlening en Re-integratie.
- Team Schuldhulpverlening: hier zijn de consulenten schuldhulpverlening ondergebracht, een procesbegeleider en de administratief medewerkers.

Sociale recherche
Binnen dit taakveld vallen volgende taken:
- Afhandeling maandelijkse signalen Inlichtingen Bureau (IB);
- Controle van tips zowel intern als extern;
- Fraudesignalen onderzoeken;
- Bij preventieonderzoeken en thematische onderzoeken.

Dit taakveld is ondergebracht bij team Sociale Veiligheid en Buurten van het domein Maatschappij.
Adresonderzoek & bijhouden van de BRP
Op grond van artikel 5.9, eerste lid sub i van het Besluit SUWI, heeft team Burgerzaken toegang tot Suwinet tbv extra controle van adresgegevens via de loonaangifte. Dit gebeurt alleen voor adresonderzoeken ingeval van twijfel over de BRP-registratie.
Deze autorisatie geldt uitsluitend voor de functionarissen die belast zijn met het bijhouden van persoonsgegevens in de BRP en dan zeer specifiek voor ambtenaren die het adresonderzoek uitvoeren.
Dit taakveld is ondergebracht bij team Burgerzaken van domein Inwoners. Team Burgerzaken is voor inwoners de eerste ingang voor contact met de gemeente.
Juridische ondersteuning
Juridische ondersteuning bij de uitvoering van wettelijke taken binnen de gemeente Heerlen wordt geleverd door het team Juridische Zaken van het domein Organisatie.
Voor deze juridische ondersteuning is incidenteel directe toegang nodig tot Suwinet.
Inburgering
Medewerkers die de inburgering verzorgen mogen via Suwinet gebruik maken van het inburgeringsportaal.
Dit taakveld is ondergebracht bij Team Re-integratie van het domein Economie, binnen het functieprofiel Consulent Re-integratie. Team Re-integratie is een samenvoeging van Re-integratie en het jongerenloket. In dit team worden bemiddelbare uitkeringsgerechtigden begeleid naar de arbeidsmarkt.
Gemeentelijke belastingdeurwaarder
De taak gemeentelijke belastingdeurwaarder is gedelegeerd aan de gemeenschappelijke regeling BsGW.
Regionaal Meld- en Coördinatiepunt (RMC) binnen de gemeente Heerlen

Voortijdige Schoolverlaters en RMC

De gemeente Heerlen is een contactgemeente voor de RMC taken. Een contactgemeente is een aangewezen gemeente voor het regionaal uitvoeren van de RMC-functie door het Rijk. In totaal zijn 39 gemeenten hiervoor aangewezen.

De gemeente Heerlen is contactgemeente voor regio 39 (Zuid-Limburg). Er zijn drie zelfstandige subregio's in Zuid-Limburg, waaronder subregio Parkstad Limburg. Deze RMC-functie voor Parkstad is belegt bij het team VSV van Domein Economie. Dit team coördineert de meldingen en registratie van voortijdige schoolverlaters van Parkstad en zorgt voor mogelijkheden van doorverwijzing en herplaatsing in het onderwijs. Het gebruikersbeheer Suwinet voor de hele regio Zuid-Limburg is toegewezen aan de contactgemeente. Uitgangspunt met betrekking tot de informatiebeveiliging, en dus ook voor Suwinet , is dat de gemeente

Heerlen in deze zelf verantwoordelijk is en blijft; deze verantwoordelijkheid ligt niet bij de RMC-functie. Gegevensuitwisseling voor het RMC

Alle gegevensuitwisseling vindt altijd plaats tussen bureau VSV en het Inlichtingenbureau. Dit gaat via een beveiligde verbinding. RBL Westelijke Mijnstreek en RBL Maastricht en Mergelland leveren bestanden aan via Bureau VSV, en krijgen deze ook terug via bureau VSV. Er zijn medewerkers van bureau VSV aangewezen om de daadwerkelijke uitwisseling af te handelen. Zij zijn geautoriseerd door het Inlichtingenbureau.
De bestanden worden bij uitwisseling beveiligd door gebruikmaking van versleutelde zipbestanden. De wachtwoorden voor de zipbestanden worden separaat uitgewisseld. Verder wordt er gebruik gemaakt van een beveiligde verbinding met de webapplicatie. Suwinet zelf wordt beveiligd door het BKWI.
De RMC-functionaris mag dus beperkt Suwinet-gegevens opvragen middels de RMC-Inkijk module. Gegevens uit Suwinet zouden kunnen leiden tot een mutatie in deze geregistreerde gegevens. Dat gebeurt met name als een jongere werkt of in een traject zit bij sociale dienst of UWV. Het betreft hier alleen gegevens van jongeren van 18 tot en met 22 jaar woonachtig binnen de RMC-regio die zijn uitgeschreven op een school en niet opnieuw zijn ingeschreven. Deze gegevens worden door het Inlichtingenbureau beschikbaar gesteld.
Maandelijks wordt een SUWI-overzicht van alle mogelijke voortijdig schoolverlaters (vsv'ers), aangeleverd aan het Inlichtingenbureau (BKWI). Het Inlichtingenbureau 'verrijkt' deze informatie met gegevens over werk en/of uitkering en geeft een prioriteit aan en retourneert deze gegevens. De gegevens worden vervolgens door de RMC-functionaris verwerkt en aan de hand van deze gegevens kan hij of zij besluiten actie te ondernemen.
De ontvangen gegevens kunnen verwerkt worden in het leerlingvolgsysteem. Dat kan op twee manieren gebeuren, beide manieren komen al dan niet gecombineerd voor.

Verwerking in de RMC-module

Een jongere van 12 tot en met 22 jaar die Wordt begeleid of benaderd door een RMC-consulent, wordt geregistreerd in de RMC-module. De gegevens uit Suwinet kunnen leiden tot een mutatie in deze module. Dat gebeurt met name als een jongere werkt of in een traject zit bij sociale dienst of UWV.
De geregistreerde gegevens zijn dan:

- Einddatum RMC-registratie = Datum aanvang werk/traject
- Reden einde RMC-registratie. Bijvoorbeeld:
  - Werk: Tijdelijk werk.
  - Werk: Vast werk
  - Overige: Re-integratietraject
  - Overige: Wajong

Verwerking in aantekeningen en acties Alle ondernomen acties en gebeurtenissen worden geregistreerd. Dit is niet gestructureerd. Mogelijk wordt hierin een vermelding gemaakt van de opzoekingen uit SUWI/Inlichtingenbureau als dit gevolgen heeft voor het traject dat met de jongere doorlopen wordt. Gegevensuitwisseling derden

Bureau VSV levert geen op persoon herleidbare informatie uit aan derden tenzij:

- dit een wettelijke verplichting betreft;
- dit ingekochte trajecten of producten van bureau VSV betreft, waarbij in het kader van rechtmatigheid BSN, naam, geboortedatum, adres, geslacht, aanvang traject/product, einde traject/product, en afsluitreden wordt aangeleverd;
- er in het kader van subsidieverstrekking informatie moet worden verstrekt. Gestreefd wordt naar dataminimalisatie, en de ontvangende partij moet een geheimhoudingsverklaring tekenen.
- binnen de kaders van de AVG wordt met andere partijen informatie gedeeld over individuele jongeren, om binnen een traject de inspanningen op elkaar af te stemmen.

Hoofstuk 3 – Aansluitbeleid Suwinet

Inleiding

Elke organisatie ontwikkelt voor de beveiliging van haar ICT omgeving een informatiebeveiligingsbeleid. Met dit informatiebeveiligingsbeleid geeft de organisatie enerzijds richting aan de te nemen beveiligingsmaatregelen ten behoeve van een veilige dienstverlening conform wet en regelgeving. Anderzijds geeft dit beleid handvatten om aan te geven dat de organisatie aantoonbaar aan de verplichtingen uit de wet en regelgeving voldoet.
Een van de verplichtingen rond de wet en regelgeving heeft betrekking op Suwinet en de Suwinet diensten. Het is daarom van belang dat de organisatie expliciet aandacht besteed aan de beveiliging van 'de eigen delen' van Suwinet.

Het is gewenst dat de organisatie vanuit haar ICT omgeving adequate beveiligingsmaatregelen treft ten aanzien van Suwinet en dat zij deze ook aantoonbaar transparant maakt.
Het is daarom van belang een specifiek aansluitingsbeleid op Suwinet, als onderdeel van haar beveiligingsbeleid, te formuleren. Een aansluitbeleid is het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens.
Het doel van het aansluitbeleid Suwinet is richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet.

Taken en bevoegdheden aansluitbeleid Suwinet

Als gemeente zijn wij verplicht de taken en verantwoordelijkheden ten aanzien van coördinatie van aansluitingsbeveiliging en ontwikkeling van aansluitingsbeleid te beleggen en toe te wijzen aan daartoe bevoegde functionarissen. De ISO tbv Suwinet is hiervoor verantwoordelijk.
Naast de autorisaties heeft ook BKWI als beheerder gegevens nodig voor de volgende rollen:

1. Applicatiebeheerder
2. Gemandateerde
3. Security Officer

Ad 1. De applicatiebeheerder is binnen de organisatie het aanspreekpunt en de verantwoordelijke voor het beheer van de applicatie Suwinet. Binnen de gemeente Heerlen is deze rol belegd bij team Functioneel Beheer.
Ad 2. De gemandateerde is binnen de organisatie gemachtigd tot het aanvragen en ontvangen van specifieke rapportages aangaande het gebruik van Suwinet. Binnen de gemeente Heerlen is deze rol belegd bij privacy officers binnen team Informatie Management.
Ad 3. De security officer is binnen de organisatie het aanspreekpunt en de verantwoordelijke voor alle activiteiten, op het gebied van informatiebeveiliging rondom Suwinet en rapporteert direct aan B&W. Binnen de gemeente Heerlen is deze rol belegd bij information security officers binnen team Informatie Management.
De aanmelding voor deze rollen dient ondertekend te worden door een, namens burgemeester en wethouders van de gemeente bevoegd persoon (gemeentesecretaris / algemeen directeur).

Toetsing en toezicht

In het Informatiebeveiligingsbeheer Suwinet is vastgelegd hoe de beveiligingsmaatregelen door de uitbestedende partij gecontroleerd worden (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

- Het aansluitingsbeleid is gericht op de, door de bronhouders vastgestelde, risicoklasse van de gegevens die uitgewisseld worden.
- Het aansluitingsbeleid geeft inzicht in het type maatregelen voor de beveiliging van de eigen delen van Suwinet (bijv.: (organisatorische-, technisch- en, beheersingsmaatregelen)
- In het aansluitingsbeleid werkt de Afnemer de vanuit Suwinet gestelde eisen uit voor de eigen organisatie.
- Wanneer besloten wordt tot uitbesteden van taken en diensten in relatie tot Suwinet, legt Afnemer in de overeenkomst vast dat de aan haar gestelde beveiligingseisen voor Suwinet onverkort van toepassing zijn bij deze uitbesteding.

Gebruikte Suwinet Services

Binnen de gemeente Heerlen wordt gebruik gemaakt van de volgende Suwinet Services:

- Suwinet-Inkijk
- Suwinet-Meldingen
- Suwinet-Mail

De gemeente Heerlen ontvangt voor de volgende niet Suwitaken gegevens:

- Suwinet-Inkijk voor burgerzaken
- Suwinet-Inkijk voor het RMC

Autorisatie Suwinet

De gemeente Heerlen heeft haar Suwinet-autorisaties ingericht volgens een fijnmazige autorisatiestructuur in een autorisatiematrix; dit wordt nader uitgewerkt in het document informatiebeveiligingsbeheer Suwinet. Deze fijnmazige autorisatiestructuur bevorderd ‘proportionaliteit van gegevenslevering’ en gaat daarmee overmatig gegevensgebruik tegen. De toegang tot gegevens word beter afgestemd op wat voor de uitoefening van een taak noodzakelijk is. Hierbij wordt uitgegaan van de functieprofielen zoals in gebruik binnen de gemeente Heerlen.

Hoofdstuk 4 - Inwerkingtreding

Dit informatiebeveiligingsbeleid Suwinet treedt in werking na publicatie. Dit beleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, geëvalueerd, beoordeeld en zo nodig bijgesteld en vastgesteld. Aanpassingen van dit beleid worden bekendgemaakt. De meest actuele versie van dit beleid is te vinden op www.overheid.nl.

Aldus besloten in de vergadering van het college der gemeente Heerlen op 6 oktober 2020.
de burgemeester,
drs. R. Wever
de secretaris,
L. Schouterden