RAADSINFORMATIEBRIEF
15R.00432

gemeente
WOERDEN

Van : college van burgemeester en wethouders
Datum : 30 juni 2015
Portefeuillehouder(s) : wethouder Duindam
Portefeuille(s) : Sociaal Domein
Contactpersoon : S. Nicolasen
Tel.nr. : 8450
E-mailadres : Nicolasen.s@woerden.nl

Gemeente Woerden
15R.00432

Onderwerp:

Vragen uit de rondvraag van de fractie D66
m.b.t. het voldoen aan het Suwinet-normenkader

Kennisnemen van:

De antwoorden op de vragen uit de rondvraag van de fractie van D66 inzake het voldoen aan het Suwinet-normenkader.

Inleiding:

In de rondvraag van de raad zijn door de fractie van D66 vragen gesteld in hoeverre de gemeente Woerden voldoet aan de 7 door de inspectie geselecteerde normen in het kader van SuWi-net.

Korte toelichting op de 7 gestelde normen:
Via Suwinet Services kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen.
Door gegevens binnen de overheid te delen kunnen burgers sneller en beter worden geholpen en hoeven zij geen gegevens te verstrekken die de overheid al heeft.
Suwinet Services zijn primair bedoeld voor UWV, SVB en de gemeentelijke sociale diensten, maar inmiddels maken ook andere overheidsorganisaties gebruik van Suwinet Services. Voor het correcte gebruik van Suwinet zijn regels opgesteld. Het correct toepassen van deze regels wordt gemeten door de zelfevaluatie Suwinet. In die zelfevaluatie gaat het om 7 normen, die hierna bij het antwoord op vraag 2 zijn opgenomen.

Antwoorden:

Vraag 1: Van de gemeenten voldoet 17% aan zeven door de inspectie geselecteerde normen. Hoort Woerden bij die 17% ?

Het antwoord op deze vraag is nee.

Van de medewerkers van de gemeente Woerden heeft op dit moment niemand toegang tot Suwinet.

Voor 'Werk en inkomen' (gemandateerd aan de GR FermWerk) is de gemeente Woerden echter verantwoordelijk. FermWerk maakt gebruik van de aansluiting van de gemeente Woerden op Suwinet. De verantwoordelijkheid van de gemeente Woerden blijkt echter uit het volgende:

In artikel 4 van de dienstverleningsovereenkomst met FermWerk staat:

Gegevensverwerking

a Opdrachtnemer[1] zorgt voor verwerking en archivering van gegevens conform geldende wet- en regelgeving en neemt alle technische en organisatorische maatregelen die nodig zijn voor een adequate beveiliging van de gegevens.

b Opdrachtnemer waarborgt de privacy conform de Wet bescherming persoonsgegevens (Wbp) en daaruit voortvloeiende regelgeving. Opdrachtgever[2] is verantwoordelijke in de zin van de Wbp, opdrachtnemer is bewerker in de zin van de Wbp.

c Opdrachtnemer verwerkt persoonsgegevens uitsluitend ter uitvoering van de opdracht zoals verstrekt in deze overeenkomst en neemt geheimhouding in acht.

d Partijen verstrekken geen informatie aan derden tenzij deze informatie:

1. *openbaar gemaakt moet worden op grond van wet- en regelgeving of een rechterlijke uitspraak,*
2. *reeds openbaar is,*
3. *partijen hiermee schriftelijk instemmen.*

Daarmee zijn in algemene termen de verantwoordelijkheden en bevoegdheden van de opdrachtgever en de opdrachtnemer vastgelegd. Expliciet is verwezen naar de Wbp. In artikel 14 van de Wbp staat:

1 Indien de verantwoordelijke[3] persoonsgegevens te zijnen behoeve laat verwerken door een bewerker[4], draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.

2 De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

3 De verantwoordelijke draagt zorg dat de bewerker

a) de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en

b) de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13.

4 Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b.

5 Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

Uit DVO en Wbp blijkt de toezichthoudende rol van de verantwoordelijke. Daarnaast blijkt uit artikel 4 DVO onder a dat FermWerk is gehouden aan wet- en regelgeving. Relevant in deze context is dat Rekenkamer opmerkt dat er geen bepaling is opgenomen die de gemeente Woerden bevoegdheid geeft om bij de GR onderzoek te doen. Er is dus nu geen bepaling opgenomen dat wij bv de zelfevaluatie mogen uitvoeren bij Ferm Werk of een auditor kunnen sturen. Artikel 9.c van de DVO geeft echter opdrachtgever het recht informatie te vragen over de uitvoering van de overeenkomst.

---

[1] Opdrachtnemer is FermWerk.
[2] Opdrachtgever is de gemeente Woerden.
[3] Verantwoordelijke is i.c. de gemeente Woerden.
[4] Bewerker is i.c. FermWerk.

In goed onderling overleg met FermWerk is daarom begin van dit jaar gezamenlijk gekeken naar de zelfevaluatie. Daaruit bleek dat FermWerk niet aan alle normen voldeed. Sindsdien is er echter al veel werk verzet, hetgeen blijkt uit het antwoord op vraag 2.

Vraag 2: Zo nee, op welke normen scoort Woerden nog niet positief, en wat is daarvan de reden?

In onderstaande tabel zijn de 7 normen opgenomen met de stand van zaken.

1. Norm 1.3: Het informatiebeveiligingsbeleid en -plan (Suwinet) zijn formeel goedgekeurd/vastgesteld door het management en/of de directie en/of het college van burgemeester en wethouders (College B&W).	Het informatiebeveiligingsbeleid en –plan van FermWerk ligt voor bij het bestuur van FermWerk ter vaststelling.
2. Norm 1.4: Het informatiebeveiligingsbeleid en –plan (Suwinet) wordt (op reguliere basis) door de gemeente uitgedragen binnen de organisatie.	Na vaststelling van het informatiebeveiligingsbeleid en –plan zal dat binnen FermWerk worden uitgedragen.
3. Norm 1.5: Het informatiebeveiligingsbeleid en –plan (Suwinet) wordt op reguliere basis (bijvoorbeeld jaarlijks) door de gemeente geëvalueerd en indien noodzakelijk geactualiseerd.	Afgesproken is met FermWerk, dat jaarlijkse evaluatie zal worden uitgevoerd door FermWerk, waarop controle zal plaatsvinden door een accountant of EDP-auditor. De rapportage zal ter beschikking worden gesteld van de gemeente Woerden.
4. Norm 2.2: De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van (Suwinet)-gegevens, -applicaties, -processen en -infrastructuur dienen te zijn beschreven, en duidelijk en afhankelijk van de schaalomvang van de organisatie, gescheiden te zijn belegd (Functiescheiding).	Deze norm is meegenomen in het informatiebeveiligingsbeleid en –plan van FermWerk.
5. Norm 2.2: De Security Officer beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van Suwinet. Zodanig dat de beveiliging van Suwinet overeenkomstig met de wettelijke eisen is geïmplementeerd.	Deze norm is meegenomen in het informatiebeveiligingsbeleid en –plan van FermWerk.
6. Norm 13.1: De organisatie autoriseert en registreert de toegang die gebruikers hebben tot (Suwinet)-applicaties, op basis van formele procedures.	Conform. De controle van de zgn. loggings zal in de rapportage van accountant c.q. EDP-auditor worden opgenomen.
7. Norm 13.5: De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.	Alle bevragingen van medewerkers van FermWerk zijn en worden in logbestanden opgeslagen. Controle vindt steeksproefgewijs plaats.

Wat is de reden dat (nog) niet aan alle normen wordt voldaan?
De reden is de prioriteitstelling in het werk dat bij Ferm Werk moet gebeuren.

Vraag 3: Hoe en op welke termijn verwacht Woerden dat zij op alle zeven normen positief scoort?

Naar verwachting zal in het vierde kwartaal van 2015 aan alle normen worden voldaan.

Bijlagen:

15i.02302 Het Suwinet-normenkader en de BIG
15.013185 Vragen uit rondvraag D66

De secretaris

drs. M.H.J. van Kruijsbergen

De burgemeester

V.J.H. Molkenboer

INFORMATIE
BEVEILIGINGS
DIENST

HET SUWINET-NORMENKADER EN DE BIG

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de collectieve keuze van gemeenten voor coördinatie en ondersteuning op het gebied van informatiebeveiliging via de IBD. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

Eén van de doelen van de IBD is het bieden van gerichte projectmatige ondersteuning op deelgebieden als het gaat om informatiebeveiliging. Deze folder geeft de samenhang weer tussen het normenkader Gezamenlijke elektronische Voorzieningen Suwi (GeVS) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de overeenkomsten in de aanpak van beide normenkaders en tenslotte aanwijzingen over hoe deze aanpak binnen een gemeente tot een win-win-situatie kan leiden. Dit kan door samen te werken tussen de verschillende beleidsvelden van gemeenten en/of Intergemeentelijke Sociale Diensten (ISD-en).

BASELINE INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN (BIG)

De BIG is gebaseerd op de ISO 27001, de ISO 27002 en op de Baseline Informatiebeveiliging Rijksdienst (BIR). De IBD heeft hiervan een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt: de BIG. Dit heeft een aantal producten opgeleverd:

- Een Strategische- en Tactische BIG
- Een serie operationele BIG-producten die het gemeenten makkelijk maken de BIG te implementeren.

In de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente', onderschrijft iedere gemeente het informatieveiligheidsbeleid vast te stellen aan de hand van deze BIG. De operationele producten van de BIG helpen bij de implementatie ervan.

SAMENHANG NORMENKADER GEVS EN BIG

Het normenkader GeVS hanteert zeven normen. Deze normen zijn te vertalen naar de normen uit de BIG. Een voordeel van deze vertaling is, dat de inspanning die nodig is om deze zeven normen te implementeren, een gedeelde inspanning kan zijn. Als een gemeente bezig is met de implementatie van de BIG, bestaat immers de mogelijkheid dat de zeven normen al op enige manier binnen de gemeente uitgewerkt zijn.

OVEREENKOMSTEN TUSSEN BEIDE NORMENKADERS

Beide normenkaders zijn van toepassing op (een deel van) de gemeentelijke informatievoorziening. Het doel van de normenkaders voor gemeenten is, dat gemeenten op een verantwoorde manier omgaan met de aan hen toevertrouwde (persoons)gegevens. Tevens staan beide normenkaders toe om andere (compenserende) beveiligingsmaatregelen te selecteren én te implementeren, in plaats van de norm of maatregel uit het respectievelijke normenkader.[1]

Voor beide normenkaders zijn de eisen, die gelden voor de risicobeheersing ten aanzien van de informatiehuishouding, ontleend aan:

- De code voor Informatiebeveiliging ISO 27002.[2] 'Beveiliging van persoonsgegevens'.
- Achtergrondstudies en Verkenningen nr. 23 (A&V23).[3]
- Voorschrift Informatiebeveiliging Rijksdienst (VIR).[4]

VERSCHILLEN TUSSEN BEIDE NORMENKADERS

Het beveiligingsniveau van beide normenkaders is bijna gelijk. Onder voorwaarde dat voor de verwerking van persoonsgegevens bij de BIG uitgegaan wordt van risicoklasse II[5] en het Normenkader GeVS uitgaat van risicoklasse II en III[6]. Daarnaast beschrijft de BIG de beveiligingsmaatregelen die nodig zijn voor het (gemeentelijk) basis vertrouwelijkheidsniveau 'Vertrouwelijk'[7], en persoonsvertrouwelijke informatie, zoals bedoeld in Artikel 16 van de Wet Bescherming Persoonsgegevens (WBP).

Tevens zitten er verschillen in de wijze waarop verantwoording afgelegd dient te worden. Zo wordt in de Verantwoordingsrichtlijn GeVS uitgegaan van een verantwoording door middel van een managementverklaring, gebaseerd op alle hoofdstukken van het Normenkader GeVS. Deze verklaring wordt vergezeld door een rapportage van een auditor, waarbij is vastgesteld dat de verklaring van het management in overeenstemming is met de resultaten van het onderzoek van de auditor. Deze audit geldt alleen voor een gemeente als niet-Suwi partij (autorisaties voor de GBA, gemeentelijke gerechtsdeurwaarders, en het Regionaal Meld- en Coördinatiepunt (RMC). De BIG gaat uit van een verantwoording op basis van Verplichtende Zelfregulering, waarbij het college van Burgemeester en Wethouders (college van B&W) horizontale verantwoording aflegt aan de Raad en aan de inwoners van de gemeente. Dit middels een paragraaf in het jaarverslag.

Een ander groot verschil is dat de BIG betrekking heeft op de gehele bedrijfsvoering van een gemeente. Dat wil zeggen dat de BIG informatiebeveiliging ziet als een integraal onderdeel van alle systemen, processen en procedures die de gemeente ondersteunen bij het uitvoeren van haar (primaire) processen. De Verantwoordingsrichtlijn en het bijbehorend Normenkader GeVS daarentegen, richt zich

alleen op GeVS (gegevensuitwisseling via de GeVS en verwerking daarvan) en wordt om die reden eigenlijk alleen maar uitgevoerd door de gemeentelijke (I)SD-en.

VERGELIJKING OP BASIS VAN DE ZEVEN BEVEILIGINGSMAATREGELEN UIT DE RAPPORTAGE

Onderstaand wordt de vergelijking, op basis van de zeven normen uit het Normenkader GeVS en de overeenkomstige beveiligingsmaatregelen uit de BIG, nader uitgewerkt. In de praktijk is deze vergelijking te maken op alle normen van het Normenkader GeVS en de BIG, en is een veel grotere samenwerking mogelijk. Het is een besparing bij de implementatie van een gemeentebreed informatiebeveiligingsbeleid, -plan en alle daaraan gerelateerde beveiligingsmaatregelen. Door uit te gaan van de beveiligingsmaatregelen uit de BIG, die gemeentebreed geïmplementeerd dienen te worden, kan door aanvulling op deze beveiligingsmaatregelen, met Suwinet specifieke aspecten voldaan worden aan het Normenkader GeVS. In het eerdere, door VNG uitgegeven stappenplan, is reeds een link gelegd naar de intergemeentelijke samenwerking in stap 1 van de verbeteraanpak Veilig Suwinet. Die intergemeentelijke samenwerking is gewenst omdat daarmee dubbel werk voorkomen kan worden. Deze ontdubbeling moet er zorg voor dragen dat maatregelen zo hoog als mogelijk binnen een gemeente genomen worden, zodat daar alleen nog Suwi-specifieke zaken aan toegevoegd dienen te worden.

Vanwege de leesbaarheid worden de Suwi-normen hier onder niet volledig uitgewerkt, maar slechts kort aangehaald. Zie voor een uitgebreidere beschrijving ook het stappenplan dat door VNG is uitgegeven.[8]

Vanwege de nauwe relatie worden Norm 1.3, 1.4 en 1.5 gezamenlijk beschreven/behandeld.

Norm 1.3: Het informatiebeveiligingsbeleid en -plan[9] (Suwinet) zijn formeel goedgekeurd/vastgesteld door het management en/of de directie en/of het college van burgemeester en wethouders (College B&W).
Norm 1.4: Het informatiebeveiligingsbeleid en -plan (Suwinet) wordt (op reguliere basis) door de gemeente uitgedragen binnen de organisatie.
Norm 1.5: Het informatiebeveiligingsbeleid en -plan (Suwinet) wordt op reguliere basis (bijvoorbeeld jaarlijks) door de gemeente geëvalueerd en indien noodzakelijk geactualiseerd.

Informatiebeveiligingsbeleid

Het bestuur en management van de gemeente geeft een duidelijke richting aan informatiebeveiliging. Zij spelen een cruciale rol bij het opstellen, uitdragen, uitvoeren en handhaven van dit informatiebeveiligingsbeleid.

Informatiebeveiligingsplan

De doelstelling van het informatiebeveiligingsplan is inzicht geven in de status en de volledigheid van te nemen beveiligingsmaatregelen voor de gemeente. Dit door de genoemde actiehouders, en daarmee de betrouwbaarheid, voor de informatievoorziening van de gemeente te garanderen.

Planning & Control cyclus (P&C-cyclus)

Het is noodzakelijk dat het management periodiek beveiligingsaudits uitvoert of laat uitvoeren. Over het functioneren van de informatiebeveiliging binnen de gemeente wordt, conform de P&C-Cyclus, jaarlijks gerapporteerd aan het management aan de hand van een 'in control statement'.[10]

Borgen

Een informatiebeveiligingsbeleid en -plan zonder opvolging en naleving is zinloos. Daarom dient de gemeente actief het informatiebeveiligingsbeleid en -plan binnen de eigen organisatie uit te dragen. Om zo te borgen dat haar medewerkers bekend zijn met de inhoud en betekenis van het informatiebeveiligingsbeleid en -plan.

Bewijsvoering

- De gemeente kan een informatiebeveiligingsbeleid en -plan overleggen dat is voorzien van een recente formele goedkeuring door, of namens het college van B&W. Het informatiebeveiligingsbeleid bevat de normenkaders op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.
  - Er is een specifiek op Suwinet gericht informatiebeveiligingsbeleid of -plan aanwezig, of er is in een algemeen informatiebeveiligingsbeleid een Suwi-specifieke passage opgenomen.
  - Dit informatiebeveiligingsbeleid/ -plan of deze passage heeft specifiek betrekking op de gemeente.
  - De goedkeuring is formeel vastgelegd. Dit betekent dat het informatiebeveiligingsbeleid/ -plan of de passage is ondertekend. Of dat er expliciet melding wordt gemaakt van de goedkeuring in het verslag van de betreffende vergadering. Voor ISD-en dient elke gemeente in het samenwerkingsverband apart het informatiebeveiligingsbeleid en/of plan te accorderen. Dit is afhankelijk van het mandaat en de taakstelling die het samenwerkingsverband van de deelnemende gemeenten heeft.
- Het informatiebeveiligingsplan geeft:
  - Een overzicht van de te nemen (ontbrekende) beveiligingsmaatregelen en inzicht in de toewijzing van de beveiligingsmaatregelen aan een verantwoordelijke partij (welke mensen en middelen worden hiervoor beschikbaar gesteld en hoe is de naleving geregeld?).
  - Een overzicht van de beveiligingsmaatregelen waar reeds invulling aan is gegeven door identificatie van de reeds aanwezige beveiligingsmaatregelen binnen de gemeente.

- De mogelijkheid om de voortgang met betrekking tot de implementatie van beveiligingsmaatregelen binnen de gemeente, te monitoren en hierover te rapporteren. De beheersing van deze planning dient hiervoor opgenomen te worden in de P&C-cyclus. Deze dient jaarlijks geëvalueerd te worden.

- Op basis van aangeleverde informatie kan worden aagetoond dat het informatiebeveiligingsbeleid en -plan door de gemeente op reguliere basis wordt geëvalueerd en geactualiseerd (tenminste eens in de twee jaar). Documenteer de evaluatie, de conclusies en het besluit. Houdt hierbij rekening met het feit dat:
  - De laatste evaluatie minder dan een jaar oud is.
  - De laatste evaluatie is vastgesteld door het management, en/of de directie en/of college van B&W.
- Op basis van aangeleverde informatie kan worden aangetoond dat het informatiebeveiligingsbeleid en -plan binnen de gemeente actief is uitgedragen. Documenteer hoe het informatiebeveiligingsbeleid en -plan is uitgedragen. Denk hierbij aan het feit dat:
  - Het informatiebeveiligingsbeleid en -plan voor alle medewerkers beschikbaar is (het is bijvoorbeeld aan iedereen gemaild of het staat op Intranet).
  - Er het afgelopen jaar minimaal twee keer een actie geweest is om de medewerkers (opnieuw) te attenderen op het bestaan van het informatiebeveiligingsbeleid en -plan.

Relatie met de BIG

- Zie voor de relatie met de BIG onderstaande paragrafen uit de Tactische BIG. Zie hiervoor de pagina Downloads op www.ibdgemeenten.nl:
  - Paragraaf 3.4 'Maak een implementatieplan en rapporteer'.
  - Paragraaf 5.1.1 'Beleidsdocumenten voor informatiebeveiliging'.
  - Paragraaf 5.1.2 'Beoordeling van het informatiebeveiligingsbeleid'.
  - Paragraaf 6.1.1 'Betrokkenheid van het college van B&W bij beveiliging'.
  - Paragraaf 6.1.8 'Beoordeling van het informatiebeveiligingsbeleid'.
  - Paragraaf 8.2.2 'Bewustwording, opleiding en training ten aanzien van informatiebeveiliging'.
  - Paragraaf 15.2.1 'Naleving van beveiligingsbeleid en –normen'.
- Voorbeeld Informatiebeveiligingsbeleid Gemeenten: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Information Security Management System: op het moment dat deze folder werd gepubliceerd was het operationele BIG document 'Information Security Management System' nog in ontwikkeling. Kijk voor de actuele situatie op www.ibdgemeenten.nl.
- Handreiking Communicatieplan en Bewustwording: op het moment dat deze folder werd gepubliceerd was het operationele BIG document 'Handreiking Communicatieplan en Bewustwording' nog in ontwikkeling. Kijk voor de actuele situatie op www.ibdgemeenten.nl.

Norm 2.2: De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van (Suwinet)-gegevens, -applicaties, -processen en -infrastructuur dienen te zijn beschreven, en duidelijk en afhankelijk van de schaalomvang van de organisatie, gescheiden te zijn belegd (Functiescheiding).

Bewijsvoering

- Op basis van de aangeleverde informatie dient uw gemeente te kunnen aantonen waarom welke functionarissen welke autorisaties hebben (binnen Suwinet). Denk hierbij aan:
  - Dat de scheiding van functies schriftelijk is vastgelegd.
  - Dat er een aanvullend document aanwezig is, waaruit blijkt dat er ten aanzien van functiescheidingen duidelijke keuzes zijn gemaakt bij het beleggen van diverse taken. Indien dit er niet is dient er een onderbouwde verklaring te zijn waarom dit document ontbreekt en er dient een alternatieve aanpak te zijn om misbruik te voorkomen (bijvoorbeeld extra controle op functies waar functiescheiding niet of minder goed mogelijk is).
- De taken, verantwoordelijkheden en bevoegdheden (ten aanzien van Suwinet) dienen te zijn beschreven en belegd bij de juiste personen. Het is hierbij belangrijk dat de volgende functies bij verschillende personen zijn belegd:
  - Uitvoering van taken (het gebruik van Suwinet).
  - Het beheer van autorisaties (toegang verlenen tot Suwinet).
  - Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet).
  - Management (beslissen over bevoegdheden van functiegroepenen/of individuele medewerkers, het uitdragen van het belang van goed gebruik, het bijsturen na oneigenlijk gebruik en optreden na misbruik (Suwinet).

Relatie met de BIG

- Zie voor de relatie met de BIG onderstaande paragrafen uit de Tactische BIG. Zie hiervoor de pagina Downloads op www.ibdgemeenten.nl:
  - Paragraaf 10.1.3 'Functiescheiding'.
  - Paragraaf 11.2.1 'Registratie van gebruikers'.
- Voorbeeld Informatiebeveiligingsbeleid Gemeenten: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Beleid Logische Toegangsbeveiliging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Aanwijzing Logging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.

Norm 2.2: De Security Officer beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van Suwinet. Zodanig dat de beveiliging van Suwinet overeenkomstig met de wettelijke eisen is geïmplementeerd.

Bewijsvoering

- Er is een functieomschrijving inclusief takenoverzicht.
- Er is een medewerker verantwoordelijk gesteld om (periodiek, ten minste twee keer per jaar) naar de beveiliging te kijken (waaronder Suwinet).
- Deze medewerker rapporteert en adviseert periodiek rechtstreeks aan het management en de directie en/of het college van B&W.

Voor ISD-en dient de Security Officer van de ISD naar elke gemeente apart te rapporteren en adviseren.

Relatie met de BIG

- Zie voor de relatie met de BIG onderstaande paragrafen uit de Tactische BIG. Zie hiervoor de pagina Downloads op www.ibdgemeenten.nl:
  - Paragraaf 6.1.2 'Coördineren van beveiliging'.
- Voorbeeld Informatiebeveiligingsbeleid Gemeenten: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Beleid Logische Toegangsbeveiliging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.

Norm 13.1: De organisatie autoriseert en registreert de toegang die gebruikers hebben tot (Suwinet)-applicaties, op basis van formele procedures.

Bewijsvoering

- Er is een formeel vastgelegde autorisatieprocedure. Hierin worden functies aan autorisaties en, in het verlengde daarvan, aan rollen gekoppeld. Er zijn (specifiek op Suwinet gerichte) autorisatieprocedures (inclusief een autorisatiematrix) aanwezig. In de autorisatiematrix dienen:
  - In plaats van afdelingen de functies vermeld te staan.
  - In plaats van tekstueel beschreven taken de rollen vermeld te staan.
- Er dient te kunnen worden aangetoond dat er een registratie wordt bijgehouden voor het registreren en afmelden van gebruikers (voor Suwinet), en voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten (waaronder Suwinet). Elke gebruiker (van Suwinet) dient geautoriseerd te worden.
- Er dient te kunnen worden aangetoond dat autorisatieprocedures (inclusief een autorisatiematrix) periodiek op actualiteit worden gecontroleerd. Het accountbestand wordt meerdere keren per jaar gecontroleerd en aansluitend hierop worden inactieve accounts verwijderd.

Relatie met de BIG

- Zie voor de relatie met de BIG onderstaande paragrafen uit de Tactische BIG. Zie hiervoor de pagina Downloads op www.ibdgemeenten.nl:
  - Paragraaf 11.2.1 'Registratie van gebruikers'.
  - Paragraaf 11.5.2 'Gebruikersidentificatie en –authenticatie'.
- Voorbeeld Informatiebeveiligingsbeleid Gemeenten: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Beleid Logische Toegangsbeveiliging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Wachtwoordbeleid, zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.

Norm 13.5: De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.

Bewijsvoering

- Er dient te kunnen worden aangetoond dat op basis van documentatie van controleresultaten, de gemeente controles uitvoert op toegang en gebruik. De beoordeling van deze rapportage (door wie en langs welke criteria) is centraal belegd.
- Er dient te kunnen worden aangetoond dat er een procedure is waarin is opgenomen hoe de gemeente de controle op het autoriseren en het gebruik uitvoert en waarop wordt gelet gedurende deze controle.
- Een medewerker van de gemeente vraagt tenminste meerdere keren per jaar een rapportage op over het gebruik van de autorisaties (Bijvoorbeeld bij Bureau Keteninformatisering Werk en Inkomen (BKWI), in verband met Suwinet-inkijk).

Relatie met de BIG

Zie voor de relatie met de BIG onderstaande paragrafen uit de Tactische BIG. Zie hiervoor de pagina Downloads op www.ibdgemeenten.nl:

- Paragraaf 10.10.1 'Aanmaken audit-logbestanden'.
- Paragraaf 10.10.2 'Controle van systeemgebruik'.
- Paragraaf 11.2.4 'Beoordeling van toegangsrechten van gebruikers'.

- Voorbeeld Informatiebeveiligingsbeleid Gemeenten: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Beleid Logische Toegangsbeveiliging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.
- Aanwijzing Logging: zie hiervoor de pagina Downloads op www.ibdgemeenten.nl.

1 Zie in de BIG de laatste alinea in paragraaf 1.1 en de 2e alinea in paragraaf 9.5 in Verantwoordingsrichtlijn GeVS.
2 www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022007-nl.htm.
3 www.privacy.nl/uploads/presentaties/av23%20beveiliging.pdf. De 'Richtsnoeren beveiliging van persoonsgegevens' die door het CBP in 2013 zijn gepubliceerd vervangen de A&V23 (www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf).
4 wetten.overheid.nl/BWBR0022141/ of zoek.officielebekendmakingen.nl/stcrt-2007-122-p11-SC81084.pdf of erfgoedinspectie.nluploads/documents/vir_sc81084[1].pdf.
5 A&V23 risicoklasse II betekent verhoogd risico. Extra negatieve gevolgen voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens.
6 A&V23 risicoklasse III betekent hoog risico. Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren.
7 Departementaal Vertrouwelijk volgens het Besluit Voorschrift. Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) wetten.overheid.nl/BWBR0033507.
8 VNG Stappenplan voor een veiliger gebruik van Suwinet www.vng.nl/files/vng/20140217-stappenplan-suwi.pdf
9 Het Beveiligingsplan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen.
10 In control statement: Binnen de gebruikelijke P&C-cyclus moet door B&W een in control statement worden afgegeven over het BIG. De in control verklaring moet inzicht geven aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd.

INFORMATIEBEVEILIGINGSDIENST VOOR GEMEENTEN (IBD)

T IBD-HELPDESK 070 - 373 80 11
E INFO@IBDGEMEENTEN.NL
I WWW.IBDGEMEENTEN.NL

KING
NASSAULAAN 12
2514 JS DEN HAAG

MEER INFORMATIE?

MEER INFORMATIE OVER ONZE DIENST-VERLENING KUNT U VINDEN IN DE ANDERE FACTSHEETS VAN HET DIENSTENPORTFOLIO VAN DE IBD. VIA DE WEBSITE WWW.IBDGEMEENTEN.NL HOUDT DE IBD GEMEENTEN EN ANDERE BETROKKEN PARTIJEN OP DE HOOGTE VAN HAAR DIENSTVERLENING, ACTIVITEITEN EN PROJECTEN OP HET VLAK VAN INFORMATIEBEVEILIGING. BOVENDIEN KUNNEN GEMEENTEN VIA DE BESLOTEN COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN.
VOOR VRAGEN OVER DE IBD KUNT U CONTACT OPNEMEN MET DE HELPDESK VAN DE IBD 070 3738011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL.

Rondvraag privacy

Bij 83 procent van de gemeenten zijn voor het opvragen van persoonsgegevens via Suwinet nog steeds niet voldoende beveiligingsmaatregelen getroffen. Slechts bij 17 procent van de gemeenten is dat wel het geval. De Inspectie van het Ministerie van SZW komt tot die conclusie[1].

Dat is een probleem. Immers, gemeenten moeten niet alleen de verantwoordelijkheid voelen voor een veilig gebruik van gegevens, maar deze ook intern doorvertalen zodat het veilig gebruik van gegevens onderdeel wordt van de dagelijkse praktijk. In 2002 zijn zeven normen vastgesteld over een veilige gegevensuitwisseling van persoonsgegevens.

De RIB van het college van november 2014 over privacy doet vermoeden dat de gemeente Woerden op alle zeven normen positief scoort. Zekerheid is er echter niet. Daarom hebben wij de volgende vragen aan het college:

- Van de gemeenten voldoet 17% aan zeven door de inspectie geselecteerde normen. Hoort Woerden bij die 17%?

- Zo nee, op welke normen scoort Woerden nog niet positief, en wat is daarvan de reden?

- Hoe en op welke termijn verwacht Woerden dat zij op alle zeven normen positief scoort?

Namens de fractie van D66

Ruud Niewold

[1] http://www.inspectieszw.nl/actueel/nieuwsberichten/veel-gemeenten-bewaken-opvragen-persoonsgegev.aspx