Informatiebeveiliging en privacy
Gemeente Geldrop-Mierlo

Rekenkamercommissie Geldrop-Mierlo

Mei 2019

Auteur: drs. Etienne Lemmens,
Prae Advies en onderzoek, Utrecht

Inhoudsopgave

1 Voorwoord

Informatiebeveiliging en privacy zijn actueel. Sinds de invoering van de AVG in mei 2018 hebben velen een beeld daarover gekregen en een besef van urgentie ervan. Gemeenten hebben net als andere organisaties te maken met informatiebeveiliging en privacy. Van de overheid wordt verwacht dat die de zaken voor elkaar heeft. De overheid gaat immers dagelijks om met privacygevoelige gegevens van haar burgers. Als het fout gaat dan is ook de impact groot en zou het beeld van de betrouwbare overheid schade kunnen toebrengen.

De rekenkamercommissie van de Gemeente Geldrop-Mierlo vindt informatiebeveiliging en privacy belangrijk. De rekenkamercommissie heeft dit gegeven met de auditcommissie van de gemeenteraad gedeeld. Daar bleek draagvlak te zijn om in een rekenkameronderzoek na te gaan in hoeverre de gemeente Geldrop-Mierlo de informatiebeveiliging en privacy voldoende heeft georganiseerd en geborgd.

Het onderzoek is gestart in februari 2019, de interviews zijn afgenomen in maart, april stond in het teken van de ambtelijke check op de bevindingen. In mei 2019 zijn de conclusies en aanbevelingen geformuleerd en is het concept rapport aangeboden aan het college van B&W voor een bestuurlijke reactie. Deze reactie is aan het eind van dit rapport integraal opgenomen. In juni 2019 is het rapport aangeboden aan de gemeenteraad van de gemeente Geldrop-Mierlo.

De rekenkamercommissie dankt de onderzoeker Etienne Lemmens die het onderzoek voortvarend en met kennis van zaken heeft uitgevoerd. De rekenkamercommissie is ook veel dank verschuldigd aan de deskundige medewerkers van de gemeente Geldrop Mierlo en de Dienst Dommelvallei die constructief en in een goede samenwerking hun bijdrage aan dit onderzoek hebben geleverd.

De conclusie van het rapport is dat de gemeente Geldrop Mierlo met ondersteuning van de Dienst Dommelvallei hard werkt aan informatiebeveiliging en privacy. Verder stelt de rekenkamercommissie vast dat het een organisch proces is, steeds zet de gemeente stappen om verder met informatiebeveiliging en privacy te komen. De basis en governance op het gebied van informatiebeveiliging en gegevensbescherming zijn bij de gemeente Geldrop-Mierlo deels op orde. Er is nog werk aan de winkel. Dit rapport hoopt daar een bijdrage aan te leveren. Verder hoopt de rekenkamercommissie dat dit onderzoek de gemeenteraad inzicht te geeft in de staat van de informatiebeveiliging en privacy in de gemeente Geldrop-Mierlo en hoe de gemeenteraad haar kaderstellende en controlerende rol op dit terrein nog beter vorm kan geven.

Mr. drs. A.M.M. (Sandra) van Breugel

Voorzitter rekenkamercommissie gemeente Geldrop-Mierlo

2 Inleiding

Gemeenten krijgen steeds meer taken vanuit de Rijksoverheid naar zich toegeschoven, denk bijvoorbeeld aan het sociaal domein, zo ook de gemeente Geldrop-Mierlo. Gevolg hiervan is, onder andere, dat gemeenten in toenemende mate steeds meer persoonlijke en gevoelige data verwerken. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder meer blijkt uit datalekken bij gemeenten en recente onderzoeken van andere rekenkamer(commissie)s. Wat gebeurt er bijvoorbeeld als die informatie op straat komt te liggen? Of als de digitale dienstverlening aan burgers niet meer mogelijk is? Naast financiële, juridische en technische gevolgen kunnen deze crises het imago van de gemeente en de privacy van burgers aantasten.

Beveiliging van informatie is een must voor alle organisaties. Overheden, waaronder gemeenten, hebben, gelet op de toename van de hoeveelheid aan vertrouwelijke data in informatiesystemen, dit goed te organiseren. De Algemene Verordening Gegevensbescherming (AVG, ook bekent als General Data Protection Regulation, GDPR) schrijft voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeente zelf. De Autoriteit Persoonsgegevens registreerde in 2018 20.881 datalekken, tegenover 10.009 in 2017. De overheid is verantwoordelijk voor 17% van de datalekken. De toename van het aantal geregistreerde datalekken is uiteraard mede te 'danken' aan de aandacht die de AVG heeft gegenereerd.

De taak van gemeenten is complex en de praktijk is steeds in ontwikkeling, vooral in het sociaal domein. Informatiebeveiliging wordt soms alleen als een technisch vraagstuk benaderd. De ervaring leert dat men het technisch nog zo goed voor elkaar kan hebben, wat op zich te organiseren is, de cruciale factor in beveiliging is houding en gedrag van de menselijke actor.

2.1 Leeswijzer

In hoofdstuk 3 gaan we in op de algemene beleidsmatige context van gemeenten met betrekking tot informatiebeveiliging en privacy. Ook worden de doelstelling van het onderzoek en de onderzoeksvragen die in het onderzoek centraal staan gepresenteerd. In hoofdstuk 4 behandelen we de gehanteerde onderzoeksaanpak om de vragen te beantwoorden. Hoofdstuk 5 bevat de bevindingen, geordend aan de hand van de onderzoeksvragen. Deze bevindingen zijn getoetst door zowel bij dit onderzoek betrokken medewerkers van de gemeente Geldrop-Mierlo als van de Dienst Dommelvallei. In hoofdstuk 6 staan de conclusies en aanbevelingen.

In de bijlagen is achtereenvolgens een verklarende woordenlijst opgenomen, de bestudeerde documenten en geïnterviewde bestuurders en ambtenaren, het dreigingsbeeld 2019-2020 van de Informatiebeveiligingsdienst Gemeenten (IBD) en tot slot de normen, gekoppeld aan de onderzoeksvragen.

Tot slot is de bestuurlijke reactie op dit rekenkamerrapport opgenomen aan het einde van dit rapport.

3 Doelstelling en onderzoeksvragen

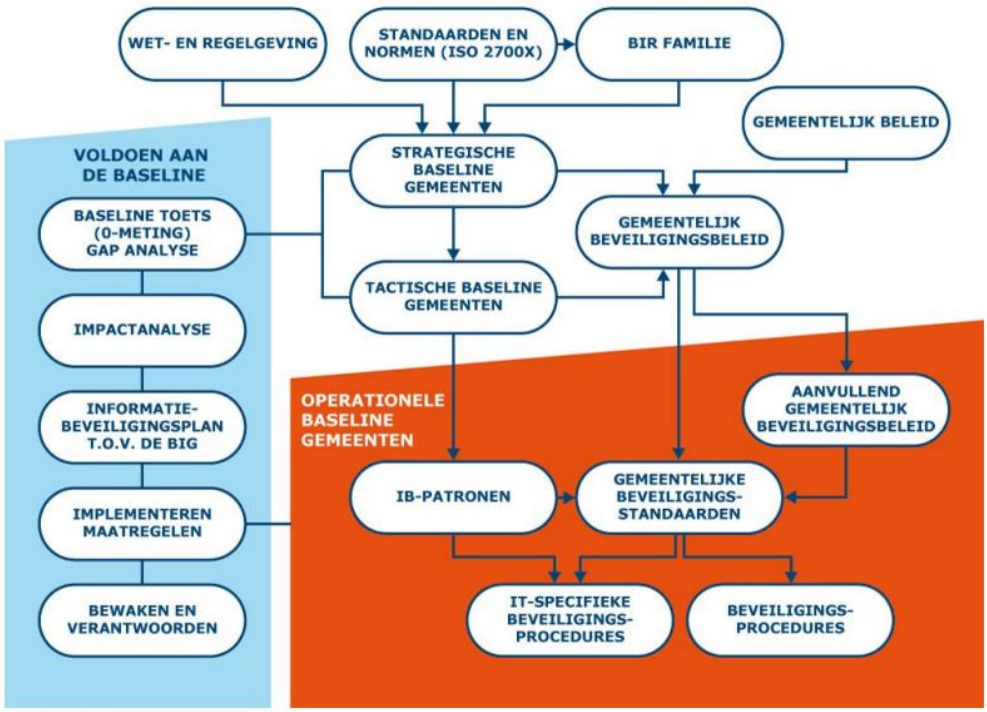
3.1 Context

Informatiebeveiliging

Deze ze paragraaf handelt in over de eisen die aan alle gemeenten worden gesteld met betrekking tot informatiebeveiliging. Het is het raamwerk van eisen en uitgangspunten waar gemeenten aan dienen te voldoen. 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 naar toe werken. De BIG bestaat uit een strategische variant, met richtlijnen over de inrichting van het beleid en de verantwoordelijkheden die belegt 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 de BIG is afgesproken dat het informatiebeveiligingsbeleid minimaal driejaarlijks wordt geüpdatet, met behulp van een GAP-analyse. Dat wil zeggen een assessment in hoeverre de beveiligingssituatie van de gemeente van de gewenste situatie afwijkt. Daarnaast kan de gemeente eigen beveiligingsbeleid formuleren. Op basis daarvan wordt jaarlijks een informatiebeveiligingsplan opgesteld voor de te nemen maatregelen. Afgesproken is dat het lijnmanagement bij de analyses en de maatregelen betrokken wordt. In onderstaand schema is de huidige context van het gemeentelijk informatiebeveiligingsbeleid weergegeven.

Figuur 1. Context Baseline Informatiebeveiliging Gemeenten (BIG).



Bron: Informatiebeveiligingsdienst Gemeenten (IBD)

De BIG wordt in 2020 geüpdatet met de BIO (Baseline Informatiebeveiliging Overheid). Deze is onder andere meer gericht op risicomanagement. Vanaf 2018 is voor het eerst met behulp van de Eenduidige normatiek single information audit (ENSIA) gerapporteerd. In 2018 ging dat over de stand van zaken op 31 december 2017. Deze systematiek gaat de verticale verantwoording richting landelijke toezichthouders en de horizontale verantwoording richting de gemeenteraad op informatiebeveiliging en privacy vormgeven. De richtlijnen uit de BIO en de rapportagevereisten van ENSIA worden in 2020 op elkaar afgestemd.

Context gegevensbescherming

Voor de bescherming van persoonsgegevens is op 25 mei 2016 de opvolger van de Wet Bescherming Persoonsgegevens (Wbp) van kracht geworden, de Algemene Verordening Gegevensbescherming (AVG). 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 zijn gemeenten verplicht een privacyverklaring te 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. En gemeenten moeten op bijzonder privacygevoelige processen data protection impact assessments (dpia) uitvoeren, om op voorhand de risico's te inventariseren die de verwerking van persoonsgegevens met zich mee brengt.

3.2 Centrale onderzoeksvraag

De centrale onderzoeksvraag die de rekenkamercommissie wil beantwoorden luidt:

- In hoeverre heeft de gemeente Geldrop-Mierlo de informatiebeveiliging voldoende georganiseerd en geborgd?

De centrale vraag wordt beantwoord aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

1.	**Stuurt het college 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 commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het informatiebeveiligingsbeleid uit?**
2.	**Heeft de gemeente de risico's op informatiebeveiliging benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?**
3.	**In hoeverre bereidt de gemeente zich voor op de Baseline Informatiebeveiliging Overheid (BIO)?**
4.	**Hoe ver is de gemeente gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het privacybeleid uit?**
5.	**Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatieveiligheidsaspecten, en zo ja hoe?**
6.	**Rapporteert en bespreekt de organisatie het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (college en raad)?**

7.	**Wat is de status van de aansluiting van de gemeente bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?**
8.	**In hoeverre heeft de gemeente zich voorbereid op ENSIA?**
9.	**Wordt jaarlijks getoetst of de organisatie in control is 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? Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?**
10.	**Op welke wijze wordt aandacht besteed aan de bevordering van awareness bij medewerkers van de gemeente? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwen zij hierop voort?**

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 4.

4 Aanpak

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch en interviewverslagen. De documenten bevatten beleid en rapportages van de gemeente Geldrop-Mierlo en de Dienst Dommelvallei (DD) op het gebied van informatiebeveiliging en privacy. In de DD werken de gemeente Geldrop-Mierlo met Nuenen c.a. en Son en Breugel samen op de zogenoemde PIOFA-taken (Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering). De documenten die zijn bestudeerd zijn in bijlage 2 opgenomen, evenals de functies van de in totaal negen bestuurders en functionarissen van de gemeente Geldrop-Mierlo en DD die zijn geïnterviewd. De deskresearch vond plaats in de periode januari-februari 2019. De interviews zijn in maart 2019 afgenomen, in aanwezigheid van de voorzitter van de rekenkamercommissie.

5 Bevindingen

In dit hoofdstuk worden de bevindingen per onderzoeksvraag weergegeven.

5.1 Governance op informatiebeveiliging en privacy

In deze paragraaf geven we antwoord op vraag 1. [1]

Het college van B&W van Geldrop-Mierlo heeft december 2015 het informatiebeveiligingsbeleid, gebaseerd op de BIG, vastgesteld. Het beleid gold breed voor de bij de DD aangesloten gemeenten. De laatste GAP- en risicoanalyse, nodig voor het vaststellen van beleid en de jaarplannen op informatiebeveiliging zijn in 2015-2016 uitgevoerd. Het op basis van dat beleid laatst vastgestelde jaarplan informatiebeveiliging stamt uit 2016. Nog niet alle activiteiten uit het jaarplan uit 2016 zijn op het moment van het onderzoek (kwartaal 1 2019) uitgevoerd. Wel zijn vanaf 2017 op basis van de audits en assessments jaarlijks verbetermaatregelen vastgesteld en in een informatienota naar het college gestuurd.

[1] Stuurt het college 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 commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het informatiebeveiligingsbeleid uit?

In 2016 is op gebied van privacy geïnventariseerd wat de gemeente moest doen om te voldoen aan de Wet bescherming persoonsgegevens (Wbp). Een plan van aanpak is opgesteld, mede om voor te bereiden op de Algemene Verordening Gegevensbescherming (AVG) die in 2016 is ingegaan. Onderdelen uit het plan van aanpak uit 2016 moeten nog uitgevoerd worden, volgens respondenten.

De VNG heeft in het kader van informatiebeveiliging de gemeente en de DD in 2015 gevisiteerd. Vooral op governance zijn daarbij aanbevelingen gedaan. Volgens respondenten is daar meer duidelijkheid op gekomen, en zijn de verantwoordelijkheden belegd tussen gemeenten en DD. Functioneel beheer ligt bij de gemeenten die bij de DD aangesloten zijn.

De thema's informatiebeveiliging en privacy worden, volgens bijna alle respondenten, gedragen door college en MT. Er is een wethouder met speciaal informatiebeveiliging en privacy in zijn portefeuille, die uit de automatiseringsbranche komt. Gemeld wordt dat de afstemming met de andere portefeuillehouders goed gaat. Een paar respondenten vindt dat het nog meer op de agenda mag komen en dat het bewustzijn nog groeiende is. Chief Information Security Officer (CISO) en Functionaris Gegevensbescherming (FG) komen ad hoc bij het MT aan tafel om stand van zaken en maatregelen door te nemen. Zo is de CISO langs geweest voor onder andere de Eenduidige Normatiek Single Information Audit (ENSIA, zie §5.3) en samen met de privacybeheerder is de FG langs geweest voor de data protection impact assessments (dpia's, zie §5.4) De wens van beide kanten is dat op structurele basis te gaan doen, het idee is eenmaal per kwartaal.

Gevraagd naar wat volgens de respondenten goed gaat op informatiebeveiliging en privacy antwoorden ze bijna allemaal dat de awareness bij medewerkers groeit (zie daarvoor §5.9.) en de functies daarop zijn bezet. De belangrijkste functies op informatiebeveiliging en privacy voor de gemeente Geldrop-Mierlo zijn belegd bij de Dienst Dommelvallei, namelijk de CISO en de FG. Beide werken voor alle bij de DD aangesloten gemeenten en de DD zelf. De CISO heeft een aanstelling voor 32 uur. De FG is sinds februari 2018 in dienst bij de DD met een aanstelling voor 24 uur, in het begin 32 uur om de AVG op te starten. Nu staat er, mede op advies van de FG, een vacature open om de functie voor 40 uur fulltime in te vullen.

De CISO en FG hebben op hun gebied een controlerende en adviserende rol, maar veel vragen op operationeel vlak komen bij hen terecht. Op operationeel gebied wordt de CISO bij de gemeente bijgestaan door een informatiebeveiligingsbeheerder zoals bijvoorbeeld bij de applicatie voor de Basisregistratie Personen (BRP). Op gebied van de gegevensbescherming is in de gemeente juridisch medewerker aanwezig die een deel van haar aanstelling van 24 uur per week als privacybeheerder optreedt. Daarvoor loopt een vacature om deze functie voor 32 uur in te vullen, grotendeels aan privacy in te vullen. Er is op enig moment voor gekozen de CISO en FG centraal bij de DD te beleggen. Er is voor gekozen geen algemene informatiebeveiligingsbeheerders bij de gemeente aan te stellen, wel privacybeheerders.

Volgens een aantal respondenten zijn de verschillende taken, zoals die tussen gemeente en DD, en de rollen van CISO en FG, ondertussen uitgekristalliseerd. Zodat duidelijk zou moeten zijn wie waarvoor verantwoordelijk is. Maar niet iedereen vindt de rolverdeling helder. Zo worden de FG en CISO nog als meewerkende medewerkers gezien, in plaats van de advies-, coördinatie- en controlefunctie die zij hebben. Overigens is dit bij meer gemeenten in het land het geval. Bij de gemeente is er volgens een aantal respondenten voor de CISO te weinig uitvoerende capaciteit. Privacybeheerder zijn de operationele handen van de FG in de gemeente. Een dergelijke

operationele functie op informatiebeveiliging ontbreekt bij de gemeente, behalve specifiek bij de applicatie Basisregistratie personen bij Burgerzaken.

De meeste respondenten vinden de afstemming tussen gemeente en DD voldoende, en de functionarissen bij de DD voelen geen afstand met de gemeentelijke organisatie. Zo is er om de 4-6 weken een privacy-overleg tussen CISO, FG, controller en de privacybeheerders van de deelnemende gemeenten. Uit het overleg zijn werkgroepen ontstaan, zoals voor de dpia's en communicatie. Verder is er de werkgroep privacy, conform de privacyverordening, maar die is al enige tijd niet meer bijeen gekomen. De zaken die hier besproken worden zijn de meer generieke aspecten op informatie-beveiliging en privacy. Met vakspecifiek beleid moeten de gemeentelijke afdelingen zelf aan de slag gaan, waar nodig met ondersteuning van de privacybeheerders.

De rol van CISO en FG zijn momenteel elk in een persoon vertegenwoordigd. Bij ziekte/verlof wordt de FG door de CISO vervangen, met name voor de incidenten en datalekken. De CISO wordt vervangen door de controller. Dat is volgens de betrokken respondenten een aandachtspunt, vanwege de specialistische kennis die (meer structureel) onvoldoende vervangen kan worden.

Respondenten geven aan dat middelen voor informatiebeveiliging en privacy hoog geprioriteerd zijn. Informatiebeveiliging heeft binnen de gemeente of binnen de DD weliswaar geen eigen budget, maar in het kader van het Informatiebeleidsplan is budget bij DD aanwezig. Incidentele aanvragen worden daaruit bekostigd. Extra budget voor de DD kan via een begrotingswijziging worden aangevraagd. Benodigde uitgaven in het kader van informatiebeveiliging worden doorgaans goedgekeurd, zo is de ervaring van meerdere respondenten. Maar het is zeker niet zo dat alles vanzelfsprekend toegekend wordt. Het budget moet nog wel bediscussieerd worden, maar dat lijkt volgens respondenten wel beter te gaan dan een aantal jaren geleden.

5.2 Risicogerichtheid van het beleid

In deze paragraaf geven we antwoord op vraag 2. [2]

Een aantal respondenten vindt de gemeente in redelijke mate in control op informatiebeveiliging en privacy, maar een aantal is daar niet van overtuigd. Daarbij wordt met name gewezen op het nog niet op voldoende niveau zijn van het bewustzijn op risico's bij de medewerkers (zie §5.9.) Er wordt volgens sommigen onvoldoende afweging gemaakt welke risico's geaccepteerd worden en op welke geacteerd moet worden. De laatste GAP-analyse en algemene risicoanalyse op informatiebeveiliging is in 2016 uitgevoerd. Wel is op specifieke applicaties een risicoanalyse uitgevoerd, zoals op de Basisregistratie Personen (BRP). Behalve in 2018 is vanwege andere prioriteiten ervoor gekozen geen analyse op risico's uit te voeren. Volgens sommige respondenten is het nemen van maatregelen op informatiebeveiliging nogal ad hoc. De organisatie is bezig met voorkomende problemen oplossen, niet met risico's te analyseren.

Afdelingshoofden zijn integraal eindverantwoordelijk voor de assessments en audits, maar zijn niet betrokken bij inventariseren van de risico's. Adviseur publiekszaken/dienstverlening is bij de

[2] Heeft de gemeente de risico’s op informatiebeveiliging benoemd? Is helder in hoeverre risico’s beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?

zelfevaluatie op de BRP betrokken, en de functioneel beheerders op de assessments/audits op de andere applicaties.

Veelal worden risico's geconstateerd op het verlenen en wijzigen van autorisaties op de toegang van gegevens in de applicaties. Gemeld wordt dat er sinds kort een strikte procedure is afgesproken en deze is nog niet geëvalueerd. Er is een format voor indiensttreding die in de flow wordt opgenomen door de afdeling POI. Afhankelijk van de functie gaat deze langs bij de functioneel beheerder, gaat daarna langs bij het afdelingshoofd en tot slot naar de DD. Binnen de DD wordt de toegang tot de applicaties 'aangezet'. Dit format is nu functiegericht in te vullen, zo worden meteen voor een heel pakket binnen een functie de autorisaties voor applicaties geaccordeerd. Dat zal efficiënter gaan werken, volgens de respondenten.

Bij indiensttredingen gaat het meestal goed, omdat een medewerker autorisaties moet hebben om te kunnen werken. Het is in ieders belang de autorisaties te verlenen. Autorisaties muteren/opheffen bij functiewisseling en uitdiensttreding wordt door een aantal respondenten als een risico ervaren. Structurele controle op de autorisaties heeft voor de eerste keer in 2018 op netwerkniveau plaats-gevonden, niet op het niveau van de applicaties. Het is sinds kort dat de afdelingshoofden en personeelsconsulent regelmatig met elkaar rond de tafel zitten (1 x in de 3 weken). Uitdiensttredingen zijn daar een vast agendapunt. Elk kwartaal worden de inactieve accounts gecontroleerd bij de hoofden van de afdelingen. Jaarlijks toetst adviseur publiekszaken de autorisaties op basis van lijst van P&O. Het kan gebeuren dat iemand er tussen door glipt, maar deze persoon kan niet zomaar bij de gegevens daar de toegang is afgesloten. In de praktijk moet nog blijken of het goed werkt. Een lastig punt bij uitdiensttreding is de externe inhuur, deze is niet altijd bekend bij P&O en kan niet altijd in de controleketen meegenomen worden.

5.3 Voorbereiding op BIO en ENSIA

In deze paragraaf geven we antwoord op vragen 3 en 8. [3]

De Eenduidige Normatiek Single Information Audit (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 onderstaand figuur 2.

[3] In hoeverre bereidt de gemeente zich voor op de Baseline Informatiebeveiliging Overheid (BIO)? In hoeverre heeft de gemeente zich voorbereid op ENSIA?

Figuur 2. ENSIA-model, oplevering 2019.

In 2018 is voor het eerst gerapporteerd in het format van ENSIA over 2017 en jaarlijks zal de verantwoordingsrapportage op informatiebeveiliging en privacy op die systematiek vorm gegeven worden. ENSIA bevat een aantal maatregelen op het vlak van de informatiebeveiliging (BIG) en een aantal op gegevensbescherming (AVG). Niet alleen de CISO en FG van de DD coördineren de rapportage in het kader van ENSIA, de afdelingen in de gemeente moeten ook daarvoor informatie aanleveren. De afdelingshoofden zijn integraal verantwoordelijk, en dus ook als i-manager eindverantwoordelijk voor de assessments en audits waarover in het kader van ENSIA gerapporteerd moet worden. Uit de interviews blijkt dat het vullen van de ENSIA een opgave is waar veel tijd van alle betrokkenen in gaat zitten. Zo besteedt de CISO veel tijd met het daadwerkelijk vullen van ENSIA te, in plaats van coördinatie- en adviesactiviteiten. Ook de afdelingen geven aan er veel tijd mee zoet te zijn.

Respondenten geven aan dat het vullen van de ENSIA meer gestructureerd en planmatig zou kunnen geschieden. Zo ontbreekt een Information Security Management System (ISMS) dat geautomatiseerd rapportages kan opleveren die met de ENSIA te koppelen zijn. Ook komen uit de ENSIA verbeter-maatregelen voort die in een plan van aanpak worden opgenomen. Respondenten geven aan dat op operationeel gebied nog veel te verbeteren valt.

Vanaf 2020 wordt de Baseline Informatiebeveiliging Gemeenten (BIG) vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIG bevatte meer dan 300 maatregelen die gemeenten in het kader van informatiebeveiliging zouden moeten nemen. Welke maatregelen jaarlijks genomen zouden moeten worden, moet uit een GAP- en risicoanalyse voortkomen. Zoals in §5.1 reeds is geconstateerd is een plan van aanpak op basis van een risicoanalyse voor het laatst in 2016 opgesteld. Dit plan van aanpak is nog steeds actueel, in de zin dat nog niet alle maatregelen zijn geïmplementeerd. De BIO is gebaseerd op de actuele ISO 27002 norm, bevat veel minder (verplichte) maatregelen, kent meer beveiligingsniveaus en is meer proces- en risicogestuurd dan de BIG. 2019 is een overgangsjaar van BIG naar BIO. Dat betekent dat gemeenten formeel de BIG als uitgangspunt moeten hanteren, maar zich alvast kunnen voorbereiden op de nieuwe baseline. Dat kunnen ze doen met behulp van een zogenoemde baselinetoets, GAP- en risicoanalyse en een daarop te baseren informatiebeveiligingsbeleid en jaarplan. Deze activiteiten staan gepland voor het najaar van 2019.

5.4 Implementatie AVG

In deze paragraaf geven we antwoord op vraag 4. [4]

De Algemene Verordening Gegevensbescherming (AVG), waarmee de privacywetgeving in de Europese Unie is geharmoniseerd, is vanaf 25 mei 2016 van kracht. Overheden en bedrijfsleven kregen twee jaar de tijd om zich daaraan te conformeren. Vanaf 25 mei 2018 is de handhaving van de verordening ingegaan, en die geschiedt in Nederland door de Autoriteit Persoonsgegevens (AP).

In 2016 heeft een extern bureau voor de gemeente Geldrop-Mierlo geïnventariseerd wat gedaan moest worden om te voldoen aan de privacywetgeving, dit als voorbereiding op de AVG in 2018. Op basis daarvan is een plan van aanpak opgesteld. Als gevolg daarvan is er onder andere een privacy verordening en een privacyverklaring opgesteld. Hierin geeft de gemeente aan hoe deze met privacygevoelige informatie omgaat. Tevens is in 2016 een verwerkingsregister opgesteld, waarin alle processen zijn opgenomen waarin de gemeente persoonsgegevens verwerkt. De rekenkamercommissie constateert dat de gemeente er in 2016 relatief vroeg bij was met deze initiatieven. Momenteel speelt evenwel het feit dat bijvoorbeeld het register niet meer actueel is en de privacyverordening aangepast moet worden aan de AVG. Het plan van aanpak is dus nog grotendeels actueel.

Primair is het aan iedere afdeling zelf om ervoor te zorgen dat aan de privacyregels wordt voldaan. Zo wordt door het CMD een werkgroep opgestart om privacyaspecten in het sociaal domein op te pakken. CMD heeft een eigen nieuwsbrief waarin ook al eens berichten over privacy zijn opgenomen. Bij de privacybeheerder kan de afdelingen terecht voor advies en ondersteuning. Vanzelfsprekend let de privacybeheerder ook op of er iets speelt bij een afdeling. Uit de interviews komt het beeld naar voren dat de basis op gegevensbescherming op orde is, maar dat voortdurend actie blijft op verbeteren en actualiseren. Het gereed komen van update van de verordening en verwerkings-register staan voor medio 2019 op de rol. Het register is er dus al wel, en aangegeven werd dat onlangs een uitvraag is gedaan bij de afdelingshoofden om dat eens kritisch door te lopen. Er is een formulier waarmee wijzigingen in gegevensverwerkingen of nieuwe verwerkingen gemeld kunnen worden. Daarmee kan het register waar nodig worden gewijzigd of aangevuld.

Ook op de verwerkersovereenkomsten moet nog een inhaalslag gemaakt worden. Een verwerkers-overeenkomst wordt gesloten met een partij die voor of namens de gemeente gegevens van personen verwerkt. Daarin wordt afgesproken hoe de gegevensverwerking geschiedt, het doel van de verwerking, de beveiliging van de gegevens en de verantwoordelijkheid en aansprakelijkheid bij een datalek. Bij nieuwe aanbestedingen worden de nieuwe overeenkomsten, die AVG-proof zijn, gebruikt. Daarbij is het de bedoeling de nieuwe standaard van de Informatiebeveiligingsdienst Gemeenten (IBD) te gebruiken. Een voorstel daartoe ligt volgens een van de respondenten binnenkort voor bij het college. Organisaties met oude contracten zonder verwerkersovereenkomst worden aangeschreven om een nieuw contract te sluiten. De indruk van de respondenten is dat de afdelingen er hard mee aan de slag zijn. De privacybeheerder krijgt een kopie van de nieuwe

[4] Hoe ver is de gemeente gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het privacybeleid uit?

verwerkersovereenkomsten, maar zolang het verwerkingsregister nog niet volledig geactualiseerd is ontbreekt een goed overzicht.

Bij privacygevoelige verwerkingsprocessen moet het risico in kaart gebracht worden, met een zogenoemd data protection impact assessment (dpia). De gemeente is bezig een checklist waarmee een vakafdeling zelf kan toetsen of zo'n assessment nodig is. Op moment van onderzoek is één dpia gehouden, op vroegsignalering bij schulden. Deze is voor advies voorgelegd aan de FG. Drie assessments lopen nog, waaronder een naar de peutermonitor. Voorlopig trekken een medewerker van de vakafdeling en de privacybeheerder samen op bij het uitvoeren van een dpia. In de toekomst moeten de afdelingen daar zelf meer in gaan doen. Formulieren voor nieuwe projecten gaan in de toekomst standaard samen met de checklist voor een dpia. Zo loopt de aanbesteding voor een nieuw systeem voor zaakgericht werken, waarmee ook zaakgericht werken in het kader van het sociaal domein gekoppeld kan worden. Dat is nu niet het geval. Op dit nieuwe zaaksysteem zal een dpia moeten worden uitgevoerd.

Een procedure beveiligingsincidenten en datalekken was al ruim voor 2018 opgesteld, deze moet geactualiseerd worden. Zo is de rol van de FG niet beschreven, daar die functie op moment van opstellen van de procedure er nog niet was. In 2018 zijn in totaal zes datalekken geregistreerd waarvan vier gemeld als datalek bij de AP. In een enkel geval, als er vanwege een datalek mogelijk consequenties zijn voor de betrokken burger(s), moeten deze geïnformeerd zodat zij indien nodig actie kunnen ondernemen om erger of misbruik te voorkomen. Er is in 2018 een datalek geweest waarbij betrokkenen geïnformeerd moesten worden. Dat betreft een lek vanwege een foute adressering waardoor gegevens op een verkeerde plek werden bezorgd.

5.5 Samenwerking met derden

In deze paragraaf geven we antwoord op vraag 5. [5]

De gemeente en de DD hebben in algemene zin de partijen die gegevens verwerken voor of namens de gemeente in beeld. Maar, zoals in de vorige paragraaf aangegeven, is de gemeente bezig met een inhaalslag op het verwerkingsregister en verwerkersovereenkomsten. Al veel overeenkomsten zijn op de nieuwe AVG-leest geschoeid, maar het proces is nog niet afgerond. Vaak is er bij de overeenkomsten discussie over de inhoud en de aansprakelijkheid bij boetes op datalekken. Inkoopcontracten en de onderliggende verwerkersovereenkomsten verschillen tussen aanbieders. Dat hangt onder andere af van de langdurigheid van de relatie. Zoals met Centric van wie de applicaties al jarenlang bij de gemeente en DD draaien, is er een andere relatie dan met nieuwere leveranciers. Bij die laatsten moeten veel meer zaken op informatiebeveiliging geregeld worden. Dat geeft de gemeente en de DD een sterkere positie tegenover leveranciers om afspraken af te dwingen.

De vakafdelingen zijn, in het kader van integraal management, verantwoordelijk voor het sluiten en up-to-date houden van de verwerkersovereenkomsten. Daarbij wordt over het algemeen advies ingewonnen van de privacybeheerder, een jurist en automatiseringsdeskundigen. Bij overeenkomsten waarin relatief veel informatiebeveiligingsaspecten aan de orde komen, schakelen

[5] Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatie-veiligheidsaspecten, en zo ja hoe?

de vakafdelingen de CISO voor advies in. Uiteindelijk ziet de FG toe op de uitvoering en kan de verwerkersovereenkomsten controleren op aspecten met betrekking tot privacy.

Als voorbeeld kan Senzer in Helmond dienen. Uitvoering van de Sociale Dienst is belegd bij Senzer, behalve de Bijzondere Bijstand die voert de gemeente Geldrop-Mierlo zelf uit. Senzer scoorde een onvoldoende op de audit op SUWInet in 2017, met name op gebied van de administratieve organisatie. In 2018 zijn verbeteringen hierop door Senzer doorgevoerd. Met Senzer is in 2018 een nieuwe verwerkersovereenkomst gesloten die AVG-proof is. Door middel van een zogenoemd 'third party memorandum' (TPM) kan de gemeente controleren of en hoe Senzer zich houdt aan de afspraken op het gebied van informatiebeveiliging en privacy.

5.6 Rapportages op informatiebeveiliging en gegevensbescherming

In deze paragraaf geven we antwoord op vraag 6. [6]

Intern rapporteren CISO en FG over informatiebeveiliging en privacy aan het MT van de Dienst Dommelvallei (DD) en de drie deelnemende gemeenten. Er is een directe lijn tussen de functionarissen en de portefeuillehouders. Dat is ook de bedoeling, daar beide functies geen lijn- maar staffuncties zijn. Los van de lijn moeten zij op hun terrein een afweging van de risico's maken en naar de hoogste leiding kunnen rapporteren. De CISO geeft aan aangesloten te zijn op het portefeuillehoudersoverleg (POHO) ICT.

Specifiek voor datalekken heeft de FG direct contact met de burgemeester. Over de audits en assessments op de applicaties, de beveiligingsincidenten en vordering van de maatregelen op de informatiebeveiliging wordt aan MT en college gerapporteerd in het kader van de P&C-cyclus. Voor de rapportages in dat kader was een geïntegreerd managementrapportagetool aanwezig, een zogenoemd Information Security Management System (ISMS), dit systeem werkte echter niet samen met ENSIA (zie §5.3), het rapportageformat voor de verticale en horizontale verantwoording vanaf 2017. Momenteel werken de ambtenaren met informatie uit verschillende systemen. Zo worden onder andere beveiligingsincidenten bijgehouden in Topdesk, gegevens in Excel overgenomen en gerapporteerd en ter informatie verwerkt met Corsa, het zaakgerichte systeem. Volgens een van de respondenten is er wel een systeem aanwezig, maar daarvan wordt nog niet alle functionaliteit gebruikt. De P&C-cyclus kan beter en efficiënter ingericht worden, vinden de respondenten. Tevens kan geconstateerd worden dat P&C-cyclus niet met de PDCA-cyclus (Plan-Do-Check-Act, de kwaliteits- en leercirkel van Deming) is verbonden (zie ook §5.9).

Naar aanleiding van ENSIA worden verbetermaatregelen geformuleerd en in een plan van aanpak opgenomen. Daarover wordt het college in een Informatienota gerapporteerd. In het MT wordt ENSIA wel genoemd, maar de informatienota wordt niet inhoudelijk besproken. De activiteiten moeten binnen de vakafdelingen opgepakt worden.

In het jaarverslag van de gemeente wordt summier verantwoording afgelegd aan de raad over inzet van middelen en maatregelen in het kader van informatiebeveiliging en privacy. Het jaarverslag van de DD gaat al iets meer inhoudelijk in op de onderwerpen. Teneinde gestructureerd de verticale verantwoording (richting landelijke toezichthouders) en de horizontale verantwoording (richting

---

[6] Rapporteert en bespreekt de organisatie het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (college en raad)?

gemeenteraad) in te richten is ENSIA ontworpen. Vanaf 2020 worden ENSIA en BIO op elkaar afgestemd.

Over het algemeen zijn de geïnterviewden het erover eens dat informatiebeveiliging geen 'hot en sexy' onderwerp is, terwijl velen het belang er zeker van inzien. Ernstige datalekken die acute actie vergen, worden besproken in het presidium van de gemeenteraad. Het onderwerp informatiebeveiliging en de maatregelen daarop worden besproken in de commissie Algemene Zaken van de gemeenteraad. De respondenten ervaren dat de gemeenteraad zich actiever opstelt en om informatie vraagt. En niet alleen als in de pers gerapporteerd wordt over een datalek of probleem elders in het land. Er is in 2018 een keer een sessie belegd met en voor de raad over Digitalisering en Betere Dienstverlening. In die bijeenkomst is niet diep ingezoomd op informatiebeveiliging. Op 6 mei 2019 staat een gezamenlijke sessie van de bij de DD betrokken gemeenteraden gepland over ondermijning. Daar wordt op hoofdlijnen ingegaan op informatiebeveiliging. Maar door het praktisch te maken en te koppelen aan een actueel onderwerp, kunnen informatiebeveiliging en privacy wel aandacht krijgen.

Zoals uit figuur 2 (p. 10) blijkt bevat ENSIA een vormvrij deel, over de maatregelen in het kader van informatiebeveiliging en privacy en het meerjarenperspectief. Respondenten geven aan daar geen aparte rapportage voor op te willen tuigen, maar dit onderdeel in de reguliere informatiecyclus mee te nemen. De raad wordt volgens respondenten overvoerd met informatie. Op die manier wordt getracht deze onderwerpen voor de raad behapbaar en toegankelijk te maken.

5.7 Aansluiting Informatiebeveiligingsdienst Gemeenten (IBD)

In deze paragraaf geven we antwoord op vraag 7. [7]

De Informatiebeveiligingsdienst Gemeenten (IBD) ondersteunt gemeenten op het gebied van informatiebeveiliging met advies, producten en diensten. De IBD krijgt bijvoorbeeld 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 (ACIB en VCIB)
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 of BIO. Aansluiting op de dienst wordt wel aangeraden in de resolutie die de gemeenten in VNG-verband in 2013 hebben aangenomen.

Alle applicaties en infrastructuur op ICT bij de gemeente draait via de Dienst Dommelvallei. De algemene contactpersoon informatiebeveiliging (ACIB) en de vertrouwde contactpersoon informatiebeveiliging (VCIB) zijn bij de DD aangewezen. De algemene contactpersoon krijgt risicomeldingen van de IBD van meer algemene aard, bijvoorbeeld wanneer software geüpdatet moet worden. De vertrouwde contactpersonen krijgen meldingen die vertrouwelijk van aard zijn,

[7] Wat is de status van de aansluiting van de gemeente bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?

zoals bijvoorbeeld van het Nationaal Cyber Security Centrum (NCSC) die door de IBD worden verzameld en doorgespeeld.

De VCIB en ACIB zijn bij de DD aangewezen, terwijl de applicatiebeheerders bij de gemeente zijn aangesteld. Er is onderling afstemming op risico's en zaken die door de IBD bij de contactpersonen worden gemeld, voor zover de informatie gedeeld moet en kan worden. De overige 2 stappen, het doorgeven aan de IBD van de bij de gemeente in gebruik zijnde IP-adressen, url's (websiteadressen) en de ICT-foto zijn ook gezet. Daarmee kan de IBD specifieke risicomeldingen op maat aan de DD doorgeven.

5.8 Controle en continuïteit

In deze paragraaf geven we antwoord op vraag 9. [8]

Bij de documentenanalyse zijn beleid en procedures aangetroffen hoe te handelen bij een calamiteit. De systemen bij de gemeente zijn gespiegeld elders opgeslagen bij de gemeenten aangesloten bij de DD. Bij uitval in Geldrop-Mierlo kan de dienstverlening relatief gemakkelijk weer op een andere site worden opgepakt. Er zijn op onderdelen continuïteitsplannen aangetroffen en deze worden technisch getest, wat een eis is in de landelijke audits van de cruciale applicaties. Maar er is geen integraal continuïteitsplan aanwezig, waarmee de verschillende deelplannen onderling worden afgestemd.

Beheersmaatregelen op informatiebeveiliging moeten door o.a. het functioneel beheer geïmplementeerd worden volgens respondenten. Daar is een procesmatige aanpak voor nodig en die capaciteit is volgens sommige respondenten nog niet volledig goed uitontwikkeld. Sommige systemen zijn verouderd en moeten op korte termijn vernieuwd of vervangen worden. De DD is bezig wijzigingsbeheer met behulp van een gestructureerd proces neer te zetten. Dat is nog in ontwikkeling.

Het dataverkeer van buiten naar binnen de organisatie wordt gecheckt met de benodigde drempels en firewalls. Intern is het dataverkeer gescheiden in compartimenten. Respondenten geven aan dat het verkeer tussen de compartimenten onderling niet door interne firewalls wordt gecontroleerd. Daarmee bestaat het risico dat malware/virus of kwaadwillende die onverhoopt binnenkomt zich makkelijk kan verspreiden in het netwerk.

Het huidige wachtwoordbeleid dat vanuit de DD wordt voorgeschreven voldoet niet geheel aan de eisen van de BIG. Door 2-staps-verificatie of 2 factor authenticatie (2FA) zal vanaf 2020, in het kader van de BIO, minder strenge eisen gelden. Op 'bring' of 'choose' 'your own device' (BYOD/CYOD) is door de DD geen expliciet geformuleerd beleid geformuleerd. Het staat volgens een van de respondenten in de planning voor 2020. Het beleid voor zogenoemd plaatsonafhankelijk werken (POW) is door de gemeente zelf opgesteld en wordt met apparatuur ondersteund door de DD. Medewerkers kunnen een chromebook ter beschikking krijgen, waarmee ze internet kunnen gebruiken en plaatsonafhankelijk kunnen werken. Met een token voor 2-staps-verificatie, waarmee ze veilig kunnen inloggen in de systemen en applicaties waarvoor ze geautoriseerd zijn. De

[8] Wordt jaarlijks getoetst of de organisatie in control is 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? Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?

applicaties draaien centraal en de gegevens staan centraal opgeslagen, zodat niets decentraal op apparaten wordt opgeslagen.

Raadsleden werken in de cloud met iBabs, dat is afgeschermd van de ICT infrastructuur van DD. Er is voor raadsleden een apart budget, die zij voor tablets gebruiken. Dat wordt beheerd en geregeld via de griffie van de gemeente.

Een belangrijk element in de controle en verantwoording is de logging van het gebruik van data. Daarmee kan achteraf gecheckt worden wie wanneer welke data heeft geraadpleegd. Oneigenlijke toegang en misbruik van data kan daarmee aangetoond worden. Automatische logging is niet in alle systemen gerealiseerd. Wel in de applicaties en verwerkingen waarvoor dat verplicht is, zoals de BRP die bij de gemeente of het landelijke SUWInet dat bij Senzer en de gemeente wordt gebruikt. Daar wordt in de landelijke audits op gecheckt. De reden waarom logging niet vaker aanwezig is niet zozeer informatiebeveiligingsinhoudelijk aangelegenheid, maar grotendeels technisch. De faciliteit daartoe ontbreekt in sommige systemen en applicaties. Aangegeven wordt dat in de nieuw aan te schaffen systemen naar de mogelijkheid voor automatische logging wordt gekeken. Daarnaast ontbreekt het volgens respondenten aan de capaciteit om iets met de data te doen die de logging oplevert.

De gemeente, noch de DD, laat pentesten uitvoeren op de technische of fysieke toegankelijkheid van de systemen. Daarmee kunnen mogelijk verborgen gebreken in de beveiliging naar boven komen. Technische testen worden wel vereist in het kader van de landelijke audits, maar deze stellen niet heel uitgebreide eisen. Respondenten melden dat er te weinig capaciteit is om eventuele pentesten te begeleiden of opvolging te geven aan de opbrengsten van deze testen. In dit onderzoek hebben dergelijke testen met behulp van een ethisch hacker niet plaatsgevonden.

5.9 Awareness

In deze paragraaf geven we antwoord op vraag 10. [9]

Gevraagd naar wat goed gaat op het gebied van informatiebeveiliging en privacy antwoordden alle respondenten dat de bewustwording op risico's bij medewerkers toeneemt. De meesten geven aan dat het altijd beter kan en nog niet op het gewenste niveau is, maar dat er aandacht voor is vanuit management en bestuur. Mede vanwege de aandacht die in de aanloop tot de handhaving van de AVG is gegenereerd.[10]

Een teken van awareness bij medewerkers is dat zij de privacybeheerder, FG en CISO weten te vinden en met vragen komen op het terrein van informatiebeveiliging en privacy. Voor zover respondenten kunnen nagaan heerst er geen terughoudendheid of angst om datalekken te melden en worden deze ook daadwerkelijk gemeld. Vraag blijft bij sommigen of medewerkers volledig beseffen hoe snel er sprake kan zijn van een datalek. Indruk bij de respondenten is ook dat men onderling oplet of beeldscherm en PC zijn afgesloten als mensen van de werkplek lopen. Een illustratief voorbeeld bij de gemeente Geldrop-Mierlo is dat bij de afdeling Burgerzaken, waar de medewerkers al lang

---

[9] Op welke wijze wordt aandacht besteed aan de bevordering van awareness bij medewerkers van de gemeente? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwen zij hierop voort?

[10] De AVG is vanaf 25 mei 2016 in de EU van kracht, en organisaties kregen 2 jaar zich daarop voor te bereiden voordat gehandhaafd zou gaan worden. Dat gebeurt door de AP vanaf 25 mei 2018.

gewend zijn met beveiligde persoonsgegevens te werken, moet op gebak getrakteerd worden als je de PC en scherm open laat staan. Dan slijten nieuwe gewoonten snel in, zo is de ervaring.

Er is een kennispagina op intranet en in het Selfservice portaal en in het algemeen plaatsen de privacybeheerder, FG of CISO regelmatig berichten over aspecten op het vlak van informatiebeveiliging en privacy. De FG, CISO en privacy beheerder geven presentaties in MT en als er vragen zijn vanuit afdelingen gaan ze daar langs. Er is voor alle medewerkers een e-learning-module over informatiebeveiliging aangeboden en gegeven in 2017-2018. Velen hebben hier aan meegedaan. November 2018 is een privacydag gehouden waarbij afdelingen langs kwamen om informatie te krijgen en vragen te stellen. De onderwerpen vergen continu aandacht. Zo wordt er nagedacht over een module over privacy, aan te haken bij de e-learning-module die P&O waarschijnlijk in 2019 gaat aanschaffen.

Alle respondenten vinden dat de awareness groeit en aandacht eraan besteed moet blijven worden, maar enkele respondenten vinden dat het intensiever mag. Een e-learning-module wordt gezien als een extensieve vorm van aandacht genereren en de vraag is of en hoe lang de kennis en awareness beklijft. Bij vragen komen de FG, CISO en privacybeheerder langs bij de afdelingen, maar aangegeven wordt dat de capaciteit ontbreekt om dat op structurele basis te doen. Op onderdelen worden zaken geregistreerd, zoals beveiligingsincidenten in Topdesk, en daarvan kan geleerd worden. Maar hiervoor is geconstateerd dat een gestructureerd rapportagesysteem (ISMS) ontbreekt, en de managementrapportages niet aan de leercyclus (PDCA-cyclus) verbonden zijn. Het risico is aanwezig dat er geen follow up wordt gegeven aan bevindingen uit de rapportages en weinig mogelijkheden zijn om te leren van de ervaringen. Tevens geven de respondenten van de DD aan dat het team te weinig capaciteit heeft om de PDCA-cyclus bij de aangesloten gemeenten te ondersteunen. De meeste respondenten geven aan dat op bewustwording en awareness nog te veel risico's zijn om 'in control' te zijn.

De gemeente, en de andere bij de DD aangesloten gemeenten, zijn relatief kleine werkgevers, en op de arbeidsmarkt is een hevige concurrentie op mensen met kennis en competenties op informatiebeveiliging en privacy. Enkele respondenten ervaren als een risico dat de organisaties mensen en kennis kwijt raken.

6 Conclusies en aanbevelingen

6.1 Conclusies

Het belang, de urgentie en de risico's van informatiebeveiliging en gegevensbescherming worden zeker erkend door zowel de gemeenteraad, bestuur als ambtenaren bij de gemeente Geldrop-Mierlo. De laatste jaren is door velen hard gewerkt aan dit onderwerp, wat wordt betiteld als taai en weinig 'sexy'. De basis en governance op het gebied van informatiebeveiliging en gegevensbescherming zijn bij de gemeente Geldrop-Mierlo deels op orde. Dat geldt dus, in het verlengde hiervan, ook voor de Dienst Dommelvallei waarin de gemeente met andere gemeenten o.a. op ICT samenwerkt. Beleid op informatiebeveiliging en privacy wordt gedragen door college en management. Middelen en menskracht voor de noodzakelijke maatregelen op informatiebeveiliging en privacy worden vrijwel altijd welwillend en tijdig ter beschikking gesteld.

De gemeente stuurt op de BIG en de AVG en de specifieke functies zoals voorzien in de BIG en de AVG zijn ingevuld. In 2015 is het informatiebeveiligingsbeleid vastgesteld, maar nog niet alle maatregelen uit het laatste jaarplan, dat dateert uit 2016, zijn in het eerste kwartaal van 2019 gerealiseerd. De noodzakelijke assessments en audits worden uitgevoerd en leiden tot de noodzakelijke verbeteringen. Dit geldt in het bijzonder vanaf 2017 mede in het kader van de ENSIA-rapportages. Het overall beeld is dat de prioriteit lijkt te liggen bij het signaleren van problemen en nemen van maatregelen dit in tegenstelling tot een meer gestructureerde aanpak op informatie-beveiliging op basis van risicoanalyses. Dat blijkt uit het niet tijdig vernieuwen van informatiebeveiligingsbeleid en -plannen. De BIG, en vooral de BIO die vanaf 2020 geldt, vergt een informatiebeveiligingsbeleid dat gericht is op een gestructureerde aanpak van risico's. De gemeente en de DD geven aan bezig te zijn zich daarop voor te bereiden vanaf het najaar 2019.

Een plan van aanpak met maatregelen in het kader van gegevensbescherming is er al vanaf 2016, nog op basis van de Wbp en nog ruim voor de implementatie van de AVG. In die tijd liep de gemeente Geldrop-Mierlo voorop wat betreft gegevensbescherming. In die tijd heeft de gemeente een aantal maatregelen genomen, die nu in het kader van de AVG geüpdatet moeten worden. Zoals de procedure melden datalekken, verwerkersovereenkomsten en het verwerkingsregister. Het verwerkingsregister moet nog door de afdelingshoofden gecompleteerd worden. Op de verwerkersovereenkomsten is de gemeente bezig met een inhaalslag, op basis van de nieuwe standaard van de IBD. Een data protection impact assessment is bijna afgerond en er staat nog een aantal in de planning. De conclusies is dat de kennis aanwezig is en dat de medewerkers van zowel de gemeente Geldrop-Mierlo als DD op dit moment hard werken om alles voor elkaar te krijgen. Hierbij ziet de rekenkamercommissie dat getracht wordt een omslag te bewerkstelligen van reactief werken (oplossen van problemen) naar een meer risicogestuurde aanpak.

De functies op informatiebeveiliging en gegevensbescherming zijn door de DD ingevuld, maar hebben voor de aantal organisaties (drie gemeenten en de DD zelf) die zij moeten bedienen een te beperkte capaciteit. De functies, bedoeld voor advies en toezicht, zijn een het overgrote deel van hun tijd operationeel bezig. Adequate vervanging bij vakantie en ziekte is op hoofdlijnen geregeld. Als zich een incident voordoet vraagt de rekenkamercommissie zich af of de vervanging in voldoende mate in staat is qua kennis en ervaring om daadwerkelijk te handelen. Dit is dan ook zeker een aandachtspunt. Voor de FG is een uitbreiding in de planning naar 40 uur per week en er staat (maart

2019) een vacature open. Op gegevensbescherming is een privacybeheerder in de gemeentelijke organisatie aanwezig, maar een dergelijke functie ontbreekt op informatiebeveiliging.

De gemeenteraad is incidenteel geïnformeerd over informatiebeveiliging en privacy. Daarover werd In het kader van bedrijfsvoering kort gerapporteerd in de jaarstukken. Vanaf 2017 krijgt de raad jaarlijks op basis van ENSIA gerapporteerd over de assessments, evaluaties en beheersmaatregelen op informatiebeveiliging en privacy. Het vormvrije deel van ENSIA-rapportage richting de gemeenteraad is in Geldrop-Mierlo nog niet nader ingevuld. College en ambtenaren geven aan hierop geen aparte rapportagestroom naar de gemeenteraad op te willen zetten. Getracht wordt deze onderwerpen op hoofdlijnen en in een praktische context te behandelen.

Ambtenaren die de assessments en evaluaties moeten uitvoeren en ENSIA moeten vullen, geven aan dat het een grote opgave is en veel tijd vraagt. Een ISMS, dat geautomatiseerd rapportages kan genereren en met ENSIA gekoppeld kan worden, ontbreekt. Daarmee ontbreekt ook een koppeling van de eventuele beheersmaatregelen die uit de rapportages naar voren komen met de PDCA-cyclus. Daardoor lijken de verbetermaatregelen te weinig te beklijven. De maatregelen moeten door het functionele beheer in de afdelingen geïmplementeerd worden, maar daarvoor ontbreekt vooralsnog een procesmatige aanpak. Een gestructureerd beheer van wijzigingen, zoals in applicaties en hardware, is in ontwikkeling. Op een aantal punten is geen expliciet beleid geformuleerd, zoals het 'bring' of 'choose your own device'. Dat staat wel in de planning, maar een aantal respondenten geeft aan dat er in het algemeen meer procedures op papier gezet en meer processen vastgelegd kunnen worden.

Verlenen en wijzigen van autorisaties op de toegang tot gegevens in applicaties is een punt van aandacht, zoals in veel organisaties. Structurele jaarlijkse controle van de autorisaties op netwerkniveau heeft voor het eerst recent plaats gevonden. Er zijn overleggen tussen afdelingshoofden en P&O hierover en controles op inactieve accounts van medewerkers vinden plaats. Bij functiewisseling en uitdiensttreding, vooral bij externe inhuur, liggen risico's op ongeautoriseerde toegang tot informatie. Een punt van aandacht in controle en verantwoording is de logging van de toegang tot informatie. In de meeste systemen die de gemeente gebruikt ontbreekt deze functionaliteit, behalve daar waar het verplicht is, zoals bij de BRP. Aangegeven wordt dat gekeken wordt naar deze functionaliteit bij vernieuwing van de systemen. Tevens wordt aangegeven dat er te beperkte capaciteit is om de vele gegevens die deze registratie oplevert te bekijken en te interpreteren.

Met betrekking tot de continuïteit van de bedrijfsvoering en de dienstverlening van de gemeente zijn op onderdelen continuïteitsplannen aanwezig, maar er ontbreekt een integraal plan. De individuele plannen worden wel getest. Op de punten waarop het vanwege de audits verplicht is worden technische testen op systemen uitgevoerd. Maar de gemeente noch de DD laten uitgebreide technische testen door externen of ethische hackers uitvoeren. De rekenkamercommissie heeft geen dergelijke technische testen uitgevoerd op de systemen en infrastructuur van de DD of de gemeente. De rekenkamercommissie kan dus geen conclusies trekken die ingaan op de kwetsbaarheid van de systemen. Ook zijn geen phishing mail-campagnes uitgevoerd om de 'awareness' of bewustwording van risico's op informatiebeveiliging bij medewerkers te testen.

De meeste respondenten geven aan dat de awareness op informatiebeveiliging en privacy bij management en medewerkers de laatste jaren is toegenomen. De FG, CISO en privacybeheerder

gaan langs bij de afdelingen als er vragen zijn, maar voor een structureel regelmatig bezoek ontbreekt de capaciteit. Medewerkers zijn bezig met deze onderwerpen en komen met vragen naar de FG, CISO en privacybeheerder. De medewerkers wijzen elkaar, volgens meerdere respondenten, in toenemende mate op risicovol gedrag en de medewerkers hebben in 2017-2018 via een e-learning module kennis kunnen opdoen van de risico's op informatiebeveiliging. E-learning is een extensieve manier van awareness ondersteunen en verstevigen, en de vraag is hoeveel kennis op de lange duur bij de medewerkers beklijft. Het is een zaak om continu en intensief inzetten op bewustwording in de gehele organisatie, daar de dreigingen toenemen, zie bijlage 3. Daarbij komt ook het feit dat de krapte op de arbeidsmarkt leidt dat het lastig kan zijn om mensen met de schaarse kennis op informatiebeveiliging en privacy aan te trekken en te binden.

6.2 Aansporingen en aanbevelingen

De rekenkamercommissie doet naar aanleiding van bovenstaande conclusies de volgende aansporingen en aanbevelingen. De rekenkamercommissie geeft aansporingen aan de gemeente en de DD. Zij zijn continu bezig met nieuw beleid en dit rapport wil suggesties meegeven om met een aantal activiteiten en aanpakken door te gaan. De rekenkamercommissie geeft een aantal aanbevelingen aan college en raad die een urgenter karakter hebben.

De rekenkamercommissie doet de gemeenten de aansporingen om:

- verder te gaan met implementatie van de AVG;
- verder te gaan met awareness campagnes en deze intensiveren;
- verder te gaan met de aanschaf van een ISMS en te koppelen aan de PDCA-cyclus;
- de procesmatige aanpak van wijzigingsbeheer te implementeren;
- de procedure op autorisaties te evalueren;
- de voorbereiding op BIO ter hand te nemen.

De rekenkamercommissie beveelt het college aan om:

- de jaarplanning en P&C-cyclus op informatiebeveiliging en privacy beter te borgen;
- pen-testen te laten uitvoeren door externe ethische hackers en daarmee het interne en externe beveiligingsniveau op het gewenste peil te brengen;
- meer risicogestuurd op informatiebeveiliging en gegevensbescherming te gaan werken
- capaciteit op informatiebeveiliging en gegevensbescherming bij de gemeente en Dienst Dommelvallei op adequaat niveau te brengen;
- de positie van de CISO te versterken (zie ook bijlage 3, Dreigingsbeeld informatiebeveiliging 2019/2020 van IBD);
- een integraal continuïteitsplan op te stellen;
- zorg te dragen voor logging op de cruciale applicaties en systemen.

De rekenkamercommissie beveelt de raden aan:

- met college in gesprek te gaan over de wijze waarop de raad geïnformeerd wil worden in het kader van ENSIA, vooral over het vormvrije deel (verbetermaatregelen, meerjarenbeleid en datalekken);
- het college de opdracht te geven in het kader van ENSIA jaarlijks te rapporteren over de bovenstaande aansporingen en aanbevelingen.

Bijlage 1. In informatiebeveiliging en privacy veel voorkomende termen 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 (zie 2-stapsverificatie)
2-staps-verificatie	zie 2FA
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
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
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligings-risico's van de informatie/applicaties zijn geënt
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
BYOD	Bring your own device, betekent dat medewerkers en externen hun eigen apparaten (laptops, smartphones, usb-sticks enz.) meenemen en inloggen op het gemeentelijk systeem
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises
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
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 al zijn aangebracht
Dongel	Een USB-modem waarmee (beveiligde) toegang tot internet verkregen kan worden
DPIA (ook PIA)	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
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.
Firewall	Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
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
iBabs	Vergadertool op internet, meestal gebruikt voor papierloos vergaderen voor bijvoorbeeld gemeenteraden.
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
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
ISMS	Information security management system
KING	Kwaliteitsinstituut Nederlandse Gemeenten, heet tegenwoordig VNG Realisatie
OWASP	Open Web Application Security Project
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidscyclus
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
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
Spoofing	Het verzenden van e-mails waarbij het e-mail adres van de afzender vervalst is
Token	Een fysiek apparaat waarmee toegang verkregen kan worden tot een elektronisch beveiligde bron of netwerk
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 uniek 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 (IBD)
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. Lijst geraadpleegde stukken en lijst respondenten

De geraadpleegde stukken en de geïnterviewde personen zijn hieronder weergegeven, per onderdeel/gemeente.

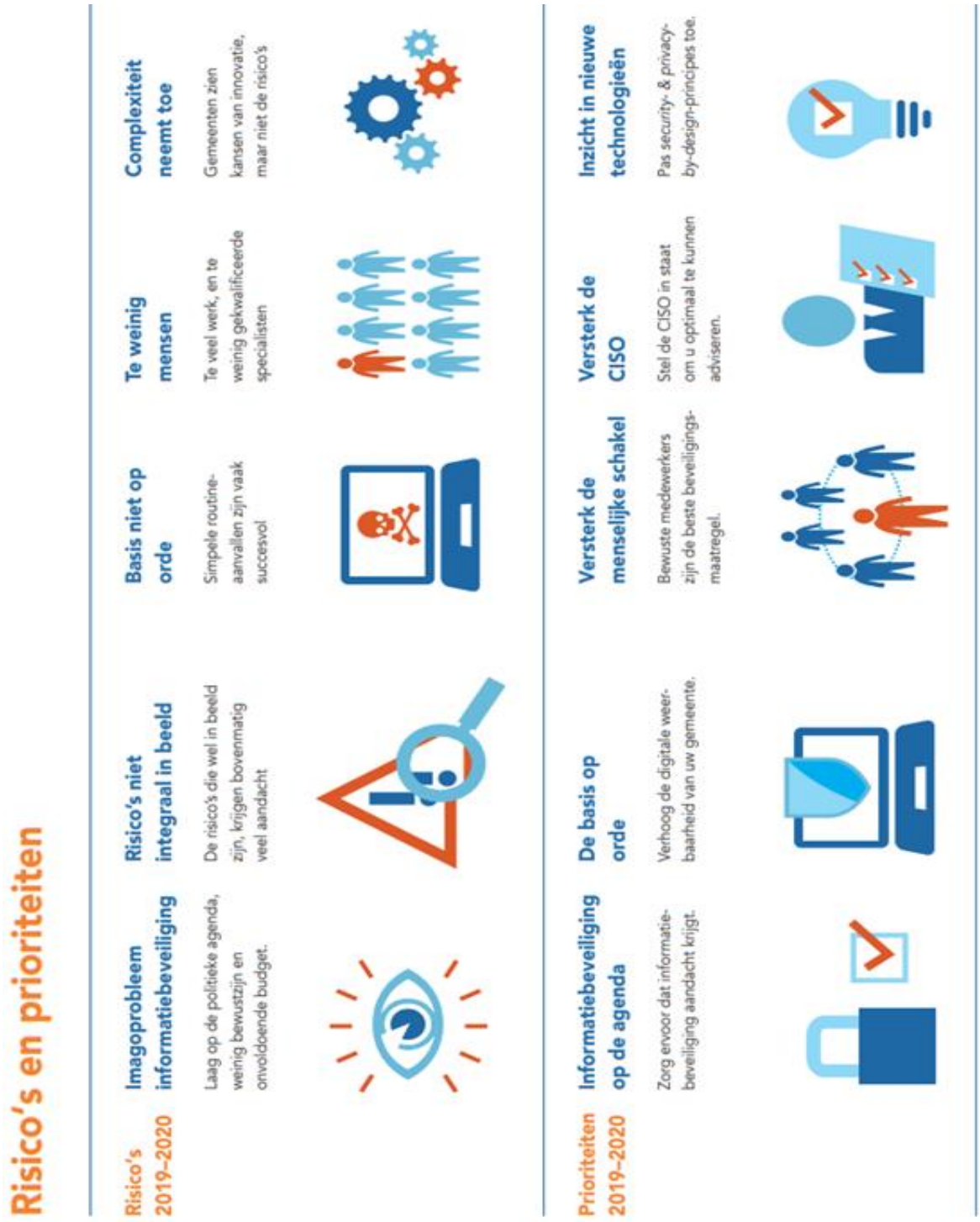
Geraadpleegde stukken

- Regeling thuiswerken Geldrop-Mierlo
- Afspraken over Thuiswerken
- Uitwijk procedure Dienst Dommelvallei
- Wachtwoordbeleid
- 2016-08 Gemeentebreed IB Geldrop-Mierlo en Plusteam v aug 2016
- Informatiebeveiligingsplan Dommelvallei organisaties v0.9
- Plan van Aanpak informatiebeveiliging Dommelvallei organisaties
- Procedure Beveiligingsincidenten en datalekken gemeente Geldrop-Mierlo
- 2017-7-4 Presentatie AB
- Bewust Intranet GM 1
- Bewust Intranet GM 2
- Bewust Intranet GM 3
- 2018-04-16 Ruimte Geldrop-Mierlo
- E-Learning traject memo afdelingshoofden
- Verordening Privacy GM 2016 gmb-2016-64765
- Privacyverklaring Geldrop-Mierlo website
- Verwerkingenregister Geldrop-Mierlo
- Model Verwerkersovereenkomst Geldrop-Mierlo
- Jaarrekening 2017 - 1 (uit paragraaf bedrijfsvoering)
- Jaarrekening 2017 - 2
- MCS GM Rapportage Ensia 2017
- Visitatiecommissie VNG 2016

Functies van geïnterviewde respondenten

- Adviseur publiekszaken/dienstverlening, gemeente Geldrop-Mierlo
- Chief Information Security Officer (CISO)/ENSIA-coördinator, Dienst Dommelvallei
- Controller, Dienst Dommelvallei
- Functionaris Gegevensbescherming, Dienst Dommelvallei
- Hoofd Publiekszaken, gemeente Geldrop-Mierlo
- Juridisch medewerker/privacybeheerder, gemeente Geldrop-Mierlo
- Functionarissen ICT-afdeling, Dienst Dommelvallei
- Wethouder, gemeente Geldrop-Mierlo

Bijlage 3. Dreigingsbeeld informatiebeveiliging 2019/2020.



Bron: Dreigingsbeeld informatiebeveiliging 2019/2020, IBD.

Bijlage 4. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIG en de AVG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van de informatiebeveiliging getoetst wordt.

Tabel 2. Onderzoeksvragen

1. Stuurt het college 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 commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? 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. Heeft de gemeente de risico's op informatiebeveiliging benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?	Het management stelt naar aanleiding van een GAP-analyse het informatiebeveiligingsbeleid op. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld.
3. In hoeverre bereidt de gemeente zich voor op de Baseline Informatiebeveiliging Overheid (BIO)?	
4. Hoe ver is de gemeente gevorderd met de implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU? Hoe is het commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? 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. Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatieveiligheidsaspecten, en zo ja hoe?	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. Rapporteert en bespreekt de organisatie het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (college en raad)?	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 gemeente bij de Informatiebeveiligingsdienst voor gemeenten (IBD)?	Aansluiting bij de IBD wordt aangeraden door de VNG.
8. In hoeverre heeft de gemeente zich voorbereid op ENSIA?	Gemeenten moeten medio 2019 op basis van ENSIA (eenduidige normatiek single information audit) horizontaal en verticaal verantwoording afleggen.
9. Wordt jaarlijks getoetst of de organisatie in control is 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? Weet de organisatie 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 gemeente? Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente 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 beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.

Bijlage 5. Bestuurlijke reactie College van B&W

Geldrop-Mierlo

Gemeente Geldrop-Mierlo
Hofstraat 4
5664 HT GELDROP

uw brief		*ons kenmerk*	2019-023715
behandeld door	Irene Kuiper	*onderwerp*	Bestuurlijke reactie op rekenkameronderzoek Informatiebeveiliging en Privacy
Geldrop	23 mei 2019		

Beste meneer/mevrouw ,

Met instemming hebben wij kennis genomen van uw bevindingen naar aanleiding van het door u uitgevoerde Rekenkameronderzoek om na te gaan in hoeverre de gemeente Geldrop-Mierlo de informatiebeveiliging en privacy voldoende heeft georganiseerd en geborgd.

U concludeert dat de gemeente Geldrop Mierlo met ondersteuning van Dienst Dommelvallei hard werkt aan informatiebeveiliging en privacy. Ook stelt u vast dat het een organisch proces is en dat de gemeente steeds stappen zet om verder met informatiebeveiliging en privacy te komen. De basis en governance op het gebied van informatiebeveiliging en gegevensbescherming zijn bij de gemeente Geldrop-Mierlo deels op orde. Er is echter nog werk aan de winkel.

De aansporingen en aanbevelingen zoals verwoordt op pagina 21 van het onderzoeksrapport onderschrijven wij. Ze zijn bij ons bekend en het merendeel daarvan is daadwerkelijk opgepakt of staat voor de komende tijd gepland. Met onze samenwerkingspartners binnen Dommelvallei verband, gaan we uw aansporingen en aanbevelingen bespreken. Aan de hand daarvan wordt bepaald of en hoe we onze aanpak binnen Informatiebeveiliging gaan aanpassen. De gemeenteraad wordt daarvan op de hoogte gesteld, via de reguliere planning en control cyclus.

Het eerstvolgende document in de planning en control cyclus is de meerjarenprogrammabegroting 2020-2023. Hierin verwerken wij de aanbevelingen van de Rekenkamercommissie door de gemeenteraad te informeren over de voortgang van maatregelen vanuit de ENSIA. Graag vernemen wij dan van de gemeenteraad of dit voldoet aan hun wensen om daarover geïnformeerd te worden. Daarnaast informeren wij de gemeenteraad over de voortgang van de in uw rapport genoemde aansporingen en aanbevelingen.

Bezoekadres: **Dwarsstraat 70, 5666 BE Geldrop**: Publiekszaken (balies) | Centrum voor Maatschappelijke Deelname | PlusTeam | Ruimte | Informatie DienstVerlening | Facilitaire Dienst
Bezoekadres: **Stationsstraat 33, 5664 AP Geldrop**: College van Burgemeester en wethouders | Griffier | Ondersteuning | Maatschappelijke Ontwikkeling | Trouwzaal
Postadres: Postbus 10101 | 5660 GA Geldrop | T **14 040** | E gemeente@geldrop-mierlo.nl | www.geldrop-mierlo.nl | facebook.com/gemeente.geldropmierlo | twitter.com/gGeldrop_Mierlo

Heeft u nog vragen over deze brief? Of wilt u meer informatie? Neemt u dan contact op met behandelende afdeling/cluster, te bereiken via telefoon-nummer 14 040. Houd het kenmerk/zaaknummer van deze brief bij de hand.

Met vriendelijke groet,
namens burgemeester en wethouders,

Hans van de Laar
wethouder

Bijlagen: 0