**RAADSINFORMATIEBRIEF**
17R.00914

gemeente WOERDEN

**Van** : college van burgemeester en wethouders
**Datum** : 5 december 2017
**Portefeuillehouder(s)** : Burgemeester, wethouder Ten Hagen
**Portefeuille(s)** : Informatieveiligheid en Privacy
**Contactpersoon** : S. Nicolasen
**Tel.nr.** : 8450
**E-mailadres** : nicolasen.s@woerden.nl

**17R.00914**

**Onderwerp:**

Jaarverslag Informatieveiligheid en Privacy 2016

---

**Kennisnemen van:**

Het jaarverslag Informatieveiligheid en Privacy

---

**Inleiding:**

Uw raad heeft te kennen gegeven geïnformeerd te willen worden over de stand van zaken betreffende privacy en informatieveiligheid in onze organisatie. Dit doen wij in de vorm van een jaarverslag In de hoofdstukken 2 en 3 wordt ingegaan op de achtergronden van resp. informatieveiligheid en privacy. In hoofdstuk 4 wordt vervolgens de stand van zaken van informatieveiligheid aan de hand van een zgn. GAP-analyse gevisualiseerd, waarna de onderwerpen van de Baseline Informatieveiligheid zijn uitgewerkt. In hoofdstuk 5 treft u een overzicht aan van hetgeen in 2016 op het gebied van privacy is gerealiseerd. Tot slot zijn Tot slot zijn onder 6 nog een aantal bijlagen opgenomen met betrekking tot gerelateerde onderwerpen.

---

**Kernboodschap:**

Onze organisatie heeft de zaken in belangrijke mate op orde, maar heeft bovenal inzicht verkregen in eventuele kwetsbaarheden. Uiteraard zijn er nog verbeterpunten en zullen er telkens weer nieuwe aandachtspunten bijkomen door externe invloeden. Als voorbeeld kan het Petya-virus dienen, waarmee dit jaar op grote schaal ransomware werd verspreid.
Belangrijk om te vermelden, is de groei in bewustwording van de bedreigingen in de digitale wereld, de zgn. awareness. De organisatiecultuur kenmerkt zich verder door een grote openheid over zaken die niet goed zijn gegaan. Zoals blijkt uit het jaarverslag, zijn er meerdere datalekken gemeld bij de Autoriteit Persoonsgegevens. Wij juichen toe dat gemaakte fouten vanuit de organisatie worden gemeld, geanalyseerd, op correcte wijze worden opgevolgd en geëvalueerd om lering te trekken, zoals dat uiteraard ook hoort.

---

**Financiën:**

n.v.t.

---

**Vervolg:**

Door invoering van een nieuwe verantwoordingssystematiek (ENSIA, Eenduidige Systematiek Single Information Audit) zullen wij in 2018 voor 15 juli uw raad informeren over deze onderwerpen. Desgewenst kan de raad afzonderlijk over deze systematiek worden geïnformeerd.

**Bijlagen:**

Jaarverslag Informatieveiligheid en Privacy 2016, Corsanummer 17i.04418

De secretaris,

drs. M.H.J. van Kruijsbergen MBA

De burgemeester,

V.J.H. Molkenboer

WERKEN voor Oudewater en Woerden


# INFORMATIEVEILIGHEID EN PRIVACY

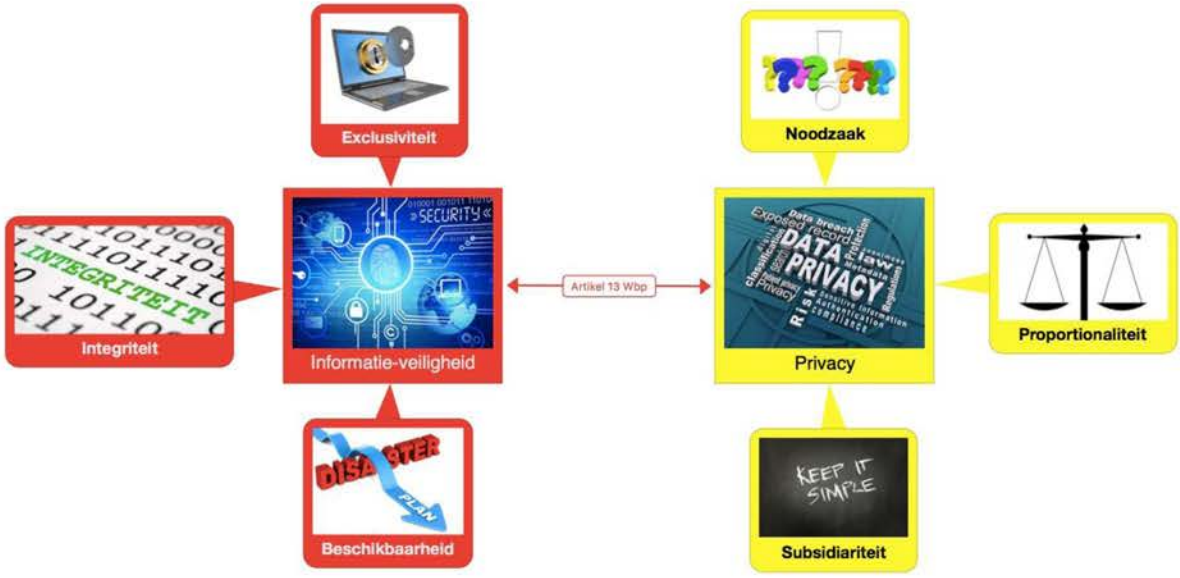
JAARVERSLAG 2016

Functionaris Gegevensbescherming
nicolasen.s@woerden.nl

# Inhoudsopgave

# 1 Inleiding

Dit document heeft als doel het bestuur te informeren over hetgeen in 2016 is gedaan aan de onderwerpen Informatieveiligheid en Privacy. Deze thema's zijn niet scherp van elkaar te scheiden. Informatieveiligheid is een voorwaarde om te kunnen voldoen aan de privacywetgeving, zoals de Wet bescherming persoonsgegevens (Wbp). De relatie tussen Informatieveiligheid en Privacy wordt expliciet benoemd in artikel 13 van de Wbp.




***Artikel 13 Wbp***

*De verantwoordelijke legt **passende technische en organisatorische maatregelen** ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Artikel 13 Wbp richt zich tegen 'verlies of enige vorm van onrechtmatige verwerking van gegevens'. Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.

De volgende twee hoofdstukken gaan nader in op de verhouding tussen en de inhoud van respectievelijk informatieveiligheid en privacy.

# 2 Informatieveiligheid

Informatiebeveiliging is niet alleen van belang om te voldoen aan de eisen van de privacywetgeving, maar bovendien een belangrijke randvoorwaarde voor het functioneren van gemeenten. Het kunnen beschikken over juiste en actuele informatie is een belangrijke voorwaarde voor de uitvoering van gemeentelijke taken.

Bij informatiebeveiliging gaat het in de kern om drie essentiële beginselen, de zogenaamde BEI-principes:

1. **Beschikbaarheid**
   Beschikbaarheid waarborgt de betrouwbare en tijdige toegang tot data of computercapaciteit. Dat wil zeggen dat computersystemen beschikbaar zijn op het moment dat ze nodig zijn om de werkprocessen te kunnen uitvoeren.
2. **Exclusiviteit**
   Exclusiviteit of vertrouwelijkheid bepaalt de mate waarin toegang tot informatie wordt beperkt tot een bepaalde groep gerechtigden die inzage mag hebben in de data.
3. **Integriteit**
   Integriteit gaat over de bescherming tegen ongeoorloofde aanpassing van (data in) software en hardware. Het gaat erom te waarborgen dat data betrouwbaar is.

- Alle beveiligingsmaatregelen, mechanismen en controles worden geïmplementeerd om één of meer van de BEI-principes in te vullen.
- Alle risico's, dreigingen en kwetsbaarheden worden beoordeeld op hun potentie om één of meerdere van deze BEI-principes schade toe te brengen.

Om informatiebeveiliging op orde te brengen, zijn er normen ontwikkeld waaraan moet worden voldaan om de BEI-principes te realiseren. Twee belangrijke normen binnen de informatiebeveiliging zijn de ISO 27001 en de ISO 27002[1]. De hierna beschreven Baseline Informatiebeveiliging Gemeenten (BIG) gebruikt deze ISO-normen als uitgangspunt.

## *2.1 Baseline Informatiebeveiliging Gemeenten*

In 2012 is door alle Nederlandse gemeenten gezamenlijk de Informatie Beveiligingsdienst (IBD[2]) opgericht en ondergebracht bij VNG/KING[3]. De IBD werkt voor alle Nederlandse gemeenten, hun ICT- samenwerkingsverbanden, intergemeentelijke sociale diensten en gemeentelijke belastingsamenwerkingen.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft in 2013 opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten, die is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Ten aanzien van het derde doel, het verminderen van de auditlast, treedt in 2017 aanvullend de Eenduidige Normatiek Single Information Audit (ENSIA) in werking. Daarover wordt het bestuur afzonderlijk geïnformeerd.

Bij het opzetten van de BIG is gekozen voor een driedeling: strategisch, tactisch en operationeel. De hierna opgenomen figuur geeft de verhouding tussen de onderdelen van de baseline weer. Daarna is deze driedeling verder toegelicht.

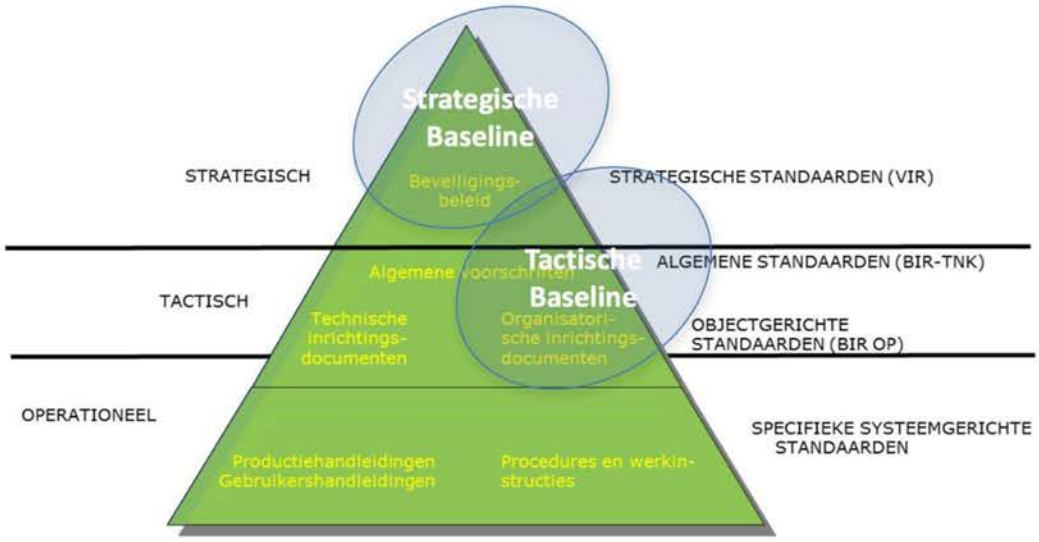
---

[1] Deze internationale norm geeft richtlijnen en algemene principes voor het initiëren, implementeren, handhaven en verbeteren van de informatiebeveiliging in een organisatie. De doelstellingen die worden beschreven geven generale richtlijnen voor de algemeen aanvaarde doelen van informatiebeveiliging. De beheersdoelstellingen en beheersmaatregelen van deze internationale norm zijn bedoeld voor implementatie om te voldoen aan de eisen die in een risicobeoordeling zijn vastgesteld.

[2] De Informatie Beveiligingsdienst (IBD) bestaat uit een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen bij een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen maar ook preventie en preparatie.

De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

[3] KING, het Kwaliteitsinstituut Nederlandse Gemeenten, is opgericht in 2009 door de VNG om gemeenten te ondersteunen bij het verbeteren van hun informatievoorziening, om zo de dienstverlening aan inwoners en ondernemers te optimaliseren.




### *2.1.1 Strategische BIG*

De strategische BIG is de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. De strategische BIG geldt voor alle gemeenten met de daaronder vallende diensten, bedrijven en instellingen, zoals werkpleinen.

In de Strategische Baseline staan o.m. de randvoorwaarden op de beveiliging van de gemeenten, zoals:

- Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement.
- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement.
- Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging.
- Kennis en expertise zijn essentieel voor een toekomst vaste informatiebeveiliging en moeten geborgd worden.
- Informatiebeveiliging vereist een integrale aanpak, zowel binnen de gemeenten als voor overheid brede gemeenschappelijke voorzieningen.

De strategische BIG laat zich ook uit over de verantwoordelijkheden van het College en het lijnmanagement:

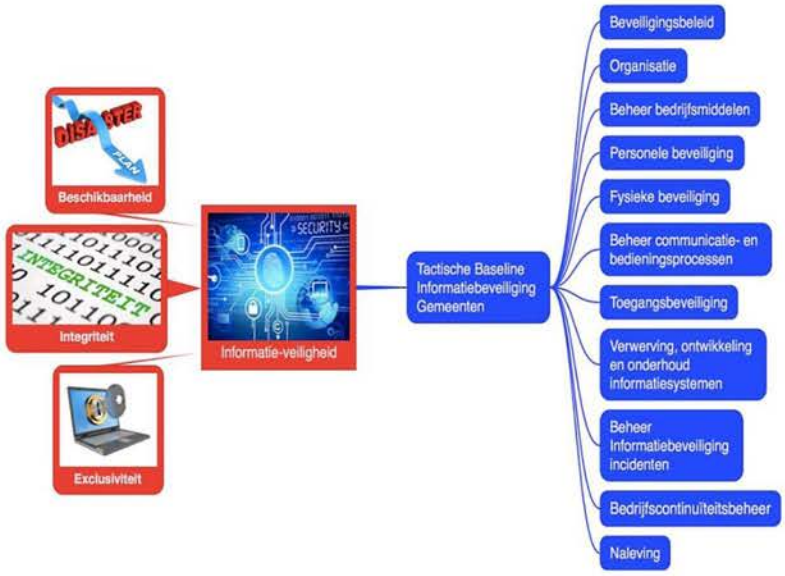
*Het College van Burgemeester en Wethouders van een gemeente stelt het informatiebeveiligingsbeleid vast en draagt dit uit. Het beleid omvat ten minste:*

- *De strategische uitgangspunten en randvoorwaarden die de gemeente hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.*
- *Het doel van het informatiebeveiligingsbeleid.*
- *De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.*
- *De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers.*
- *De gemeenschappelijke betrouwbaarheidseisen en normen die voor de gemeente van toepassing zijn.*
- *De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.*
- *De bevordering van het beveiligingsbewustzijn.*

*Het lijnmanagement:*

- *stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast.*
- *is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.*
- *controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze maatregelen worden nageleefd.*
- *evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij.*
- *rapporteert over de implementatie van de maatregelen in de management rapportages.*

### 2.1.2 *Tactische BIG*




De tactische BIG bevat informatiebeveiliging-controls en maatregelen die door iedere gemeente moeten worden geïmplementeerd. De tactische BIG is opgezet rondom bestaande normen zoals de ISO 27002. Voor specifieke maatregelen is in de tactische BIG ook gebruik gemaakt van de Wet bescherming persoonsgegevens (Wbp), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (de SUWI-wet), de Wet Basisregistratie Personen Gemeentelijke Basisadministratie Personen (BRP), de Wet Basisregistratie Adressen en Gebouwen (BAG) en de Paspoortuitvoeringsregeling (PUN).

De hoofdstukken 1 tot en met 4 van de Tactische BIG vormen het algemene deel met uitleg, relaties met ICT-architectuur, hoe met de Tactische Baseline kan worden omgegaan etc. In de hoofdstukken 5 tot en met 15 volgt de set aan maatregelen, nader onderverdeeld als in het schema weergegeven.

De hoofdstuknummering (5 $^{t}/_{m}$ 15) wordt gebruikt in de navolgende GAP-analyse (zie § 4.1). Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie.

Het doel van de GAP-analyse in de BIG is om gemeenten inzicht te geven of en in hoeverre de maatregelen uit de tactische variant van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten zijn geïmplementeerd.

### 2.1.3 *Operationele BIG*

Om de implementatie van de strategische en tactische Baseline te ondersteunen, zijn en worden door de IBD producten ontwikkeld op operationeel niveau.

Voorbeelden van dergelijke producten zijn factsheets en handleidingen betreffende:

- Cloud Computing
- Contractmanagement
- Encryptiebeleid
- Logische toegangsbeveiliging
- Screening personeel
- Geheimhoudingsverklaringen
- Bedrijfscontinuïteitsbeheer
- Dataclassificatie
- Penetratietesten
- Enz.

Deze documenten dienen als basis voor het opstellen van gemeente specifieke documenten, waarmee wordt voldaan aan de in de tactische BIG uitgewerkte normen.

# 3 Privacy

Privacy is een veelomvattend begrip. In dit verslag wordt alleen ingegaan op de informationele privacy. Onderwerpen als lichamelijke integriteit en territoriale privacy blijven buiten beschouwing. Informationele privacy wordt in dit verslag verder aangeduid met 'privacy'.

Bij privacy zijn er drie kernbegrippen:

***Noodzaak***

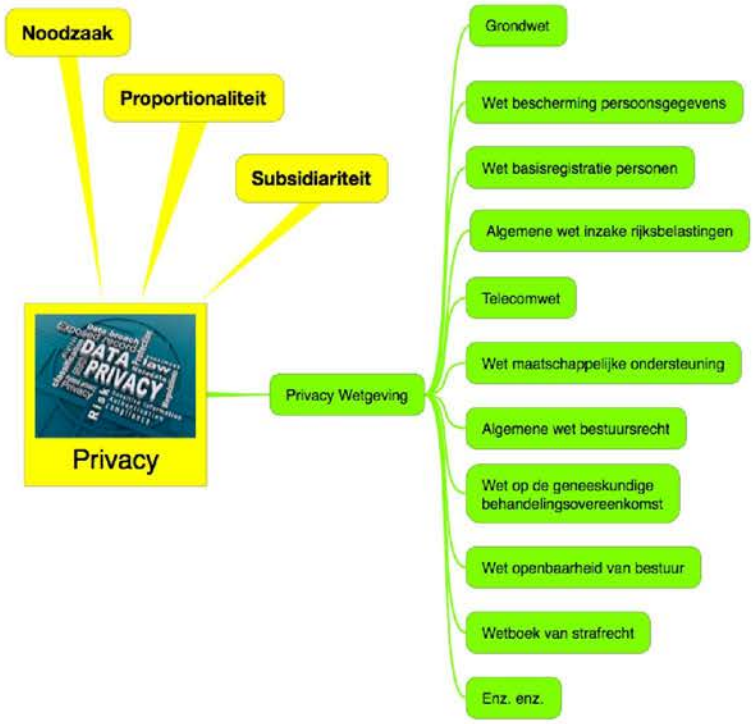
Er is alleen sprake van noodzaak wanneer de inmenging in de persoonlijke levenssfeer beantwoordt aan een dringende maatschappelijke behoefte.

***Proportionaliteit***

De inmenging in de persoonlijke levenssfeer moet evenredig zijn aan het nagestreefde de doel.

***Subsidiariteit***

De aangevoerde gronden voor de inmenging in de persoonlijke levenssfeer moeten relevant en toereikend zijn.




Deze kernbegrippen spelen een rol in alle wetgeving op het gebied van privacy. In veel wetten zijn privacybepalingen opgenomen, zoals is weergegeven in nevenstaand (onvolledig) schema.

De basis voor privacy ligt o.m. in artikel 8 EVRM en in artikel 10 van onze Grondwet:

> *1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
>
> *2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
>
> *3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

Als er geen bepalingen betreffende privacy zijn opgenomen in specifieke wetten, is de Wet bescherming persoonsgegevens (Wbp) van toepassing. In die gevallen moet aan de hand van de Wbp worden getoetst of er sprake is van noodzaak, proportionaliteit en subsidiariteit.

Op de volgende pagina is schematisch de Wbp weergegeven.

Het schema betreft de hoofdlijnen. Er wordt niet ingegaan op details als de verwerking van bijzondere gegevens en uitzonderingen op de voorgeschreven transparantie en doelbinding.

De in dit hoofdstuk opgenomen schema's zijn gebaseerd op het geldende recht. De Wbp stamt uit 2001 en zal uiterlijk 25 mei 2018 in deze vorm komen te vervallen. De reden daarvoor is dat dan de (Europese) General Data Protection Regulations (GDPR) in werking treden. In Nederland spreken we van de Algemene Verordening Gegevensbescherming (AVG). De noodzakelijke aanpassingen zijn opgenomen in de nog vast te stellen Uitvoeringswet AVG[4].

[4] Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming).


De rechten en plichten zoals nu opgenomen in de Wbp zullen met de komst van de AVG worden uitgebreid. De AVG versterkt de positie van betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden (compliance).

De 9 belangrijkste en voor ons relevante stappen om straks klaar te zijn voor de AVG zijn in bijlage 6.1 benoemd.

# 4 Realisatie Informatieveiligheid

In dit hoofdstuk is aangegeven hoe de organisatie scoort op het gebied van informatieveiligheid, welke acties daarop zijn ingezet en welke resultaten er zijn behaald.

## *4.1 GAP analyses 2016 en 2017*

Eén van de producten van de Operationele BIG (zie 3.1.3) is de GAP-analyse. Een GAP-analyse is zoals beschreven een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie.

Het doel van de GAP-analyse is om gemeenten inzicht te geven of en in welke mate de maatregelen uit de tactische variant van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten zijn geïmplementeerd. Dat onderzoek is in het eerste kwartaal van 2016 en in het eerste kwartaal 2017 uitgevoerd door het beantwoorden van telkens ca. 500 vragen. De resultaten van de analyses zijn in het volgende overzicht opgenomen.

Per onderwerp moeten in de GAP-analyse vragen worden beantwoord. Per onderwerp kan maximaal een bepaald aantal punten worden behaald ('Max'). In de derde kolom is de verhouding tussen de behaalde en de maximaal te behalen score in procenten uitgedrukt. Daaruit blijkt, dat de eindscore is opgelopen van 68% naar 79%.

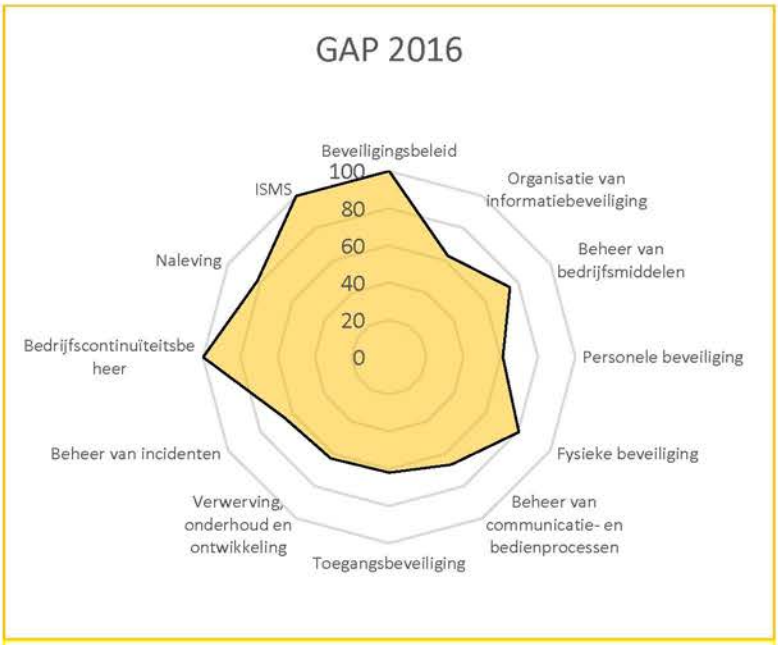
| | Resultaten GAP Analyse | 2016 | | | 2017 | | |
|---|---|---|---|---|---|---|---|
| BIG | Onderwerp | Punten | Max | Score % | Punten | Max | Score %2 |
| 5 | Beveiligingsbeleid | 4 | 4 | 100 | 4 | 4 | 100 |
| 6 | Organisatie van informatiebeveiliging | 34 | 54 | 63 | 37,5 | 54 | 69 |
| 7 | Beheer van bedrijfsmiddelen | 15 | 20 | 75 | 16,5 | 20 | 83 |
| 8 | Personele beveiliging | 22 | 36 | 61 | 22,5 | 36 | 63 |
| 9 | Fysieke beveiliging | 66 | 82 | 80 | 70 | 82 | 85 |
| 10 | Beheer van communicatie- en bedienprocessen | 108 | 162 | 67 | 129 | 162 | 80 |
| 11 | Toegangsbeveiliging | 67 | 108 | 62 | 86,5 | 108 | 80 |
| 12 | Verwerving, onderhoud en ontwikkeling | 54 | 86 | 63 | 68,5 | 86 | 80 |
| 13 | Beheer van incidenten | 13 | 20 | 65 | 16,5 | 20 | 83 |
| 14 | Bedrijfscontinuïteitsbeheer | 10 | 10 | 100 | 9,5 | 10 | 95 |
| 15 | Naleving | 18 | 22 | 82 | 19 | 22 | 86 |
| | ISMS | 2 | 2 | 100 | 2 | 2 | 100 |
| | Eindtotaal | 413 | 606 | 68 | 481,5 | 606 | 79 |

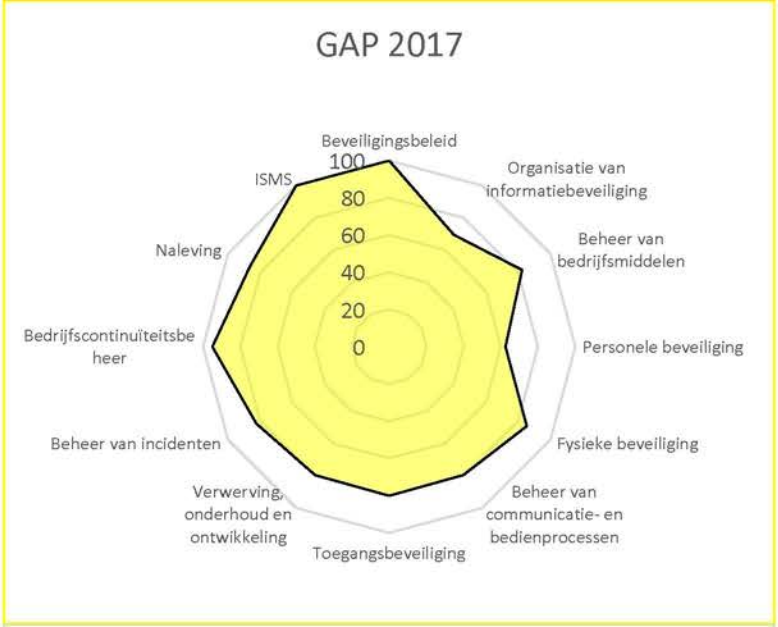
De nummering onder de kop 'BIG' heeft betrekking op het desbetreffende hoofdstuk in de Tactische Baseline (zie 3.1.3).

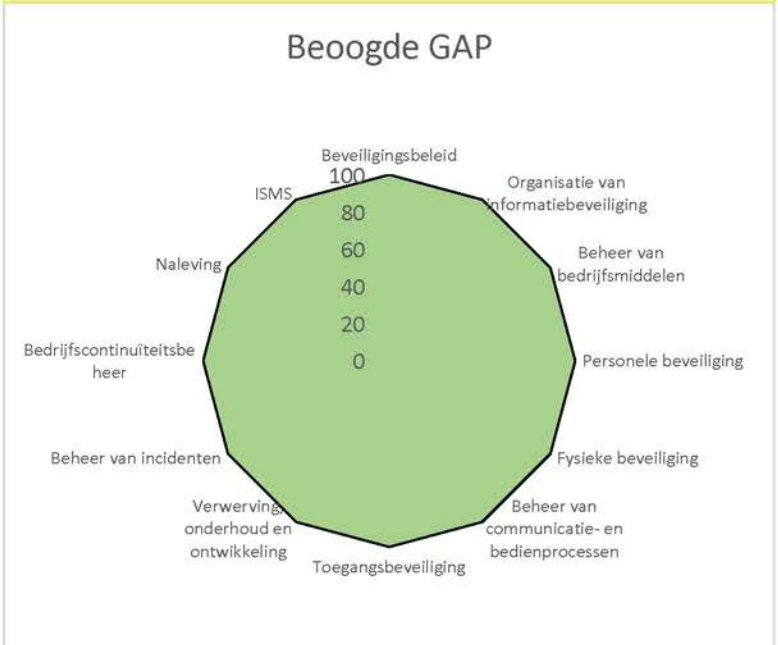
Pas als volledig wordt voldaan aan alle normen worden er 606 punten behaald. Hierbij moet worden opgemerkt, dat perceptie een zekere rol speelt bij de antwoorden op de vragen. Om die reden zijn de antwoorden tot stand gekomen door het bevragen van meerdere personen.

Op de volgende pagina zijn de resultaten van 2016 en 2017 grafisch weergegeven. Tenslotte is de aangegeven hoe de resultaten van de GAP analyse moeten worden als we volledig voldoen aan de BIG. Om misverstanden te voorkomen: volledig voldoen aan de BIG staat gelijk aan het minimale niveau van informatiebeveiliging waaraan moet worden voldaan.

De resultaten en inspanningen zijn vervolgens per onderwerp in afzonderlijke paragrafen toegelicht.


GAP 2016
Beveiligingsbeleid
Organisatie van informatiebeveiliging
Beheer van bedrijfsmiddelen
Personele beveiliging
Fysieke beveiliging
Beheer van communicatie- en bedienprocessen
Toegangsbeveiliging
Verwerving, onderhoud en ontwikkeling
Beheer van incidenten
Bedrijfscontinuïteitsbeheer
Naleving
ISMS
100
80
60
40
20
0


GAP 2017
Beveiligingsbeleid
Organisatie van informatiebeveiliging
Beheer van bedrijfsmiddelen
Personele beveiliging
Fysieke beveiliging
Beheer van communicatie- en bedienprocessen
Toegangsbeveiliging
Verwerving, onderhoud en ontwikkeling
Beheer van incidenten
Bedrijfscontinuïteitsbeheer
Naleving
ISMS
100
80
60
40
20
0


Beoogde GAP
Beveiligingsbeleid
Organisatie van informatiebeveiliging
Beheer van bedrijfsmiddelen
Personele beveiliging
Fysieke beveiliging
Beheer van communicatie- en bedienprocessen
Toegangsbeveiliging
Verwerving, onderhoud en ontwikkeling
Beheer van incidenten
Bedrijfscontinuïteitsbeheer
Naleving
ISMS
100
80
60
40
20
0

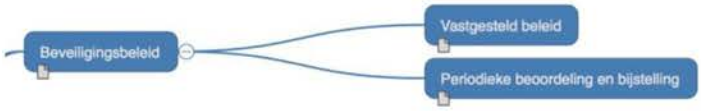
## 4.2 Acties op basis GAP analyse 2016

Bij de GAP-analyses tekent zich af, op welke terreinen aanvullend maatregelen moeten worden getroffen. In de volgende paragrafen wordt per onderwerp weergegeven wat de stand van zaken is en wat er is gerealiseerd. Gemakshalve zijn de geformuleerde doelstellingen uit de tactische BIG per onderwerp opgenomen.

### 4.2.1 Beveiligingsbeleid

**Doelstelling**

- *Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.*




Op 6 oktober 2015 hebben het college van Woerden en het college van Oudewater het Beleidsplan en de Richtlijnen Informatieveiligheid & Privacy vastgesteld. De Ondernemingsraad heeft ingestemd met de genoemde richtlijnen met als kanttekening dat er een privacyreglement diende te worden opgesteld met betrekking tot privacygevoelige zaken van medewerkers. In 2016 is daarop een 'Privacyreglement personeel' opgesteld en vastgesteld door het college. Het reglement is in 2017 aangeboden aan de OR in verband met het instemmingsrecht.

Op grond van de BIG moet het beleidsplan één keer per drie jaar worden beoordeeld en zo nodig bijgesteld. Om aan deze eis tegemoet te komen, zal een geactualiseerd beleidsplan ter vaststelling worden aangeboden aan de colleges in 2018.

### 4.2.2 Organisatie Informatiebeveiliging

**Doelstelling**

- *Beheren van de informatiebeveiliging binnen de organisatie.*


Dit onderwerp betreft zowel de interne organisatie als de omgang met externe partijen.

***De interne organisatie***

De colleges van B&W hebben de informatiebeveiligingsdoelstellingen vastgesteld om te voldoen aan de kaders zoals gesteld in de Baseline Informatieveiligheid. Jaarlijks wordt aan de colleges gerapporteerd over de opzet, het bestaan en de werking van de informatiebeveiligingsmaatregelen.

De rollen van de CISO (Chief Information Security Officer) en het lijnmanagement zijn beschreven. De CISO bevordert en adviseert gevraagd en ongevraagd over de beveiliging van de gemeente, verzorgt rapportages over de status, controleert of m.b.t. de beveiliging van de gemeente de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente. De CISO onderhoudt contact met de IBD.

Elke teammanager is verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar team. Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.

Naast de algemene geheimhoudingsplicht voor ambtenaren zoals geregeld in de Ambtenarenwet art. 125a, lid 3 moeten alle personen die te maken hebben met vertrouwelijke Informatie een geheimhoudingsverklaring te ondertekenen. Hierbij is tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.

***Externe partijen***

Informatiebeveiliging wordt meegewogen bij het besluit een externe partij wel of niet in te schakelen. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur wordt bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst afgesloten.

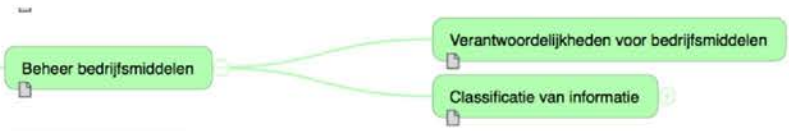
Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

Geconstateerd is, dat niet in alle gevallen een bewerkersovereenkomst is aangegaan of dat deze geactualiseerd moet worden naar aanleiding van de meldplcht datalekken. Om deze reden komt de score in de GAP-analyse uit op 69%. In 2017 wordt aandacht geschonken aan de vereiste bewerkersovereenkomsten, zowel wat betreft het bestaan daarvan als de actualiteit. Met het in werking treden van de Algemene Verordening Gegevensbescherming per 25 mei 2018 verandert er voor bewerkers veel. Bewerkers moeten compliance organiseren en kunnen aantonen.

### 4.2.3 *Beheer bedrijfsmiddelen*

***Doelstellingen***

- *Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.*
- *Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.*




***Verantwoordelijkheden bedrijfsmiddelen***

Er moet een actuele registratie zijn van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden. Van elk middel moet de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend zijn. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit moet een verantwoordelijke lijnmanager zijn benoemd.

Hoewel de verantwoordelijkheden op dit gebied in beginsel zijn toebedeeld, is er geen allesomvattende actuele registratie. Door organisatorische wijzigingen zijn verantwoordelijkheden verschoven tussen teams en zijn (nieuwe) teammanagers niet altijd op de hoogte van de eigen verantwoordelijkheden. Dit kan bij een audit leiden tot een compliance-probleem.

Er wordt nog onvoldoende tegemoet gekomen aan de eis, dat er regels moeten zijn opgesteld voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). Dit geldt ook ten aanzien van extern personeel (vastgelegd in het contract). Er zijn wel 'regels' opgesteld, maar veelal verdeeld over meerdere documenten, onvoldoende geformaliseerd (door of namens de directie vastgesteld), niet consistent, daardoor onvoldoende kenbaar waardoor ook naleving ontbreekt. Een voorbeeld: het vigerende 'Beleid mobiele telefonie en data' is vastgesteld op 16 november 2011. Er zijn naar aanleiding van de herhuisvesting en invoering van Het Nieuwe Werken nieuwsbrieven (vraag en antwoord) op intranet gepubliceerd, waarin 'regels' omtrent mobile devices zijn opgenomen. Deze regels moeten echter worden samengebracht in een vast te stellen MDM (mobile device management) om compliance te kunnen aantonen.

De conclusie luidt dan ook, dat beheermaatregelen zoals opgenomen in de 'Richtlijnen Informatieveiligheid en Privacy' d.d. 6 oktober 2015 deels nog invulling moeten krijgen.

***Classificatie***

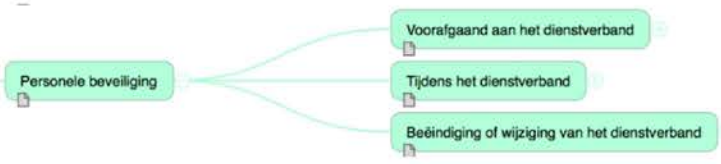
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

Met classificatie overeenkomstig de normen uit de BIG is in 2017 een begin gemaakt en moet 25 mei 2018 zijn afgerond.

### 4.2.4 *Personele beveiliging*

***Doelstellingen***

- *Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.*
- *Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen.*



- *Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.*

---

De procedure die wordt gevolgd alvorens iemand aan te stellen biedt in de veel gevallen voldoende waarborgen. Bij vertrouwensfuncties is het raadzaam niet te volstaan met een VOG (verklaring omtrent het gedrag), maar een VGB (verklaring van geen bezwaar[5]) te vragen. Dit geldt overigens ook ten aanzien van externen die (tijdelijk) een vertrouwensfunctie gaan bekleden.

Tijdens een dienstverband moet er meer aandacht zijn voor te wijzigen autorisaties als gevolg van functiewijziging. De verantwoordelijkheid daarvoor ligt bij het lijnmanagement. Periodieke (bijvoorbeeld jaarlijkse) controles van de betrouwbaarheid van in dienst zijnde medewerkers ontbreken.

Bij het beëindigen van vaste dienstverbanden worden autorisaties in de regel correct en tijdig ingetrokken. Dat is vaak niet het geval als het gaat om externen. Het ondersteunen van het lijnmanagement door middel van een checklists kan voorkomen dat de vereiste meldingen achterwege blijven.

Aan de teammanager Communicatie en Personeel zijn verbeterpunten aangereikt met betrekking tot de privacy van het personeel en verbeteren van processen rond de indiensttreding. Deze aandachtpunten worden opgepakt door het team Communicatie & Personeel.

---

### *4.2.5 Fysieke beveiliging*

***Doelstelling***

- *Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.*


---

Voorschrift is, dat toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) zijn aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

Het Stadhuis van Woerden en het Stadskantoor van Oudewater en de omgeving daarvan zijn ingedeeld in verschillende zones:

- Zone 0: de omgeving en het gebouw
- Zone 1: de wachtruimten en de spreekkamers
- Zone 2: de werkruimten
- Zone 3: de ICT-ruimte/beveiligde ruimte voor bijvoorbeeld paspoortopslag.

Door de invoering van Het Nieuwe Werken is het risico bij zone 2 afgenomen, onder voorwaarde dat iedere medewerker zich bewust is van het risico van niet-vergrendelde werkstations, onbeheerde mobile devices e.d.. Daar ligt een punt van zorg, reden waarom in 2016 is geïnvesteerd in de bewustwording van de gevaren, de zgn. awareness (zie hierna). Bij enige teams zijn nog papieren dossiers in gebruik. Daaroor zijn in 2017 persoonlijke lockers geplaatst, waarin documenten en dossiers kunnen worden bewaard.

***Bevorderen Awareness***

In 2016 is door een mysterie-guest onderzoek gedaan naar het gedrag van medewerkers wat betreft informatieveiligheid en privacy. De resultaten waren alarmerend: aangetroffen werden onder meer gele Post-it's met wachtwoorden, niet vergrendelde computerschermen en onbeheerd achtergelaten iPads. Vervolgens is op basis van de onderzoeksresultaten met de hele organisatie gesproken over informatieveiligheid en privacy.

Door middel van een campagne op intranet (PIM), mails aan medewerkers en awareness-sessies bij de meeste teams is uitgelegd welke belangrijke bedreigingen er zijn op het gebied van informatieveiligheid en privacy. Ten aanzien van privacy is bovendien benadrukt dat het niet alleen gaat om datalekken, maar ook om het recht op vertrouwelijke omgang met alle persoonsgegevens die wij ontvangen van onze inwoners en anderen zoals vastgelegd in Wet bescherming persoonsgegevens

In 2017 en volgende jaren zal dit onderwerp op de agenda blijven. Een 100% veilige digitale omgeving is vooralsnog een illusie. Dat betekent dat we onze medewerkers bewust moeten blijven maken van bestaande en komende bedreigingen.

[5] Een verklaring van geen bezwaar (VGB) is een verklaring die na een veiligheidsonderzoek door of namens de minister van Binnenlandse Zaken wordt afgegeven aan een persoon die in aanmerking komt voor een vertrouwensfunctie. Een veiligheidsonderzoek is diepgaander dan een onderzoek voor een Verklaring Omtrent het Gedrag (VOG).

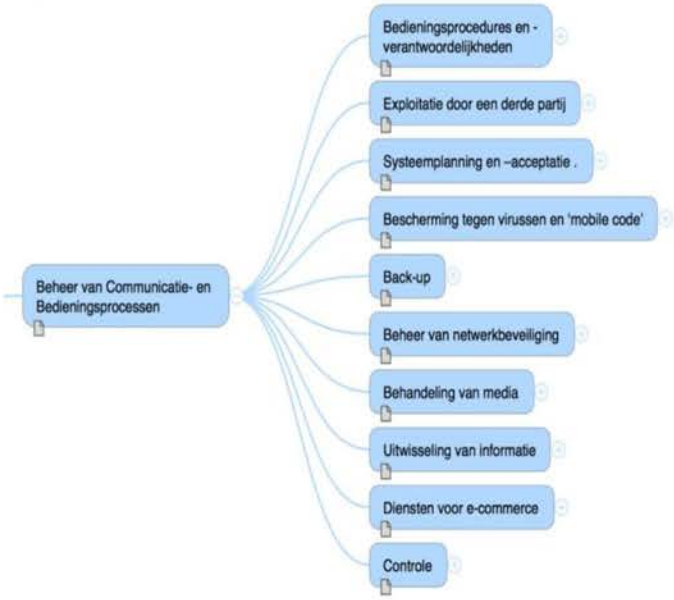

Voor de teams binnen het sociale domein is een projectleider Privacy is aangesteld. Kennis van de processen binnen het sociaal domein is een vereiste om te kunnen voldoen aan de privacywetgeving.

De awareness-sessie in het Oudewater heeft alleen met het secretariaat plaatsgevonden. De overige sessie werden steeds kort tevoren afgezegd als gevolg van een te laag aantal deelnemers. Ook de sessie met het college van Oudewater kon geen doorgang vinden.

### *4.2.6 Beheer Communicatie- en bedieningsprocessen*

***Doelstellingen***

- *Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.*
- *Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.*
- *Het risico van systeemstoringen tot een minimum beperken.*
- *Beschermen van de integriteit van programmatuur en informatie.*
- *Handhaven van de integriteit en beschikbaarheid van informatie en ICT-voorzieningen.*
- *Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.*
- *Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.*
- *Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.*
- *Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.*
- *Ontdekken van onbevoegde informatieverwerkingsactiviteiten.*




De maatregelen om de genoemde doelstellingen te verwezenlijken, zijn voor het overgrote deel afdoende, hetgeen ook blijkt uit de resultaten van bijv. de DigiD-audit. Voor de laatste van bovengenoemde doelstellingen heeft de gemeenteraad al budget beschikbaar gesteld, maar blijkt in de praktijk moeilijk te verwezenlijken. Ondanks herhaalde oproepen is het nog niet gelukt een gekwalificeerde kracht aan te trekken die voortdurend netwerkactiviteiten monitort en analyseert.

Onderzocht wordt of dit extern kan worden belegd.

Overigens moeten beschrijvingen van de procedures worden geactualiseerd, gelet op de accountability-eis.

### *4.2.7 Toegangsbeveiliging*

***Doelstelling***

- *Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.*


De maatregelen om de genoemde doelstelling te verwezenlijken, zijn eveneens voor het grootste deel afdoende. Er is echter geen "Toegangsbeleid" vastgesteld. Gelet op de accountability-eis is dat echter wel noodzakelijk.

Het feitelijke beheer van toegangsrechten is in technische zin goed geregeld. De verantwoordelijkheden van gebruikers vergen nog wel aandacht, zoals het verplicht locken van schermen bij afwezigheid.

### 4.2.8 *Verwerving, ontwikkeling en onderhoud van Informatiesystemen*

***Doelstellingen:***

- *Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.*
- *Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.*
- *Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.*
- *Beveiliging van systeembestanden bewerkstelligen.*
- *Beveiliging van toepassingsprogrammatuur en -informatie handhaven.*
- *Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.*


Om de genoemde doelstellingen te realiseren zijn ICT-consulenten aangewezen, die bij verwerving, ontwikkeling en onderhoud van informatiesystemen worden betrokken. Bij de aanschaf of ontwikkeling van nieuwe software geldt Privacy by design.

In 2016 betrof dit de applicatie 'Cumulus'. In bijlage 6.4 is beschreven op welke wijze daaraan gevolg is gegeven.

Ten aanzien van het onderhoud van informatiesystemen kan verder worden gemeld, dat alle meldingen van de Informatie Beveiligingsdienst (IBD) inzake internetbedreigingen direct door het team ICT worden beoordeeld op toepasselijkheid en urgentie. Als daartoe aanleiding is, worden direct maatregelen genomen om de risico's als gevolg van de beschreven technische kwetsbaarheden te verminderen, c.q. te elimineren. In een bijlage 6.2 zijn bedreigingen en incidenten toegelicht.

Het vastleggen van de genomen maatregelen is een aandachtspunt. Vaak ontbreekt daarvoor de tijd, terwijl na invoering van ENSIA per 1 juli 2017 registratie noodzakelijk is (accountability).

### 4.2.9 *Beheer van Informatiebeveiligingsincidenten*

***Doelstelling***

- *Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.*
- *Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.*

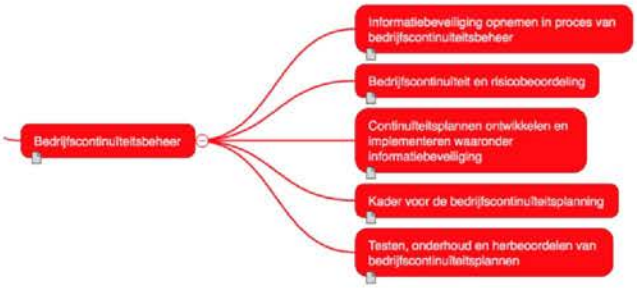

Informatiebeveiligingsincidenten worden vastgelegd in de applicatie TopDesk.

Evaluatie van incidenten blijft - als gevolg van tijdgebrek – vaak achterwege. Dit wordt veroorzaakt door het ontbreken van een vaste medewerker bij team ICT die belast is met informatieveiligheid. De vacature blijkt – zoals hiervoor vermeld - moeilijk vervulbaar.

### 4.2.10 *Bedrijfscontinuïteitsbeheer*

***Doelstelling***

- *Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.*

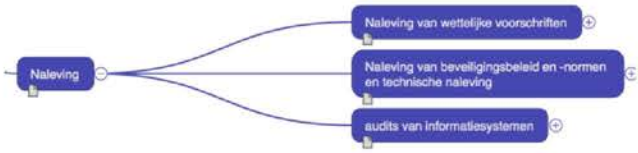



Op het gebied van de informatievoorziening zijn doeltreffende maatregelen genomen. Niet alle teammanagers beschikken over actuele bedrijfscontinuïteitsplannen. Daaraan zal in 2017 aandacht worden geschonken.

### 4.2.11 Naleving van wettelijke voorschriften

**Doelstelling**

- *Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en van enige beveiligingseis.*
- *Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.*
- *Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.*




De naleving van voorschriften, beleid en normen maakt deel uit van wettelijk voorgeschreven audits en zelfevaluaties. In 2016 zijn de hierna beschreven resultaten geboekt.

#### 4.2.11.1 Zelfevaluatie PNIK 2016

Het team KCC heeft in 2016 de verplichte zelfevaluatie PNIK uitgevoerd, zowel voor de gemeente Oudewater als de gemeente Woerden. Het uitgifteproces rond paspoorten en Nederlandse identiteitskaarten (PNIK) moet zorgvuldig en veilig verlopen. Gemeenten evalueren daarom ieder jaar zelf of de onderdelen van het proces juist worden uitgevoerd. Gemeenten maken voor de controle gebruik van vragenlijsten die zijn opgesteld door de Rijksdienst voor Identiteitsgegevens: de Kwaliteitsmonitor.

Met de Kwaliteitsmonitor kunnen gemeenten o.m.:

- de kwaliteit van de processen toetsen op basis van de afgesproken normen;
- de resultaten van de bestandscontroles vergelijken met afgesproken normen en met eerdere resultaten.

De resultaten zijn hierna vermeld.

**Zelfevaluatie PNIK Woerden**

| Thema | Wettelijke norm | Aanbevelingen | Totaal | Totaal percentage | Norm-percentage | Totaal resultaat |
|---|---|---|---|---|---|---|
| **Beleid en regelgeving** | 108 (108) | 5 (5) | 113 (113) | 100% | 90% | goed |
| **Processen** | 248 (262) | 20 (24) | 268 (286) | 94% | 90% | voldoende |
| **Gegevens** | 54 (54) | 2 (6) | 56 (60) | 93% | 90% | voldoende |
| **Personeel** | 197 (206) | 0 (0) | 197 (206) | 96% | 90% | goed |
| **Fysieke beveiliging** | 149 (162) | 13 (18) | 162 (180) | 90% | 90% | voldoende |
| **Calamiteiten** | 54 (54) | 6 (6) | 60 (60) | 100% | 90% | goed |
| **Architectuur** | 12 (12) | 0 (0) | 12 (12) | 100% | 90% | goed |
| **Naleving** | 12 (12) | 0 (0) | 12 (12) | 100% | 90% | goed |

**Zelfevaluatie PNIK Oudewater**

| Thema | Wettelijke norm | Aanbevelingen | Totaal | Totaal percentage | Norm-percentage | Totaal resultaat |
|---|---|---|---|---|---|---|
| **Beleid en regelgeving** | 106 (108) | 5 (5) | 111 (113) | 98% | 90% | goed |
| **Processen** | 258 (262) | 24 (24) | 282 (286) | 99% | 90% | goed |
| **Gegevens** | 54 (54) | 2 (6) | 56 (60) | 93% | 90% | voldoende |
| **Personeel** | 173 (206) | 0 (0) | 173 (206) | 84% | 90% | **onvoldoende** |
| **Fysieke beveiliging** | 140 (162) | 12 (18) | 152 (180) | 84% | 90% | **onvoldoende** |
| **Calamiteiten** | 54 (54) | 6 (6) | 60 (60) | 100% | 90% | goed |
| **Architectuur** | 12 (12) | 0 (0) | 12 (12) | 100% | 90% | goed |
| **Naleving** | 12 (12) | 0 (0) | 12 (12) | 100% | 90% | goed |

Voor Woerden geldt, dat het resultaat van zelfevaluatie op grond van artikel 94 van de Paspoortuitvoeringsregeling Nederland 2001 (PUN) als voldoende is gekwalificeerd.

De gemeente Oudewater scoort in de zelfevaluatie over het geheel genomen voldoende op de beveiliging en overige aspecten van het aanvraag- en uitgifteproces Paspoorten en NIK (Nederlandse Identiteitskaart). De gemeente Oudewater bereikt 92% van de maximaal te behalen waardering. De minimale norm is 90%.

#### *4.2.11.2 Zelfevaluatie Basisregistratie Personen (BRP) 2016*

Het team KCC heeft in 2016 tevens de verplichte zelfevaluatie PNIK uitgevoerd, zowel voor de gemeente Oudewater als de gemeente Woerden. De resultaten zijn hierna vermeld.

**Zelfevaluatie Gegevenskwaliteit BRP**

| | | | Woerden | | | Oudewater | | |
|---|---|---|---|---|---|---|---|---|
| Groep | Klasse | Omschrijving | Behaalde score % | Norm % | Resultaat | Behaalde score % | Norm % | Resultaat |
| 1 | A | Persoon en overlijden | 99,93 | 99,7 | √ | 99,94 | 99,7 | √ |
| | B | Adres | 99,69 | 99,7 | X | 99,94 | 99,7 | √ |
| | C | Relaties | 99,55 | 99,6 | X | 99,77 | 99,6 | √ |
| 2 | D | Identificatienummers en nationaliteit | 99,94 | 99,5 | √ | 99,94 | 99,5 | √ |
| | E | Overig algemene gegevens | 99,84 | 99,5 | √ | 99,98 | 99,5 | √ |
| 3 | F | Administratieve gegevens | 99,19 | 99,4 | X | 99,93 | 99,4 | √ |

De inhoudelijke toetsing van de kwaliteit van de Basisregistratie Personen van Woerden heeft aangetoond dat er enige verbeterpunten zijn. De verschillen van de metingen met de gestelde normen zijn klein, zoals ten aanzien van de adresgegevens: 0,01%.

De inhoudelijke toets laat zien, dat de kwaliteit van de BRP-gegevens van Oudewater op alle onderzochte gebieden aan de norm voldoet.

**Zelfevaluatie Processen BRP**

| | | | | | Woerden | | | | | Oudewater | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Thema | Wettelijke norm | Aanbe-velingen | Totale score | Norm % | Resultaat wettelijke norm | Resultaat aanbevelingen | Behaald | Totaal Resultaat % | Totaal eind-resultaat | Resultaat wettelijke norm | Resultaat aanbevelingen | Behaald | Totaal Resultaat | Totaal eind-resultaat |
| **Beleid en regelgeving** | 108 | 5 | 113 | 90 | 105 | 4 | 109 | 96% | Goed | 108 | 3 | 111 | 98% | Goed |
| **Processen** | 197 | 20 | 217 | 90 | 195 | 15 | 210 | 97% | Goed | 195 | 15 | 210 | 97% | Goed |
| **Gegevens** | 224 | 6 | 230 | 90 | 202 | 6 | 208 | 90% | Voldoende | 191 | 6 | 197 | 86% | **Onvoldoende** |
| **Personeel** | 73 | 5 | 78 | 90 | 67 | 5 | 72 | 92% | Voldoende | 62 | 5 | 67 | 86% | **Onvoldoende** |
| **Fysieke beveiliging** | 42 | 0 | 42 | 90 | 42 | 0 | 42 | 100% | Goed | 42 | 0 | 42 | 100% | Goed |
| **Calamiteiten** | 102 | 0 | 102 | 90 | 102 | 0 | 102 | 100% | Goed | 92 | 0 | 92 | 90% | Voldoende |
| **Brondocumenten** | 74 | 7 | 81 | 90 | 71 | 4 | 75 | 93% | Voldoende | 67 | 4 | 71 | 88% | **Onvoldoende** |

Uit de uitgevoerde zelfevaluatie blijkt dat de gemeente Woerden voldoende scoort op de processen (de inrichting, de werking en de beveiliging van de basisregistratie personen).

Per themagebied zijn actiepunten en aanbevelingen opgenomen in de rapportage, die leiden tot verbetering van de resultaten.

Voor wat betreft de toetsing van de BRP-processen van Oudewater geldt dat de gemeente over het geheel genomen voldoende scoort op de inrichting, de werking en de beveiliging van de basisregistratie. De tabel waarin de thema's zijn uitgewerkt laat echter zien, dat er een aantal aandachtsgebieden zijn.

Ten aanzien van de als onvoldoende gekwalificeerde onderdelen zijn in 2017 verbeteracties gestart en de verwachting is, dat in 2017 op alle onderdelen minimaal voldoende zal worden gescoord.

#### 4.2.11.3 DigiD audit

In april en mei 2016 heeft het jaarlijkse ICT-beveiligingsassessment (de zogenaamde DigiD-audit) plaatsgevonden. Alle organisaties die DigiD gebruiken, moeten voldoen aan een beveiligingsnorm. Deze norm is gebaseerd op de ICT-beveiligingsrichtlijnen voor webapplicaties van de NCSC[6]. In het kader van DigiD zijn de richtlijnen die de meeste impact hebben op de veiligheid van DigiD en de met DigiD ontsloten gegevens gekwalificeerd als de norm en onderdeel van de toetsing[7]. Nadat de organisatie heeft vastgesteld dat de noodzakelijke maatregelen zijn getroffen om aan de norm te voldoen, moet dat worden getoetst door een Register EDP-auditor[8].

De gemeente Woerden en de gemeente Oudewater zijn geslaagd voor deze audit. Daarnaast is in 2016 door Logius[9] toestemming verleend om de gezamenlijke aansluiting voor beide gemeenten te mogen blijven gebruiken.

### 4.2.12 ISMS

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening te waarborgen.

Om een goed overzicht te hebben en te houden van alle maatregelen en procedures wordt gewerkt met een ISMS. (Information Security Management System).

Eind 2015 is gestart met de inrichting van een ISMS. Om alle gegevens, documenten, procedures enz. in onderling verband, incl. versiebeheer in alle gevallen toegankelijk op te slaan, wordt gewerkt met een maximaal beveiligde cloud-oplossing.

Deze applicatie biedt de mogelijkheid om georganiseerd te registreren en archiveren en de mogelijkheid om op medewerkersniveau al dan niet toegang te geven tot vertrouwelijke documenten. Daarnaast biedt het programma de mogelijkheid taken toe te wijzen, gezamenlijk aan documenten te werken en voortgangscontrole uit te oefenen.

Bij een audit kan aan een (externe) auditor toegang worden verleend tot die documenten, die deze beroepsmatig moet inzien, zoals registraties van datalekken, ICT-incidenten, vastgestelde procedures en andere bewijsstukken.

[6] National Cyber Security Centrum, het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland.

[7] De scope van de toetsing is "de internet-facing webpagina's, systeemkoppelingen en infrastructuur die met DigiD gekoppeld zijn en betrekking hebben op het proces". Met systeemkoppelingen wordt met name de system-to-systemkoppeling (authenticatieverzoek en uitwisselen RID en verificatieverzoek van webdienst)bedoeld.

[8] Een in het register van de NOREA (Nederlandse Orde van Register EDP-Auditors) ingeschreven Register EDP-auditor.

[9] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De diensten en standaarden van Logius zijn voor de gehele overheid ontwikkeld. Logius is verantwoordelijk voor het beheer, de doorontwikkeling en de overheidsbrede toepassingen van deze diensten en standaarden.

# 5 Realisatie Privacy

## 5.1 Privacyreglement personeel

Zoals eerder in deze rapportage vermeld heeft de Ondernemingsraad heeft met de Richtlijnen Informatieveiligheid & Privacy met als kanttekening dat er een privacyreglement diende te worden opgesteld met betrekking tot privacygevoelige zaken van medewerkers. In 2016 is daarop een 'Privacyreglement personeel' opgesteld en vastgesteld door het college. Het reglement is in 2017 aangeboden aan de OR in verband met het instemmingsrecht.

## 5.2 Beantwoorden vragen / geven van advies

### 5.2.1 Vertrouwelijkheden DMS

In het Document Management Systeem (Corsa) wordt aan documenten c.q. dossiers een vertrouwelijkheid (mate van geheimhouding) toegevoegd. Deze vertrouwelijkheid bepaalt wie welke documenten of dossiers mag inzien. In 2016 is onderzoek gedaan naar het aantal vertrouwelijkheden. Gebleken is, dat er erg veel vertrouwelijkheden zijn, die bovendien als gevolg van reorganisaties in het verleden nog zijn verbonden aan teams en afdelingen die zijn opgeheven. Aanpassing aan de huidige situatie is in 2016 voorbereid en moet in 2017 worden doorgevoerd. Om te voldoen aan de voorschriften van de AVG zal bovendien een module moeten worden aangeschaft van Corsa, waardoor het mogelijk wordt te loggen wie welke documenten of dossiers heeft ingezien.

### 5.2.2 Handboek vervanging (DIV)

De essentie van het 'Handboek Vervanging' is de vervanging van papieren documenten door digitale bestanden, waarbij inhoud en vorm behouden moeten blijven. De authenticiteit moet worden gewaarborgd. Het handboek beschrijft procedures en maatregelen die ervoor zorgen dat de digitale reproductie van het originele document als betrouwbaar kan worden bestempeld, de digitale reproductie treedt in de plaats van het papieren origineel. Na vervanging mag het papieren exemplaar worden vernietigd.

In het kader van het nieuwe werken, met o.m. plaats- en tijdonafhankelijk werken, is besloten om per 1 januari 2017 volledig digitaal te gaan werken en archiveren. Om dat te bereiken is het Handboek Vervanging 2011, vorig jaar geactualiseerd en tevens van toepassing verklaard voor de documenten van de gemeente Oudewater. In het geactualiseerde handboek zijn de mogelijkheden om te kunnen vervangen verruimd wat inhoudt dat ook de te bewaren documenten mogen worden vervangen.

In 2016 is de audit-regeling digitale archivering gemeente Woerden vastgesteld. Deze regeling biedt het kader om te bepalen of het proces van vervanging optimaal verloopt. In juni 2017 zal de eerste audit met betrekking tot vervanging worden uitgevoerd. De rapportage hierover zal worden gestuurd naar de gemeentelijke archiefinspecteur en het college van burgemeester en wethouders. Een voorstel om de genoemde auditregeling en het Handboek Vervanging van overeenkomstige toepassing te laten zijn voor de gemeente Oudewater wordt in 2017 voorgelegd aan het college van Oudewater.

### 5.2.3 Cameratoezicht

In verband met overlast is in 2016 vanuit het subteam 'Openbare orde en veiligheid' advies gevraagd over de mogelijkheden om cameratoezicht in te stellen in de openbare ruimte. Het uitgebrachte advies is in bijlage 6.5 opgenomen.

### 5.2.4 Potentieel radicaliserende inwoners

Begin 2016 heeft de directie de FG gevraagd om van advies te dienen inzake een aan het college voor te leggen convenant, opgesteld door het Veiligheidshuis (formeel het Bureau Regionale Veiligheidsstrategie) Midden-Nederland[10]. Het voorstel was van het team Jeugd, Leefbaarheid en Veiligheid.

Dit convenant met onderliggend Privacyreglement betrof het uitwisselen van gegevens van potentieel radicaliserende inwoners van de gemeente Woerden met omliggende gemeenten. Het Privacyreglement kon als basis dienen voor het uitwisselen van gegevens van personen die als potentieel radicaliserend werden beschouwd.

*"Doel van de verwerking van persoonsgegevens op basis van dit reglement is:*

- *het gezamenlijk in kaart brengen en analyseren van signalen die mogelijkerwijs kunnen duiden op radicalisering, uitreizen, terugkeer en op behoefte aan hulp van achterblijvers;*

[10] Een veiligheidshuis is een lokaal of regionaal samenwerkingsverband tussen verschillende veiligheidspartners gericht op een integrale, probleemgerichte aanpak om de objectieve en subjectieve sociale veiligheid te bevorderen. In het Veiligheidshuis werken verschillende organisaties samen die bij veiligheid en handhaving zijn betrokken en nu letterlijk onder één dak de werkzaamheden verrichten. Hierdoor vindt vrijwel doorlopend informatie-uitwisseling plaats over zorg- en risicojongeren.

- *het op basis van deze signalen en analyses in gang zetten en afstemmen van acties gericht op het voorkomen van uitreizen, het bevorderen van de-radicalisering, het stimuleren van gedragsverandering, het beperken van de veiligheidsrisico's bij terugkeer en het bieden van hulp aan achterblijvers."*

Echter – ondanks het klaarblijkelijke maatschappelijke belang – moet uitwisseling van persoonsgegevens mogelijk zijn op grond van de wet. Over de bevoegdheid om gegevens vanuit bijvoorbeeld het sociaal domein door de gemeente te laten aanleveren was het convenant erg onduidelijk.

*De grondslag voor de verwerking van persoonsgegevens, waaronder ook bijzondere persoonsgegevens, op grond van dit reglement is:*

- *voor de gemeentebesturen gelegen op het terrein van de openbare orde en op het terrein van de maatschappelijke ondersteuning van burgers die deze ondersteuning behoeven;*
- *(...)*

In de wetten daarover is echter die grondslag niet te vinden. In tegendeel: met name de Jeugdwet bevat strenge geheimhoudingsbepalingen. Daarnaast stonden er in het convenant verwijzingen naar artikelen in de Wet Politiegegevens die niet aansluiten op het verstrekken van gegevens uit die registers.

Gelet op het belang (openbare orde en veiligheid) is door de FG geadviseerd om (tijdelijk) naar de geest van het reglement te handelen, maar gelijktijdig bij de opstellers een nadere onderbouwing te vragen betreffende de rechtmatigheid van de beoogde gegevensuitwisseling. De opstellers bleken niet gediend van deze kritische beoordeling en (in eerste reactie) evenmin geneigd tot aanpassingen.

Om verdere discussie te vermijden is besloten om het reglement voor te leggen aan de toezichthouder, de Autoriteit Persoonsgegevens, om op die wijze convenant en reglement te laten toetsen aan de wettelijke vereisten. Van de AP kwam als reactie een groot aantal vragen terug naar aanleiding van deze melding. Met de opstellers van het convenant (Bureau Regionale Veiligheidsstrategie Midden Nederland) heeft vervolgens een gesprek plaatsgevonden waarin door de opstellers is toegezegd samen met de Autoriteit Persoonsgegevens een duidelijkere versie op te stellen. Daarop is melding van de FG van deze gemeenten aan de AP ingetrokken. De toezegging van RVS-Midden Nederland (Bureau Regionale Veiligheidsstrategie Midden Nederland) om deze vraag voor te leggen aan de AP is bij ons weten niet nagekomen. Deze kwestie valt verder onder de verantwoordelijkheid van het Team JLV.

Het college van Woerden heeft het betreffende Privacyreglement niet goedgekeurd. Het college van Oudewater wel, maar met als kanttekening dat het moest worden voorgelegd aan de AP.

### *5.2.5 Afvalpas*

Voor wat betreft privacy in het kader van de invoering van de Afvalpas is geen advies gevraagd aan de FG. Dit is aangegrepen als een leermoment voor de organisatie. Blijkbaar was de positie van de FG nog onvoldoende duidelijk gemaakt aan het management. Met het management zijn afspraken gemaakt voor de toekomst.

## *5.3 Suwinet*

In 2016 is het onderzoek van het ministerie van Sociale Zaken naar de veilige gebruik van Suwinet[11] gezamenlijk opgepakt met Ferm Werk. De aansluiting die werd gebruikt door FermWerk stond in 2016 nog op naam van de gemeente Woerden, waardoor deze gemeente niet alleen eindverantwoordelijk was, maar ook door het Ministerie verantwoordelijk werd gehouden voor het aanleveren van de voorgeschreven rapportages[12]. Door middel van interviews is gezamenlijk met FermWerk onderzoek gedaan naar nader genoemde aspecten en gerapporteerd.

Later in 2016 is eveneens samengewerkt aan een her controle van de 5 belangrijkste normen van het onderzoek. Het college heeft afsluitend een verklaring afgegeven dat gelet op onze bevindingen Ferm Werk voldoet aan alle normen. Ferm Werk is geslaagd voor de her controle.

## *5.4 E-mail, CryptShare en Govroam*

Een e-mail is te vergelijken met een postkaart, niet verpakt en alle informatie is direct uit te lezen. Waar komt de kaart vandaan, wat staat erop en voor wie is die bedoeld? Al deze informatie kan iemand direct van een postkaart uitlezen. Op een postkaart zetten we doorgaans een kleine leuke boodschap hoe het met ons gaat.

[11] Via Suwinet-inkijk worden vanuit verschillende bronnen (onder andere BRP, DUO, Kadaster en RDW) gegevens beschikbaar gesteld aan partijen zoals gemeenten, SVB en UWV.

[12] Organisaties die Suwinet gebruiken moeten zich verantwoorden over de beveiliging van Suwinet. Dit doen zij door jaarlijks een rapportage te verstrekken aan het BKWI conform de SUWI-Verantwoordingsrichtlijn. Deze richtlijn schrijft een rapportagemodel voor en stelt regels aan het achterliggende onderzoek dat nodig is voor deze rapportage.

In een e-mail zetten we daarentegen zeer vertrouwelijke informatie. Vertrouwelijke bedrijfsgegevens en persoonlijke of financiële gegevens, sturen wij zonder nadenken met een e-mail mee. Bijna niemand beseft echter dat deze informatie daarmee semi-openbaar wordt. De e-mail hoeft alleen nog maar onderschept te worden door een nieuwsgierige persoon of kwaadwillende en het bericht kan, met bijlagen, volledig worden uitgelezen. Een e-mail kan niet alleen onderschept en uitgelezen worden, maar ook de inhoud en de afzender kunnen worden veranderd. Het manipuleren van e-mails is erg aantrekkelijk, omdat de ontvanger geen argwaan krijgt, aangezien de e-mail afkomstig lijkt te zijn van een contact of betrouwbaar persoon.

Het internetverkeer loopt via vele knooppunten van kabels en routers, dat geldt ook voor e-mail. Wanneer een e-mail verstuurd wordt, kan deze 1, 33 of 99 landen passeren. Al deze landen hebben het recht om de e-mail te 'scannen'. Op e-mailverkeer zit (nog) geen briefgeheim en mag dus zonder uitspraak van de rechter geopend worden.

Standaard e-mails, die 99% van de gebruikers gebruikt is zo onveilig, dat iedereen zich moet afvragen of het nog wel vertrouwelijke informatie via de e-mail kan verzenden. E-mail biedt de gebruiker geen enkele beveiliging en kan door iedereen onderschept, ingelezen en zelfs veranderd worden!

E-mailproviders hebben zelfs toegang tot de inbox van hun klanten en scannen deze op inhoud. De privacy van e-mailgebruikers is tot op heden ver te zoeken. De beveiliging die zij bieden is zeer beperkt, want wanneer de gebruiker een e-mail verstuurt of ontvangt, gebeurt dit zonder enige mate van beveiliging. Kortom: Standaard e-mails zijn zo onveilig, dat het niet meer gebruikt zou moeten worden om vertrouwelijke informatie met anderen uit te wisselen.

De vele berichten van en naar inwoners, instellingen (waaronder ketenpartners) en bedrijven met vertrouwelijk informatie vormden daarom de aanleiding te zoeken naar een veilige manier om informatie uit te wisselen. Na onderzoek van de bestaande mogelijkheden is gekozen voor CryptShare.

Cryptshare maakt het mogelijk om op relatief eenvoudige wijze veilig te versturen. Bij het versturen van de bestanden worden deze niet op de mailserver opgeslagen maar op de Cryptshare server. Deze server staat binnen het netwerk van de gemeente Woerden achter de firewall in de DMZ[13]. De bestanden worden daar met een AES-versleuteling opgeslagen terwijl zowel de upload als de download via SSL-verbindingen[14] verlopen. Daarmee is Cryptshare een high-end securityoplossing die organisaties in staat stelt om bestanden veilig te versturen.

De verzender heeft niet meer dan het e-mailadres van de ontvanger nodig terwijl de ontvanger geen lokale software hoeft te installeren. De communicatie werkt bi-directioneel zodat bestanden zowel heen als terug gestuurd kunnen worden via dezelfde Cryptshare installatie. Cryptshare wordt via een browser benaderd en beschikt over connectoren voor zowel Outlook als voor Lotus Notes.

Uiteraard kan de gemeente van inwoners niet eisen dat zij gebruik maken van CryptShare, maar we bieden dat wel aan. Onderstaande tekst is opgenomen op de website www.woerdenwijzer.nl

**Hoe kan ik het ondersteuningsplan verzenden?**
Bij WoerdenWijzer.nl vinden we een zorgvuldige omgang met uw persoonsgegevens van groot belang. Wij bieden u daarom de mogelijkheid om uw ondersteuningsplan en e-mails met vertrouwelijke informatie versleuteld naar ons te versturen. Hiervoor maken we gebruik van CryptShare (veilig mailen).

Via deze verbinding kunt u uw gegevens veilig naar ons toe mailen. Lees verder **de handleiding voor het gebruik van cryptshare**. Let op: Als u de door u *gestuurde* e-mails ook zelf wilt bewaren, kunt u uw eigen e-mailadres ook opnemen bij de ontvangers.
Verder is het van belang dat u via sms of WhatsApp het wachtwoord en uw emailadres naar ons toestuurt. Op die manier kunnen wij het bestand openen. Als u uw gegevens naar info@woerdenwijzer.nl mailt, kunt u het wachtwoord in een berichtje sturen naar 06 - 2009 4736. Als u direct een mail verstuurt naar één van onze medewerkers, dan kunt u zijn/haar mobiele nummer gebruiken. Mocht u dat nummer niet hebben, kunt u het wachtwoord en de naam van betrokken medewerker in een berichtje sturen naar 06 - 2009 4736.

Na een pilot in het sociaal domein medio 2016, is CryptShare organisatie breed geïmplementeerd in Outlook.

Voor het verzenden van grote bestanden is CryptShare ook geschikt. Om die reden worden grote bestanden naar bijvoorbeeld bouwondernemingen binnen afzienbare tijd niet meer verzonden met WeTransfer. Ook het verzenden van bestanden via WeTransfer kan er namelijk toe leiden dat bestanden op straat komen te liggen. Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) werkt aan LocalBox, het antwoord voor ambtenaren om bestanden te delen. Via LocalBox wordt het mogelijk om bestanden veilig online te delen én op te slaan.

Tijdens een live hackdemonstratie werd recent de kwetsbaarheid van de ambtenaren zichtbaar. Via een nagemaakte open Wifi-verbinding kregen hackers moeiteloos inzicht in alle data die via deze verbinding gaat. De hackers wisten adressen te

[13] DMZ (Demilitarized) zone betekent in de informatica een netwerksegment tussen het interne netwerk en het internet.

[14] Met SSL wordt vertrouwelijke informatie versleuteld verzonden, zodat gegevens niet onderschept kunnen worden.

achterhalen en zagen dat iemand babykleding bekeek op internet. Tijdens deze demonstratie ging het nog om persoonlijk informatie, maar via deze constructie is het ook mogelijk dat ambtenaren onbewust informatie lekken over burgers. Hackers kunnen nep Wifi-verbindingen instellen op openbare plaatsen en als ambtenaren hiervan gebruik maken om nog even snel een werk gerelateerd mailtje te sturen, kunnen deze gegevens op straat komen te liggen.

Gelukkig wordt er op dit moment gewerkt aan Wifi voor ambtenaren: Govroam. Het biedt ambtenaren toegang tot internet in de eigen organisatie én bij alle andere deelnemende overheidsorganisaties. Na één keer inloggen, kan je als ambtenaar uiteindelijk overal online. Ideaal én veilig, want Govroam maakt gebruik van de nieuwste beveiligingsstandaarden.

Onderzocht wordt, of toetreden op dit moment – gelet op de investeringen te doen voor de nieuwe huisvesting van de gemeente Woerden – geen desinvestering zou betekenen. Als dat niet het geval is, zal Govroam nog in 2017 beschikbaar komen voor de medewerkers en bestuurders van de gemeenten Woerden en Oudewater.

De conclusie luidt, dat de middelen om veilig informatie te delen binnen afzienbare tijd beschikbaar zijn of komen. De opgave zal zijn medewerkers, inwoners, ketenpartners en bedrijven ervan te doordringen dat internet niet veilig is als het gaat om vertrouwelijke informatie. Daarop wordt in de volgende paragraaf aandacht geschonken. Feit is dat er nog veel informatie wordt gedeeld door grote partijen waarmee de gemeenten Woerden en Oudewater zaken moeten doen via het onbeveiligde email-kanaal. Maar ook medewerkers drukken nog vaak op 'verzenden' terwijl het niet een bericht is van @woerden.nl naar @woerden.nl.

## 5.5 Proces datalekken

In 2016 is een protocol opgesteld, waarin de stappen, rollen en verantwoordelijkheden ingeval van een datalek zijn opgenomen. Het werkproces is vastgesteld door de directie en ter kennisgeving aan de colleges van burgemeester en wethouders gestuurd.

De schematische weergave van het werkproces is in bijlage 6.6 opgenomen. Alle stappen zijn in detail uitgeschreven zodat bij afwezigheid van de Functionaris gegevensbescherming anderen adequaat kunnen reageren op een datalek.

## 5.6 Geconstateerde datalekken

In 2016 is melding gedaan bij de Autoriteit Persoonsgegevens van slechts één datalek. Dat betrof een publicatie op de website www.woerden.nl van verleende vergunningen, waarbij in plaats van de voor publicatie geschikte informatie, ook persoonsgegevens waren gepubliceerd. Na ontdekking zijn die gegevens direct verwijderd van de website en van de archief website. Daarna zijn de betrokkenen in kennis gesteld en is de AP geïnformeerd. Het ging in deze kwestie om een zeer beperkt aantal personen.

Daarnaast is in een tweetal gevallen een bericht verzonden aan een ander dan de beoogde ontvanger. In beide gevallen is dat direct gesignaleerd en gemeld, waarop terstond contact is opgenomen met de onbedoelde ontvangers en betrokkenen. In beide gevallen was er sprake van een datalek zoals bedoeld in de Wbp. Niet ieder datalek hoeft echter te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding worden gedaan aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. In beide gevallen is geconcludeerd, dat daarvan naar redelijke verwachting geen sprake was. Uiteraard zijn aan betrokkenen excuses aangeboden.

Dit betekent echter geenszins, dat er niet meer datalekken zijn geweest in 2016. De kennis van de medewerkers op dit gebied zal de komende tijd worden vergroot.

## 5.7 Aanwijzing Functionaris gegevensbescherming (FG)

Was een FG onder de Wet bescherming persoonsgegevens nog optioneel, de Algemene Verordening Gegevensbescherming stelt deze verplicht. Aangezien de gemeenten Woerden en Oudewater op 25 mei 2018 moeten voldoen aan alle eisen die de AVG stelt, is nu reeds een FG aangewezen met als opdracht de organisatie daarop voor te bereiden.

## 5.8 Dataclassificatie

Informatiebeveiliging draait om het beperken van risico's. En dat gaat verder dan uitsluitend techniek. Maar wat zijn nou daadwerkelijk de risico's op een informatie veiligheidsincident voor onze organisatie? Middels dataclassificatie en een risicoscan

op onze bedrijfsprocessen krijgen we zicht op de belangrijkste aandachtspunten. Aan de hand van deze risico's kunnen er tegenmaatregelen en beleid worden opgesteld.

In de datakwalificatie wordt – met het oog op de invoering van de AVG - in eerste instantie voor alle dataverzamelingen met persoonsgegevens opgenomen hoe privacygevoelig de opgenomen gegevens zijn.

## 5.9 Bewerkersovereenkomsten

In 2016 is gestart met onderzoek naar de aanwezigheid van zogenaamde bewerkersovereenkomsten. Een bewerkersovereenkomst of data processing agreement (DPA) is een begrip uit de privacyregelgeving.

Twee termen uit de privacyregelgeving dienen te worden toegelicht. Dit zijn de begrippen 'verantwoordelijke' en 'bewerker'.

- De verantwoordelijke (controller) is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Denk hierbij aan het team Communicatie en Personeel, dat persoonsgegevens van de werknemers bijhoudt met het oog op de salarisadministratie (naam, adres, bankrekeningnummer enz.). Het team C&P is verantwoordelijk voor de gegevens.
- De bewerker (processor) is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. In bovengenoemd voorbeeld is het salarisadministratiekantoor ADP, dat voor de gemeente Woerden de salarisadministratie afhandelt, bewerker.

De bewerkersovereenkomst is de overeenkomst tussen verantwoordelijke en bewerker, waarin wordt vastgelegd hoe de bewerker met de persoonsgegevens moet omgaan. In bovengenoemd voorbeeld moeten team C&P en het salarisadministratiekantoor dus een schriftelijke overeenkomst met elkaar aangaan. De verantwoordelijke (zoals bedoeld in de Wbp) moet er voor zorgen dat dit ook gebeurt.

Uit dit eerste onderzoek kwam naar voren, dat in enige gevallen een bewerkersovereenkomst ontbrak, zoals van de gemeente Oudewater als verantwoordelijke voor de BRP met de gemeente Woerden als bewerker. Daarnaast is een aantal bewerkersovereenkomsten niet aangepast aan de wijziging van de Wbp per 1 januari 2016, waarbij de meldplicht datalekken in de wet is opgenomen.

Een verdergaand onderzoek naar alle ketenpartners waarmee een bewerkersovereenkomst moet zijn c.q. worden aangegaan staat gepland voor 2017.

# 6 Bijlagen

## 6.1 Bijlage Stappen AVG

***Stap 1: Bewustwording***

De relevante mensen in onze organisatie[15] (zoals beleidsmakers) moeten op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op onze huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

***Stap 2: Rechten van betrokkenen***

Onder de AVG krijgen betrokkenen (van wie wij persoonsgegevens verwerken) meer en verbeterde privacyrechten. Daarbij gaat het om bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering, maar ook om nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moeten wij ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop wij met hun gegevens omgaan. De AP is verplicht deze klachten te behandelen.

***Stap 3: Overzicht verwerkingen***

Al onze gegevensverwerkingen moeten in kaart zijn gebracht. Daarbij moeten we documenteren welke persoonsgegevens wij verwerken, met welk doel, waar deze gegevens vandaan komen en met wie wij de gegevens delen. Onder de AVG hebben wij een documentatieplicht, wat inhoudt dat wij moeten kunnen aantonen dat onze organisatie in overeenstemming met de AVG handelt.

Dit overzicht is ook nodig als betrokkenen hun privacyrechten uitoefenen. Als zij vragen hun gegevens te corrigeren of verwijderen, moeten wij dit doorgeven aan de organisaties waarmee wij hun gegevens hebben gedeeld.

In het overzicht moet ook per categorie van gegevens worden aangegeven op basis van welke wettelijke grondslag wij deze gegevens verwerkt. De grondslagen in de AVG voor gegevensverwerking zijn grotendeels hetzelfde als die in de huidige Wbp.

***Stap 4: Privacy impact assessment (PIA)***

Onder de AVG zijn wij verplicht een zogeheten privacy impact assessment (PIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Wij moeten een PIA uitvoeren als de beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. Komt uit een PIA naar voren dat de verwerking een hoog risico oplevert waarvoor onvoldoende maatregelen zijn te treffen om het risico te beperken, dan moet de AP worden geraadpleegd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG.

***Stap 5: Privacy by design & privacy by default***

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Dit beginsel wordt al toegepast bij de ontwikkeling van Cumulus.

Privacy by default houdt in dat wij technische en organisatorische maatregelen moeten nemen om ervoor te zorgen dat wij alléén persoonsgegevens verwerken die noodzakelijk zijn voor het specifieke doel dat wij willen bereiken. Bijvoorbeeld door:

- een app die wij aanbieden niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- nooit meer gegevens te vragen dan nodig is.

***Stap 6: Functionaris voor de gegevensbescherming***

Onder de AVG zijn overheidsorganisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Voor de gemeenten Oudewater en Woerden is daarin voorzien. Bovendien is een plaatsvervangend FG aangewezen.

***Stap 7: Meldplicht datalekken***

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in onze organisatie hebben voorgedaan. Met deze documentatie moet de AP kunnen controleren of wij aan de meldplicht hebben voldaan. Dit gaat overigens verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken. Wij moeten voortaan alle datalekken documenteren. Daarmee is overigens in 2016 al begonnen.

***Stap 8: Bewerkersovereenkomsten***

Als wij onze gegevensverwerking hebben uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd), dan rust op ons de plicht te beoordelen of de overeengekomen maatregelen in bestaande contracten met onze bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, dan moeten wij tijdig de noodzakelijke wijzigingen aanbrengen.

***Stap 9: Toestemming***

Onze gegevensverwerking kan zijn gebaseerd op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Het is noodzakelijk te evalueren de manier waarop wij toestemming vragen, krijgen en registreren. Nieuw is dat wij moeten kunnen aantonen dat wij geldige toestemming van mensen hebben gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

[15] Waar in dit verslag 'organisatie' staat, wordt bedoeld de ambtelijke organisatie die werkt voor de gemeenten Oudewater en Woerden.

## 6.2 Bijlage: ICT beveiligingsincidenten

### 6.2.1 Bedreigingen

Er zijn tal van bedreigingen op internet, zoals phishing, malware en de bijzondere vorm van malware, ransomware.

Bij phishing proberen kwaadwillenden gevoelige informatie te verkrijgen door zich voor te doen als een betrouwbaar persoon of bedrijf. Op deze manier wordt geprobeerd om zaken als inloggegevens te achterhalen.

Malware is de term die gebruikt wordt voor alle vormen van software met slechte bedoelingen (malicious software). Hieronder vallen bijvoorbeeld virussen, trojans, spyware en ransomware. Malware wordt net als phishing gebruikt om vertrouwelijke gegevens te achterhalen, maar ook om computers over te nemen of te blokkeren. Spam is ongevraagde bulk e-mail met meestal een commerciële boodschap. Dit is een plaag op internet door de hoeveelheid spam die wordt verstuurd: geschat wordt dat circa 80% van het wereldwijde e-mailverkeer bestaat uit spam. Netwerken en mailservers worden trager door de extra belasting.

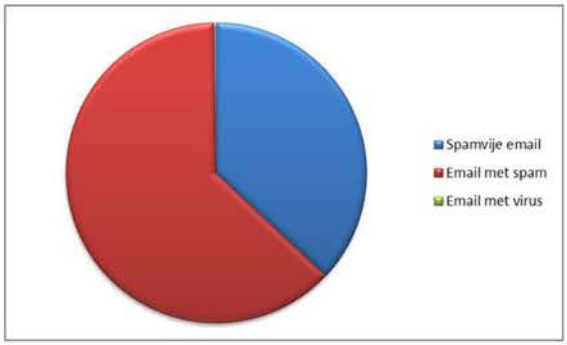
Een met ransomware (gijzelsoftware) geblokkeerde computer is een sterk toenemende vorm van malware. Door op een onverdachte link te klikken worden bestanden versleuteld (encrypted). Voor de sleutel moet veelal in bitcoins worden betaald.

In de volgende paragrafen zijn nadere bijzonderheden opgenomen.

### 6.2.2 Externe email

Bij onze organisatie komt email binnen voor de volgende domeinen:

- dsgwerk.nl
- fermwerk.nl
- kringloop.nl
- oudewater.nl
- sluisgroep.nl
- woerden.nl
- woerdenwijzer.nl




| | | |
|---|---|---|
| *Totaal aantal binnengekomen e-mail*[16] | *2.671.680* | |
| *Waarvan spam* | *1.682.101* | *62,96 %* |
| *Waarvan virus* | *5.296* | *0,2 %* |

Hoewel spam vervelend is, zijn de bijna 5400 e-mails met virussen in potentie gevaarlijker. Iedere dag van het jaar zijn er zo'n 15 e-mails onderschept waarin een virus is of kan zijn verstopt. Ieder virus kan de bedrijfsvoering en/of de privacy in gevaar brengen.

### 6.2.3 Malware

Voor servers en werkplekken gebruiken we twee verschillende anti-malware producten, niet gecombineerd. Gezamenlijk hebben deze producten 147 meldingen gegenereerd, met de volgende kanttekeningen:

- Meldingen kunnen mogelijk test malware[17] betreffen.
- Meldingen bevatten mogelijk 'false-positives'. Enige producten die wij gebruiken, veroorzaken in sommige situaties deze false-positives.
- Ogenschijnlijk unieke meldingen kunnen betrekking hebben op dezelfde poging tot infectie.

Elke melding krijgt als prio 1 de volledige aandacht.

### 6.2.4 Incidenten

In 2016 is tweemaal een cryptolocker[18] actief geweest.

- *Begin maart 2016.*
  Een gebruiker zoekt op het internet naar vakgerelateerde zaken. Op een voor de gebruiker niet bekende site, maar wel vakgerelateerd, werd een (Windows) gebruikersnaam/wachtwoord dialoog gestart en de gebruiker vulde zijn netwerkverificatiegegevens (credentials) in. Daarop werd een cryptolocker actief. Direct na ontdekken is het virtuele netwerk van de betreffende werkplekserver geblokkeerd (disabled), waardoor ongeveer 30 medewerkers niet meer konden werken.
  Uit nader onderzoek bleek dat maar een gedeelte van de malware actief was geworden. Een gedeelte werd geblokkeerd door een

[16] Interne e-mails zijn niet in deze telling opgenomen.

[17] The EICAR test file is ontwikkeld door het European Institute for Computer Antivirus Research (EICAR)en heft als doel de reacties van computer antivirus (AV) programma's te testen.[2] In plaats van echte malware, die schade zou kunnen aanrichten, maakt de EICAR test file het mogelijk veilig antivirus software te testen.

[18] Cryptoware of CryptoLocker is een ransomware, een vorm van malware waarbij alle computerbestanden verloren kunnen gaan. Cryptoware sluipt binnen via het Windows-systeem en versleutelt computerbestanden.

weblinkscanner. Deels werd de malware gedetecteerd door onze antimalware software, een ander gedeelte was actief gedurende 20 minuten. Uiteindelijk waren overal restanten van instructies te vinden, maar geen werkelijk versleutelde documenten of programmatuur. Zekerheidshalve is het profiel en wachtwoord van de gebruiker vervangen. Tevens is de complete getroffen werkplekserver verwijderd en uit de nachtelijke backup teruggehaald.

- *Eind april 2016.*
  Bij een vakteam zijn tegelijkertijd een aantal malafide e-mails verspreid, die nauwelijks van echt waren te onderscheiden. Deze waren zo nieuw dat ze niet werden afgevangen door onze emailbeveiliging. Twee medewerkers hebben de e-mail geopend en een link aangeklikt. Via één medewerker is een cryptolocker geactiveerd binnen het account. Vervolgens zijn hierdoor ± 15.000 bestanden versleuteld geraakt op locaties waar de gebruiker rechten had. Een kwartier later is de gebruiker uitgelogd en daarmee is verdere verspreiding gestopt. Bij de tweede medewerker bleek uiteindelijk niets geactiveerd. Vervolgens heeft systeembeheer specifieke preventieve acties uitgevoerd om herhaling te voorkomen. Betrokken profielen zijn verwijderd en opnieuw ingesteld. Omdat alleen bestanden en geen programmatuur was aangetast kon worden volstaan met het terugplaatsen van bestanden vanuit de back-up. De uiteindelijke schade was minimaal.

### *6.2.5 Beveiliging tegen malware*

Op diverse niveaus kunnen we malware detecteren en verspreiding tegengaan. Hieronder de belangrijkste maatregelen die in 2016 zijn uitgevoerd.

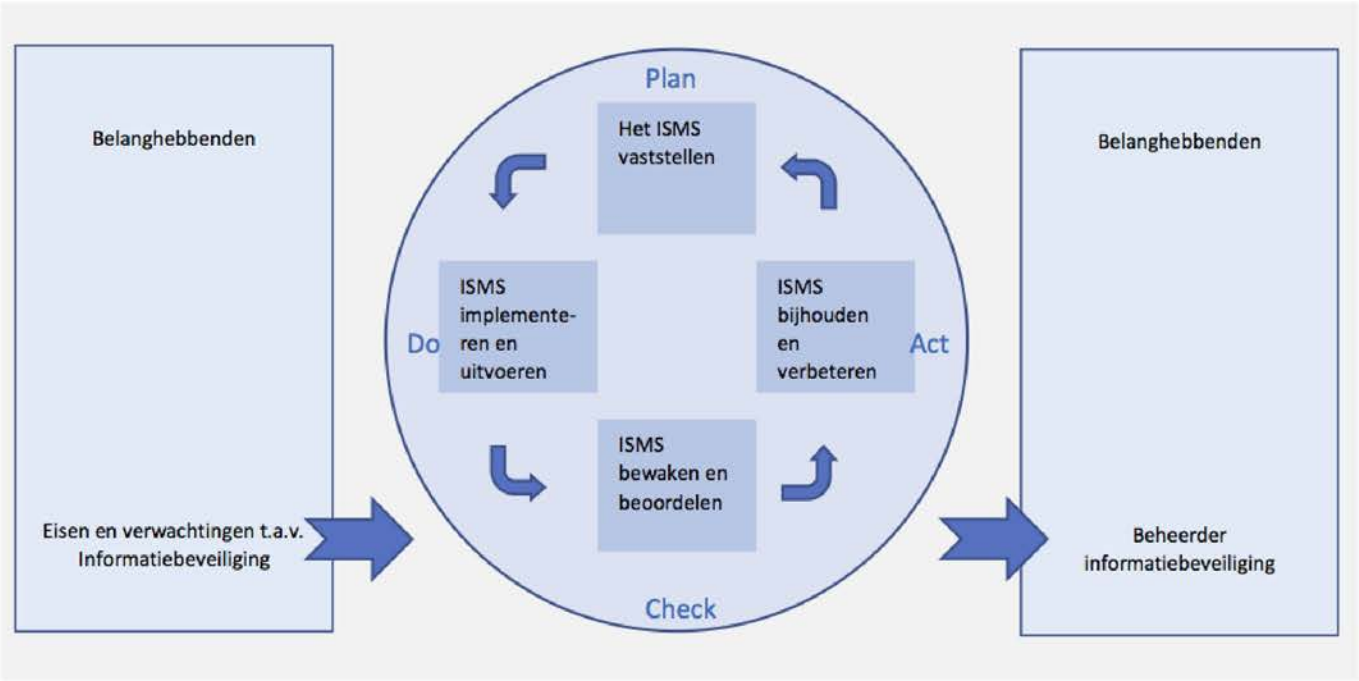
- Dubbel uitgevoerde fysieke firewall, waarop meerdere malen per jaar door een externe partij een penetratietest wordt uitgevoerd.
- Firewall binnen besturingssystemen.
- Malicious Software Removal Tool (Windows standaard ingebouwde tool, scant o.a. bij opstarten en updaten).
- Geavanceerde third party antimalware software op desktops.
- Geavanceerde third party antimalware software voor servers en virtuele omgeving.
- Webreputation scanner (controleert realtime of een link te vertrouwen is).
- Whitelisting op werkplekken.
- 80% van de werkplekken gevirtualiseerd (minder risico).
- Grotendeels geautomatiseerd patchmanagement systeem.
- Proactief patchen n.a.v. nieuwsberichten, IBD, NCSC of andere bronnen.

In het geval er toch malware actief wordt, dan hebben we diverse mogelijkheden om recente data terug te halen. Hieronder een lijst met de maximale leeftijd van teruggehaalde gegevens:

- bestandsdata maximaal 2 uur oud;
- belangrijkste databases 1 minuut oud;
- overige databases maximaal 12 uur oud;
- virtuele servers maximaal 24 uur oud.

## 6.3 Bijlage ISMS

De kracht van een ISMS is dat een doorlopend proces van (het beoordelen van) informatiebeveiliging wordt gerealiseerd. Informatiebeveiliging is een dynamisch gebied waarin dagelijks nieuwe ontwikkelingen zijn die de informatie binnen de organisatie kunnen bedreigen.




| | | |
|---|---|---|
| **Plan** | ISMS vaststellen | Het vaststellen van het ISMS en de doelstellingen, processen en procedures die relevant zijn voor het risicomanagement en de verbetering van de informatiebeveiliging, teneinde resultaten te leveren die in overeenstemming zijn met onze algemene beleidslijnen en doelstelling van onze organisatie. |
| **Do** | ISMS implementeren en uitvoeren | Het implementeren en uitvoeren van het ISMS, beheersmaatregelen, processen en procedures. |
| **Check** | ISMS controleren en beoordelen | Beoordelen en, voor zover van toepassing, meten van procesprestaties ten opzichte van het ISMS en de doelstellingen en ervaring uit de praktijk, en rapportage van de resultaten aan directie en college ter beoordeling. |
| **Act** | ISMS bijhouden en verbeteren | Corrigerende en preventieve maatregelen nemen op basis van de resultaten van de interne ISMS-audit (GAP-analyse) en andere relevante informatie om een continue verbetering van het ISMS te bewerkstelligen. |

## 6.4 Bijlage: Privacy by design Cumulus

Ter vervanging van de Centric-applicatie GWS4All van het sociaal domein, is er voor gekozen een applicatie te laten bouwen die aansluit bij de gewenste Woerdense praktijk. Deze applicatie heeft de naam Cumulus gekregen. Cumulus moet – in tegenstelling tot GWS4All - niet alleen de administratieve proces in het Sociaal Domein ondersteunen, maar ook het concept van de 'Inwonercloud' mogelijk maken[19].

Voor het ontwikkelen van nieuwe software geldt het beginsel 'Privacy by design'. Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht wordt besteed aan privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Daarnaast wordt gestreefd naar dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt (alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.) Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

Privacy by design draagt ook bij aan ons organisatiebelang. Wanneer privacy risico's van een product of dienst niet in een vroegtijdig stadium worden onderkend, maar pas als de ontwikkeling ervan al een eind is gevorderd, dan is de kans groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn.

Om aanpassingen achteraf te voorkomen, is in het (scrum) ontwikkelproject van Cumulus bij alle tussentijdse opleveringen van de sprints een externe deskundige betrokken, die toeziet op o.a. privacy verhogende maatregelen en dataminimalisatie.

***Auditnormen opgesteld Cumulus***

Daarnaast zijn er auditnormen opgesteld voor Cumulus voor wat betreft DigiD, Secure Software Development en Privacy. In feite gaat het daarbij om een aanvullend programma van eisen op het gebied van informatieveiligheid en privacy.

Eisen ten aanzien van DigiD zijn bijvoorbeeld:

- *Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.*
- *Penetratietests worden periodiek uitgevoerd.*
- *Vulnerability assessments (security scans) worden periodiek uitgevoerd.*
- *Policy compliance checks worden periodiek uitgevoerd.*

Eisen ten aanzien van Secure Software Development zijn bijvoorbeeld:

- *Beveiliging van mobile code.*
- *Sessie versleuteling.*
- *Vaststellen identiteit van een externe c.q. interne gebruiker.*
- *Functiescheiding.*
- *Least Privilege.*
- *Registreren van Unsuccessful Login Attempts.*

Eisen ten aanzien van privacy zijn bijvoorbeeld:

- *Persoonsgegevens worden alleen verzameld en verwerkt voor vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden en worden niet verder verwerkt voor andere doelen die hiermee onverenigbaar zijn.*
- *Interne gedragscode voor medewerkers*
- *Noodzakelijkheid en limitering van verzamelen en gebruik van gegevens. De verzameling en verwerking van persoonsgegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. Minimalistisch gegevensgebruik is het uitgangspunt. Identificatie en traceerbaarheid van het individu duurt niet langer dan strikt noodzakelijk is om het doel te bereiken.*

[19] In dit kader kan hierbij worden aangetekend, dat de opvatting dat 'onze privacy gered is als iedereen maar controle heeft over zijn eigen gegevens' niet onomstreden is. Zie o.m. van Evgeny Morozov: 'The Net Delusion, The Dark Side of Internet Freedom' en 'To Save Everything, Click Here'.

## 6.5 Bijlage Advies Cameratoezicht

### Wanneer kan er gebruik worden gemaakt van cameratoezicht?

Cameratoezicht ondersteunt de aanpak van tijdelijke, maar hardnekkige overlast door hangjongeren, drugsdealers, straatrovers en zakkenrollers. Op cameratoezicht is de Wet bescherming persoonsgegevens (Wbp) van toepassing zodra personen herkenbaar in beeld komen.

### Cameratoezicht op openbare plaatsen

De overheid mag gebruikmaken van cameratoezicht op openbare plaatsen, zoals bij uitgaanscentra. Dit mag alleen als het nodig is voor:

1. de handhaving van de openbare orde;
2. de verkeersveiligheid;
3. de opsporing van strafbare feiten;
4. als andere maatregelen niet voldoende zijn gebleken.

### Flexibel cameratoezicht in gemeenten

Gemeenten mogen mobiele camera's inzetten om de openbare orde te bewaken. Gemeenten bepalen zelf welke vorm van cameratoezicht zij inzetten. Dit kan vast of flexibel cameratoezicht zijn of een combinatie van beide soorten toezicht.

Voordelen flexibel cameratoezicht:

- Inzetbaar voor bestrijding van overlast die zich verplaatst.
- Levert tijdwinst op, doordat gemeenten geen vaste camera's meer hoeven te verplaatsen. Daarvoor is steeds een aparte aanvraag nodig.

### Cameratoezicht op openbare plaatsen

Gemeenten mogen camera's op openbare plaatsen hangen als dat noodzakelijk is om de openbare orde te handhaven. Er gelden wel enkele voorwaarden voor het cameratoezicht door gemeenten.

### Voorwaarden cameratoezicht gemeente

Belangrijke voorwaarden zijn:

- Andere maatregelen zijn niet voldoende gebleken om de openbare orde te handhaven.
- De inzet van camera's staat niet op zichzelf, maar gebeurt in combinatie met andere maatregelen, zoals (betere) straatverlichting of toezicht op straat.
- De gemeente moet mensen informeren over het cameratoezicht, bijvoorbeeld met bordjes.
- Nemen de camera's ook geluid op? Of worden er op een andere manier geluidsopnames gemaakt, dan moet de gemeente mensen daarover ook informeren.
- De gemeente mag de camerabeelden niet langer dan 4 weken bewaren.

### Wettelijk kader

Publiek uitkijken van camerabeelden is gebaseerd op de wettelijke taak van de (lokale) overheid om de openbare orde te handhaven. De doelstelling van het publieke cameratoezicht is primair gebaseerd op artikel 151c van de Gemeentewet, de Politiewet en de Wet politiegegevens.

### Gemeentewet 151c: Handhaven van de openbare orde

In artikel 151c van de Gemeentewet is bepaald dat bij de toepassing van gemeentelijk cameratoezicht het doel het handhaven van de openbare orde is. Hieronder valt ook de algemene bestuurlijke voorkoming van strafbare feiten die invloed hebben op de orde en rust in de gemeentelijke samenleving.

### Aanpassing artikel 151c Gemeentewet sinds 1 juli 2016

Sinds 1 juli 2016 is de Gemeentewet aangaande cameratoezicht aangepast. Deze wijziging betekent dat 'vast' cameratoezicht vervangen is door 'cameratoezicht'. Daarnaast zijn twee nieuwe leden ingevoegd.

### Artikel 3 Politiewet

Bij cameratoezicht is artikel 3 de grondslag voor het toepassen van flexibel cameratoezicht (o.a. onvoorziene ordeverstoringen of (de vrees voor) ordeverstoringen van tijdelijke aard, bijvoorbeeld bij een risicowedstrijd in het betaalde voetbal). De algemene politietaak om, in ondergeschiktheid van het bevoegde gezag en in overeenstemming met de geldende rechtsregels, te zorgen voor de daadwerkelijke handhaving van de rechtsorde, vormt de legitieme basis.

### Artikel 13 Politiewet: Driehoeksoverleg

Artikel 13 van de Politiewet verwijst naar het reguliere driehoeksoverleg. Conform artikel 151c van de Gemeentewet kan het driehoeksoverleg een periode vaststellen waarin, in het belang van de handhaving van de openbare orde, daadwerkelijk gebruik van de camera's plaatsvindt en de met de camera's gemaakte beelden in elk geval rechtstreeks worden bekeken.

### Wet politiegegevens

Op grond van artikel 151c lid 3 van de Gemeentewet is de operationele regie bij cameratoezicht in handen gelegd van de politie. Ondanks dat de politie verantwoordelijk is voor de operationele regie van cameratoezicht, kunnen camerabeelden ook door andere personen dan politiefunctionarissen (bijvoorbeeld beveiligingspersoneel) worden uitgekeken.

### Mobiel, flexibel, dynamisch, tijdelijk cameratoezicht

Om begripsverwarring tegen te gaan en om cameratoezicht eenduidig te verankeren in de wet, is in het nieuwe artikel 151c van de Gemeentewet onder andere de term 'vast' cameratoezicht verdwenen. Hiermee volgt de wetgever de praktijk om alle vormen van cameratoezicht en de voorwaarden die daaraan verbonden zijn te verankeren in de wet.

## 6.6 Bijlage Proces Datalekken