Rekenkameronderzoek naar informatiebeveiliging en privacy Achtkarspelen en Tytsjerksteradiel

Rekenkameronderzoek 2018 naar informatiebeveiliging en privacy

Achtkarspelen en Tytsjerksteradiel

Rekenkamercommissies Achtkarspelen en Tytsjerksteradiel

Bevindingenonderzoek en advisering aan rekenkamercommissies:

drs. E.J.M. (Etienne) Lemmens, Prae Advies en onderzoek, Utrecht

8 april 2019

Colofon

Rekenkamercommissies Achtkarspelen en Tytsjerksteradiel

De rekenkamercommissies van Achtkarspelen en Tytsjerksteradiel willen met hun werkzaamheden bijdragen aan de kwaliteit van het lokale bestuur in de gemeenten Achtkarspelen en Tytsjerksteradiel, aan de transparantie van het gemeentelijke handelen en de versterking van de publieke verantwoording daarover. De commissies doen dat door de doeltreffendheid, de doelmatigheid en de rechtmatigheid van het door de gemeenten gevoerde beleid en bestuur te onderzoeken en de gemeenteraden hierover te rapporteren en te adviseren.

De commissies hebben een onafhankelijke positie binnen de gemeenten. Zij bestaan uit externe leden, die geen binding hebben met het gemeentelijke apparaat en een ambtelijk secretaris.
Sinds 1 januari 2015 vormen de beide rekenkamercommissies een personele unie met dezelfde leden.
Nadere informatie vindt u op de websites van de gemeenteraden van de beide gemeenten:
www.raad-achtkarspelen.nl/Wie is wie/Rekenkamercommissie (RKC)
www.raad.t-diel.nl/Wie is wie/Rekenkamercommissie

Samenstelling

A. Visser, voorzitter
H.S. Halbersma, lid
J.P.M. Vervoort, lid
J. Westinga, lid
W. Zuurbier, lid tot 1 januari 2019
R. de Vries-Mulder, ambtelijk secretaris rekenkamercommissie Achtkarspelen
A. Dam, ambtelijk secretaris rekenkamercommissie Tytsjerksteradiel

Contact

Rekenkamercommissie Achtkarspelen
Postbus 2
9285 ZV Buitenpost
raadsgriffie@achtkarspelen.nl
0511 - 54 86 98

Rekenkamercommissie Tytsjerksteradiel
Postbus 3
9250 AA Burgum
griffie@t-diel.nl
0511 - 46 09 32

Inhoud

Bestuurlijk rapport

Rapport van bevindingen

Lijst van afbeeldingen

Voorwoord

Informatiebeveiliging en privacy spelen een steeds grotere rol. In zijn roman '1984' schetst George Orwell een somber beeld van een alles wetende overheid. Hij zat er, behalve het jaartal, niet ver naast lijkt het soms.

Die alles wetende overheid is gelukkig wel in staat met wetgeving als de AVG (de Algemene verordening Gegevensbescherming) en andere maatregelen daar weer paal en perk aan te stellen. En is verplicht daarom zelf het goede voorbeeld te geven! Wat lastig genoeg is met alle razendsnelle ontwikkelingen en nieuwe bedreigingen.

Rekenkamers hebben de afgelopen jaren diverse onderzoeken gedaan. Trots melden zij dat ze met hulp van ethische hackers tot in het postbakje van de burgemeester zijn gekomen.

En dan? De directeur van de Rotterdamse rekenkamer Paul Hofstra gaf in een lezing een voorbeeld. "Alle maatregelen van het normenkader waren afgevinkt, de zaak was technisch 100% op orde, maar toch kwamen we binnen." De meeste incidenten komen voort uit onbewust handelen. Hofstra: "Investeer vooral in alertheid bij alle medewerkers die met informatie en burgers omgaan".

Veilig omgaan met informatie is toch vooral mensenwerk.

Wij hebben er daarom voor gekozen om 'breed' te praten met bestuurders en medewerkers, om inzicht te krijgen, ook in hun alertheid. Hackerstesten hebben we achterwege gelaten, dat moet u vooral zelf (laten) doen. En ervan te leren.

Natuurlijk hebben we ook gekeken naar de interne organisatie en de (technische) maatregelen. En die zijn nog niet op het gewenste niveau. U loopt risico's. Er is gelukkig een breed besef dat er hard aan gewerkt moet worden.

We kunnen nu twee dingen doen: de gemeenten op de vingers tikken omdat het nog niet op orde is of ze een duwtje in de rug geven. Ga vooral door, maar wel beter en sneller.

We kiezen voor het laatste. Onverlet dat er nog veel moet gebeuren. Doe dat meer planmatig en met voldoende middelen. It is mei sizzen net te dwaan.

Het onderwerp is meer dan een zaak van bedrijfsvoering. Het raakt een maatschappelijk belang en raakt daarmee ook de raden. Uw rol is belangrijk, maak als raden goede afspraken met de colleges over de wijze waarop u de voortgang kunt volgen.

Met dit rapport willen we u daar handvatten voor geven.

Bestuurlijk rapport

Dit bestuurlijk rapport is gericht aan de raad, het is zelfstandig leesbaar, zonder kennis te moeten nemen van het verslag van bevindingen, dat overigens wel is meegezonden. Zo is het voor de lezer wel mogelijk om conclusies en aanbevelingen ook zelf te kunnen herleiden.

Het bestuurlijk rapport bestaat uit vijf hoofdstukken, geschreven door en onder de verantwoordelijkheid van de twee rekenkamercommissies. Het adviesbureau Prae Advies en onderzoek heeft de rekenkamercommissies over het bestuurlijke rapport geadviseerd. De rekenkamercommissies hebben zich gebaseerd op de rapportage van bevindingen van Prae Advies en onderzoek.

Na een inleiding over de relevantie van het onderwerp gaan we in hoofdstuk 2 in op de doelstelling en vragen die in dit onderzoek centraal staan. Ook wordt hier ingegaan op de beleidscontext van informatiebeveiliging en privacy bij gemeenten. In hoofdstuk 3 behandelen we kort de aanpak van het onderzoek. Een samenvatting van de bevindingen en conclusies komen in hoofdstuk 4 aan bod en de aanbevelingen voor de raden en aansporingen voor de gemeentelijke organisaties in hoofdstuk 5.

Diverse afbeeldingen zijn opgenomen ter verduidelijking en ter illustratie.

1 Inleiding

Aanleiding: Belang van digitalisering neemt toe en daarmee ook de risico's

Door de toenemende digitalisering, cyberaanvallen en het gebruik van sociale media en berichtendiensten is informatieveiligheid een steeds relevanter thema voor gemeenten om actief op te sturen en op te monitoren. Beveiligingsincidenten kunnen immers grote gevolgen hebben voor het schenden van vertrouwelijkheid van informatie inclusief de privacy van burgers en medewerkers. Ook kan de veiligheid in het geding zijn door het compromitteren van de integriteit en beschikbaarheid van informatie. Data kunnen niet alleen worden gestolen of openbaar gemaakt maar ook vervalst, veranderd, vernietigd of misbruikt worden. Tot slot kunnen cyberaanvallen de beschikbaarheid en continuïteit van dienstverlening van gemeenten aantasten. Al deze verschillende vormen van inbreuk op de informatieveiligheid kunnen grote impact hebben op de reputatie, financiën, of operationele processen van een gemeente. En op burgers. Informatieveiligheid werd tot dusver vaak gezien als een voornamelijk technisch probleem. Nu de maatschappelijke relevantie toeneemt, hebben recentelijk hebben veel gemeenten en gemeentelijke rekenkamer(commissie)s nader onderzoek uitgevoerd naar de stand van de informatieveiligheid en de controlerende rol van het bestuur.

Probleemstelling: Hoe krijgen colleges en raden voldoende zicht om te sturen op informatieveiligheid

Het is van belang om een goed inzicht te krijgen hoe de gemeenten Achtkarspelen en Tytsjerksteradiel op het punt van de informatieveiligheid (vanuit verschillende invalshoeken) voldoen aan wet- en regelgeving en algemeen geldende eisen rond informatieveiligheid. Omdat informatieveiligheid steeds meer van een technisch naar een maatschappelijk vraagstuk verschuift, is het logisch dat ook de aandacht bij de volksvertegenwoordigers voor dit onderwerp toeneemt. Tegelijkertijd is het een zeer specifiek onderwerp waarbij het de vraag is op welke wijze de raden in staat worden gesteld zich een beeld en een oordeel te vormen over hoe het ervoor staat in de eigen gemeente.

Achtergrond/toegevoegde waarde van het onderzoek

Het is in onze visie van belang dat de raden op logische momenten worden voorzien van de juiste informatie om hun kaderstellende en controlerende rol te kunnen uitvoeren. Het domein van informatieveiligheid is daarbij zo breed en vaak zo specialistisch dat daarbij een juist niveau en reikwijdte moeten worden gekozen om de raden in stelling te kunnen brengen.

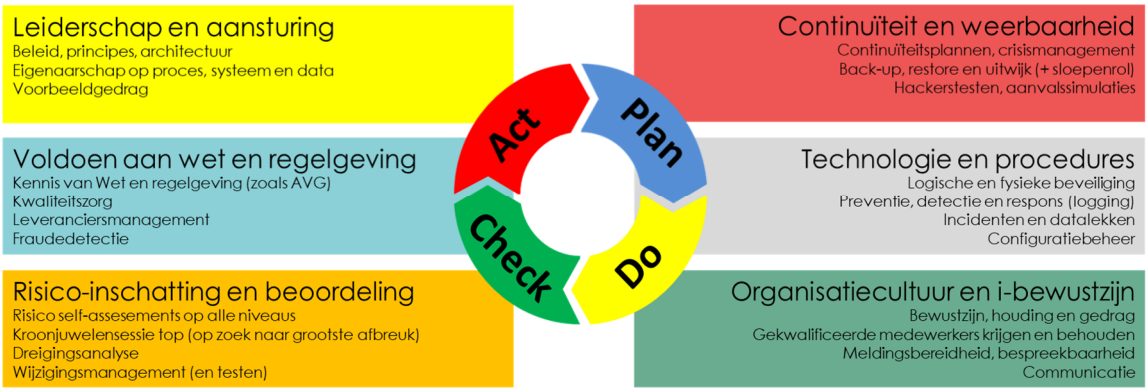
Met ingang van mei 2018 is de Algemene Verordening Gegevensbescherming van kracht geworden, met als doel persoonsgegevens beter te beschermen en die bescherming in de gehele EU gelijk te trekken. Organisaties moeten (nog) duidelijk(er) maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data worden bewaard. Ook moeten ze burgers desgevraagd inzage geven in de opgeslagen data. Voor organisaties betekent dit een extra inspanning om de informatieveiligheid en gegevensbescherming op het gewenste niveau te brengen.

Normenkader, diverse invalshoeken spelen een rol

De rekenkamercommissies hanteren als globaal toetsingskader de onderstaande (zes) invalshoeken, aspecten die in totaal het domein 'informatieveiligheid' afdekken. Mede om aan te geven dat bij informatiebeveiliging niet de technische dimensie dominant is, maar dat het een domein betreft met meerdere gelijkwaardige dimensies. Van organisatorische maatregelen tot en met bewustzijn en cultuur. Deze zes invalshoeken worden wereldwijd (ISO) erkend als toetssteen voor een volwassen uitvoering van informatiebeveiligingsbeleid.

- *Leiderschap en aansturing (governance)*
- *Compliance, voldoen aan wet en regelgeving*
- *Risico-inschatting en -beoordeling*
- *Continuïteit en weerbaarheid*
- *Technologie en procedures*
- *Organisatiecultuur en i-bewustzijn*

Afbeelding 1 Globaal normenkader



Een toets op de verschillende invalshoeken op het terrein van informatieveiligheid geeft een beeld van de volwassenheid die de organisatie kenschetst. Maar dat is nog niet genoeg, er moet vooral ook een houding aanwezig zijn om constant te willen leren en bij te sturen. Plan do check act.

Het onderzoeksbureau heeft deze invalshoeken uitgewerkt in onderzoeksvragen en in een normenkader (hoofdstuk 2 en bijlage 3), dit ook op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). In de BIG staan de feitelijke veldnormen waaraan een gemeente (minimaal) zou moeten voldoen. In de BIG zijn ook weer de 6 bovenstaande invalshoeken terug te vinden. Ook geldt uiteraard wetgeving als de AVG.

Peildatum is 1 december 2018

Het beleidsveld informatiebeveiliging en privacy is sterk in beweging bij de gemeenten. Dat is terecht, alleen al gezien de toenemende bedreigingen vanuit een turbulente omgeving. Dat heeft consequenties voor de resultaten van het onderzoek. Het onderzoek betreft een momentopname vanwege de autonome dynamiek van het beleidsveld. Wellicht ook al door de aandacht die een rekenkameronderzoek genereert (‘voorwerking’).

Dat is onontkoombaar, maar maakt de analyse en aanbevelingen van de rekenkamercommissies niet minder urgent. De bevindingen moeten worden gelezen als de stand op 1 december 2018. Tijdens de fase van hoor en wederhoor hebben de gemeenten beschreven alweer stappen te hebben gemaakt. Dat beoordelen wij als positief, het onderwerp staat op de agenda. Daarom ook is een aantal aanbevelingen verwoord als aansporingen, aansporingen om door te gaan met de ingezette maatregelen.

2 Doelstelling, context en onderzoeksvragen

2.1 Doelstelling

Doel van het onderzoek is inzicht te verkrijgen in de stand van de informatiebeveiliging en gegevensbescherming bij de gemeenten Achtkarspelen en Tytsjerksteradiel en de wijze waarop de raden in staat worden gesteld dit periodiek te controleren. Hieronder gaan we eerst in op de context van informatiebeveiliging en privacybescherming bij gemeenten.

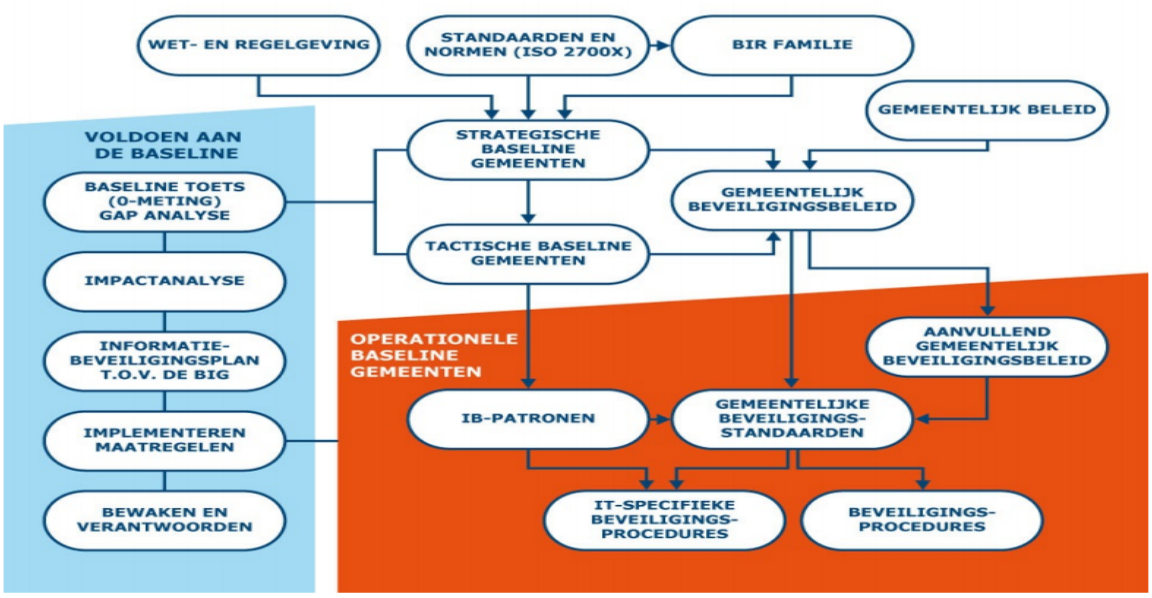
2.2 Context: wat speelt er rond informatiebeveiliging bij gemeenten?

Gemeenten hebben in 2013 afgesproken te voldoen aan de maatregelen uit de Baseline Informatiebeveiliging Gemeenten (BIG). Daar is geen deadline voor gesteld, verwacht wordt dat gemeenten daar naartoe werken. De BIG bestaat uit een strategische variant, met richtlijnen over de inrichting van het beleid en de verantwoordelijkheden die belegd moeten worden bij bestuur en management, ook governance genoemd. De BIG kent ook een tactische variant, met een grote hoeveelheid maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het minimumniveau van de BIG te voldoen.

In onderstaande afbeelding 2 is de huidige context van het gemeentelijk informatiebeveiligingsbeleid weergegeven. Centraal staan de strategische en tactische baseline gemeenten (BIG), als onderdeel van het geheel aan baselines voor de overheid (de BIR-familie). In de BIG is afgesproken dat het informatiebeveiligingsbeleid twee- of driejaarlijks wordt geüpdatet, met behulp van een GAP-analyse. Dat wil zeggen een toets om te bepalen in hoeverre de beveiligingssituatie van de gemeente voldoet aan de BIG. Daarnaast kunnen de gemeenten eigen beveiligingsbeleid formuleren. Op basis daarvan wordt jaarlijks een informatiebeveiligingsplan opgesteld voor de te nemen maatregelen. Uiteindelijk moeten deze stappen leiden tot specifieke beveiligingsstandaarden en algemene en IT-gerelateerde procedures. Belangrijk is dat het informatiebeveiligingsbeleid niet alleen een zaak van ICT is. Afgesproken is dat het lijnmanagement bij de analyses en de maatregelen betrokken wordt en dat medewerkers zich bewust zijn van de procedures en afspraken.

De BIG wordt in 2020 geüpdatet met de BIO (Baseline Informatiebeveiliging Overheid). Deze is onder andere meer gericht op risicomanagement. Tevens is er de ENSIA (Eenduidige Normatiek Single Information Audit), deze bundelt de verplichte audits en assessments op informatiebeveiliging en privacy in een verticale verantwoording richting landelijke toezichthouders en in een horizontale verantwoording richting de gemeenteraden. De richtlijnen uit de BIO en de rapportagevereisten van ENSIA worden in 2020 op elkaar afgestemd.

Afbeelding 2. Context gemeentelijk informatiebeveiligingsbeleid.



Bron: Informatiebeveiligingsdienst Gemeenten (IBD)

2.3 Context: wat speelt er rond gegevensbescherming bij gemeenten?

Voor de bescherming van persoonsgegevens is op 25 mei 2016 de opvolger van de Wet Bescherming Persoonsgegevens van kracht geworden, de Algemene Verordening Gegevensbescherming (AVG, ook bekend als General Data Protection Regulation, GDPR). Daarmee is de privacywetgeving in de gehele EU geharmoniseerd. Overheden en bedrijven kregen tot 25 mei 2018 de tijd zich daarop voor te bereiden. Ongeveer 80-85% van de maatregelen zijn dezelfde als onder de WBP. Nieuw is onder andere dat gemeenten een functionaris gegevensbescherming (FG) als adviseur en controleur moeten aanstellen. Verder moeten gemeenten een privacyverklaring publiceren, waarin zij in begrijpelijke taal uitleggen hoe zij omgaan met persoonsgegevens. Verder moeten zij een verwerkingsregister opstellen, waarin zij alle processen waarin persoonsgegevens worden verwerkt opnemen, en verwerkersovereenkomsten afsluiten met partijen die gegevens voor of namens de gemeente verwerken. Ook moeten gemeenten op bijzonder privacygevoelige processen Data Protection Impact Assessments (DPIA) toepassen, om op voorhand de risico's te inventariseren die de verwerking van persoonsgegevens met zich meebrengt.

2.4 De onderzoeksvragen

In deze context luiden de centrale onderzoeksvragen van de rekenkamercommissies als volgt:

---

(1) Voldoet de beleidsuitvoering van de gemeenten Achtkarspelen en Tytsjerksteradiel ten aanzien van informatieveiligheid en privacywetgeving, vastgelegd in beleid, kaders en procedures aan gestelde (wettelijke) eisen en worden ze (ook in houding en gedrag) gehandhaafd?

(2) Worden de raden in staat gesteld dit periodiek te controleren?

Afbeelding 3. Dreigingsbeeld en prioriteiten 2019-2020. (bron IBD)

Deze onderzoekvragen zijn naar deelvragen uitgewerkt in de volgende tabel

Tabel 1. Onderzoeksvragen in deelvragen uitgewerkt
1. Sturen de colleges van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)? Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het informatiebeveiligingsbeleid uit?
2. Hebben de gemeenten de risico's op informatiebeveiliging benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden?
3. Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen?
4. Hoe ver zijn de gemeenten gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het privacybeleid uit?
5. Kennen de gemeenten de leveranciers en partners waarmee ze samenwerken en toetsen zij hen op informatieveiligheidsaspecten, en zo ja hoe? Zijn de gemeenten transparant over het informatiebeveiligingsbeleid richting de ketenpartners?
6. Rapporteren en bespreken de organisaties het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (colleges en raden)?
7. Wat is de status van de aansluiting van de gemeenten bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?
8. Voldoet de wijze waarop de gemeenten de informatiestroom in processen en applicaties organiseren aan de vereisten op het gebied van informatiebeveiliging en privacy? Zijn de autorisaties, wie van de medewerkers bij welke informatie moet of kan, adequaat geregeld?
9. Wordt jaarlijks getoetst of de organisaties in control zijn op het gebied van informatieveiligheid via peer reviews, audits, self assessments (zelf tests) of pen-testen? Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weten de organisaties hoe te handelen bij een (ernstig) informatieveiligheid incident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?
10. Op welke wijze wordt aandacht besteed aan de bevordering van awareness bij medewerkers van de gemeenten? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houden de gemeenten kennis vast en bouwen zij hierop voort?

In de bevindingenrapportage worden deze deelvragen uitgewerkt en getoetst aan normen (bijlage 5)

3 Aanpak van het onderzoek

Voor dit onderzoek zijn door de rekenkamercommissies achtereenvolgens de volgende stappen gezet:

Startbijeenkomst, inclusief groepsgesprek met raadsleden op 11 juli 2018
In deze startbijeenkomst is de onderzoeksopzet gepresenteerd aan raadsleden en ambtenaren. Tevens zijn twee groepsgesprekken met raadsleden van de twee gemeenten gehouden om verwachtingen ten aanzien van het onderzoek te inventariseren.

Dataverzameling: deskresearch en interviews
In de periode augustus tot en met oktober 2018 zijn documenten op informatiebeveiligings- en privacybeleid bestudeerd en geanalyseerd. Een overzicht van de documenten is opgenomen in bijlage 4. De informatie uit de deskresearch vormde de input voor de interviews met ambtenaren, management en portefeuillehouders. Een lijst met respondenten is ook opgenomen in bijlage 4.

Twee casestudies
In november 2018 zijn twee processen waarin de gemeente persoonsgegevens verwerkt nader bestudeerd. De twee processen zijn een aanvraag uitkering in het kader van de Participatiewet en het indienen van een klacht in het kader van de leefomgeving. Onderzocht is onder andere welke (bijzondere) persoonsgegevens geregistreerd worden, wie geautoriseerd zijn de gegevens in te zien en/of te bewerken, met welke externe partijen deze gedeeld worden en welke gevoeligheden de gegevens hebben. De analyse van de casestudies is in bijlage 3 opgenomen.

Werkconferentie met raadsleden op 4 oktober 2018
Op de werkconferentie zijn de voorlopige onderzoeksresultaten gepresenteerd aan leden van de twee gemeenteraden. Ook is ingegaan op de wijze waarop de raden worden geïnformeerd over informatiebeveiliging en privacy en welke wijzigingen ENSIA (eenduidige normatiek single information audit) in 2019 daarop zal aanbrengen. In een interactieve sessie met de raadsleden is geïnventariseerd waarop en wanneer de raden het liefst geïnformeerd willen worden op de twee terreinen.

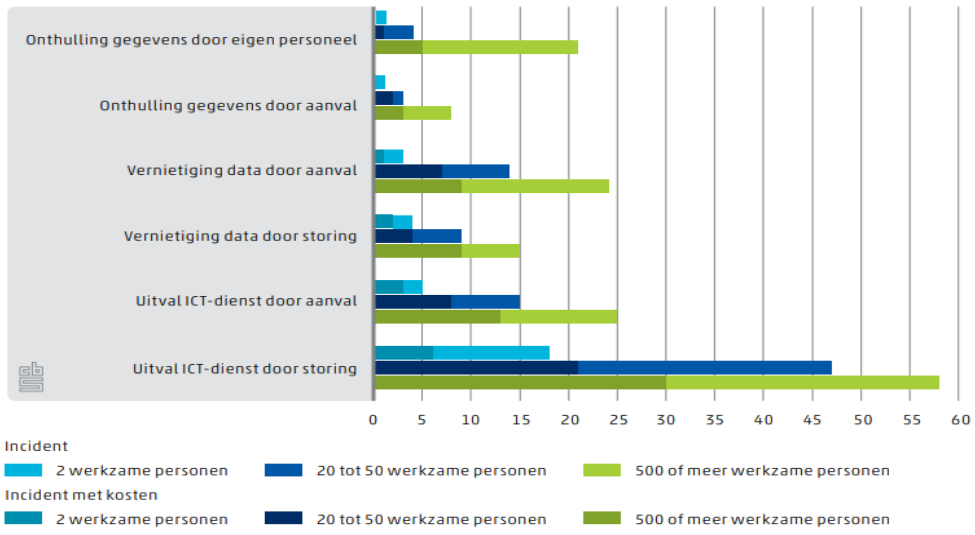
Analyse en opstellen conceptrapport van (voorlopige) bevindingen
In de periode december 2018 – januari 2019 is op basis van het onderzoek een conceptrapport opgesteld waarin de voorlopige bevindingen zijn gepresenteerd.

Waarderende sessie met stakeholders op 16 januari 2019
In een zogenaamde waarderende sessie zijn de in het onderzoek betrokken ambtenaren en bestuurders bijgepraat over de voorlopige bevindingen en zijn succesfactoren en conclusies samen verkend. Waar nodig heeft dat geleid tot aanpassing van de bevindingen en het conceptrapport, nog vóór het formele wederhoor en het heeft bijgedragen aan het formuleren van aanbevelingen.

Feitelijk wederhoor
Het conceptrapport is op 16 januari door de rekenkamercommissies vastgesteld en daarna voor feitelijk wederhoor naar de beide gemeentesecretarissen gezonden. Op 14 februari 2019 is hierop een reactie van de gemeente-secretarissen ontvangen.

Opstellen van het eindrapport
Op basis van de reacties is het rapport van bevindingen afgerond en in het bestuurlijk rapport samengevat en van conclusies voorzien. Op basis daarvan zijn de aanbevelingen opgesteld door de rekenkamercommissies. Het eindrapport is op 13 maart 2019 door de rekenkamercommissies vastgesteld.

Afbeelding 4. ICT-Veiligheidsincidenten Nederlandse bedrijven en daaruit voortvloeiende kosten, 2016



Bron: Cybersecuritymonitor, CBS, 2018.

4 Samenvatting en conclusies

4.1 De antwoorden op de twee hoofdvragen

(1) Voldoet de beleidsuitvoering van de gemeenten Achtkarspelen en Tytsjerksteradiel ten aanzien van informatieveiligheid en privacywetgeving, vastgelegd in beleid, kaders en procedures aan gestelde (wettelijke) eisen en worden ze (ook in houding en gedrag) gehandhaafd?

> *De rekenkamercommissies concluderen dat het **beleid actueel** is, dat cruciale **functies zijn ingevuld.** Maatregelen worden (terecht) vanuit de afweging van het risico geprioriteerd. In alle geledingen is men er zich van bewust dat informatieveiligheid en privacybescherming **hoog op de agenda** moeten. Dat bewustzijn is laat op gang gekomen. De daadwerkelijke **uitvoering** van dat beleid en de handhaving via beheersmaatregelen (als patchmanagement en logging) is **niet op het nodige niveau.** In de afgelopen periode hebben andere zaken (als de reorganisatie) invloed gehad op de urgentie en inzet maar dat mag en kan geen excuus zijn of blijven. Er is echter voldoende draagvlak om stappen te zetten. Dat is ook nodig omdat er op dit moment **te veel risico** wordt gelopen. Het is niet goed genoeg. Verder wachten nog **grote uitdagingen** doordat de bedreigingen toenemen en de verdere implementatie van de AVG en nieuwe landelijke normeringen forse inspanningen vereisen. Er is kortom werk aan de winkel!*

(2) Worden de raden in staat gesteld dit periodiek te controleren?

> *De rekenkamercommissies concluderen dat de raden **wel, maar te summier** worden ingelicht over de voortgang en de maatregelen. De raden hebben hun informatiebehoefte inmiddels uitgesproken en landelijke ontwikkelingen in het kader van de jaarrapportage geven **voldoende aanknopingspunten om** het informatieverkeer tussen de colleges en de raden in overleg **te verbeteren**. Gelet op de kritieke risico's die gemeenten en burgers lopen op dit terrein is de controlerende **rol van de raden essentieel**.*

4.2 Samenvatting van de bevindingen

In onderstaande samenvatting gaan we in op de belangrijkste punten uit de bevindingen. Deze worden conform de 6 eerdergenoemde invalshoeken gerangschikt. Ook de 10 deelvragen zijn hierin verwerkt. De invalshoeken zijn:

- *Leiderschap en sturing (governance)*
- *Compliance, voldoen aan wet en regelgeving*
- *Risico-inschatting en -beoordeling*
- *Continuïteit en weerbaarheid*
- *Technologie en procedures*
- *Organisatiecultuur en i-bewustzijn*

In afbeelding 1 (bladzijde 12) zijn deze invalshoeken op informatiebeveiliging, samen met de PDCA-cyclus weergegeven.

Bevindingen op Leiderschap en sturing

Bewust onbekwaam: doordrongen van het belang

Bewust onbekwaam is geen diskwalificatie maar (nu nog) bedoeld als compliment. Het betekent dat college en management en de organisatie zich realiseren dat er nog heel wat moet gebeuren. Het probleem onder ogen zien en willen leren. Het huidige beleid op informatiebeveiliging en privacy bij de gemeenten Achtkarspelen en Tytsjerksteradiel

is aanwezig, relatief recent vastgesteld en op een risicoanalyse en de BIG gebaseerd. De gesignaleerde risico's zijn geclassificeerd naar risico's die meteen aangepakt moeten worden, op de langere termijn aangepakt kunnen worden en (vooralsnog) geaccepteerd kunnen worden. Uit de bestudeerde stukken en de interviews blijkt dat de aandacht voor en betrokkenheid bij informatiebeveiliging laat op gang zijn gekomen, in vergelijking met andere gemeenten. De beide gemeenten zijn, ook volgens andere externe analyses, onvolledig in control op informatiebeveiliging. Begin 2018 is de volwassenheid van Achtkarspelen en Tytsjerksteradiel op ICT door een extern bureau nog als laag gekwalificeerd. De huidige bestuurlijke en ambtelijke top is (inmiddels) wel doordrongen van het belang van de onderwerpen.

Organisatorische transitie belemmert voortgang

De governance op informatiebeveiligingsbeleid is in opzet geregeld, de benodigde functies zijn toegewezen (portefeuillehouder, secretaris, Chief Information Security Officer [CISO] en de functionaris gegevensbescherming [FG]). De werking van het informatiebeveiligingsbeleid in de dagelijkse praktijk is mager en leidt niet altijd tot urgentie en acties. De onafhankelijke en controlerende positie van de CISO is niet goed geregeld, wat ten koste gaat van effectiviteit van die functie. Er zijn zorgen met betrekking tot de continuïteit en overdracht/vasthouden van de kennis. De huidige functionaris gaat minder werken en per medio 2019 met pensioen. Er is nog geen opvolging geregeld waardoor tijd voor de overdracht van dossiers en kennis als te krap wordt ervaren. Met het oog op het door de IBD geschetste dreigingsbeeld 2019-2020 (zie afbeelding 2) wordt versterking van de positie van de CISO als een van de prioriteiten aangemerkt.

De reorganisatie (en de naweeën) kost(en) veel tijd. De dienstverlening gaat door, maar veel procedures en processen staan min of meer 'on hold' tot na de reorganisatie en wachten op inventarisatie en toewijzing van de verantwoordelijken om in te vullen en te realiseren. Daardoor staat voor eerste helft van 2019 heel veel op de rol, in het kader van informatiebeveiliging en privacy, waarbij de vraag rijst of dat gezien middelen, bemensing en aanwezige kennis realistisch is. De gemeenten lopen hierop het risico achter te lopen op de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG), die in 2020 wordt vervangen door de Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Met achterstand op de implementatie van de AVG lopen de gemeenten het risico boetes opgelegd te krijgen door de Autoriteit Persoonsgegevens (AP).

Raden worden summier geïnformeerd

De gemeenteraden krijgen summier gerapporteerd over informatiebeveiliging en privacy in het kader van de P&C-cyclus, en incidenteel op problemen met ICT en informatiebeveiliging mede in het kader van de actieve informatieplicht, o.a. over datalekken. De raden krijgen naar aanleiding van audits en assessments op de applicaties rapportages aangeboden. Verder zijn er ook de commissies waar informatie met de raden wordt gedeeld.

In 2019 wordt de Eenduidige Normatiek Single Information Audit (ENSIA) volledig ingericht, onder andere om de horizontale verantwoording naar de raden toe te ondersteunen. De gemeenten hebben hiertoe reeds de eerste stappen gezet. De raden geven in de werkconferentie aan meer behoefte te hebben aan informatie op:

- Risicobewustzijn bij medewerkers, externe inhuur en de ketenpartners
- Borging van de continuïteit van de dienstverlening
- Incidenten, datalekken en de beheersmaatregelen

Bevindingen op Compliance, voldoen aan wet- en regelgeving

Implementatie van maatregelen is op gang, rapportage moet beter

Implementatie van de maatregelen op informatiebeveiliging (BIG) en privacy (AVG) is in gang, maar kan nog verder versterkt en versneld worden. De verplichte assessments en audits worden uitgevoerd en meestal meteen met succes afgerond. Een enkele keer moet binnen marges een herstelactie plaatsvinden. De samenhang, onderlinge koppeling en het interne rapportageproces kunnen beter, en daar moet het informatiemanagementsysteem op informatiebeveiliging (ISMS) op ingericht worden.

Meer inzet nodig voor analyse op privacy risico's

Een stappenplan voor de implementatie van de maatregelen in het kader van de AVG is begin 2018 opgesteld en de structuur voor de AVG staat in beginsel. Eind mei 2018 is de functie van de Functionaris Gegevensbescherming (FG) ingevuld. De privacyverklaring, onder meer over de wijze waarop de gemeente met persoonsgegevens omgaat, is gepubliceerd. De registratie en melding van incidenten en datalekken zijn opgesteld. Een standaard voor de verwerkersovereenkomsten is ontwikkeld, daarmee worden de nieuwe overeenkomsten AVG-proof opgesteld en de oude worden daarmee langzamerhand uitgefaseerd. Het verwerkingsregister, waarin alle bewerkingen van of namens de gemeenten zijn opgenomen, is nog niet volledig gevuld. Voorts is een model voor de data protection impact assessment (DPIA) opgesteld, waarmee privacygevoelige verwerkingsprocessen vooraf op risico's gecheckt kunnen worden. Eén brede DPIA is ondertussen gerealiseerd, op de jeugdzorg. Dat is een van de meest centrale en kwetsbare processen als het gaat om verwerking van (bijzondere) persoonsgegevens door de gemeente en diens partners. Er moeten nog de nodige DPIA's op gemeentelijke processen uitgevoerd worden, maar daarvoor moet eerst het verwerkingsregister volledig gevuld zijn.

Visie is nodig voor op te stellen eisen aan ICT-leveranciers

De gemeenten ontwerpen geen eigen applicaties en zijn daarvoor afhankelijk van derden. Bij de doorlichting van de AVG in juli 2018 is opgeroepen een visie op 'privacy by design' te ontwikkelen. Daarmee kunnen de gemeenten duidelijker aan de ontwerpers van de software eigen eisen stellen op het gebied van de verwerking van persoonsgegevens en efficiënter applicaties inrichten. Zo lang deze visie niet geformuleerd en geïmplementeerd is, lopen de gemeenten een risico op effectiviteit en efficiëntie.

Koppeling tussen informatiebeveiliging en privacy maatregelen beter inregelen

De koppeling tussen informatiebeveiliging en privacy moet nog goed ingeregeld worden in het beleid, daar bijvoorbeeld de AVG nog niet in het informatiebeveiligingsbeleid is ingebed. Enkele respondenten ervaren dat de inzet op informatiebeveiliging slechts beperkt is vastgelegd in processen en tijd en er meer resources nodig zijn. Daarmee lopen de gemeenten het risico niet tijdig te voldoen aan de eisen van de AVG.

Bevindingen op Risico-inschatting en -beoordeling

Informatiebeveiligingsbeleid is actueel maar aanpassingen blijven continu nodig

In 2016 zijn in het kader van de GAP- en risicoanalyse risico's op informatiebeveiliging benoemd, op fysiek en digitaal gebied. Deze zijn geprioriteerd, in overleg met het lijnmanagement. Eind 2017 is een keuze gemaakt welke risico's geaccepteerd werden. Zoals het bijhouden en vastleggen van activiteiten (als wijzigen en raadplegen) van gebruikers en beheerders van informatiesystemen (logging) dat slechts in beperkte mate gebeurt. En risico's waarop geacteerd moest worden, zoals de fysieke beveiliging van de twee gemeentelijke locaties en de centrale regeling van de toegangspassen van medewerkers en bezoekers.

De rekenkamercommissies stellen vast dat het informatiebeveiligingsbeleid en -plan in principe actueel zijn, gebaseerd op de risicoanalyse uit 2016. Er zijn evenwel ontwikkelingen die nopen tot een bijstelling van het informatiebeveiligingsbeleid. Zo zijn er de reorganisatie van de twee gemeenten en de ontwikkeling van een werkmaatschappij, waarin het grootste deel van de werkzaamheden wordt ondergebracht. Ook externe en beleidsmatige ontwikkelingen geven aanleiding tot bijstelling van het informatiebeveiligingsbeleid, zoals de introductie van ENSIA in 2018 en BIO in 2020. Voor de BIO is 2019 een overgangsjaar, waarin van de gelegenheid gebruik gemaakt kan worden om de benodigde analyses te maken en voor 2020 een nieuw en up-to-date informatiebeveiligingsbeleid en -plan te formuleren. Ondertussen is het aan te bevelen aan de slag te gaan met de bevindingen uit dit rapport.

Bevindingen op Continuïteit en weerbaarheid

Gemeenten zijn kwetsbaar bij uitval

De datacenters van Achtkarspelen en Tytsjerksteradiel zijn gekoppeld en de back-up van de beide locaties staat op een derde locatie. Bij een uitval kan de andere locatie de dienstverlening overnemen. Op de applicaties die in het primaire proces van de gemeenten draaien en landelijk worden gemonitord, is een continuïteitsplan aanwezig. Het berichtenverkeer kan snel hersteld worden en binnen 72 uur kunnen de meeste basisapplicaties weer draaien. De continuïteit van de gehele gemeentelijke dienstverlening wordt jaarlijks getest op technisch gebied. De uitwijk is nog niet organisatorisch en in de praktijk getest, door medewerkers tussen locaties te verplaatsen of thuis te laten werken.

Er is geen kader voor de bedrijfscontinuïteitsplanning of integraal continuïteitsplan aangetroffen, zoals de BIG voorschrijft. Er leven zorgen met betrekking tot de continuïteit, onder andere vanwege de juridische problemen met de softwareleverancier. Aan een oplossing wordt gewerkt, maar deze zal niet eerder dan medio 2019 zijn gerealiseerd.

De gemeenten zijn volledig aangesloten op de informatiebeveiligingsdienst gemeenten (IBD). Geconstateerd is dat hetgeen is gemeld bij de IBD geüpdatet moet worden om verzekerd te zijn van de juiste kwetsbaarheidsmeldingen. Op een paar onderdelen ontbreekt beleid of is beleid verouderd. Zo is patchmanagement, het beheer van de updates van de software, niet op orde. Dit betekent dat de organisatie hierop kwetsbaar is voor dreigingen, als niet gegarandeerd is dat noodzakelijke veiligheidsupdates tijdig worden geïnstalleerd.

Incidentopvolging is risicovol buiten kantooruren

Incidenten worden aan de helpdesk gemeld. Deze worden daar geregistreerd en indien nodig worden daarop opvolgacties ondernomen. Evenwel wordt buiten kantooruren, als de helpdesk niet bemenst is, geen opvolging gegeven aan de meldingen. Daarmee lopen de gemeenten een risico op effectiviteit.

Geen praktijktoetsen door het ontbreken van hackerstesten

De gemeenten hebben voor zover bekend tot nu toe geen (periodieke) pen-testen (hackerstesten) op de systemen laten uitvoeren door een externe partij. Hiermee kunnen kwetsbaarheden en risico's aan het licht komen waarop verbetermaatregelen getroffen kunnen worden. Wel heeft men via phishing-mails de awareness van medewerkers getest (zie hierna bij kopje 'Organisatiecultuur en i-bewustzijn'). De rekenkamercommissies hebben in dit onderzoek geen pen- of inlooptesten laten uitvoeren. Zij vinden echter wel dat deze van grote waarde kunnen zijn ter controle op een juiste uitvoering van maatregelen. Immers de *"proof of the pudding is in the eating"*.

Bevindingen op Technologie en procedures

De invoering van beleidsmaatregelen gaat te traag en daardoor zijn de gemeenten niet 'in control'

Geconstateerd wordt dat de gemeenten onvoldoende in control zijn op informatiebeveiliging. Dat oordeel wordt ondersteund door andere externe beoordelingen. Wat betreft governance is beleid geformuleerd, maar op de werkvloer ontbreekt het aan de nodige handvatten om informatiebeveiliging goed georganiseerd te krijgen. Zo zijn bijvoorbeeld in 2016 risico's op ICT geschetst, op ketenautomatisering en een versnipperde informatie architectuur, die niet of nauwelijks zijn opgepakt. Regels over hoe om te gaan met smartphones en tablets ('devices'), van de gemeente of de medewerker zelf, moeten nog grotendeels ontwikkeld worden (Bring of Choose Your own Device, BYOD of CYOD). De organisaties zijn volop in beweging door de reorganisatie van de twee gemeenten en de werkmaatschappij. Die vergt veel aandacht, tijd en energie. Maar de dienstverlening van de gemeente gaat door tijdens de reorganisatie, 'de winkel is open tijdens de verbouwing.'

Risico's door te weinig sturing op maatregelen, autorisaties en logging

Autorisaties voor de applicaties, die regelen welke functies bij welke gegevens mogen komen, zijn nog niet gekoppeld aan HRM/PSA. In lijn hiermee is geconstateerd dat niet overal de benodigde functiescheiding is aangebracht. Door het ontbreken van logging op een aantal systemen in 2017 als risico te accepteren is een goede vastlegging van en verantwoording over wie toegang heeft tot informatie en persoonsgegevens niet goed mogelijk. Dat betekent dat daar niet op gemonitord of gehandhaafd kan worden. Dat houdt een risico op onrechtmatigheid en ineffectiviteit in. Er wordt gewerkt aan een organisatiebrede oplossing. Het loggingsysteem was volgens een van de respondenten in 2017 al verouderd en het benodigde onderhoud was niet geregeld. Deze procedure heeft momenteel hoge prioriteit, maar wacht nog op voltooiing vanwege de reorganisatie. Hiermee loopt de gemeente grote risico's op effectiviteit en rechtmatigheid.

Clean desk policy is aanwezig, dat medewerkers voorschrijft documenten niet onbeheerd op hun bureaus te laten liggen en dat computerschermen met informatie afgesloten worden als iemand van zijn/haar bureau wegloopt. Op de vraag of dat wordt nageleefd zijn de reacties van respondenten wisselend.

Het managementsysteem op informatiebeveiliging (ISMS) is een instrument om het organisatieleren op informatiebeveiliging en privacy effectief en efficiënt in te richten, mede door een koppeling met een leer-cyclus, zoals de PDCA (Plan-Do-Check-Act). Het ISMS is nog niet volledig ingericht (zie onder andere §6.5) en bijgevolg nog niet in staat het organisatieleren adequaat te ondersteunen, kennis vast te houden en uit te bouwen.

Risico ten aanzien van de registratie van datalekken/incidenten en verwerkingsovereenkomsten

Er is een protocol voor het melden van beveiligingsincidenten en datalekken, maar er is nog geen automatische tool om incidenten en datalekken te registreren. Dat gebeurt nog grotendeels handmatig. Dat is een risico op het vlak van efficiëntie en effectiviteit.

In het sociaal domein wordt veel gewerkt met kleine derde partijen. De vraag of de gemeenten hierop op informatiebeveiliging en privacy volledig in control zijn, kan volgens de respondenten niet volmondig met 'ja' beantwoord worden. Dat is nog niet volledig in verwerkersovereenkomsten gedekt. Dat kan een risico op het vlak van effectiviteit en rechtmatigheid inhouden.

Raadsleden terecht onzeker over de veiligheid van hun ICT-voorzieningen

Raadsleden gaven aan risico's te ervaren bij het wachtwoordbeleid op hun tablets, omdat er geen beleid is opgesteld om bijvoorbeeld regelmatig de wachtwoorden te wijzigen. En dat ook niet gebeurt. Gelet op de mogelijk gevoelige informatie waar raadsleden over beschikken is dit een terechte waarneming.

Bevindingen op Organisatiecultuur en i-bewustzijn

Veel aandacht voor bewustwording, maar beklijven doet het nog onvoldoende

Een van de grootste risico's op informatiebeveiliging en privacy is bekendheid met en naleving van de regels en voorschriften op informatiebeveiliging en privacy. 'Awareness' of bewustzijn bij medewerkers krijgt aandacht van management, maar uit extern onderzoek blijkt dat te weinig te beklijven. Zo bleek uit een enquête begin 2018 dat veel medewerkers nog niet wisten waar ze een lek moesten melden. Uit interviews komt het beeld naar voren dat bewustwording een langzaam proces is, maar dat de richtlijnen meer en meer worden geïnternaliseerd. Enkele medewerkers geven aan dat aandacht besteden aan informatiebeveiliging en privacy tijd kost en druk oplevert. Door te weinig tijd en middelen is de werkdruk hoog en vindt een enkele medewerker de mogelijkheden om adequaat met informatiebeveiliging en privacy om te gaan te beperkt. De werkdruk in het algemeen wordt herkend door management en bestuur.

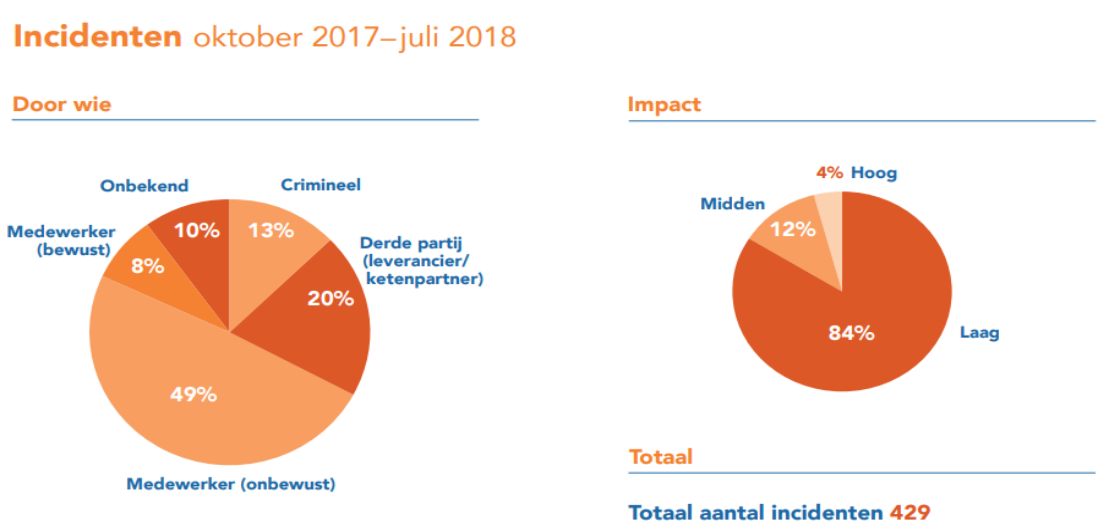
AVG bevordert bewustwording

De aandacht voor de AVG heeft zeker bijgedragen aan de bewustwording. Met name op afdelingen waar men al langer persoonsgegevens verwerkt, zoals burgerzaken, is de awareness groot. Medewerkers beginnen samenhangen met hun eigen vakgebied te zien. Tevens wordt ervaren dat het belang van informatiebeveiliging en privacy wordt gedragen door managers en teamopbouwers.

De middelen zijn aanwezig om veilig data heen en weer te sturen, via Cryptshare, maar het vergt een extra handeling. Daarom wordt het nog wel eens vergeten of medewerkers vinden het 'vervelend, het kost alleen maar tijd'. Dat levert een risico op met betrekking tot effectiviteit en rechtmatigheid.

Afbeelding 5. Incidenten oktober 2017 – juli 2018.

In de periode oktober 2017 – juli 2018 zijn de volgende beveiligingsincidenten bij de IBD gemeld.



Bron: Dreigingsbeeld 2019-2020, IBD 2018.

5 Aanbevelingen en aansporingen

In dit hoofdstuk worden de belangrijkste aanbevelingen en aansporingen per invalshoek opgenomen. Aanbevelingen betreffen voorstellen tot belangrijke (nieuwe) maatregelen.

Aansporingen zijn bedoeld als oproep aan de gemeentelijke organisaties bij een aantal urgente maatregelen de reeds ingeslagen weg met *elan* en planmatig door te zetten. Ook daar zijn essentiële maatregelen nodig ter beperking van belangrijke risico's. We bevelen de raden aan deze aansporingen met klem onder de aandacht van de colleges te brengen, opdat ze met prioriteit door de ambtelijke organisatie worden opgepakt.

Leiderschap en sturing

Aanbevelingen

1. Geef de colleges de opdracht de CISO-functionaris tijdig te vervangen en deze de rol van adviseur en controleur op het terrein van informatiebeveiliging conform de richtlijnen uit de landelijke Baseline te geven.
2. Stel voldoende middelen beschikbaar voor het door de colleges (jaarlijks) op te stellen Uitvoeringsplan Informatiebeveiliging en privacy.
3. Ga in gesprek met de colleges over wanneer en waarop de colleges de raden informeren op ontwikkelingen op informatiebeveiliging en privacy, de voortgang van het Uitvoeringsplan en mede gericht op invulling van het vormvrije deel van de landelijke ENSIA. Inspiratie kan in de uitkomsten van de werkconferentie van 4 oktober 2018 gevonden worden.
4. Verzoek de colleges halfjaarlijks over de vorderingen op de aansporingen te rapporteren en in het kader van de ENSIA-rapportage medio 2019 over de aanbevelingen te rapporteren.

Aansporingen

- Stel prioriteiten in de activiteiten en stem de technische en organisatorische maatregelen en middelen daarop meer planmatig af (via het operationeel Uitvoeringsplan).
- Wijs verantwoordelijken aan voor de verschillende processen in het kader van informatiebeveiliging en privacy.
- Bereid de organisatie en de bestuurlijke informatievoorziening voor op ENSIA in 2019 en BIO in 2020.

Compliance, voldoen aan wet en regelgeving

Aanbeveling

5. Vraag het college een visie op *privacy by design* te ontwikkelen (*zo gaan wij hiermee om*) opdat de gemeente duidelijker aan de ontwerpers van software eigen eisen kan stellen op het gebied van de verwerking van persoonsgegevens en het efficiënter de applicaties kan inrichten.

Aansporingen

- Ga door met het uitfaseren van oude verwerkersovereenkomsten en vervang die door overeenkomsten die AVG-proof zijn.
- Stel in de verwerkersovereenkomsten het gebruik van cryptshare (versleuteling) voor de uitwisseling van gegevens verplicht.

- Voer met voorrang Data Protection Impact Assessments (DPIA's) uit op alle hoog privacygevoelige verwerkingsprocessen.

Risico-inschatting en -beoordeling

Aanbeveling

6. Vraag het college zo spoedig mogelijk een nieuwe GAP-analyse (verschil tussen de norm en de stand van zaken) uit te voeren en een risicoanalyse op te stellen en voor 2020 en daarna een nieuw informatiebeveiligingsbeleid en -plan op te stellen op basis van nieuwe voorschriften (zoals de BIO).

Continuïteit en weerbaarheid

Aanbevelingen

7. Geef het college de opdracht zo spoedig mogelijk een integraal continuïteitsplan (als uitwijk) op te stellen en dit regelmatig te testen.
8. Geef het college de opdracht regelmatig inloop- en hackerstesten uit te laten voeren door ethische hackers en geef dit een plaats in bewustwordingscampagnes.

Aansporingen

- Maak gegevens up-to-date met betrekking tot aansluiting IBD.
- Beleid doorvoeren en waar nodig updaten voor de uitgifte van apparatuur (BYOD of CYOD), het patchmanagement (*essentieel*!: zorg voor de laatste versies van systeemsoftware), wachtwoordenbeleid (ook raadssystemen).
- Automatiseer de melding en registratie van incidenten/datalekken met behulp van het systeem ISMS.
- Richt het ISMS per direct in op de situatie van na de reorganisatie en met een koppeling aan de PDCA-cyclus.
- Check de fysieke beveiliging op locatie.[1]

Technologie en procedures

Aanbeveling

9. Stel in samenspraak met de colleges en de griffies een gedragscode op voor informatiebeveiliging en privacy onderwerpen die spelen voor raadsleden.

Aansporingen

- Voltooi en update de logging (*essentieel*!: na kunnen gaan van bewerkingen) op de gemeentelijke systemen.
- Breng adequate functiescheiding/autorisaties aan binnen de (digitale) processen.
- Koppel de autorisaties van systemen aan de personele registratie (HRM/PSA) en leg het daarin vast.
- Richt ISMS volledig in en koppel deze aan de leercyclus in de organisatie (PDCA).

[1] *In verband met de veiligheidsrisico's wordt hierover separaat en vertrouwelijk gerapporteerd*

Organisatiecultuur en i-bewustzijn

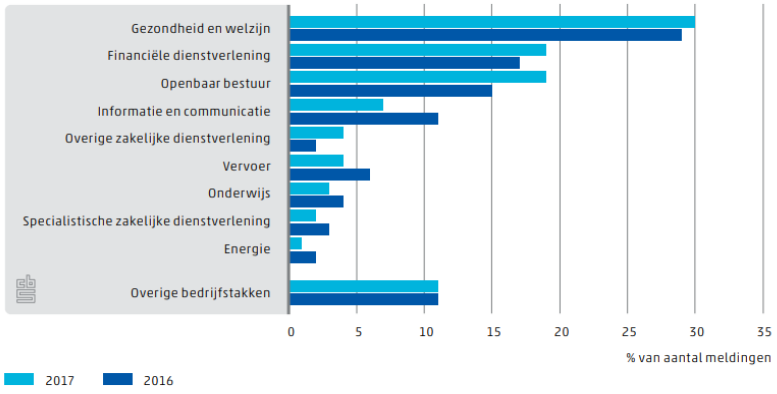
Aanbeveling

10. Geef het goede voorbeeld door een goed beveiligingsniveau van de eigen ICT-hulpmiddelen na te streven en in gedrag te borgen (zoals de beveiliging van het raadssysteem iBabs).

Aansporingen

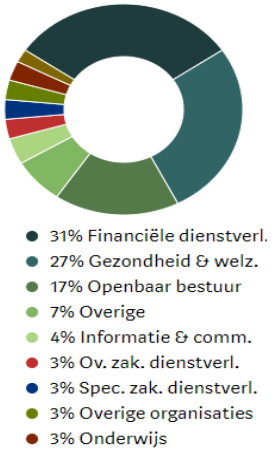
- Zet om te leren continu bewustwording op de agenda bij medewerkers, door campagnes en door het bespreken van resultaten van periodieke testen en incidenten, deel successen en falen.
- Bevorder (hiermee) een cultuur om elkaar onderling aan te spreken bij niet naleven van de richtlijnen.

Afbeelding 6. Meldingen datalekken bij de Autoriteit persoonsgegevens per bedrijfstak, 2016-2017



Bron: Cybersecuritymonitor, CBS 2018.

Afbeelding 7. Meldingen datalekken bij de Autoriteit persoonsgegevens naar sector 1e helft 2018.



Bron: Autoriteit Persoonsgegevens.

Rapport van bevindingen

De bevindingen waarop het bestuurlijk rapport is gebaseerd vindt u in dit deel: hoofdstuk 6 en de bijbehorende bijlagen. Dit rapport is geschreven door Prae Advies en onderzoek en aangepast op basis van de ambtelijke reactie van 14 maart 2019 in het kader van hoor- en wederhoor.

Informatiebeveiliging en privacy zijn moeilijke onderwerpen, met veel jargon, Engelse termen en afkortingen. Vandaar dat in bijlage 1 een verklarende woordenlijst is opgenomen. In bijlage 2 is het verslag van de werkconferentie van 4 oktober 2018 met de twee gemeenteraden opgenomen. De bevindingen van de twee casestudies vindt u in bijlage 3. In bijlage 4 is een lijst met geraadpleegde stukken en geïnterviewde personen opgenomen. Tot slot zijn in bijlage 5 de onderzoeksvragen en de normen waartegen de vragen zijn gehouden ondergebracht.

6 Verslag van bevindingen

In dit hoofdstuk worden de bevindingen van het onderzoek op de deelvragen weergegeven. Op 16 januari 2019 heeft aan het merendeel van de respondenten een informele terugkoppeling plaatsgevonden waarbij ook een doorkijkje is gegeven naar eerste conclusies, zodat de respondenten na konden gaan hoe de rekenkamercommissies de bevindingen voorlopig duidden. Na feitelijk wederhoor is dit hoofdstuk definitief door de rekenkamercommissies vastgesteld.

6.1 Sturing en commitment op informatiebeveiliging

In deze paragraaf geven we antwoord op deelvraag 1: Sturen de colleges van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)? Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het informatiebeveiligingsbeleid uit?

De colleges sturen op de afspraken in de BIG. In 2015 is door de colleges van de gemeenten Achtkarspelen en Tytsjerksteradiel besloten informatiebeveiliging in de Werkmaatschappij 8KTD onder te brengen. Het informatiebeveiligingsbeleid van de gemeenten Achtkarspelen en Tytsjerksteradiel en de Werkmaatschappij is in augustus 2016 door de colleges van de twee gemeenten vastgesteld. Doelstelling was om eind 2018 volledig aan de BIG te voldoen, maar die ambitieuze doelstelling wordt niet gehaald, zo erkent de bestuurlijke en ambtelijke top van de organisatie.

In 2015 is ook besloten tot het opstellen van een gecombineerde GAP-analyse naar de stand van zaken op informatiebeveiliging bij de twee gemeenten. De update van de GAP-analyse dateert van oktober 2016. Deze analyse op informatievoorziening en ICT is verricht met college, directie en de teamopbouwers. De afdelingshoofden geven aan niet bij de GAP-analyse of de risicoanalyse betrokken te zijn geweest, maar de CISO heeft een aantal zaken bij hen getoetst. In de update van de GAP-analyse werd gesteld dat 47% van de BIG-maatregelen volledig was geïmplementeerd, 41% deels, gepland voor 2017 staat 3% van de maatregelen en 9% is aangemerkt als geaccepteerd risico. In het informatiebeveiligingsplan 2017, vastgesteld in april 2017, staat vermeld dat deze gemeentebrede analyse niet tot op het laatste detail is uitgevoerd.

De indruk uit de bestudeerde stukken en uit de interviews is dat de aandacht voor en betrokkenheid bij informatiebeveiliging in de gemeenten Achtkarspelen en Tytsjerksteradiel relatief laat op gang is gekomen, in vergelijking met andere gemeenten. In interviews geven respondenten aan dat het vorige college ICT, informatiebeveiliging en de signalen hierover uit de organisatie heeft onderschat. Begin 2018 is de volwassenheid van de twee gemeenten op ICT door een extern bureau als laag gekwalificeerd. Colleges en management, die ook betrokken zijn geweest bij deze analyse, beginnen steeds meer interesse in het onderwerp te tonen. Geconstateerd kan worden dat momenteel het onderwerp informatiebeveiliging, samen met privacy in het kader van de AVG, gedragen wordt door de top van de organisaties. Maar een stevig actieplan om de achterstand in te lopen ontbreekt nog. Door wisselingen in de ambtelijke top is daar de kennis over informatiebeveiliging en privacy toegenomen en geeft men aan er bovenop te zitten.

De governance aan de top is goed geregeld. De portefeuilles zijn belegd en het beleid wordt, volgens de meeste respondenten, uitgedragen door colleges en management. De Chief Information Security Officer (CISO) is door de colleges van Achtkarspelen en Tytsjerksteradiel aangewezen. Deze is gepositioneerd in de werkmaatschappij. Daarbij is echter een discussie ontstaan over de invulling van de taken van de CISO. Uit de interviews blijkt dat deze door de opeenvolgende teamopbouwers in de werkmaatschappij werden toegewezen aan informatiebeheer. De CISO heeft een controlerende en toezichthoudende functie en is geen staffunctie. Hij/zij moet onafhankelijk van de lijn worden gepositioneerd. Daardoor heeft hij/zij een directe lijn met de bestuurlijke en ambtelijke top van de organisaties en kan managers vanuit die rol aanspreken. Die onduidelijkheid in de functie bestaat al sinds 2016 en dat heeft de rol en slagkracht beperkt. De indruk uit de interviews is evenwel dat de huidige CISO door de medewerkers en de bestuurlijke en ambtelijke top van de gemeenten in zijn controlerende en toezichthoudende functie wordt erkend. Er dreigt een leemte bij het aanstaande vertrek van de CISO. Er wordt nog geen opvolger gezocht.

Voor de strategische planning en tactische afstemming is het Platform Informatieveiligheid ingericht. Daarin zijn de CISO, de concerncontrollers van de beide gemeenten en de informatiemanager vertegenwoordigd. Daaronder zit het applicatiebeheerders-overleg, waarin de CISO de applicatiebeheerders over voor hen belangrijke ontwikkelingen informeert. Dat is nog een relatief jonge ontwikkeling en over de positie en bevoegdheden moeten nog afspraken gemaakt worden. Voorts is er in verband met de reorganisatie in het kader van de ICT de zogenoemde Change Advisory Board (CAB). Daarin zijn de programmamanager ICT, informatiemanagers, coördinator ICT en een expert informatiebeveiliging vertegenwoordigd. Omdat de laatstgenoemde functie niet ingevuld is, schuift de CISO als expert aan, ondanks het gegeven dat deze een controlerende functie heeft.

6.2 Risicobeheersing

In deze paragraaf gaan we in op de deelvragen 2 en 3. Hebben de gemeenten de risico's op informatiebeveiliging benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen?

In 2016 zijn in het kader van de GAP-analyse risico's op informatiebeveiliging benoemd, op fysiek en digitaal gebied. Naast algemene risico's zijn drie specifieke risico's benoemd: beheer ICT, ketenautomatisering en versnipperde informatie architectuur. Er is in december 2017 een bewuste keuze gemaakt welke risico's geaccepteerd werden, zoals een aantal technische zaken als automatische logging die slechts in beperkte mate aanwezig is en waarop geacteerd moest worden, zoals de fysieke beveiliging van de twee gemeentelijke locaties en de centrale regeling van de toegangspassen van medewerkers en bezoekers. Daarbij is al rekening gehouden met de AVG, doordat de toegangspassen geen persoonsgegevens meer bevatten, maar nummers.

De gemeenten zijn volgens externe analyses niet geheel in control op informatiebeveiliging. Volgens de SMA van begin 2018 ontbreekt het aan de 'doorvertaling van beleid naar operationele processen, beheersmaatregelen en bijbehorende procedures en instructies.' Anders geformuleerd, qua governance zijn de verantwoordelijkheden belegd en is beleid geformuleerd, maar op de werkvloer ontbreekt het aan de nodige handvatten om informatiebeveiliging goed georganiseerd te krijgen. Tevens zijn de organisaties volop in beweging door de reorganisatie van de twee gemeenten en de werkmaatschappij. Die vergt veel aandacht, tijd en energie.

Qua governance zijn de verantwoordelijkheden redelijk goed belegd, zie §6.1, maar door de reorganisatie zijn processen en projecten nog niet geheel geïnventariseerd en zijn vaak nog geen proceseigenaren aangewezen. Autorisaties en daarvan afhankelijke toegang tot informatie kunnen dan pas adequaat worden afgegeven. Mede door de keuze om automatische logging, in samenhang met het personeelssysteem, niet tot prioriteit te maken en als risico te accepteren is een goede monitoring en verantwoording over wie toegang heeft tot informatie en persoonsgegevens niet goed mogelijk (zie ook de beschrijving van de cases in bijlage 2). Het loggingsysteem houdt niet bij wat in het kader van monitoring noodzakelijk is. Het was volgens een van de respondenten in 2017 al verouderd en het benodigde onderhoud was niet geregeld. Deze procedure heeft momenteel hoge prioriteit, zo blijkt uit de interviews. Er loopt een gemeenschappelijke aanbestedingsprocedure voor een loggingsysteem en gemeenten kunnen naar aanleiding daarvan besluiten het product aan te schaffen. Dat zal waarschijnlijk op zijn vroegst in het eerste kwartaal 2019 geregeld zijn.

Op basis van het vastgestelde informatiebeveiligingsbeleid en -plan kunnen we constateren dat het beleid actueel is, gebaseerd op de risicoanalyse van 2017. Er zijn evenwel interne ontwikkelingen die nopen tot een bijstelling van het informatiebeveiligingsbeleid. Zo is er de reorganisatie van de twee gemeenten en de ontwikkeling van een werkmaatschappij met beperkte onderdelen naar een werkmaatschappij waarin het grootste deel van de werkzaamheden wordt ondergebracht. In de systemen moeten de afdelingsnamen geharmoniseerd worden om vanaf begin 2019 goed te kunnen functioneren. Sommige onderdelen moeten door een externe partij worden aangepast en dat maakt het volgens respondenten ingewikkeld. Tevens doet zich het probleem voor van een achterstand op ICT-gebied. Door software die niet voldoet en een nog lopende (gerechtelijke) procedure daarover, moest gewerkt worden met meerdere suboptimale oplossingen naast elkaar. Tot slot hebben de decentralisaties vanaf 2015 en de invoering van de AVG in 2018 veel tijd gekost. Door deze ontwikkelingen hebben de organisaties een achterstand opgelopen.

Een externe ontwikkeling die in 2019 noopt tot bijstelling van het informatiebeveiligingsbeleid is de introductie van het normenkader voor informatiebeveiliging voor de gehele overheid, de Baseline Informatiebeveiliging Overheid (BIO). Deze zal waarschijnlijk vanaf 2020 voor gemeenten de BIG gaan vervangen, 2019 zal een overgangsjaar zijn. De BIO is minder georiënteerd op maatregelen zoals de BIG met 303 afvinkbare maatregelen, en is meer gericht op risicomanagement. Ook de Eenduidige Normatiek Single Information Audit (ENSIA) is een ontwikkeling op het gebied van verantwoording waar de gemeenteraden volgend jaar mee te maken krijgen (zie daarvoor §6.5).

6.3 Implementatie AVG en commitment op privacybeleid

Hier geven we antwoord op deelvraag 4. Hoe ver zijn de gemeenten gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het privacybeleid uit?

In het kader van de AVG moesten gemeenten voor 25 mei 2018 een aantal zaken rond de bescherming van persoonsgegevens hebben geregeld. De Vereniging Nederlandse Gemeenten (VNG) heeft bij de Autoriteit Persoonsgegevens (AP) gevraagd waarop deze zou gaan handhaven. De AP gaf aan dat gemeenten in ieder geval per 25 mei 2018 een Functionaris Gegevensbescherming (FG) zouden moeten aanwijzen en er moest een implementatieplan zijn om aan de andere eisen in het kader van de AVG in 2018 te voldoen. Die eisen behelzen onder andere het aanwezig zijn van een verwerkingsregister (een overzicht van processen binnen de gemeente waarin [bijzondere] persoonsgegevens worden verwerkt), het opstellen en publiceren van een privacyverklaring, een procedure en een register voor datalekken, verwerkersovereenkomsten met derde partijen die voor de gemeenten persoonsinformatie verwerken en data protection impact assessments (DPIA) voor verwerkingsprocessen met een hoge privacygevoeligheid.

Begin 2018 is een stappenplan voor de implementatie van de AVG voor de twee gemeenten Achtkarspelen en Tytsjerksteradiel vastgesteld. Een van de medewerkers van de juridische afdeling werd als projectleider aangewezen om de implementatie van de AVG organisatorisch te begeleiden. Per 25 mei is tijdelijk een FG aangewezen en per 1 juli is de functie via externe werving ingevuld. Voorts is de FG aangesloten bij een 6-wekelijks provinciaal overleg van functionarissen gegevensbescherming.

Er is een privacyverklaring op de website gepubliceerd over de wijze waarop de gemeenten omgaan met (bijzondere) persoonsgegevens. Het verwerkingsregister is nog niet volledig gevuld. Eerst moeten alle processen waarin persoonsgegevens worden verwerkt geïnventariseerd worden, en dat verloopt traag vanwege de reorganisatie. Het verwerkingsregister moet dus verder en blijvend worden geactualiseerd. Er is een standaard verwerkersovereenkomst opgesteld. Nieuwe verwerkersovereenkomsten worden volgens dat format opgesteld. De oudere overeenkomsten worden uitgefaseerd en indien nodig opnieuw afgesloten waarbij voldaan wordt aan de AVG.

Er is een modelrapportage opgesteld voor de interne registratie van beveiligingsincidenten en datalekken en dit formulier is via de Informatiebeveiligingsdienst gemeenten (IBD) aan alle Nederlandse gemeenten als voorbeeld ter beschikking gesteld. Op het formulier staat een evaluatie en terugkoppeling over wat er met de melding is gebeurd, wat ervan geleerd kan worden en hoe het voorkomen kan worden. Er is een lijst met vragen opgesteld voor identificatie van mogelijke datalekken. Deze is op SharePoint, het intranet van de gemeenten, gepubliceerd, met uitleg en een voorbeeld.

Een model voor uitvoering van het afnemen van een DPIA is opgesteld. Door een extern bureau is zo'n assessment uitgevoerd voor de jeugdzorg, omdat daar hoog privacygevoelige verwerkingsprocessen plaatsvinden. In het verwerkingsregister moeten nog alle werkprocessen waarin persoonsgegevens worden verwerkt in beeld gebracht worden. Dat zijn er naar schatting 300. Op basis van een risicoanalyse moet nog bepaald worden welke voor een DPIA in aanmerking komen.

De AVG was nog niet ingebed in het informatiebeveiligingsbeleid, zo wordt nog in de beleidsstukken de voorloper ervan aangehaald, de Wet bescherming persoonsgegevens (Wbp). Aanpassing daarvan is in het stappenplan voor de implementatie van de AVG opgenomen, net als het opstellen van een up-to-date privacybeleid. Daarvoor is gewacht op de aanstelling van de FG, zodat gelijk advies zou kunnen worden ingewonnen. Het privacybeleid is ten tijde van deze rapportage in de laatste fase van vaststelling aanbeland. De MT's van Achtkarspelen en Tytsjerksteradiel hebben het privacybeleid vastgesteld, alleen de colleges van B&W moeten het nog definitief vaststellen en laten publiceren. Uit de ambtelijke reactie blijkt dat het privacybeleid is vastgesteld en intern en extern is gepubliceerd. Ook is een privacyreglement voor medewerkers opgesteld en in de besluitvorming opgenomen.

In juli 2018 is de stand van zaken rond de AVG doorgelicht. Volgens de respondenten zijn processen en ondersteuning aanwezig en staat de structuur voor de AVG er. Deze moet nog deels worden ingevuld. De reorganisatie maakt het evenwel soms lastig om de vraag te beantwoorden wie nu waarvoor verantwoordelijk is. Enkele respondenten ervaren dat de inzet slechts beperkt is vastgelegd in processen en tijd en er meer resources nodig zijn om aan de eisen van de AVG te voldoen.

De gemeenten werken op ICT-gebied vooral met applicaties van derden. Dat stelt eisen aan de wijze waarop de gemeenten de bescherming van persoonsgegevens adresseren. De gemeenten zijn bij de doorlichting van de AVG in juli

2018 opgeroepen een visie op 'privacy by design' te ontwikkelen. Daarmee kan de gemeente duidelijker aan de ontwerpers van de software de eigen eisen stellen op het gebied van de verwerking van persoonsgegevens.

6.4 Informatiebeveiligingsbeleid en privacy in de keten

In deze paragraaf beantwoorden we deelvraag 5. Kennen de gemeenten de leveranciers en partners waarmee ze samenwerken en toetsen zij hen op informatieveiligheidsaspecten, en zo ja hoe? Zijn de gemeenten transparant over het informatiebeveiligingsbeleid richting de ketenpartners?

De gemeenten kennen de externe leveranciers en partners waarmee gegevens worden uitgewisseld en zijn bezig deze in het kader van de AVG in het verwerkingsregister op te nemen. Er zijn verwerkersovereenkomsten gesloten, maar deze zijn nog niet allermaal gekoppeld aan het verwerkingsregister, zodat niet getoetst kan worden of ze AVG-proof zijn. De oudere verwerkersovereenkomsten faseren langzaam uit en de nieuw af te sluiten overeenkomsten worden AVG-proof opgesteld. Bij een van de overeenkomsten zijn vanuit de gemeente vraagtekens gesteld, omdat de derde partij de veiligheid van de informatie niet kon garanderen en de aansprakelijkheid bij datalekken wilde delen.

In het sociaal domein wordt veel gewerkt met kleine derde partijen. De vraag of de gemeente daarop volledig in control is, kan volgens de respondenten niet volmondig met ‘ja’ beantwoord worden. Sommige partnerorganisaties willen bijvoorbeeld geen versleutelde mail via Cryptshare ontvangen. Door externe partijen en aanbieders van diensten wordt het ervaren als een extra eis erbij.

Externe leveranciers en gebruikers van data komen alleen via een beveiligde VPN-verbinding in de systemen. De logging daarop moet nog adequaat worden ingeregeld, waardoor de gemeente hierop niet volledig in control is.

Bij de medewerkers die met (bijzondere) persoonsgegevens omgaan, is volgens respondenten aandacht voor privacyaspecten en sensitiviteit welke informatie met derden gedeeld mag worden. In principe niet meer dan strikt noodzakelijk, maar de landelijke normen in het kader van de AVG geven geen strikte aanwijzingen daarvoor zoals de BIG dat doet voor informatiebeveiliging. Er zijn wel richtlijnen opgesteld voor het sociaal domein, maar respondenten stellen dat vaak eerst ervaren moet worden wat wel en niet uitgewisseld kan worden. Het is een leerproces waarbij de FG van advies dient.

Het sociaal domein betreft lastige materie omdat er veel (bijzondere) persoonsgegevens verwerkt worden en vanwege de verschillende rollen van partijen binnen de gemeentelijke jeugd- en dorpenteams. Vandaar dat de eerste brede DPIA volgens planning is uitgevoerd voor de Jeugdwet. In het sociaal domein werd eerder veel buiten de gemeentelijke organisaties georganiseerd, met externe partijen. Volgens de gemeentesecretarissen is besloten meer naar binnen toe te organiseren, onder andere vanwege de informatiebeveiliging. De jeugdteams van Tytsjerksteradiel vallen nu nog onder een zelfstandige organisatie, deze moet de informatiebeveiliging zelf regelen. De jeugdteams van Achtkarspelen vallen onder de gemeente. De beide gemeenten gaan de teams onderbrengen in de werkmaatschappij, waarmee de gemeenten een verwerkersovereenkomst hebben afgesloten.

6.5 Rapportage

Deelvraag 6 staat in deze paragraaf centraal. Rapporteren en bespreken de organisaties het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (colleges en raden)?

Voor de management- en sturingsinformatie op informatiebeveiliging is nog geen volledig Information Security Management System (ISMS) ingericht. Een ISMS is gericht op de interne beheersing van de risico’s door de ambtelijke organisatie. In principe zou over alles met betrekking tot informatiebeveiligingsbeleid en het informatiebeveiligingsplan gerapporteerd worden met behulp van deze structuur, zoals de vorderingen op de BIG-maatregelen, de procedures en de werkinstructies op informatiebeveiliging. Voor na de reorganisatie is gekozen voor de versie van Achtkarspelen. Deze zou nog nader ingericht moeten worden op de nieuwe governance structuur van na de reorganisatie. De organisaties wegen af of ze een managementbeheersysteem voor informatiebeveiliging (ISMS) op gaan zetten of een die geïntegreerd is met een beheersysteem op financiële risico's. Voor rapportages over functioneren van informatiebeveiliging worden ENSIA en de jaarrekening ingezet.

Momenteel krijgt de CISO de incidentmeldingen en mogelijke datalekken gerapporteerd. Daarvoor hebben de CISO en FG een meldingsformulier opgesteld. De CISO bekijkt of er een melding bij de IBD gedaan moet worden en of er sprake is van een mogelijk datalek dat bij de AP gemeld moet worden. Het melden van het datalek is een verantwoordelijkheid

van de FG. Op de formulieren staan een evaluatie en terugkoppeling met wat er met de melding is gebeurd, wat ervan geleerd is en hoe het voorkomen kan worden. De conclusies en verbeter-maatregelen stuurt de CISO door naar de portefeuillehouder. De meldingen worden evenwel niet automatisch in het ISMS opgenomen.

De gemeenteraden krijgen jaarlijks in de jaarrekening gerapporteerd over informatiebeveiliging in het kader van de P&C-cyclus. Het staat volgens de gemeentesecretarissen niet hoog op de agenda bij de raden. Aangegeven wordt dat de raden naar aanleiding van audits en assessments op de applicaties rapportages krijgen aangeboden. En de raden krijgen in het kader van de actieve informatieplicht incidenteel informatie in geval van datalekken. Tevens zijn de raden geïnformeerd over de problemen met de softwareleverancier. Verder zijn er ook de commissies waar informatie met de raden wordt gedeeld.

Afbeelding 8. ENSIA, rapportage voor de horizontale en verticale verantwoording.

HORIZONTAAL		VERTICAAL		OPLEVERING
RAPPORTAGE	**ONDERWERPEN** Beleid, doelstellingen & ambities Samenvatting beeld & resultaten 2018 Belangrijkste beheersmaatregelen Meerjarenperspectief	Stelsel	Vorm	Voor datum
		SUWI	Collegeverklaring + assurancerapport	1-5 ENSIA
		DigiD	Collegeverklaring + assurancerapport	1-5 ENSIA
		BAG	Vaststelling rapportage + agendering	1-5 ENSIA
		BGT	Vaststelling rapportage + agendering	1-5 ENSIA
		BRO	Vaststelling rapportage + agendering	1-5 ENSIA
		BRP/PUN	Ondertekening uittreksel door college	14-2 RvIG & AP
JAARVERSLAG GEMEENTE				15 -7 BZK

Medio 2019 krijgen de raden voor de tweede keer verantwoordingsinformatie op basis van ENSIA (zie afbeelding 8). ENSIA is de wijze waarop de verticale en horizontale verantwoording over informatiebeveiliging en privacy gaat plaatsvinden. De CISO is de coördinator van deze verantwoordingssystematiek. Een deel van de verantwoordingsinformatie gaat de audits en assessments van de applicaties bevatten, met een verklaring door het college van B&W en een extern assurancerapport. Het andere deel wordt jaarlijks gevuld door het college met informatie over beheersmaatregelen en een meerjarenperspectief, specifiek erop gericht de gemeenteraden te informeren over de stand van zaken rond informatiebeveiliging en privacy (zie ook het verslag van de werkconferentie in bijlage 1).

6.6 Aansluiting IBD

Hier gaan we in op deelvraag 7. Wat is de status van de aansluiting van de gemeenten bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?

De IBD krijgt landelijk meldingen van mogelijke dreigingen op hard- en software binnen en zet deze door naar de gemeenten die aangesloten zijn. Indien nodig kunnen deze daarop actie ondernemen. Dat kunnen algemene meldingen zijn, zoals virusaanvallen, of meldingen van vertrouwelijke aard, zoals potentiële datalekken. Voor de aansluiting bij de IBD moeten vier stappen gerealiseerd zijn:

1-2. Benoeming van algemene en vertrouwde contactpersonen
3. Doorgeven van in gebruik zijnde IP-adressen en URL's aan IBD
4. Doorgeven van bij de gemeente in gebruik zijnde hard- en software (de zogenoemde ICT-foto).

Aansluiting op de IBD is overigens geen maatregel in de BIG. Aansluiting is wel aangeraden in de resolutie die de gemeenten in VNG-verband in 2013 hebben aangenomen.

De gemeenten Achtkarspelen en Tytsjerksteradiel zijn volledig aangesloten bij de IBD. Er zijn functionarissen aangewezen die de rol van algemeen en vertrouwde contactpersonen op informatiebeveiliging (ACIB en VCIB) vervullen. Aandachtspunt is dat een van de twee VCIB's door gezondheidsproblemen deze rol niet meer vervult. De andere VCIB,

namelijk de CISO, gaat vanaf december 2018 terug in werktijd. Door de reorganisatie en discussie over de plaats van de CISO (zie §6.1) is daar op moment van rapportage nog geen opvolging voor.

Alle stappen voor de aansluiting bij de IBD zijn door de gemeenten gezet, hetgeen betekent dat de gemeenten kwetsbaarheidsmeldingen van de IBD krijgen die toegesneden zijn op de soft- en hardware die bij de gemeente voorhanden is. Het is een structurele taak om de registratie bij de IBD van de in gebruik zijnde IP-adressen, URL's, hard- en software up-to-date te houden. Deze update is op korte termijn noodzakelijk, teneinde gegarandeerd te zijn van de juiste meldingen.

6.7 Processen en autorisaties

In deze paragraaf gaan we in op deelvraag 8. Voldoet de wijze waarop de gemeenten de informatiestroom in processen en applicaties organiseren aan de vereisten op het gebied van informatiebeveiliging en privacy? Zijn de autorisaties, wie van de medewerkers bij welke informatie moet of kan, adequaat geregeld?

De technische en organisatorische maatregelen, processen in ondersteuning op ICT en de applicaties die draaien in de gemeentelijke organisaties zijn in de basis aanwezig, maar zijn, zoals begin 2018 in een externe scan is geconstateerd, beperkt vastgelegd in beleid, verantwoordelijkheden en middelen. Zo zijn bijvoorbeeld in 2016 risico's op ICT geschetst, op ketenautomatisering en een versnipperde informatie architectuur, die niet of nauwelijks zijn opgepakt, mede door de problemen met een softwareleverancier. De gehele architectuur moet volgens een van de respondenten structureel gewijzigd worden en er is daarvoor een programmamanager aangewezen die dat moet gaan oppakken.

De monitoring op gebruikers en activiteiten, anders gezegd de logging, is beperkt. Dat wordt ook duidelijk in de casestudies (zie bijlage 2). Daardoor werken gebruikersbeheer en handhaving niet goed en scoren de gemeenten in de bovengenoemde scan onder het gemiddelde. Een voorbeeld hoe de beperkte monitoring uitwerkt is het autorisatiebeleid, dat regels stelt welke functionaris welke activiteiten in applicaties mag verrichten met de daarin opgeslagen en verwerkte gegevens (zie ook §6.2). De applicatiebeheerders kennen de autorisaties aan medewerkers toe, op basis van de functie. De medewerker kan van functie wisselen of vertrekken. Controle op de autorisaties door de applicatiebeheerders geschiedt eens per 2-3 maanden, met behulp van een lijst met autorisaties die vanuit systeembeheer wordt verstrekt. Het kan voorkomen dat een account nog korte tijd doorloopt. Ook geven teamleiders aan nog soepel met autorisaties om te gaan, zij geven aan gemakkelijk een week verlenging te geven als iemand 'piept' dat zijn/haar account is opgeheven. Men geeft aan te weten dat het niet mag, maar dan wordt er toch voor gekozen het account even te verlengen om de dienstverlening door te laten gaan. Op dit moment kan het volgens een van de respondenten nog voorkomen dat een medewerker uit dienst is en het account nog doorloopt. Dat geldt ook voor de toegangspassen, waarbij men aangeeft bezig te zijn om te regelen dat toegangspassen na uitdiensttreding niet meer actief zijn.

Respondenten geven aan te wachten op het beleid op in- en uitdiensttreding. Onduidelijk is waar de verantwoordelijkheid daarvoor ligt, onder andere door de reorganisatie. Zo troffen we in de deskresearch een opzet aan van procedures om HRM/PSA in ISMS (zie §6.5) op te nemen, daterend van juli 2018. Dat was op dat moment blijkbaar nog niet vastgesteld. Op dit vlak is ook volgens de gemeentesecretarissen nog een 'punt op de i' te zetten en dient nog voor het eind van 2018 geregeld te zijn. De organisaties zijn ook bezig de autorisaties te koppelen aan het HRM-pakket Youforce van de personeelsadministratie. Dat zou volgens de respondenten medio 2019 geregeld moeten zijn. Bij sommige afdelingen/applicaties is dat al strak geregeld, zoals in geval van SUWInet, zoals ook uit de eerste casestudy blijkt (zie bijlage 2, casestudy Participatiewet). Hier toetst een landelijke organisatie, Bureau Keteninformatisering Werk en Inkomen (BKWI), onder andere op de autorisaties. Als blijkt dat dat niet goed geregeld is, lopen gemeenten het risico niet meer aangesloten te zijn op SUWInet, met alle gevolgen voor de dienstverlening in het kader van de Participatiewet.

Aangegeven wordt dat sommige afdelingen te klein zijn om in de autorisaties een functiescheiding tussen gebruiker en beheerder toe te passen. Dat zijn rollen die in principe niet verenigbaar zijn. Zo mag, ter voorkoming van fraude en manipulatie van de gegevens, de teamleider die de autorisaties toekent niet zelf als gebruiker toegang hebben tot de gegevens. In het PNIK-assessment is gemeld dat geen functiescheiding is toegepast, en ook niet een van de alternatieve vormen. Dat vormt een risico.

Een ander vraagstuk rond autorisaties doet zich voor met betrekking tot privacy in het sociaal domein. De gemeenten werken toe naar integrale dienstverlening. Dan wordt toekennen van autorisaties op basis van functie lastig. Sommige functies krijgen geen autorisatie voor applicaties die wel nodig zijn om de integrale dienstverlening mogelijk te maken. Deze kunnen namelijk toegang geven tot bijzondere persoonsgegevens die de medewerker in die functie niet mag

inzien. Om toch de integrale dienstverlening mogelijk te maken moet daarop volgens enkele respondenten nog een en ander aan beleid ontwikkeld worden. Dat gaat overigens hier deels om landelijke wet- en regelgeving waarop de gemeenten geen grip op hebben.

Verder is er op verschillende ICT-terreinen beleid geformuleerd. Zoals het wachtwoordenbeleid, dat er is sinds 2016. Mede naar aanleiding van dit rekenkameronderzoek is over beleid op wachtwoorden voor de raadsleden gediscussieerd. Raadsleden gaven aan risico's te ervaren bij het wachtwoordbeleid op hun tablets, omdat niet is geregeld dat de wachtwoorden regelmatig gewijzigd moeten worden. Clean desk policy is aanwezig, dat medewerkers voorschrijft documenten niet onbeheerd op hun bureaus te laten liggen en dat computerschermen met informatie afgesloten worden als iemand van zijn/haar bureau wegloopt. Op de vraag of dat wordt nageleefd zijn de reacties van de respondenten wisselend. Een aantal beweert dat er niet of nauwelijks op wordt gestuurd en/of gehandhaafd, en een aantal geeft aan dat men dat meer en meer doet.

In principe zijn de werkplekken niet bereikbaar zonder toegangspas, maar het gebeurt nog wel eens dat derden worden meegenomen naar de werkplekken. Dat zijn met name leveranciers of reparateurs. Burgers komen over het algemeen niet bij de werkplekken, maar worden ontvangen in het spreekkamergedeelte of in de vergaderruimten. En als de clean desk policy adequaat wordt nageleefd is het geen bezwaar als derden, onder begeleiding, bij de werkplekken komen.

Regels over hoe om te gaan met de eigen 'devices' zoals smartphones en tablets moeten nog grotendeels ontwikkeld worden, het 'bring your own device'-beleid (BYOD). De uitgifte van 'devices' van de gemeenten wordt bijgehouden, maar ook daarvoor moeten de regels nog ontwikkeld worden. Daar gaat volgens respondenten ook nog wel eens wat mis. Zoals telefoons die niet terug worden ingeleverd bij uitdiensttredingen. Dat heeft te maken met de gebrekkige koppeling met de in- en uitdiensttredingen (zie hiervoor). De gemeenten zijn bezig met een digitaal formulier waarop de dienstperiode, welke functie en voor welke autorisaties en devices de medewerker recht heeft bijgehouden wordt.

Patchmanagement, beheer van de updates van de software, is nog niet op orde. Dit betekent dat de organisatie hierop kwetsbaar is, daar niet gegarandeerd is dat noodzakelijke veiligheidsupdates tijdig worden geïmplementeerd. Adequaat patchmanagement is zeker nodig als er verschillende besturingssystemen naast elkaar worden gebruikt. In een externe scan is begin 2018 geconstateerd dat er nog twee apparaten op een verouderde versie van een besturingssysteem draaiden dat sinds enkele jaren geen veiligheidsupdates meer krijgt. Bij navraag klopt dat, maar dat betreft offline apparaten, die niet op het internet zijn aangesloten, en nog draaiende worden gehouden om gegevens uit verouderde applicaties te kunnen raadplegen. Dat betekent dat deze systemen geen risico vormen online gehackt te worden.

Op de rol staat dat de gemeenten iDocs gaan implementeren. Zij gaan een project aan om de post- en archiefstromen te digitaliseren en centraliseren. Dat betekent onder andere dat de harde schijven van de individuele computers moeten worden gescreend op documenten die centraal bewaard moeten worden en mailboxen moeten worden opgeschoond. Nu nemen medewerkers nog wel eens dossiers mee naar huis, weliswaar in afsluitbare trollies. Als iDocs functioneert hoeft dat niet meer, dan kunnen medewerkers op een externe plek met een beveiligde vpn-verbinding en '2-factor-beveiliging' bij de centraal opgeslagen dossiers. Op veilig bewaren van documenten zijn ook al stappen gezet, zo heeft de salarisadministratie kasten die beter op slot kunnen dan voorheen. Post wordt nu in postbakjes gestopt die achter slot en grendel staan. In Achtkarspelen zijn er minder open kasten en bureaulades dan in Tytsjerksteradiel (zie ook casestudy, bijlage 2).

Afspraken over hoe de medewerkers van het schoonmaakbedrijf omgaan met stukken die medewerkers op de bureaus laten liggen zijn er niet in Tytsjerksteradiel. Zo maakt het schoonmaakbedrijf daar overdag schoon, terwijl de werkplekken operationeel zijn. In Achtkarspelen zijn daar wel afspraken over gemaakt. De bureaus worden daar in de avonduren schoongemaakt en zijn dan in principe 'clean'.

6.8 Assessments, audits en continuïteit van de dienstverlening

Hieronder wordt antwoord gegeven op deelvraag 9. Wordt jaarlijks getoetst of de organisaties in control zijn op het gebied van informatieveiligheid via peer reviews, audits, self assessments (zelf tests) of pen-testen? Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weten de organisaties hoe te handelen bij een (ernstig) informatieveiligheid-incident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?

De benodigde assessments en audits worden gehouden op de applicaties zoals BRP, BAG, SUWInet enz. Zie ook de casestudy op de Participatiewet. De meeste recente die we in het kader van dit onderzoek hebben ingezien, zijn van april 2018. Op de applicaties die in het primaire proces van de gemeenten draaien, en deels landelijk worden

gemonitord, is een continuïteitsplan aanwezig. Daar wordt ook op getest door de toezichthouders. Op SUWInet werd in de laatste audit een administratieve onvolkomenheid geconstateerd, de audit is zonder succes afgerond.

De verplichte audits en assessments worden gehouden, maar volgens de gemeentesecretarissen kan de samenhang en koppeling beter. Het interne rapportageproces kan beter, en daar moet het ISMS op ingericht worden (zie ook §6.5). Daarnaast zorgen de uitdagingen waar de gemeenten voor zijn gesteld, de decentralisaties, de reorganisatie en problemen rond de softwareleverancier, dat men niet het gevoel heeft in control te zijn op informatiebeveiliging.

Uitwijktesten, die testen wat er moet gebeuren in geval van bijvoorbeeld een calamiteit waardoor de gemeentelijke systemen uitvallen, worden jaarlijks uitgevoerd. In september 2017 zijn de uitwijktesten uitgevoerd en zijn problemen met een back-up geconstateerd. In november zijn de testen succesvol herhaald. In 2018 zijn opnieuw uitwijktesten uitgevoerd. De testverslagen waren ten tijde van deze rapportage nog niet gereed, maar zijn naar verluidt succesvol afgerond.

De datacenters van de twee gemeenten zijn gekoppeld en de back-up van de beide locaties staat op een derde locatie. Zodra duidelijk is dat er een storing is die langer dan 4 uur duurt, wordt met de directie besproken welke maatregelen genomen moeten worden. Valt de applicatie uit, dan zal de provider snel met een oplossing moeten komen. Vallen de systemen uit, dan moeten andere oplossingen worden geregeld, waaronder een eventuele organisatiebrede uitwijk. Binnen 72 uur moeten de basis-applicaties zoals BAG en de GBA op de uitwijk draaien en het berichtenverkeer moet ondertussen in stand gehouden kunnen worden. Respondenten geven aan dat de uitwijk wel technisch wordt getest, maar niet organisatorisch en in de praktijk met medewerkers die op de andere locatie terecht moeten of vanuit thuis kunnen werken. In de bestuurlijke top leven zorgen op gebied van de continuïteit. Het uitwijkcontract loopt tot en met 2018 met de softwareleverancier waarmee de gemeenten in een juridische procedure zijn verwikkeld. Er wordt een nieuw contract gesloten met een andere leverancier waardoor medio 2019 dit op orde moet zijn.

Er is een protocol voor het melden van beveiligingsincidenten en datalekken, maar er is nog geen automatische tool om incidenten en datalekken te registreren en gebeurt nog grotendeels handmatig door de CISO. Samen met de FG moet dat overgezet worden naar SharePoint, zodat registratie en rapportages van daaruit automatisch gegenereerd worden. Volgens een van de respondenten is de vraag wat er moet gebeuren met de opvolging van incidenten die buiten de kantooruren om plaatsvinden, als er geen helpdesk aanwezig is. Dat is nu nog niet geregeld, noch intern noch extern belegd.

Er zijn vele verschillende testen om de kwetsbaarheid van de ICT en gedrag van medewerkers te beproeven. Eind 2017 en medio 2018 zijn zogenoemde vulnerability-analyses uitgevoerd. Dat zijn geautomatiseerde testen die bekende kwetsbaarheden van de ICT-systemen zoeken. Een keer is met behulp van een phishing mail op de bewustwording van medewerkers getest (zie §6.9). Dat is een pen-test, maar andere pen-testen zoals met behulp van ethisch hackers proberen in te breken op de systemen, worden niet uitgevoerd. Er wordt gewezen op het feit dat de problemen met de software hierop een bottleneck zijn waardoor pen-testen hoogstens reeds bekende informatie en risico's zullen opleveren. De gemeenten zijn van plan, als de systemen vanaf medio 2019 stabiel zijn, regelmatig pen-testen uit te voeren.

De interne ICT-systemen zijn van de buitenkant afgeschermd, o.a. met firewalls. Intern wordt geen encryptie, of versleuteling van gegevens, nodig geacht. Voor externe opslag van gegevens in de cloud wel. Medewerkers en derden die vertrouwd worden, kunnen met een beveiligde VPN-verbinding toegang krijgen tot het interne netwerk. Het beveiligingsconcept van de gemeenten gaat nog niet uit van 'zero trust', dat wil zeggen, interne activiteiten kunnen ook verdacht zijn. Als een virus of hacker door de eerste beschermingswal heen komt, heeft deze relatief vrij spel. De systemen zijn niet opgedeeld in aparte compartimenten en onderling beschermd met interne firewalls.

Volgens de gemeentesecretarissen zijn er in kwantitatieve zin voldoende middelen en mensen om informatiebeveiliging en privacy op een adequate wijze in te vullen. In kwalitatieve zin ook, maar de organisaties kunnen daarop nog verder professionaliseren. Echter, merken zij op, is de arbeidsmarkt op dit soort functies erg lastig. Volgens andere respondenten mogen er meer middelen ter beschikking worden gesteld. Zij geven aan dat systemen verouderd zijn en er te weinig menskracht aanwezig is voor de opgaven waarvoor de gemeenten hierop staan.

6.9 Bewustzijn op informatiebeveiliging en privacy

Tot slot gaan we in deze paragraaf in op deelvraag 10. Op welke wijze wordt aandacht besteed aan de bevordering van awareness bij medewerkers van de gemeenten? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houden de gemeenten kennis vast en bouwen zij hierop voort?

Medewerkers zijn belangrijke schakels, zo niet de belangrijkste, op het terrein van informatiebeveiliging en privacy. Een organisatie kan het technisch en organisatorisch nog zo goed op orde hebben, als medewerkers niet alert zijn en de richtlijnen en tips niet volgen, kan het alsnog mislopen. Aandacht voor het bewustzijn, of awareness, van medewerkers op de risico's is essentieel. Op verschillende wijzen wordt hier door de gemeenten aandacht aan besteed. Interne nieuwsbrieven over informatiebeveiliging en privacy worden regelmatig verstuurd. In 2017 is een door de CISO verzorgde e-learning cursus informatiebewustzijn aangeboden aan de medewerkers in 2017, op vrijwillige basis. De e-learning heeft na 2017 geen vervolg gekregen. In 2017 is de bijeenkomst "komt een vrouw bij de hacker" georganiseerd voor medewerkers. Daarna is een phishing mail uitgezet door een extern bedrijf. Sommige medewerkers hebben de verdachte mail gemeld bij ICT en de CISO, anderen hebben toch geklikt in het bericht. Tot slot zijn eind 2017 twee inloopsessies over de basisbeginselen van de AVG gehouden. Het onderwerp 'bewustzijn bij medewerkers' scoorde bij externe toets begin 2018 beneden gemiddeld. Zo bleek uit een enquête begin 2018 dat veel medewerkers nog niet wisten waar ze een lek moesten melden. Aanbevolen werd om met spoed middelen te besteden voor de implementatie van de AVG en aanstelling van de FG. De FG is in mei 2018 aangesteld, maar daarvoor al heeft de voorloper van de FG, de functionaris privacy awareness-sessies in teamoverleggen gegeven. Medewerkers geven aan de praktische insteek van de sessies te waarderen.

Respondenten zien grote verschillen tussen afdelingen, namelijk afdelingen die al langer met persoonsgegevens werken zijn verder dan andere afdelingen. Respondenten geven aan dat de bewustwording bij medewerkers in het algemeen groeit en dat zij samenhangen met hun eigen vakgebied beginnen te zien. Tevens wordt ervaren dat het belang van informatiebeveiliging en privacy wordt gedragen door managers en teamopbouwers. Nieuwe medewerkers en externen krijgen informatie over privacy bij de introductie in het introductiepakket mee. Privacy is ook een onderwerp tijdens de jaargesprekken tussen medewerker en leidinggevende, geeft een van de respondenten aan.

De meldingsbereidheid van incidenten op informatieveiligheid neemt toe en wordt als voldoende ervaren. Dat betekent dat hiervoor een veilig klimaat is geschapen, volgens de portefeuillehouders. Vervolgsessies op awareness zijn vanaf het najaar 2018 gepland in de werkmaatschappij. Mede om medewerkers met de relatief recent aangestelde FG kennis te laten maken en input voor een FAQ-lijst op de SharePoint op te halen. Voor 2019 staat een plan voor scholing op privacy op de agenda.

Enkele medewerkers geven aan dat aandacht besteden aan informatiebeveiliging en privacy tijd kost en druk oplevert. Door te weinig tijd en middelen is de werkdruk hoog en vindt een enkele medewerker de mogelijkheden om adequaat met informatiebeveiliging en privacy om te gaan te beperkt. De werkdruk in het algemeen wordt herkend door de gemeentesecretarissen. De middelen zijn aanwezig om veilig data heen en weer te sturen, via Cryptshare, maar het vergt een extra handeling. Daarom wordt het nog wel eens vergeten of medewerkers vinden het "vervelend, kost alleen maar tijd". In de eerste concept ENSIA-rapportage wordt geconstateerd dat niet of nauwelijks wordt gecontroleerd of ambtenaren en ingehuurd personeel zich houden aan de beveiligingsregels. Het ISMS kan een instrument zijn om het organisatieleren op informatiebeveiliging en privacy in te richten, door een koppeling met een leer-cyclus zoals de PDCA (Plan-Do-Check-Act). Het ISMS is nog niet volledig ingericht (zie onder andere §6.5) en bijgevolg nog niet in staat het organisatieleren adequaat te ondersteunen, kennis vast te houden en uit te bouwen. Een vraagstuk dat de komende tijd gaat spelen op gebied van personeelsmanagement en behoud van kennis is de opvolging van de CISO. De huidige functionaris gaat minder werken en per medio 2019 met pensioen. Er is nog geen opvolging geregeld waardoor tijd voor de overdracht van dossiers en kennis als te krap wordt ervaren.

Fysieke beveiliging gebeurt met name door de medewerkers die achter de receptiebalie zitten en vragen waar men voor komt. Dat is goed geregeld volgens de respondenten. Ook de medewerkers hebben hierop een verantwoordelijkheid, maar volgens de respondenten zal waarschijnlijk niet iedereen checken of degene die meeloopt naar de afgescheiden ruimten ook wel gerechtigd is toegang te hebben. Gedacht wordt dat medewerkers het vervelend vinden om dat te vragen/checken.

Elkaar aanspreken op gedrag zit niet zozeer in de cultuur, volgens de meeste respondenten. De attitude daarop kan nog wel verbeteren en vergt constant aandacht. Eenmaal binnen dan speelt naleving van protocollen/procedures als wachtwoordbeleid, ‘bring your own device’-beleid en clean-desk policy een belangrijke rol en dat vergt bewustwording bij medewerkers.

Op een locatie constateert de onderzoeker een risico van ongewenst (fysiek) binnenkomen op locatie. Hierover wordt separaat en vertrouwelijk gerapporteerd.

Bijlage 1. Verklarende woordenlijst en afkortingen

2FA	Twee factor authenticatie, zo wordt op 2 verschillende manieren gecheckt of degene die inlogt degene is die hij/zij aangeeft te zijn
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation)
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband
BIO	Baseline Informatiebeveiliging Overheid, verwachting is dat hier de BIR en BIG in zullen opgaan vanaf 2020
BIR	Baseline Informatiebeveiliging Rijksdienst, geldt als basis voor de BIG
BIR-familie	Geheel van Baselines Informatiebeveiliging die voor de overheid gelden, deze gaan vanaf 2020 op in de Baseline Informatiebeveiliging Overheid (BIO)
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
BKWI	Bureau Keteninformatisering Werk en Inkomen
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
BYOD	Bring your own device, beleid dat inhoudt dat dat medewerkers en externen hun eigen apparaten (laptops, smartphones, usb-sticks enz.) meenemen en inloggen in het gemeentelijk systeem
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
Cryptshare	Via een derde partij georganiseerde beveiligde wijze van mail verzenden, die alleen door de geadresseerde ontvangen kan worden
CYOD	Choose your own device, beleid dat inhoudt dat medewerkers en eventueel externen apparaten (laptops, smartphones, usb-sticks enz.) kunnen kiezen uit een beperkt assortiment, waarop de veiligheidsmaatregelen reeds zijn aangebracht
DPIA	Dataprotection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacyrisico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIG geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie AVG)
GBA	Gemeentelijke Basisadministratie
GR	Gemeenschappelijke regeling
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
iDocs	Intermediate Document, format om digitale gegevens uit te wisselen
IMO	Informatie Management Overleg

IP-adres	Internetprotocol adres, bestaande uit (momenteel) 4 setjes van drie cijfers. Met behulp van deze set cijfers is elke computer en apparaat dat op internet is aangesloten te traceren
IPv6	Is de opvolger van het traditionele IP-adres. De oude IP-adressen, eigenlijk IPv4, raakten op. Onder andere vanwege de groei van het aantal apparaten dat op internet aangesloten wordt
ISAM	Indexed sequential access method, een manier om snel gegevens op te halen uit diverse bestanden
ISMS	Information security management system
ISO	International Standards Organisation
KING	Kwaliteitsinstituut Nederlandse Gemeenten, heet tegenwoordig VNG Realisatie
Logging	Bijhouden en vastleggen van activiteiten (zoals wijzigen en raadplegen) van gebruikers en beheerders, ten behoeve van monitoring- en handhavingsdoeleinden
OWASP	Open Web Application Security Project
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidscyclus
PKI-certificaat	Public Key Infrastructure. Een PKI(overheid)-certificaat is een internationale standaard voor de digitale ondertekening bij het versturen van gegevens en berichten.
Privacy by default	Onderdeel van privacy by design, waarbij de standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
RIVG	Rijksdienst voor Identiteitsgegevens
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen inzake informatiebeveiliging
Url	Uniform Resource Locator. Verwijst naar een unieke adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres
VCIB	Vertrouwd Contactpersoon Informatiebeveiliging, ontvangt berichten van vertrouwelijke aard van de Informatiebeveiligingsdienst voor gemeenten
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)

Bijlage 2. Werkconferentie van de raden over informatiebeveiliging en privacy 4 oktober 2018

Op de werkconferentie zijn de gemeenteraden van Achtkarspelen en Tytsjerksteradiel bijgepraat over de voortgang en eerste bevindingen van het onderzoek en gevraagd op welke manier(en) de gemeenteraden over informatiebeveiliging geïnformeerd willen worden. De input van de gemeenteraden is belangrijk om passende aanbevelingen te geven over de informatiebeveiliging van Achtkarspelen en Tytsjerksteradiel.

In het eerste deel van de werkconferentie bespreekt Etienne Lemmens de eerste uitkomsten van het onderzoek. Van belang is de constatering dat de informatiebeveiliging technisch goed geregeld is, maar dat er nog veel te ontwikkelen is. Gesproken is over de awareness bij medewerkers als een risicofactor en of er ook pentesten worden uitgevoerd. Immers 'the proof of the pudding is in the eating', aldus een van de raadsleden. Het advies is om altijd te toetsen: het initiatief daartoe moet bij de gemeente liggen en 'laat je testen'.

Men moet zich er bewust van zijn dat er geen 100% zekerheid bestaat. Wel kunnen de gemeenten zich zoveel als mogelijk beschermen tegen de risico's die ze kennen en erkennen, maar absolute veiligheid bestaat niet. Mocht bijvoorbeeld een medewerker bewust iets laten lekken, is daar niets tegen te doen. Overigens is het systeem zo ingericht dat men later wel kan nagaan wie allemaal gelekt hebben. Het punt is dat als het beschermingsniveau op een goed niveau is, kwaadwillenden sneller naar een ander slachtoffer zoeken.

Een lid van een van de gemeenteraden vraagt of het zinvol is om de IBD (Informatiebeveiligingsdienst voor gemeenten) voor pentesten in te schakelen. Zij kennen de systemen. Tot nu toe maakt deze service nog geen onderdeel uit van het dienstverleningspakket van de IBD.

Verder zijn er vragen over het gebruik van allerhande apparatuur. Hoe veilig is het werken met apparaten als laptops, tablets etc. Aanwezigen geven aan dat er geen protocol is over hoe gemeenteraadsleden daarmee om moeten gaan. Ook over beveiliging van wachtwoorden, het tijdig wijzigen etc. Immers de mens is vaak de zwakste schakel.

Etienne Lemmens merkt op dat dat juist is, maar er zijn ook nog wel zaken waar je hoe dan ook iets aan kunt doen: wel een protocol en instructie maar ook zorgen dat je software up-to-date is. Bij protocol/beleidskader gaat het vooral om goede procedures. Procedures voor raadsleden over omgaan met veiligheid, maar ook procedures bijvoorbeeld over een goede registratie van in- en uitdiensttredingen in verband met de autorisaties.

Etienne Lemmens benoemt in het algemeen als risico's op informatiebeveiliging:

- Beschikbaarheid, integriteit en vertrouwelijkheid (biv) van de informatie is niet gewaarborgd
- Haperingen van de dienstverlening aan burgers/bedrijven/instellingen
- Datalek bij de gemeente en/of een ketenpartner
- Financiële en emotionele schade voor inwoners
- Angst en onrust bij burgers/bedrijven/instellingen
- Boete als bij een incident blijkt dat niet alle benodigde beveiligingsmaatregelen zijn getroffen
- Medewerkers onvoldoende bewust van de kroonjuwelen van de gemeente
- Onvoldoende score op audits met gevolg dat de toezichthouders maatregelen opleggen
- Onvoldoende voortgang op BIG-maatregelen
- Bestuurlijk verantwoordelijken moeten aftreden na beveiligingsincident
- Gemeente kan in de pers 'ge-named and –shamed' worden

De raadsleden wordt gevraagd welk risico zij het belangrijkst vinden en waarover zij graag geïnformeerd willen worden. De aanwezigen krijgen de mogelijkheid om via post-its aan te geven waar ze vooral meer over zouden willen weten. De raadsleden mogen daarbij zelf aangeven hoe goed ze ingevoerd ze zijn in de onderwerpen informatiebeveiliging en privacy, via post-its:

Geel : Ik weet weinig tot niets van informatiebeveiliging en/of privacy
Groen : Ik weet wel het een en ander over informatiebeveiliging en/of privacy
Rood : Ik weet heel veel over informatiebeveiliging en/of privacy

Expliciet wordt gemeld dat de gele en groene post-its niet minder waard zijn dan de rode, het gaat hierbij om te weten wat het kennisniveau van de raadsleden is en waarop men dan geïnformeerd wil worden. De raadsleden konden met een 'Achtkarspelen' of 'A aangeven dat ze uit Achtkarspelen komen en met een 'T' of 'TD' uit Tytsjerksteradiel.

In totaal zijn er 72 post-its geplakt: gemeenteraadsleden uit Tytsjerksteradiel hebben 32 post-its geplakt, 40 post-its zijn geplakt door gemeenteraadsleden uit Achtkarspelen. 2 gemeenteraadsleden hebben 3 rode post-its geplakt, de anderen geel (38 x waarvan 18 gemeenteraadsleden Tytsjerksteradiel en 20 Achtkarspelen) en 31 groene (14 gemeenteraadsleden Tytsjerksteradiel en 17 Achtkarspelen).

De meeste post-its kwamen terecht bij:

1. Risicobewustzijn bij medewerkers, externe inhuur en ketenpartners (18: 9 geel en 9 groen): 8 gemeenteraadsleden Tytsjerksteradiel (4 geel, 4 groen) en 10 gemeenteraadsleden Achtkarspelen (5 groen en 5 geel)
2. Borging van de continuïteit van de dienstverlening aan burgers/bedrijven/instellingen (15: 8 geel en 7 groen): 7 gemeenteraadsleden Tytsjerksteradiel (5 geel, 2 groen) en 8 gemeenteraadsleden Achtkarspelen (5 groen en 3 geel)
3. Incidenten, datalekken, en de beheersmaatregelen (12: 6 geel, 6 groen): 10 gemeenteraadsleden Achtkarspelen (5 groen en 5 geel) 2 gemeenteraadsleden Tytsjerksteradiel (1 geel, 1 groen)
4. Borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in ketens (6: 4 geel en 2 groen): 5 gemeenteraadsleden Tytsjerksteradiel (3 geel, 2 groen) en 1 gemeenteraadslid Achtkarspelen (1 geel)
5. Borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in ondersteunende processen (personeelsbeleid, enz.) (5: 3 geel en 2 groen): 3 gemeenteraadsleden Achtkarspelen (2 geel, 1 groen) en 2 gemeenteraadsleden Tytsjerksteradiel (1 geel en 1 groen)
6. Risico's die de gemeente accepteert en die de gemeente niet accepteert (5: 2 geel en 3 groen): 2 gemeenteraadsleden Achtkarspelen (1 groen en 1 geel) 3 gemeenteraadsleden Tytsjerksteradiel (1 geel en 2 groen)
7. Voortgang op de maatregelen uit het informatiebeveiligingsplan (BIG) (4: 2 groen, 2 geel): 3 gemeenteraadsleden Tytsjerksteradiel (2 geel en 1 groen), 1 gemeenteraadslid Achtkarspelen (1 groen)
8. Of de gemeente voldoet aan wet- en regelgeving (AVG, BIG, SUWI net, enz.) (4: 2 geel, 1 rood en 1 groen): 2 gemeenteraadsleden Achtkarspelen (1 rood en 1 geel) 2 gemeenteraadsleden Tytsjerksteradiel (1 geel en 1 groen)
9. Gebruik vertrouwelijke informatie door de raden (3: 2 geel en 1 groen): Allen gemeenteraadsleden Achtkarspelen (2 geel en 1 groen)
10. Meldingen aan de AP en aan betrokkenen (medewerkers, burgers, bedrijven, instellingen, enz.) (0)

Verder hebben sommige raadsleden aanvullende boodschappen op hun post-it geschreven. Bij het onderdeel risico's accepteren is aangegeven dat er iets minder vertrouwen en iets meer controle moet komen en dat een ambtenaar belast moet zijn met identificatie.

Etienne Lemmens gaf uitleg wanneer en hoe de gemeenteraden geïnformeerd worden op informatiebeveiliging en privacy. Dat is tot nu toe heel summier. In de BIG (Baseline Informatiebeveiliging Gemeenten) staat de gemeenteraad maar 1x genoemd. Namelijk, dat de gemeenteraad 1x per jaar over informatiebeveiliging geïnformeerd wordt in de P&C-cyclus. Daar gaat verandering in komen, en wel door middel van een nieuwe horizontale verantwoordingslijn, ENSIA (Eenduidige Normatiek Single Information Audit).

Een deel van de verantwoordingsrapportage aan de raden ligt vast, en wordt gevuld door informatie over de audits en assessments op de applicaties van de gemeenten. Daarop komt een verklaring van de colleges van B&W en een onafhankelijke assurancerapport. Het andere deel van ENSIA, over onder andere beheersmaatregelen en meerjarenperspectief, is vormvrij. Daarop moeten de raden en colleges met elkaar in gesprek waarover en hoe men geïnformeerd wil worden. Belangrijk is dat de raden ook aangeven of en wanneer zij naast de jaarlijkse ENSIA geïnformeerd willen worden.

Dat konden de aanwezige raadsleden met de post-its aangeven. Geen van de raadsleden heeft aangegeven bij het jaarverslag van de Werkmaatschappij 8KTD te willen worden geïnformeerd. De meesten hebben wel aangegeven bij het gemeentelijke jaarverslag te willen worden geïnformeerd (16 post-its: 4 gele post-its en 12 groen). Uitgesplitst naar gemeente: Tytsjerksteradiel 7 groene post-its en 4 gele pot-its, Achtkarspelen: 5 groene post-its.

Met betrekking tot de bestuursrapportages (Beraps) in Tytsjerksteradiel hebben 3 gemeenteraadsleden aangegeven bij de 1e Berap te willen worden geïnformeerd (3 gele post-its, Tytsjerksteradiel) en 1 gemeenteraadslid heeft een groene post-it geplakt bij de 2e Berap. Daarbij is aangegeven dat er een risicoanalyse zou moeten komen.

Bij de commissievergaderingen hebben 9 gemeenteraadsleden aangegeven geïnformeerd te willen worden: 3 afkomstig uit Tytsjerksteradiel en 6 uit Achtkarspelen. 3 raadsleden willen 2 maal per jaar in de controlecommissie geïnformeerd worden, allen afkomstig uit Achtkarspelen.

Tot slot hebben twee raadsleden aangegeven wanneer ze geïnformeerd willen worden. 1 raadslid tussen maart/april (Achtkarspelen) en 1 tussen juni en juli. 1 raadslid uit Tytsjerksteradiel die aangegeven heeft: rapportage bevinding steekproef.

Bijlage 3. Bevindingen twee casestudies

Per case behandelen we de volgende onderwerpen:

- Procesbeschrijving
    - Doel
    - Welke persoonsgegevens worden geregistreerd?
    - Welke bijzondere persoonsgegevens worden geregistreerd?
- Wat gaat goed?
- Wie zijn geautoriseerd om bij de geregistreerde gegevens te komen?
- Welke externe partijen kunnen bij de gegevens? Aan welke derde partijen worden de gegevens verstrekt?
- Kunnen cliënten hun gegevens inzien en wijzigen?
- Zijn bewaartermijnen van de gegevens vastgesteld?
- Welke gevoeligheid hebben de gegevens die de gemeente registreert?

Case 1. Aanvraag bijstandsuitkering in het kader van de Participatiewet

Procesbeschrijving
Doel van dit proces is de vaststelling van het recht op en de hoogte van een uitkering in het kader van de Participatiewet. De Participatiewet kent een aantal aanvraagprocessen, namelijk

- Aanvraag Wet werk en bijstand (WWB) 27+ (mensen ouder dan 27 jaar) en WWB 27- (mensen tot en met 27 jaar)
- Aanvraag levensonderhoud (tijdelijke inkomensondersteuning)
- Aanvraag IOAW (uitkering voor oudere werklozen)

Voor deze case zijn we nader ingegaan op de aanvraag WWB 27+. Het verschil tussen de aanvraag voor 27+ en 27- is dat er een wachtperiode van 4 weken is voordat de uitkering ingaat. De meeste jongeren vinden tegenwoordig in de tussentijd werk en zetten de aanvraag niet door. Voorheen was er ook voor 27+ers een wachtperiode, tegenwoordig wordt de aanvraag meteen ingepland.

Aanvragers geven hun gegevens in op de landelijke site werk.nl, met behulp van inloggen met DigID. Daarna komen ze bij de Poortwachterfunctie die op basis van de gegevens constateert of er een recht op een uitkering bestaat. Indien nee, dan wordt de klant uit het proces gehaald. Als er wel een recht op uitkering wordt geconstateerd, gaat het dossier naar de inkomensconsulent die de aanvraag toetst en op basis daarvan een advies geeft. Daarna toetst de kwaliteitsmedewerker de aanvraag. Bij goedkeuring door de kwaliteitsmedewerker gaat het dossier door naar de administratie voor de administratieve afhandeling. Bij afwijzing door de kwaliteitsmedewerker gaat het dossier voor eventuele aanpassing terug naar de consulent. Daarna toetst de kwaliteitsmedewerker weer en gaat het dossier door naar de administratie. De administratie heeft een laatste toets waarna bij positief advies een beschikking wordt opgesteld. Daarna gaan de gegevens van de klant door voor de betaling.

Wanneer er kans bestaat op bemiddeling naar de arbeidsmarkt wordt de intake bij de inkomensconsulent gecombineerd met een intake bij de werkconsulent.

Bij Werk.nl wordt gevraagd naar inkomenssituatie, contactgegevens (naam, adresgegevens, BSN), betaalgegevens en relatiegegevens. Inkomenssituatie en BSN zijn bijzondere persoonsgegevens. Na de doorgeleiding van Werk.nl werken de ambtenaren van de gemeenten in SUWInet en de eigen systemen met een uniek zaak- en cliëntnummer, het BSN is dan niet meer te traceren. Voor het onderzoek worden de vermogensgegevens opgevraagd en gecheckt. Medische gegevens worden niet geregistreerd.

De gegevens worden alleen vastgelegd voor het vaststellen van het recht op een uitkering in het kader van de Participatiewet. Voor andere doeleinden worden de gegevens niet gebruikt. Vroeger werden risicoprofielen opgesteld, maar dat gebeurt tegenwoordig niet meer. Mogelijk kunnen de gegevens worden gebruikt bij bemiddeling naar de arbeidsmarkt, maar dan alleen met toestemming van de klant.

Wat gaat goed?
Men is relatief tevreden met de voortgang die is geboekt op privacy en informatiebeveiliging op dit proces. De afdeling is bezig met volledig digitaal te gaan werken, met behulp van iDocs. Dat zal het fysieke probleem van de zware kasten met archiefstukken uit Tytsjerksteradiel die naar Achtkarspelen zijn overgebracht gaan oplossen. Het berichtenverkeer

is grotendeels digitaal, en naar externen toe beveiligd met Cryptshare. Alleen nog naar handhaving toe, dat is een ander proces, wordt er gewerkt met papieren dossiers, en deze gaan achter slot en grendel als de medewerkers er niet mee werken.

Er is een security officer speciaal voor het sociaal domein aangesteld, die de medewerkers adviezen geeft. De onderwerpen privacy en informatiebeveiliging worden regelmatig besproken in de teamoverleggen. Medewerkers worden erop aangesproken als men zich niet houdt aan de afspraken in verband met bijvoorbeeld clean desk policy. Medewerkers wordt voorgehouden "hoe zou jij willen dat met jouw gegevens wordt omgegaan"?

Wie zijn geautoriseerd om bij de geregistreerde gegevens te komen?
De poortwachter, de inkomensconsulent, de kwaliteitsmedewerker en de medewerker uitkeringsadministratie hebben toegang tot de gegevens in SUWInet. Iedereen heeft vanuit de eigen functie en rol toegang tot het systeem en kan op basis daarvan alleen gegevens inzien of wijzigingen aanbrengen. Dat is wettelijk bepaald wie welke toergang heeft tot de informatie on SUWInet. Voor de interne processen moet een sub proces aangemaakt worden, bijvoorbeeld als er gehandhaafd moet worden, of als er bezwaar wordt aangetekend tegen een beslissing. Dan moet een medewerker handhaving of juridisch advies toegang tot de gegevens verleend worden.

De teamleider van de afdeling kan autorisaties aanvragen, en deze worden door een van de drie applicatiebeheerders toegekend. Eens in de twee tot drie maanden krijgt de teamleider van ICT-beheer een overzicht van autorisaties en mailadressen. De teamleider legt die naast de eigen lijst die hij in de mailbox bijhoudt. Zo kan hij zien wie nog actief op een account is. De teamleider geeft aan dat, meteen als iemand uit dienst gaat, hij een mutatieformulier invult als iemand uit dienst gaat. Dan kan de betreffende medewerker niets meer doen in het systeem. Er is functiescheiding aanwezig. De teamleider mag autorisaties aanvragen, maar heeft zelf geen account en kan zelfs geen gegevens raadplegen.

Het bestaan van het dossier is kenbaar voor medewerkers van andere afdelingen waar een cliënt een voorziening heeft lopen, zoals jeugdhulp of Wmo. Dan is het mogelijk dat een medewerker van die afdeling te weten kan komen dat er uitkeringsgegevens van een persoon in de gemeentelijke systemen aanwezig zijn. De medewerker kan niet verder op de gegevens inzoomen. Dat gebeurt ook andersom. Medewerkers van de afdeling die de Participatiewet afhandelt, kunnen van het bestaan van eventuele andere voorzieningen op de hoogte raken, maar niet precies welke.

Op SUWInet wordt consequent en automatisch bijgehouden wie toegang heeft gehad tot informatie. Op deze logging en monitoring wordt door BKWI, de landelijke toezichthouder op SUWInet, gecontroleerd. Intern, op de lokale systemen wordt een beperkte logging bijgehouden (zie ook §6.2).

Welke externe partijen kunnen bij de gegevens? Aan welke derde partijen worden de gegevens verstrekt?
De gegevens in de applicatie worden extern gehost bij Pink, in iDocs en iSam. Daar kunnen alleen de geautoriseerden bij komen. Met Pink hebben de gemeenten een verwerkersovereenkomst afgesloten, met afspraken over informatiebeveiliging en privacy.

Blijenhof is een externe partij die voor hun klanten uitkeringen kunnen aanvragen. Dat kunnen zij alleen doen met toestemming en machtiging van de klanten. De gegevens met betrekking tot de uitkeringsaanvraag worden dan met de contactpersoon van Blijenhof uitgewisseld. Blijenhof verwerkt geen gegevens voor de gemeenten, hetgeen betekent dat er geen verwerkersovereenkomst hoeft gesloten te worden met deze partij.

Communicatie met persoonsgegevens vindt beveiligd via Cryptshare plaats. Het wordt medewerkers makkelijk gemaakt om e-mails via Cryptshare te versturen en daar houden de medewerkers zich volgens de respondenten aan. Er zijn cursussen in gegeven, supergebruikers aangewezen die wat meer weten en die andere medewerkers kunnen helpen. Tevens worden dit soort zaken, op informatiebeveiliging en privacy, regelmatig besproken in het teamoverleg. Bovendien is het gemakkelijk gemaakt.

Kunnen cliënten hun gegevens inzien en wijzigen?
Cliënten kunnen in principe de gegevens die zij hebben aangeleverd in SUWInet inzien en eventueel wijzigen. Dat kan men op Werk.nl met behulp van DigID doen. Binnenkort kunnen cliënten dat via Mijnoverheid.nl doen, dat is een landelijk project. In de gemeentelijke systemen kan dat nog niet en men is bezig die mogelijkheid in te richten.

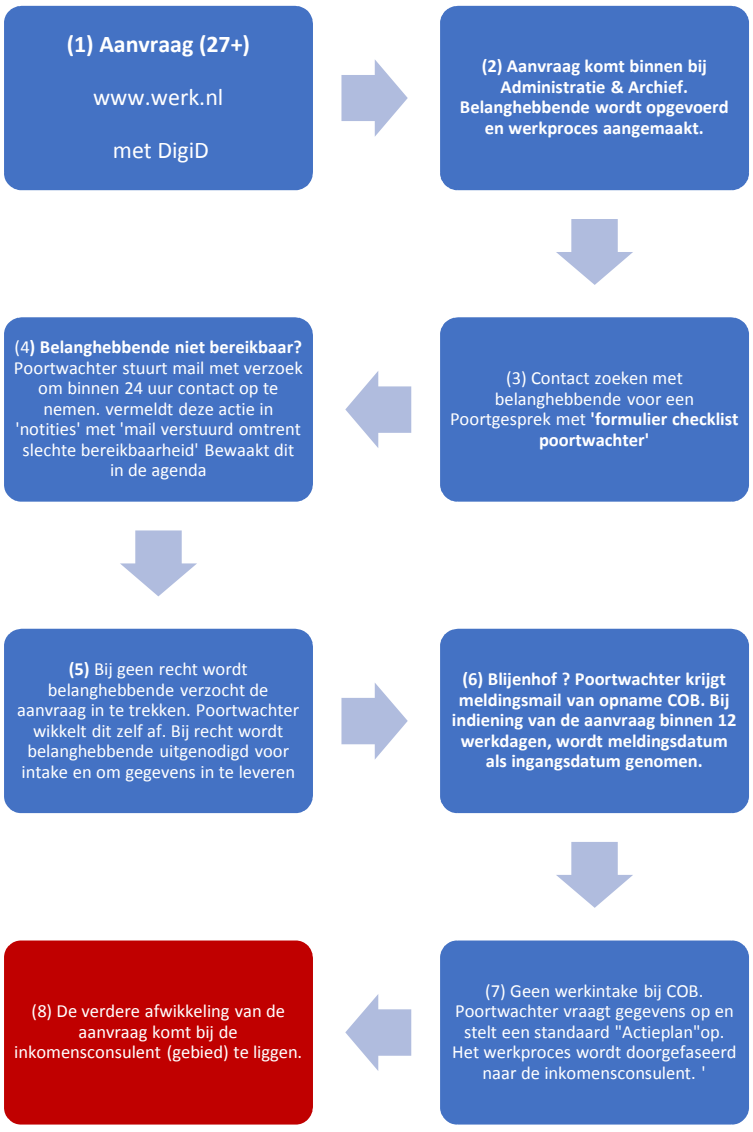
Zijn bewaartermijnen van de gegevens vastgesteld?
Voor de gegevens op SUWInet bestaan bewaartermijnen die landelijk zijn vastgelegd. Zolang de dossiers actief zijn in de gemeentelijke systemen, blijven de gegevens in de dossiers bestaan. Als de dossiers worden afgesloten, worden ze niet meteen verwijderd, maar als historisch dossier opgeslagen. De betaalhistorie wordt op dat moment uit het dossier verwijderd. Echter, als de cliënt nog andere gemeentelijke voorzieningen heeft, zoals bij jeugdhulp of de Wmo, blijft het dossier bestaan in de gemeentelijke systemen.

Welke gevoeligheid hebben de gegevens die de gemeente registreert?
In SUWInet en de gemeentelijke systemen zijn (bijzondere) persoonsgegevens aanwezig over de aanvragers van een uitkering. Het betreft processen die kwetsbare mensen betreffen, in een uitkeringssituatie. Tevens zijn er forse bedragen gemoeid met de uitbetaling van de uitkeringen. Het betreft bij de aanvraag van een uitkering dus om gevoelige processen met een hoge bestuurlijke, financiële en publicitaire impact als er iets misgaat met de informatie.

Wanneer het gaat om een issue op de beschikbaarheid van de informatie, bijvoorbeeld medewerkers kunnen niet bij de gegevens omdat de systemen platliggen vanwege stroomuitval of een cyberaanval, dan lijkt de schade mee te vallen. Dat is vervelend, want de aanvragen komen niet door, medewerkers kunnen naar huis enz. Maar binnen 72 uur kan de dienstverlening opgepakt worden (voor de uitwijk zie §6.8), kunnen de systemen weer draaien, zijn recente data hersteld en is de informatie weer beschikbaar. Uitkeringen zouden mogelijk betaald kunnen worden door geld van de bank te halen en uit te keren.

Dat ligt anders bij een inbreuk op de integriteit van de informatie, als er bewust of onbewust met de informatie in de systemen is gemanipuleerd. Volgens de respondenten is dat nauwelijks voorstelbaar, vanwege de checks op de juistheid van de informatie, maar als het gebeurt is de impact voor de cliënten en de potentiële financiële en imagoschade voor de gemeenten groot. Het gaat bij het wekelijks betalen van de uitkeringen om forse bedragen, cliënten piepen heel snel en dan gaan vele alarmbellen af. Dat geldt ook als er een inbreuk is op de vertrouwelijkheid van de informatie, wanneer er (bijzondere) persoonsgegevens van de uitkeringsaanvragers betrokken zijn bij een datalek. Er zijn intern afspraken over hoe hierop te handelen, maar de schade voor gemeenten en cliënten is snel zeer ernstig.

Afbeelding 9. Stroomschema aanvraag WWB27+, in het kader van Participatiewet



Afsluitend
Bij de aanvraag van een uitkering in het kader van de Participatiewet worden persoonsgegevens door de gemeenten verwerkt. De leiding is zich bewust van de grote risico's en de navenante gevolgen. Het aanvraagproces, waarbij gebruik wordt gemaakt van SUWInet, de autorisaties en veilig mailverkeer e.d., staat onder scherp landelijk toezicht. Daar valt niet op af te dingen.

Case 2. Indienen en verwerking van klacht leefomgeving

Procesbeschrijving
Doel van dit proces is klachten met betrekking tot de leefomgeving te registreren en daarop te acteren. De procedure is voor beide gemeenten gelijk. In 2017 zijn bij de gemeente Achtkarspelen 275 meldingen behandeld, in Tytsjerksteradiel waren dat er 407. Meldingen van inwoners komen via een in te vullen formulier op de gemeentelijke website bij het Klant Contact Centrum (KCC) binnen. De meeste burgers bellen met het KCC en een aantal meldt de klacht aan de balie van het gemeentehuis. Dan vult een medewerker van het KCC het formulier in.

Gevraagd wordt naar NAW-gegevens, telefoonnummer en mailadres. En verder informatie over de aard van de klacht en over wie het gaat. Telefoonnummer en mailadres worden gevraagd om eventueel nadere informatie over de klacht in te winnen. De klager kan aangeven anoniem behandeld te worden. In de praktijk weet de beklaagde wel wie een klacht indient. De klager moet bij de gemeenten bekend zijn, anonieme klachten worden in principe niet in behandeling genomen. Behalve als de veiligheid in het geding is. De anonimiteit kan bewaard blijven, als de gemeente zelf hetgeen waarover de klacht gaat kan constateren.

In een enkel geval kan er ook een melding komen via de politie, waar deze strafrechtelijk niets mee kan maar de gemeente bestuursrechtelijk wel. De politie is zeer terughoudend met persoonsgegevens en deelt niet veel mee. Als er een straf- en bestuursrechtelijk aspect aan de melding zit wordt het samen met de politie opgepakt.

Als de klacht bij het KCC wordt gedaan en er een terugbelnotitie moet worden gemaakt, dan vraagt het KCC ook om het BSN van de klager. Daarmee kan het KCC in het systeem de klager zoeken. Het team Handhaving en vergunningen doet niets met dit gegeven en het wordt ook niet in de systemen (COSA) opgeslagen.

De afdeling maakt een afweging of en wanneer de klacht in behandeling wordt genomen. Dat gebeurt op basis van een indeling in prioriteiten, hoog-midden-laag. Dat is bepaald in het Beleidsplan Toezicht en handhaving Fysieke leefomgeving Achtkarspelen en Tytsjerksteradiel 2017. In de categorie hoog vallen bijvoorbeeld de meldingen met betrekking tot overtredingen die een serieuze bedreiging vormen, met betrekking tot veiligheid, ernstige overlast enz. Dat wordt aan de klager meegedeeld. Als de klacht gegrond wordt verklaard, op basis van de handhavingsstrategie zoals vastgesteld in het beleidsplan, gaat de afdeling ermee aan de slag.

De melding wordt in het workflowsysteem COSA ingebracht. De meeste meldingen hebben met beheer te maken, zoals een losse stoeptegel. Een aantal meldingen hebben te maken met een klacht over de leefomgeving of ‘overlast’. Deze laatste komen bij het team ‘Handhaving en vergunningen’ terecht. Een teamleider verdeelt de klachten over de medewerkers. Deze krijgen de melding in de mailbox en nemen het in behandeling. Meldingen over een bedrijf worden ook geregistreerd bij de bedrijfsgegevens. Voor Achtkarspelen is dat in Powerforms, voor Tytsjerksteradiel is dat in Squit XO. Daarin staat ook de openbare informatie van de bedrijven, behalve als deze hebben aangegeven dat het vertrouwelijke bedrijfsgegevens zijn.

Verder worden verslagen gemaakt van de contactmomenten met de beklaagde. Daarin worden soms persoonsgegevens, en een enkele keer ook bijzondere persoonsgegevens opgenomen die relevant zijn voor de behandeling en de veiligheid van de betrokken ambtenaren. Bijvoorbeeld hoe iemand woont, of iemand agressief is, het een verward persoon betreft, of er een schuldenproblematiek aanwezig is enz. Deze verslagen worden uiteindelijk ook opgenomen in het dossier, dat in COSA wordt gearchiveerd.

De afdeling hanteert geen termijnen voor de afhandeling van de melding. “Als het vandaag niet lukt, dan morgen.” Afhankelijk van de aard van de overtreding die is gemeld, en de prioriteit, vindt de afhandeling plaats. Bij prioriteit 'Hoog' vindt de afhandeling direct plaats, of wanneer de werkdruk het toelaat bij 'Midden'. De afdeling neemt de klacht meestal binnen een week in behandeling. De handhavingsstrategie hangt af van de ernst van de melding/klacht, en de bedoeling van de overtreder of de omstandigheden. Bijvoorbeeld is er sprake van onwetendheid bij de beklaagde of

een doelgerichte overtreding, is er sprake van recidive, enz. Er worden geen profielen opgesteld, op basis van de verzamelde informatie, maar de handhavers weten ongeveer wel wie er recidiveert.

Wat gaat goed?
Er wordt intern veel gecommuniceerd over informatiebeveiliging en privacy. De medewerkers letten er ook steeds meer en meer op. De FG heeft concreet aan kunnen geven wat dat betekent voor de processen van het team. De garantie dat het 100% volgens de normen en regels gaat kan niet gegeven worden, maar men geeft aan deze steeds beter na te leven. De thema's informatiebeveiliging en privacy worden op bijna elk teamoverleg geagendeerd en besproken.

Wie zijn geautoriseerd om bij de geregistreerde gegevens te komen?
Dat zijn achtereenvolgens de medewerker van het KCC die het formulier invult, de medewerker die de schifting tussen beheer en overlast doet, de teamleider die de klachten leefomgeving over de medewerkers van Handhaving en vergunningen verdeelt en de behandelend medewerker. Soms, als er strafrecht in het geding is, is een medewerker Veiligheid betrokken bij het dossier.

In principe kan eigenlijk iedere medewerker van het team bij de zaken die in COSA staan. De autorisaties worden door de teamleider van COSA beheerd. En als het gearchiveerd is in COSA kan iedere medewerker van de gemeente met een regulier account erbij. COSA is een zaakgericht workflowsysteem, met 1 dossiermap per casus. Hierin zit de melding die op een pdf-format is gearchiveerd, de status en een statusupdateformulier dat de medewerker die de zaak afhandelt bijhoudt. Daar kunnen bijlagen bij worden opgenomen, zoals eventuele gespreksverslagen (zie hiervoor). De statusupdateformulieren staan in SIM opgeslagen, dat is een cloudoplossing. Dat wil zeggen dat deze beveiligd extern worden gehost.

In COSA is geen logging mogelijk, dat zal in de toekomst in een ander digitaal archiveringssysteem wel mogelijk zijn. De afdeling zelf is bezig met de implementatie van een nieuw workflowsysteem, VTH. En daarin zijn de gebruikelijke autorisatieniveaus in aan te brengen, zoals gebruiker en beheerder.

Welke externe partijen kunnen bij de gegevens? Aan welke derde partijen worden de gegevens verstrekt?
Er kunnen geen externe partijen bij de informatie die in de systemen zijn opgeslagen. Wel wordt soms informatie met derden gedeeld. Bijvoorbeeld als er een strafrechtelijk aspect aan de melding zit, dan wordt informatie naar de politie doorgestuurd. Dan gaat het meestal om een zaak waarbij een van de medewerker Veiligheid bij betrokken is. Er vindt dan telefonisch uitwisseling plaats van de relevante gegevens.

Als het een verward persoon betreft, wordt informatie met andere externe instanties gedeeld, naast de politie, bijvoorbeeld GGD, maatschappelijk werk of jeugdzorg. Dan wordt met de professionals in het sociaal domein over het geval gesproken. Oppervlakkig en alleen de gegevens die nodig zijn, zoals NAW en de aard van de melding. De zaak hoort dan eigenlijk thuis bij de medewerkers van de afdeling Veiligheid.

Als informatie wordt gedeeld, gebeurt dat niet door derden toegang te verlenen tot de informatie in de systemen, maar dan gebeurt dat digitaal via de mail of schriftelijk.

Kunnen cliënten hun gegevens inzien en wijzigen?
De klager kan de gegevens die zijn geregistreerd inzien, maar kan deze niet zelfstandig wijzigen. De beklaagde kan de stukken inzien, maar dan gaat de afdeling eerst bij de juridische adviseurs ten rade, en tegenwoordig ook bij de FG, met de vraag welke informatie gedeeld mag worden. Zo hoeven bijvoorbeeld persoonlijke aantekeningen van ambtenaren niet gedeeld te worden. Als de aantekeningen bedoeld zijn om andere ambtenaren te informeren, dan zijn het geen persoonlijke aantekeningen en kunnen bijgevolg opgevraagd worden met een beroep op het inzagerecht in het kader van de AVG.

Zijn bewaartermijnen van de gegevens vastgesteld?
Voor COSA gelden de bewaartermijnen zoals gesteld in de Archiefwet, en dat is afhankelijk van de inhoud van het proces en de melding.

Welke gevoeligheid hebben de gegevens die de gemeente registreert?
Als de gegevens niet beschikbaar zijn, bijvoorbeeld als COSA platligt, dan heeft dat direct effect op de workflow en de dienstverlening. Er komen dan geen meldingen binnen via het KCC en kunnen de medewerkers niets registreren. Er kunnen geen klachten doorgezet worden, ook niet de ernstige zoals een serieuze vervuiling waarbij de schade met het uur kan oplopen. Dan kan het proces op de ouderwetse manier verlopen, zoals telefoon of face-to-face. Maar daar zijn geen protocollen meer voor. Het zou eventueel mogelijk zijn dat de gemeente door nalatigheid aansprakelijk gesteld kan worden voor de schade die ontstaat door niet direct op te treden.

Problemen met betrekking tot de integriteit van de informatie betreft meestal een verkeerd genoteerd adres, telefoonnummer of iets dergelijk. Dat is voorstelbaar want mensenwerk, maar dat is meestal snel en binnen acceptabele normen op te lossen. Als het gebeurt is het mogelijk lastig, maar niet onoverkomelijk. Een inbreuk op de vertrouwelijkheid van de informatie is daarentegen wel ernstig. Dan gaat het vaak om privacygevoelige informatie van bewoners die op straat komt te liggen, en dat heeft meteen serieuze gevolgen voor de inwoners en kan forse bestuurlijke, financiële en imagoschade voor de gemeente opleveren.

Afsluitend
Bij de melding en verwerking van een klacht leefomgeving is het KlantContactCentrum (KCC) en het team Handhaving en vergunningen betrokken. Bij de registratie wordt gevraagd naar het BSN, wat een bijzonder persoonsgegeven is, maar daar wordt in de afhandeling verder niets mee gedaan. In principe worden geen of weinig bijzondere persoonsgegevens geregistreerd en in het zaaksysteem COSA opgeslagen, maar het kan voorkomen. De logging op dat systeem is gebrekkig, zodat monitoring en handhaving op de activiteiten op de informatie niet mogelijk zijn.

Bijlage 4. Lijst geraadpleegde stukken en lijst van respondenten

Lijst geraadpleegde stukken:

- Aandachtspunten AVG-proof, zonder datum
- Alle processen DSP
- Artikel 44 vragen en beantwoording, Achtkarspelen, 4-11-2016
- IBD- aansluitformulieren VCIB en ACIB Achtkarspelen, 2-12-2013
- IBD- aansluitformulier ACIB Tytsjerksteradiel, zonder datum
- Afspraken Geheimhoudingsverklaring en VOG, 13-6-2016
- Communicatie I-bewustzijn, zd
- Continuïteitsplan de werkmaatschappij Achtkarspelen en Tytsjerksteradiel, versie 0.1, 27-1-2017
- Adviesnota beveiligingsbeleid, Achtkarspelen en Tytsjerksteradiel, 7-3-2016
- Uitwijkdraaiboek Tytsjerksteradiel, 9-11-2015.
- B0-12 2 Beschrijving van rollen met gebruiker 24-04-2018
- B0-12 3 Overzicht actuele gebruikers 24-04-2018
- B0-12 4 2 Overzicht IP-adressen CMS 24-04-2018
- B0-12 5 Controle gebruikers 24-04-2018
- B0-12 6 Overzicht DigiD aansluitingen 24-04-2018
- B0-13 2 Overzicht beheer actuele websites 24-04-2018
- Begrippenlijst
- Belangrijke vragen bij een mogelijk datalek
- 5.1.1 Beleidsuitgangspunten (Stuknummer S2016-18575), 2-3-2016
- BRP Tytsjerksteradiel 10-07-2018
- Cafile967142581092862773 Collegeadvies informatiebeveiliging, 31-8-2016
- Calamiteitenplan Gemeentearchief Tytsjerksteradiel, 4-2017
- Collegevoorstel TD verklaring, stuknummer S2018-18483, 11-7-2018, Bestuurlijk advies
- Dataclassificatie in het kader van de DigiD audit, 30-11-2017, SIM Groep
- DATALEKKEN met verwijzingen 06-2018
- GAP-analyse voor documenten ISMS, 25-7-2018
- Geheimhoudingsverklaring Ambtenaren
- Geheimhoudingsverklaring externe medewerkers
- Hoofdpunten uit SMA, zonder datum
- Incidenten, afhandeling, rollen en verantwoordelijkheden, zonder datum
- Informatiebeveiliging - memo colleges, 11-11-16
- Informatiebeveiliging in een notendop, samenvatting informatiebeveiligingsbeleid, 1-3-2018
- Informatiebeveiligingsbeleid gemeenten Achtkarspelen, Tytsjerksteradiel en de Werkmaatschappij Achtkarspelen en Tytsjerksteradiel, 15-7-2016
- Informatiebeveiligingsplan, 4-4-2017
- Kopie van Export-Benchmark-ENSIA---20-12-2017-144631
- Lijst geaccepteerde risico's 20-12-2017
- Module iBewustzijn: Achter je scherm, Recourse, 19-3-2018
- Namen afdelingen organogram naar systeem, 03-2018
- Notitie informatiebeveiliging directie 8KTD v4, 18-11-2015
- Offerte Recourse voor i-Bewustzijnssessie, 10-11-2016
- Offerte Recourse voor i-Bewustzijnssessie, 23-12-2016
- Opzet gebruik en inrichting DSP en Verwerkingsregister + DPIA
- Overzicht Post en Archief, zonder datum
- Plan van aanpak DSP en Verwerkingsregister
- Presentatie IB en privacy, zonder datum
- Presentatie keten Gebiedsteams, sociaal domein, zonder datum
- Integraal advies: Privacyreglement voor het gebruik van camera's ten behoeve van toezicht en bewaking van gemeentelijke gebouwen en terreinen van de gemeente Tytsjerksteradiel, 12-5-2009
- Procedure In en Uit dienst, 4-5-2017, niet vastgesteld
- Procedures HRM/PSA in ISMS, 07-2018
- Projectvoorstel Implementatie informatisering, vs 1.0, 30-11-2017
- AVG-project Securelink V10, 3-7-2018

- Randvoorwaarden aan de BIG, 19-11-2015
- Rapportage-Zelfevaluatie-Informatieveiligheid--Achtkarspelen-20180423133753 BAG en BGT, 23-4-2018
- Rapportage-Zelfevaluatie-Informatieveiligheid--Achtkarspelen-20180423133925 Compleet, 23-4-2018
- Rapportage-Zelfevaluatie-Informatieveiligheid--Tytsjerksteradiel-20180413103053, 13-4-2018
- Rapportage-Zelfevaluatie-Informatieveiligheid--Tytsjerksteradiel-20180423134256 SUWI, 23-4-2018
- Rapportage-Zelfevaluatie-Informatieveiligheid--Tytsjerksteradiel-20180423134420 BRP en PUN, 23-4-2018
- Register datalekken en meldingen
- Risico's. Waarom beveiligen en waartegen beveiligen? 17-3-2016
- Risico scorecard, 13-6-2018
- SIM Contractuele afspraken verbeteren informatiebeveiliging, mei 2017
- SIM Verwerking persoonsgegevens, Dataclassificatie in het kader van DigiD, 30-11-2017
- Security Maturity Assessment, Securelink, 30-11-2017
- Structuur ISMS
- Toelichting bij Geheimhoudingsverklaring
- Uitgifte van apparaten, 11-7-2018
- Rapport Uitwijktest 2015, Centric, september 2016
- Verklaring DMZ, B05-3 DigiD beveiligingsassessment, 24-4-2018
- Verklaring van toepasselijkheid, Achtkarspelen en Tytsjerksteradiel en werkmaatschappij 8KTD, 1-4-2017
- Verslag gesprek over Procedure in en uit dienst, 18 oktober 2017
- Verwerkingsregister gemeente Tytsjerksteradiel, 25 mei 2018
- Voorstel gebruik afdelingsnamen, zonder datum
- Wachtwoordenbeleid (oudere versie)
- Wetsartikelen bij Geheimhoudingsverklaring
- Top 25 Remediations with Details
- Kwetsbaarheden en remedies, 13-6-2018
- Verslag Applicatiebeheerdersoverleg 1-2-2018

Lijst van respondenten

- Siebe Alkema
- Lutske Alma
- Harjan Bruining
- Gerda Dijkstra-Weidenaar
- Else Fokkinga (telefonisch)
- Jeroen Gebben
- Maaike van Gils
- Pieter Hamstra
- Bert Homma
- Paul Jissink
- Herre Kampen (telefonisch)
- Rina Koning
- Erik van der Laan
- Rommie van der Laan
- Jos Meeuwsen
- Ronald Pieters
- Henk Postmus
- Annet Sijbesma
- Rommy Wijnja
- Munir Yacoub

Bijlage 5. Onderzoeksvragen en normen

De onderstaande normen waaraan per deelvraag is getoetst zijn voornamelijk ontleend aan de BIG en de AVG.

Onderzoeksvragen	Norm
1. Sturen de Colleges van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het informatiebeveiligingsbeleid uit?	Het integrale beleid op het terrein van informatiebeveiliging dient door de Colleges van B&W te worden vastgesteld en gepubliceerd voor werknemers en relevante externe partijen. De colleges dragen het beleid actief uit.
2. Hebben de gemeenten de risico's op informatiebeveiliging benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden?	Het management stelt naar aanleiding van een GAP-analyse het informatiebeveiligingsbeleid op. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld.
3. Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen?	Gemeenten evalueren het informatiebeveiligingsbeleid eens in de drie jaar, of zodra zich belangrijke wijzigingen voordoen, en stellen deze indien nodig bij.
4. Hoe ver zijn de gemeenten gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het gesteld met commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeenten? Dragen zij het privacybeleid uit?	Uiterlijk 25 mei 2018 moesten overheden en bedrijven voldoen aan de AVG van de EU. Daartoe behoort onder andere het aanstellen van een Functionaris voor de Gegevensbescherming (FG), opstellen van een privacystatement en opstellen van een register van verwerkingsactiviteiten.
5. Kennen de gemeenten de leveranciers en partners waarmee ze samenwerken en toetsen zij hen op informatieveiligheidsaspecten, en zo ja hoe? Zijn de gemeenten transparant over het informatiebeveiligingsbeleid richting de ketenpartners?	Gemeenten hebben afgesproken dat risico's op informatieveiligheid die betrekking hebben op externe partijen, die bijvoorbeeld persoonsgegevens verwerken, expliciet worden meegenomen. Daarover moet jaarlijks worden gerapporteerd. Het aspect informatiebeveiliging moet behandeld worden in overeenkomsten met derde partijen. De AVG stelt aanvullende eisen aan de overeenkomst tussen verwerkingsverantwoordelijke, in dit geval de gemeente, en de verwerker. Bijvoorbeeld met betrekking tot het toepassen van passende technische en organisatorische maatregelen. In de Resolutie van de VNG staat dat gestreefd wordt naar transparantie richting ketenpartners.
6. Rapporteren en bespreken de organisaties het functioneren van informatieveiligheid op management- en bestuursniveau (colleges en raden)?	Gemeenten hebben afgesproken dat over het functioneren van de informatiebeveiliging aan het management en bestuur (colleges en raden) wordt gerapporteerd.
7. Wat is de status van de aansluiting van de gemeenten bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?	Aansluiting bij de IBD wordt aangeraden door de VNG.
8. Voldoet de wijze waarop de gemeenten de informatiestroom in processen en applicaties organiseren aan de vereisten op het gebied van informatiebeveiliging en privacy? Zijn de autorisaties, wie van de medewerkers bij welke informatie moet of kan, adequaat geregeld?	De in de administratieve organisatie aanwezige informatie moet in overeenstemming zijn met het beveiligingsniveau op basis van classificatie op beschikbaarheid, integriteit en vertrouwelijkheid (biv).

9. Wordt jaarlijks getoetst of de organisaties in control zijn op het gebied van informatieveiligheid via peer reviews, audits, self-assessments (zelf tests) of pen-testen? Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weten de organisaties hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?	Ten aanzien van de beoordeling van het beveiligingsbeleid dienen er periodieke beveiligingsaudits te worden uitgevoerd. Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management. Op basis van een risicobeoordeling dient een continuïteitsplan met betrekking tot informatiebeveiliging te zijn opgesteld. Daarmee worden essentiële procedures voor continuïteit geïdentificeerd, zoals het veilig stellen, herstel en reconstructie van informatie enz. Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd. Vanaf 1-1-2016 moeten in het kader van de Meldplicht ernstige datalekken direct gemeld worden bij de Autoriteit Persoonsgegevens, en soms aan de betrokkenen.
10. Op welke wijze wordt aandacht besteed aan de bevordering van awareness bij medewerkers van de gemeenten? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houden de gemeenten kennis vast en bouwen zij hierop voort?	Voorwaarde voor informatiebeveiliging is onder andere dat dit een verantwoordelijkheid is van het lijnmanagement en de medewerkers. Bewustwording op en kennis en expertise van risico's zijn essentieel. Gemeenten hebben afgesproken te leren van beveiligings-meldingen met als doel beheersmaatregelen te verbeteren.