Rapport rekenkamercommissie Informatiebeveiliging en privacy

Rekenkamercommissie Son en Breugel

11 juni 2020

Voorzitter: Sandra van Breugel
Lid: Etienne Lemmens

Inhoudsopgave

Voorwoord

Informatiebeveiliging en privacy zijn actueel. Nu velen in Nederland al weken gedwongen thuis werken door de Coronacrisis is informatiebeveiliging van nog groter belang. Bovendien hebben velen, sinds de invoering van de AVG in mei 2018, een beeld over privacyaspecten en een besef van urgentie. Gemeenten hebben, net als andere organisaties te maken met informatiebeveiliging en privacy. Van de overheid wordt verwacht dat zij 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 Son en Breugel is in november 2019 ingesteld. In januari 2020 heeft de rekenkamercommissie nader kennisgemaakt met de fractievoorzitters in het presidium. Onderwerp van gesprek was onder andere wat zou een geschikt eerste onderzoek voor de nieuwe rekenkamercommissie zou kunnen zijn. De rekenkamercommissie opperde het idee om onderzoek te doen naar informatiebeveiliging en privacy. Dit onderzoek zou snel kunnen starten, omdat de rekenkamercommissie van Geldrop-Mierlo in het voorjaar van 2019 al een dergelijk onderzoek voor die gemeente heeft verricht. Zowel de gemeente Son en Breugel als de gemeente Geldrop- Mierlo heeft een deel van de informatiebeveiliging en privacy taken belegd bij Dienst Dommelvallei.

De aanwezigen van het presidium vinden informatiebeveiliging en privacy erg belangrijk en er bleek draagvlak te zijn om in een rekenkameronderzoek na te gaan in hoeverre de gemeente Son en Breugel de informatiebeveiliging en privacy voldoende heeft georganiseerd en geborgd.

Het onderzoek is gestart met een documentenanalyse medio maart 2020, de interviews zijn begin april afgenomen, daarna volgde eind april de ambtelijke check op de bevindingen. In mei 2019 zijn de conclusies en aanbevelingen geformuleerd en op 15 mei 2020 is het concept rapport aangeboden aan het college van B&W voor een bestuurlijke reactie. Deze reactie die de rekenkamercommissie op 9 juni heeft ontvangen is aan het eind van dit rapport integraal opgenomen. Direct daarna is op 11 juni 2020 het rapport aangeboden aan de gemeenteraad van de gemeente Son en Breugel.

De rekenkamercommissie heeft dit onderzoek in eigen beheer uitgevoerd. De rekenkamercommissie is veel dank verschuldigd aan de deskundige medewerkers van de gemeente Son en Breugel en Dienst Dommelvallei die constructief, in een goede samenwerking en op flexibele wijze hun bijdrage aan dit onderzoek hebben geleverd. Tijdens de Coronacrisis hebben de interviews plaatsgevonden via een video call of telefonisch.

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

Drs. E.J.M. (Etienne) Lemmens

Rekenkamercommissie gemeente Son en Breugel

1 Inleiding

Door de toegenomen taken in onder andere het sociaal domein beheren en verwerken gemeenten steeds meer persoonlijke en gevoelige data. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder meer blijkt uit datalekken bij gemeenten en recente onderzoeken van 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 gemeenten, gelet op de toename van de hoeveelheid aan vertrouwelijke data in informatiesystemen. De wetgever heeft dit erkend en mede onder invloed van Europa dwingende wet- en regelgeving gemaakt. De Algemene Verordening Gegevensbescherming (AVG, ook bekend 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 2019 26.956 meldingen van datalekken, een stijging van 29% ten opzichte van 2018. De sector Openbaar bestuur is verantwoordelijk voor 4.624 meldingen, dat is 27% meer dan een jaar eerder. 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 nog in ontwikkeling, met name 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. Anders geformuleerd: er zitten aanzienlijke risico's tussen beeldscherm en bureaustoel.

1.1 Vraagstelling

De rekenkamercommissie wil in dit onderzoek de volgende centrale vraag beantwoorden:

> *In hoeverre heeft de gemeente Son en Breugel de informatiebeveiliging voldoende georganiseerd en geborgd?*

De vraagstelling wordt hieronder in de volgende onderzoeksvragen uitgewerkt:

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 Overheid (BIO). 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. 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?

4. Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatieveiligheidsaspecten, en zo ja hoe?
5. 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?
6. Rapporteert en bespreekt de organisatie het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (college en raad)? Zo ja, hoe?
7. 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?
8. Welke opvolging heeft Dienst Dommelvallei gegeven aan de aansporingen en aanbevelingen van het onderzoek naar IB en privacy (mei 2019) van de Rekenkamercommissie Geldrop-Mierlo en wat betekent dit voor de gemeente Son en Breugel?

1.2 Aanpak

Om de onderzoeksvragen te beantwoorden hebben we de volgende aanpak gehanteerd:

- Deskresearch

Voor de deskresearch hebben we gebruik gemaakt van de beleidsstukken die de gemeente Son en Breugel en Dienst Dommelvallei hebben opgesteld in het kader van informatiebeveiliging en privacy. Een overzicht van de verkregen en bestudeerde documenten is opgenomen in bijlage 1.

- Interviews

Om de informatie uit de documenten te checken en aan te vullen hebben we 6 interviews afgenomen. Bij de burgemeester, als portefeuillehouder op deze dossiers, en medewerkers van de gemeente en Dienst Dommelvallei (DD). Voor een overzicht van de functies zie bijlage 2.

- Analyse en rapportage

De bevindingen hebben we geanalyseerd en gehouden tegen de normen, zodat we een gewogen oordeel kunnen vellen en de onderzoeksvragen kunnen beantwoorden. Voor een overzicht van de normen verwijzen we naar bijlage 3.

- Ambtelijke check van de feiten en bestuurlijke reactie.

De concept rapportage (zonder conclusies en aanbevelingen) is voorgelegd aan de ambtelijke organisatie. Over de feiten kan immers geen discussie ontstaan. De rekenkamercommissie heeft de rapportage (deels) aangepast aan de hand van de opmerkingen uit de ambtelijke organisatie. Daarna heeft de rekenkamercommissie de conclusies en aanbevelingen geformuleerd. Deze versie is voorgelegd aan het college van burgemeester en wethouders. Hun reactie op het rapport is opgenomen in bijlage 4 van het rapport.

1.3 Leeswijzer

De onderzoeksvragen worden per hoofdstuk behandeld, op de aan elkaar verwante derde en vierde onderzoeksvraag na. In hoofdstuk 9 zijn de conclusies en aanbevelingen opgenomen. In bijlage 1 zijn de verkregen en bestudeerde documenten opgenomen, de lijst van respondenten staat in bijlage 2. Bijlage 3 bevat de normen per onderzoeksvraag. Bijlage 4 geeft een afkortingenlijst. De bestuurlijke reactie op het eindrapport van het college van burgemeester en wethouders is in bijlage 5 opgenomen. Tot slot staat in bijlage 6 het nawoord door de rekenkamercommissie.

2 Beleid

In dit hoofdstuk staat de volgende onderzoeksvraag centraal: 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 Overheid (BIO). Hoe is het commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het informatiebeveiligingsbeleid uit?

Op 20 februari 2020 heeft het dagelijks bestuur van Dienst Dommelvallei het Strategisch Gemeentelijk Informatiebeveiligingsbeleid Dommelvallei-organisaties vastgesteld. Het beleid is op 3 maart 2020 ook door het college van Son en Breugel vastgesteld. Het beleid geldt voor de bij DD aangesloten gemeenten en is gebaseerd op de BIO en onder andere de 10 principes voor informatiebeveiliging zoals door de Informatiebeveiligingsdienst (IBD, onderdeel van de VNG die over informatiebeveiliging adviseert) zijn opgesteld. De BIO geeft richtlijnen hoe informatiebeveiliging op een risicogestuurde manier te implementeren. Er zijn minder maatregelen dan in de BIG (Baseline informatiebeveiliging gemeenten) die tot en met 2019 gold. De richtlijnen uit de BIO hebben wel een meer verplichtend karakter. Het door DD vastgestelde strategische beleid moet de basis leggen voor de tactische beleidsplannen en informatiebeveiliging op operationeel niveau.

De 10 bestuurlijke principes voor informatiebeveiliging zijn de volgende:[1]

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

[1] De 10 bestuurlijke principes voor informatiebeveiliging. Behorende bij de Baseline Informatiebeveiliging Overheid (BIO), VNG, 2019.

Belangrijke uitgangspunten zijn onder andere dat de bestuurders informatiebeveiliging en het gedrag erom heen bevorderen, dat het informatiebeveiliging een zaak van iedereen is (niet alleen van een functionaris als de chief information security officer, CISO) en risicogestuurd.

Het strategische beleid op informatiebeveiliging is opgesteld en er zijn stappen genomen, zoals een GAP-analyse die is uitgevoerd om te komen tot een jaarplan. De risicoanalyse die voor het jaarplan nodig is om prioriteiten vast te stellen is nog niet uitgevoerd. Door drukte en werkzaamheden heeft de CISO nog geen tijd gehad om een nieuw jaarplan op basis van BIO op te stellen. Het voornemen is dit projectmatig op te pakken, met behulp van lijnmanagement en eventueel met behulp van derden. Met de risicoanalyse wordt een top 10 van risico's opgesteld en bezien wat dat betekent voor mensen en middelen in het kader van de begroting 2020-21. Op moment van onderzoek staat het jaarplan op basis van BIO in de planning voor 1 juli 2020 gereed te komen. En uiteindelijk is het lijnmanagement verantwoordelijk voor de invoering van informatiebeveiliging op basis van de normen van BIO. Besloten is dat de prioriteiten domeingewijs worden op opgepakt, met eerst aandacht voor de afdeling ICT en Personeel.

Naast het ontbreken van een jaarplan op informatiebeveiliging ontbreekt ook een actueel en integraal privacybeleid. Op onderdelen worden de onderdelen die nodig zijn voor de implementatie van de AVG ingevoerd, zie daarvoor hoofdstuk 4.

Op onderdelen van het informatiebeveiligingsbeleid zijn protocollen en procesbeschrijvingen aangetroffen. Zo zijn er procedures voor autorisaties toekennen en controleren, eisen op wachtwoord en schermbeveiliging, hoe extern te werken, beveiligingsincidenten, datalekken. Een tweetal zaken die nog niet geregeld zijn de 'overall' inregeling van 2 factor authenticatie (authenticatie die alleen in 2 succesvolle stappen wordt afgerond) en management van mobiele apparaten en gegevensdragers.

Gevraagd naar wat goed gaat op informatiebeveiliging en privacy is bij respondenten vaak het antwoord dat de organisatie zich steeds bewuster is van de risico's en dat de beide onderwerpen structureler deel uitmaken van het bedrijfsvoeringsproces en niet meer incident gedreven zijn. De portefeuillehouder op informatiebeveiliging en privacy in Son en Breugel is de burgemeester. Het onderwerp heeft de aandacht van de portefeuillehouder en hij is actief in het portefeuilehouders-overleg zo meldden meerdere respondenten. De overige wethouders zijn zich bewust van het belang van informatiebeveiliging en privacy en stellen indien nodig vragen aan de FG en CISO. Maar in de interviews wordt gemeld dat zij vooral inhoudelijk op de eigen portefeuilles betrokken zijn.

Ook de gemeentesecretaris en het MT van Dienst Dommelvallei zijn zich bewust van het belang van beveiliging en privacy. Informatiebeveiliging wordt volgens de respondenten uitgedragen, maar een enkele respondent ervoer dat de strenge implementatie van de AVG medewerkers huiverig heeft gemaakt. Bij nader inzien blijkt vaak meer mogelijk om persoonlijke informatie te delen dan in eerste instantie mogelijk leek. De eerste beeldvorming daaromheen lijkt geen goed te hebben gedaan voor draagvlak.[2]

[2] Een voorbeeld: alle inwoners die 75 jaar oud worden krijgen een brief van de gemeente met de mededeling dat de gemeente in gesprek wenst te komen over eenzaamheid, ten minste als dat aan de orde is. De gemeente wil betekenis geven aan een maatschappelijk probleem. Dat zou niet meer mogen in het kader van de AVG. Achteraf bleek binnen de grenzen toch meer mogelijk dat eerst gedacht werd.

De portefeuillehouder laat zich leiden door de deskundigen van DD en de privacybeheerders die voor Son en Breugel en de gemeente Nuenen werken. Gevraagd naar wat goed gaat op het vlak van informatiebeveiliging en privacy antwoordt de portefeuillehouder dat de juiste expertise op de juiste plek aanwezig is. Zo zijn de posities van de CISO en de functionaris gegevensbescherming (FG) wat betreft expertise goed bezet met gespecialiseerde mensen bij Dienst Dommelvallei. Kennisniveau en alertheid van de functionarissen wordt als goed ervaren. De bezetting wordt wat betreft capaciteit als minder voldoende gekwalificeerd in de interviews. De omvang van de FG-functie is vorig jaar uitgebreid naar iets meer dan fulltime, waardoor een tweede parttime medewerker in 2019 als FG is aangesteld. De CISO-functie is op dit moment voor 32 uur bezet. Zij is weinig planmatig bezig (zie ook hierna). Met name voor de CISO-functie is geen adequate back-up geregeld. De FG weet nog het meest van informatiebeveiliging en kan de CISO deels vervangen. Dat wordt als kwetsbaar ervaren voor een gemeenschappelijke regeling die de informatiebeveiliging- en privacy-taken voor de eigen organisatie en de drie aangesloten gemeenten uitvoert.

De functie privacybeheerder bij Son en Breugel is sinds begin 2020 niet meer bezet. De functionaris vertrok omdat de functie, volgens de respondenten, niet bood wat hij ervan verwachtte. De functie is vooral gericht geweest op incidentele taken. Daardoor zijn een aantal structurele taken op gebied van privacy blijven liggen, zoals het actualiseren van de verwerkersovereenkomsten die met derden gesloten zijn voor de verwerking van persoonsgegevens (zie ook hoofdstuk 4). In de planning staat de invulling van deze functie, maar er is nog geen besluit genomen over de omvang en het niveau van de vacature.

Uiteraard speelt budget, in de vorm van middelen en mensen, een rol bij investeringen in informatiebeveiliging en privacy. Dat is zeker een aandachtspunt. In de interviews wordt gemeld dat de begroting van de gemeente onder druk staat, onder andere vanwege de tekorten in het sociaal domein. Hierdoor moeten keuzen gemaakt worden. Zo is in de begroting 2020 van Dienst Dommelvallei 1,0 fte aangevraagd in het kader van nieuw beleid en projecten op ICT. En er is een halve fte voor het jaar 2020 toegekend. Daardoor moeten prioriteiten gesteld worden. Doordat de financiële middelen uit de I&A-begroting komen, concurreren nieuwe projecten op informatie-beveiliging en privacy met andere ICT-projecten. Organisatiebrede projecten gericht op de continuïteit van de bedrijfsvoering en de dienstverlening krijgen voorrang op vernieuwing in het kader van informatiebeveiliging en privacy.

3 Risicobewustzijn

In dit hoofdstuk gaan we in op de onderzoeksvraag: 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?

Zoals in het vorige hoofdstuk al is bevonden is een strategisch beleidsplan op informatiebeveiliging opgesteld dat voldoet aan de normen van de BIO. Op basis daarvan kan een GAP-analyse plaatsvinden, waarin de huidige situatie op het gebied van informatiebeveiliging worden afgezet tegen de gewenste situatie met betrekking tot de maatregelen in het kader van de BIO. In de interviews is aangegeven dat de GAP-analyse is gemaakt. Op basis van de GAP-analyse moet een risicoanalyse gemaakt worden. De vraag is welke risico's de gemeente momenteel loopt, welke risico's worden geaccepteerd en welke geprioriteerd. Dat is de basis voor het jaarplan informatie-

beveiliging. Daarin worden middelen en mensen opgenomen om de maatregelen uit het jaarplan uit te voeren. De risicoanalyse en het jaarplan moeten nog worden opgesteld.

In de organisaties, gemeente Son en Breugel en DD, is het besef dat informatiebeveiliging een must is, anders zijn er grote risico's aanwezig. De bestuurlijke verantwoordelijkheden liggen uiteraard vast. De eindverantwoordelijken zijn aangewezen in het lijnmanagement, deze zijn betrokken bij de GAP-analyse en worden betrokken bij de risicoanalyse. Het risicobewustzijn op informatiebeveiliging en privacy is, volgens respondenten nog niet bij alle afdelingen/domeinen even goed doorgedrongen. Bij ICT, burgerzaken en sociaal domein waar medewerkers al jarenlang met bijzondere persoons-informatie verwerken is dat wel het geval. Bij andere afdelingen kunnen de onderwerpen en het risicobewustzijn nog meer gaan landen.

Er worden veel data gedeeld en in de cloud opgeslagen. Dan is goede informatiebeveiliging een must. Daarbij is belangrijk is dat bij invoering van nieuwe applicaties de risico's die de organisatie loopt op informatiebeveiliging en privacy bekend zijn en dat de protocollen en werkwijzen voldoen aan de BIO en AVG. Het blijkt uit de documenten en interviews dat het wijzigingsbeheer niet projectmatig wordt opgepakt. Zo wordt een nieuw zaaksysteem organisatiebreed geïmplementeerd bij DD en de drie gemeenten die daarin samenwerken. Bij een niet projectmatige aanpak van de implementatie kunnen risico's op efficiëntie en effectiviteit optreden. Op het nieuwe zaaksysteem zijn wel al op onderdelen Data Protection Impact Assessments (DPIA's) uitgevoerd (zie ook hoofdstuk 4).

Een ander element is de check op autorisaties. De procedure daarvoor is geëvalueerd, maar de verbeterpunten die daaruit naar voren kwamen zijn nog niet opgevolgd. De autorisaties waardoor medewerkers bij gegevens kunnen komen zijn soms te oud of te ruim. Daardoor kunnen autorisaties nog gelden voor medewerkers die niet meer in dienst zijn of voor functies die ze op niet moment niet meer vervullen. De afdeling I&A moet, samen met lijnmanagement, de controle uitvoeren op de autorisaties die de medewerkers van Son en Breugel hebben tot de gegevens. De bedoeling is deze check 2 tot 3 keer per jaar uit te voeren, maar dat gebeurt volgens respondenten niet altijd.

Functiescheiding is, met betrekking tot autorisaties, niet altijd goed mogelijk in kleinere organisaties. Het is dan lastig om de autorisaties onder het personeel te verdelen. Dat wordt door de gemeente Son en Breugel samen opgepakt met de gemeente Nuenen, die met hetzelfde vraagstuk te maken heeft. Respondenten noemen de samenwerking daarop goed.

4 Implementatie AVG

De onderzoeksvraag in dit hoofdstuk is: 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?

Ook behandelen we hier de daaraan gelieerde vraag: Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatieveiligheidsaspecten, en zo ja hoe?

De vereisten die nodig zijn voor de AVG zijn deels geïmplementeerd. Eerder gemeld is dat er nog geen actueel en integraal privacybeleid aanwezig is. Er is een privacyverklaring opgesteld en gepubliceerd op de website waarin de gemeente aangeeft hoe deze met persoonsgegevens omgaat.

Het inzagerecht dat inwoners via de AVG hebben is geregeld en op schrift gesteld. Het verwerkingsregister, waar alle verwerkingen door en/of namens de gemeente in moeten zijn opgenomen, is aanwezig.

Bij nieuwe verwerkingsprocessen waar derden bij betrokken zijn worden up-to-date verwerkers-overeenkomsten afgesloten. Bij de aandachtspunten die hen aangaan worden de FG en CISO betrokken, bijvoorbeeld of de verwerking voldoet aan de BIO- en AVG-normen of dat er sprake is van 2FA (twee factor authenticatie) in geval van uitwisseling van persoonsgegevens. Voor nieuwe verwerkersovereenkomsten worden de standaardcontracten van de IBD gebruikt. Deze worden gemakkelijker en zonder discussie door derden geaccepteerd. De actualisatie van de al bestaande verwerkersovereenkomsten is stil gevallen door het voortijdige vertrek van de privacybeheerder (zie hoofdstuk 2) begin 2020.

De verwerkersovereenkomsten bevatten afspraken op het gebied van informatiebeveiliging en omgang met (bijzondere) persoonsgegevens. Om te checken of de partij waarmee de afspraken worden gemaakt ook daadwerkelijk de afgesproken protocollen volgt, wordt gebruik gemaakt van een zogenoemd Third Party Memorandum (TPM). Dat is een door een onafhankelijke partij opgestelde verklaring waarmee de partij, waar de gemeente persoonsgegevens mee deelt, kan aantonen aan de gestelde eisen te voldoen. De TPM's worden met name gebruikt bij de verwerkingsprocessen die door landelijke toezichthouders in het kader van ENSIA streng worden gecontroleerd. Dat zijn DigID en Suwinet. Op andere terreinen vindt een dergelijke check nog niet plaats, zoals in de jeugdzorg, waarin voor de gemeente door derden veel persoonsgegevens worden verwerkt.

Er is een procedure afgesproken hoe om te gaan met datalekken. Volgens respondenten is deze bekend en wordt volgens de afspraken gehandeld door de medewerkers. Voor het uitvoeren van de Data Impact Protection Assessments (DPIA's) is een checklist met 31 vragen opgesteld, met als doel te inventariseren of een assessment nodig of verplicht is. Een zestal DPIA's die gehouden zijn, zijn aangereikt.[3] Maar er zijn nog meer processen waarin bijzondere persoonsgegevens worden verwerkt die nog aan een DPIA onderworpen moeten worden. De rekenkamercommissie heeft geen schema aangetroffen welke processen nog aan een DPIA dienen te worden onderworpen en op welke termijn dit is voorzien.

CISO en FG adviseren over AVG en verwerking van bijzondere persoonsgegevens aan het gemeente-bestuur en directie van DD. Het belang van privacy en bescherming van persoonsgegevens wordt door bestuur ingezien en uitgedragen. Er is volgens de rapportages en de respondenten evenwel nog heel wat werk te verzetten om de AVG volledig te implementeren, zoals het volledig up-to-date maken van het verwerkingsregister en de verwerkingsovereenkomsten.

[3] Dat zijn de DPIA's naar: zaaksysteem KCS, zaaksysteem Vergunningen, zaaksysteem Sprint2, Intergrip, registratie ondersteuningsvragen CMD en de nieuwjaarsfietstocht.

5 Controle

In dit hoofdstuk wordt de volgende onderzoeksvraag behandeld: 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?

Jaarlijks worden de audits en assessments gehouden, zoals de verplichte audits op DigID en SUWInet. Deze worden streng gecontroleerd door de landelijke toezichthouders. Wordt niet voldaan aan de criteria dan loopt de gemeente risico van DigID of Suwinet afgesloten te worden en stokt de gemeentelijke dienstverlening aan de inwoners en bedrijven/instellingen. Dat is een duidelijke stok achter de deur, en de gemeente is positief door de audits heen gekomen. Respondenten geven aan dat de audtits door het bestuur serieus worden genomen en grondig worden geanalyseerd. Over de audits en de zelf assessments rapporteert de gemeente in ENSIA, verticaal naar de landelijke toezichthouders en horizontaal richting gemeenteraad. Deze verantwoording kost volgens respondenten veel tijd om op te stellen, zie daarvoor hoofdstuk 6.

Er zijn verschillende testen om de fysieke en digitale veiligheid te beproeven. Pen-testen, zoals met een zogenoemde ethisch hacker de systemen op veiligheid testen, zijn niet uitgevoerd. Dit soort testen staat volgens respondenten wel in de planning, maar vooralsnog ontbreekt het aan de middelen (budget) om de test uit te voeren, de capaciteit aan menskracht om deze te begeleiden of met de resultaten aan de slag te gaan. Medio 2019 is met een mystery guest geprobeerd binnen te dringen in de fysieke omgeving van het gemeentehuis. Daar gaan we in hoofdstuk 7 dieper op in.

De continuïteit van de dienstverlening is niet geborgd in een integraal continuïteitsplan bij DD of de gemeente.[4] Onderdeel van zo'n plan is onder andere de identificatie van vitale processen. Dat was, volgens een van de respondenten een prioriteit die in 2020 opgepakt zou worden. Door de Corona-crisis is dit in een stroomversnelling geraakt. Dat was de 'trigger' om direct met elkaar in overleg te gaan en de vitale processen en activiteiten te identificeren. De infrastructuur voor het thuiswerken is essentieel gebleken, via de beveiligde omgeving ingericht. En dat werkt, daar de gemeente sinds de start van de crisis volledig operationeel is gebleven.

Er bestaan crisisteams, die crises zoals veroorzaakt door het coronavirus, oppakken. Op regionaal niveau in de veiligheidsregio en op lokaal niveau zijn er gemeentelijke beleidsteams (GBT), door de burgemeester voorgezeten. Dat zijn interdisciplinair samengestelde teams die de crises trachten te managen. Daarin heeft informatiebeveiliging, volgens een van de respondenten, nog geen plek. Daarnaast is er bij DD of de gemeente geen specifiek op informatiebeveiliging en ICT gericht crisisteam aangetroffen, zoals een Computer Emergency Response Team (CERT). Daarbij wordt verwezen naar de aansluiting bij de IBD, die in geval van een nationale crisis als zodanig kan optreden.

Het incidentmanagementproces voor beveiligingsincidenten is op basis van meldingen in Topdesk ingericht. Daarin worden problemen geregistreerd die de continuïteit van bedrijfsprocessen

[4] Dat is een bevinding die de rekenkamercommissie Geldrop-Mierlo in 2019 ook heeft gedaan.

verstoren. Incidentmanagement is erop gericht zo snel mogelijk de dienstverlening te herstellen. De meldingen worden regelmatig gecheckt en als veel dezelfde meldingen worden geregistreerd dan kan dat duiden op een mogelijk onderliggend structureel probleem dat opgelost moet worden.

Een belangrijk controlemethodiek is logging van handelingen en foutmeldingen in applicaties en systemen. Logging levert data voor het traceren en inventariseren van onder andere beveiligings-incidenten. Foutmeldingen worden vastgelegd, en wie al dan niet geautoriseerde toegang heeft gehad tot data. De logging is geregeld voor de applicaties waarvoor de landelijke wetgeving dat verplicht heeft gesteld, zoals DigiD en Suwinet. Voor de (gemeentelijke) zaaksystemen is dat nog niet volledig geregeld. Een nieuw zaaksysteem, waarin logging is opgenomen, is in de implementatiefase. Volgens de respondenten kan dat technisch goed geregeld worden, probleem is dat er capaciteit moet zijn om de loggingdata te analyseren en vervolgacties op te nemen. Los daarvan merkt een van de respondenten terecht op dat logging achteraf plaats vindt, en reactief is met betrekking tot beveiligingsincidenten. Met logging worden in principe geen incidenten voorkomen. Hiermee wordt de noodzaak des te groter de systemen goed te beveiligen en autorisaties aan de voorkant goed te regelen en regelmatig te controleren. Desalniettemin, ook al is logging reactief, het is noodzakelijk voor de bewijslast als het gaat om incidenten waarbij bijzondere persoonsinformatie in het geding is.

6 Rapportage

Hieronder gaan we in op de onderzoeksvraag: Rapporteert en bespreekt de organisatie het functioneren van informatieveiligheidsbeleid op management- en bestuursniveau (college en raad)? Zo ja, hoe?

Om integraal op management- en bestuursniveau te rapporteren kan een Information security management system/privacy management system (ISMS/PMS) gebruikt worden. Dit management-systeem is niet aanwezig. Dat betekent dat de sturings- en verantwoordingsinformatie uit verschillende bronnen samengesteld moet worden. Dat is een tijdrovende klus. Daarnaast is er door het ontbreken van een ISMS/PMS geen efficiënte link te leggen tussen de PDCA-cyclus en de verspreid aanwezige sturings- en verantwoordingsinformatie.

De verantwoordingsinformatie moet ENSIA (Eenduidige Normatiek Single Information Audit) vullen, die bedoeld is voor de verticale (richting landelijke toezichthouders) en horizontale verantwoording (richting gemeenteraad). ENSIA bevat de verplichte audits op DigiD en Suwinet en andere assessment en evaluaties op het gebied van informatiebeveiliging en privacy. Het college tekent een in control statement, wat door en assuranceverkaring door een onafhankelijke derde partij is vastgesteld. De ENSIA-rapportage over 2017 is volledig, maar de ENSIA-rapportage over 2018 is alleen gevuld met informatie over de DigiD- en Suwinet-audits en de college- en assurance verklaring. Dat betekent geen volledige verantwoordingsrapportage in het kader van de horizontale verantwoording in de richting van de gemeenteraad.

Op het in control zijn wordt gestuurd vanuit DD en de gemeenten en het 'in control statement' van het college en de assuranceverklaring fungeren zeker als een geruststelling in de horizontale verantwoording richting gemeenteraad. Maar volgens een van de respondenten heeft dat nog niet dezelfde zeggingskracht als bijvoorbeeld de goedkeuring door een accountant op de financiële rechtmatigheid. Als de goedkeuring door de accountant niet wordt afgegeven is er een groot

probleem, dat is nog niet het geval met het ontbreken van het college-statement of de assuranceverklaring. Niet alleen in bestuurlijk opzicht maar ook in de richting van de ambtelijke organisatie is het in control zijn een vraag die de raad zou kunnen stellen aan het college. De randvoorwaarden om in control te zijn, zijn er, maar het zit nog niet in de genen van alle medewerkers.

De portefeuillehouder is van mening dat technische details van informatiebeveiligingsbeleid en de maatregelen daarop in de bedrijfsvoering niet besproken hoeven te worden in de raad. Mogelijk wel in de commissie. DD geeft twee keer per jaar informatie over de stand van zaken met betrekking tot informatiebeveiligingsbeleid en de uitvoering daarvan aan de commissie AZ. Deze commissie ziet het belang van dat onderwerp in, daar het de ruggengraat van de organisatie en de dienstverlening is, meent een van de respondenten. Een tweetal commissieleden heeft er beroepsmatig mee van doen. De commissie wordt over beveiligingsincidenten geïnformeerd.

Respondenten geven aan dat het opstellen van ENSIA tijdrovend is. De CISO, als coördinerende en adviserende functionaris voor DD en de drie aangesloten gemeenten, besteedt daar veel tijd aan. De documenten en informatie zijn versnipperd in de organisaties aanwezig.[5] De functionaris wordt hierop weinig ondersteund door de gemeenten. Een ISMS//PMS zou het verzamelen van informatie kunnen verlichten. De module stond in de planning voor in 2020 en de FG en CISO zijn bezig met een voorstel voor een aanbesteding van een ISMS/PMS voor de drie gemeenten en DD. In interviews wordt aangegeven dat het een kwestie van tijd en middelen is. De afdeling I&A heeft aangegeven in 2020 geen capaciteit te hebben om nieuwe systemen te implementeren. Vanwege de vele wensen en aanvragen op het gebied van ICT is het budget en de capaciteit om de wensen toe te kennen niet toereikend, en moeten er prioriteiten gesteld worden. Dat geldt ook voor de ISMS/PMS-module.

Een aparte verantwoordingsrapportage over privacy over 2018 is er nog niet. Dat wordt, samen met de rapportage over 2019, opgepakt door de FG en is medio 2020 te verwachten.[6]

7 Bewustzijn

Op de volgende onderzoeksvraag gaan in dit hoofdstuk in: 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?

Het belang van bewustzijn van risico's bij medewerkers en de gevolgen van gedrag op het gebeid van informatiebeveiliging en privacy, is hiervoor al een paar keer benoemd. Het is essentieel dat bestuur en management deze onderwerpen ontwikkelen en verder uitdragen. Bewustzijn is een continu aandachtspunt. Gevraagd naar wat er goed gaat op het gebeid van informatiebeveiliging en privacy antwoorden de meeste respondenten dat de aandacht en bewustzijn voor risico's is toegenomen. Zo vroegen medewerkers zich bijvoorbeeld af hoe de privacyaspecten zijn geregeld bij de formulieren voor de Tozo-regeling. Mensen kregen mede door coronacrisis meer oog voor veilig werken. Maar, melden respondenten, het kan altijd nog beter. Bij de afdelingen waar al langer persoonsgegevens

[5] Dat is een bevinding die overeenkomt met de bevindingen van de accountant.

[6] Ten tijde van de interviews (april 2020) was een rapportage over Geldrop-Mierlo in concept af en naar het MT gestuurd. Dat is voor Son en Breugel nog niet gebeurd.

worden verwerkt, burgerzaken en sociaal domein, is het bewustzijn van een goed niveau. Een van de respondenten geeft aan dat de taken, verantwoordelijkheden en bevoegdheden organisatiebreed onvoldoende worden beleefd, een enkele positieve uitzondering daargelaten.

Een incident begin 2020 met een zogenoemde ceo-mail, waarin een kwaadwillende zich uitgeeft voor een leidinggevende, heeft tot een schokeffect geleid in de organisatie. Direct na het incident zijn verbeterpunten geformuleerd en geïmplementeerd, zodat dit niet nog een keer kan voorkomen. Naar aanleiding van het incident, is ook een bericht op intranet geplaatst met een waarschuwing en is een melding gedaan bij de IBD. Iedere medewerker is zich weer bewust gemaakt van de risico's en alert. De toekomst zal uitwijzen of die alertheid standhoudt, bovendien bedenken kwaadwillende lieden steeds nieuwe en meer geraffineerde methoden om op oneigenlijke wijze geld te ontvangen.

De onderwerpen informatiebeveiliging en privacy worden niet meer gezien als alleen een ‘dingetje’ van ICT. Dat besef begint door te dringen in de organisatie, onder andere door e-learning en de test met een mystery guest. Op initiatief van de CISO heeft een mystery guest getracht zich toegang te verschaffen tot de fysieke werkplekken. Deze proef toonde aan hoe kwetsbaar de gemeente hierop is. Dat heeft geleid tot een schok- en bewustwordingseffect bij management en bestuur. De test heeft tot aandacht geleid en veel verbeterpunten opgeleverd. Onder andere is de fysieke toegang gemeentehuis onder de aandacht gekomen Er gaat gekeken worden naar breder inzetbare toegangspassen dan de tags waar nu mee gewerkt wordt en de schermtijd is naar beneden bijgesteld.

De discussie over beveiliging breidde zich uit naar het ontwerp van het te renoveren gemeentehuis. Daarbij speelt de spanning tussen enerzijds maximale openheid die de gemeente wil uitstralen naar haar inwoners en anderzijds (optimale) bescherming van data en werkplekken. Volgens respondenten is een van de werkplekken in de openbare ruimte van het nieuwe klantcontact-centrum (KCC) in het kader van BIO als risicogebied aangemerkt. De dienstverlening is nog niet volledig digitaal, en kan technisch niet goed afgeschermd worden. Er moet nog goed bekeken worden hoe hiermee omgegaan moet worden. Daarbij wordt ook gekeken hoe dat is geregeld bij andere gemeenten met een vergelijkbare inrichting.

Sommige respondenten vrezen dat de aandacht, veroorzaakt door de mystery guest, met de tijd weer wegebt. Het besef is aanwezig dat deze beveiligingsaspecten en bewustwording continu onder de aandacht gebracht moeten worden. Naast de mystery guest zijn geen andere pen-testen uitgevoerd. Budget is daarvoor wel aangevraagd, maar nog niet goedgekeurd. Zoals in hoofdstuk 5 is aangegeven ontbreekt het vooralsnog aan de capaciteit de testen te begeleiden of met de verbeteracties aan de slag te gaan.

Op het gebied van bewustwording bij medewerkers zijn er zeker initiatieven te constateren. Maar door het vertrek van de privacybeheerder zijn een aantal structurele taken hierop blijven liggen. Zoals gemeld het actualiseren van de verwerkersovereenkomsten, maar ook activiteiten op awareness bij medewerkers. Daarnaast is een integrale aanpak in het kader van organisatieleren op het gebied van informatiebeveiliging en privacy is niet aangetroffen. Mede door het ontbreken van een ISMS/PMS, gekoppeld aan de PDCA-cyclus, komt dat niet van de grond.

8 Opvolging aanbevelingen

In dit hoofdstuk gaan we in op de volgende onderzoeksvraag: Welke opvolging heeft Dienst Dommelvallei gegeven aan de aansporingen en aanbevelingen van het onderzoek naar IB en privacy (mei 2019) van de Rekenkamercommissie Geldrop-Mierlo en wat betekent dit voor de gemeente Son en Breugel?

De Rekenkamercommissie Geldrop-Mierlo heeft in 2019 een onderzoek naar informatiebeveiliging en privacy gedaan. Dat betreft meer specifiek de gemeente Geldrop-Mierlo. Dienst Dommelvallei voert zowel voor de gemeente Son en Breugel als voor de gemeente Geldrop Mierlo delen van het informatiebeveiligings- en privacybeleid uit. Wellicht is een jaar vrij kort om te verwachten dat alle aanbevelingen zijn geïmplementeerd, maar de beide onderwerpen zijn dermate van belang, de risico's navenant hoog en de ontwikkelingen gaan razendsnel. De rekenkamercommissie neemt als uitgangspunt dat de aanbevelingen en aansporingen uit het rapport van de rekenkamercommissie van Geldrop Mierlo in 2019 ook effect hebben op de gemeente Son en Breugel. Immers DD werkt voor deze gemeenten, Nuenen en DD zelf. De rekenkamercommissie begrijpt dat de keuze destijds voor het samenwerken binnen DD door de drie gemeenten is ingegeven om de back office zo vorm te geven dat alle drie de gemeenten kunnen beschikken over een hoogwaardige organisatie met deskundige medewerkers. Door de volume toename van drie gemeenten kan DD een aantrekkelijke werkgever zijn voor gekwalificeerde medewerkers waaronder een CISO en FG. Om die reden hebben we de aansporingen die aan DD zijn gedaan in het rekenkamercommissierapport uit juni 2019 getoetst aan wat er in april 2020 is opgepakt door DD.

In onderstaand overzicht wordt aangegeven of en de mate waarin DD de aansporing/aanbeveling hebben opgevolgd als: - Niet; - Deels; - Wel. Voor de goede orde het betreft dus zaken die DD betreffen en ook op een bepaalde mate effect hebben voor de gemeente Son en Breugel.

De mate van opvolging van de aansporingen:

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

9 Conclusies en aanbevelingen

9.1 Inleiding

Als eerste wenst de rekenkamercommissie op te merken dat dit onderzoek tijdens de coronacrisis is uitgevoerd: schriftelijke documenten zijn op de gebruikelijke wijze bestudeerd. Alle communicatie en interviews hebben op digitale wijze plaatsgevonden (beeldbellen, mailen en telefonisch). Het is gebleken dat de gemeente, zoals velen in Nederland, in een zeer kort tijdbestek is omgeschakeld van werken op kantoor naar thuiswerken. Dit brengt ook risico's met zich mee voor informatiebeveiliging en privacy. Hoewel niet expliciet onderzocht is, is het wel aan de orde geweest in de verschillende interviews. Het blijkt dat de omschakeling relatief soepel is verlopen en dat er geen noemenswaardige incidenten hebben plaatsvonden ten tijde van het onderzoek (maart en april 2020).

De rekenkamercommissie concludeert dat de gemeente het belang en de urgentie van informatiebeveiliging en privacy onderkent. De overall conclusie van dit rekenkameronderzoek is dat de informatiebeveiliging en privacy deels op orde is en dat er nog zaken dienen te gebeuren. De afgelopen jaren is er veel gebeurd in de gemeente Son en Breugel en er kunnen (moeten) zeker nog slagen worden gemaakt. Hieronder meer in detail en soms helaas ook in jargon de conclusies uit het onderzoek naar informatiebeveiliging en privacy bij de gemeente Son en Breugel. De rekenkamer wijst in dit kader op de afkortingenlijst zoals opgenomen in de bijlagen. Daarna volgen de aanbevelingen die de rekenkamercommissie heeft gegoten in aansporingen; de gemeente is goed op weg, de conclusies uit dit onderzoek is dat de gemeente nog stappen dient te zetten op dit beleidsterrein.

Belang, urgentie en risico's worden onderkend

Het belang, de urgentie en de risico's van informatiebeveiliging en privacy in verband met de verwerking van persoonsgegevens door de gemeente Son en Breugel en Dienst Dommelvallei (DD) worden erkend door zowel het bestuur, als het management en de ambtenaren. Beleid wordt gedragen door college en management van de gemeente en DD. De laatste jaren is door de gemeente Son en Breugel zeker veel bereikt op deze onderwerpen. De basis en de governance zijn bij de gemeente deels op orde. Dat geldt ook voor de DD waarin de gemeente met de gemeenten Geldrop-Mierlo en Nuenen onder andere op het gebied van Informatie & automatisering (I&A) samenwerkt.

Organisatorische inbedding informatiebeveiliging en privacy

De centrale functies op informatiebeveiligings- en privacybeleid, de FG en CISO, zijn bezet bij DD met kundige mensen die hun kennis up-to-date houden. De FG-functie is meer dan fulltime bezet, maar de CISO -functie is met 32 uur relatief karig ingevuld. De functie is bedoeld voor advies en controle op informatiebeveiliging voor de drie gemeenten en Dienst Dommelvallei, en wordt daarnaast ook, zo blijkt in de praktijk, ook (te veel) operationeel ingezet. Bij de gemeente Son en Breugel is de functie van privacybeheerder sinds begin 2020 niet meer bezet. Daardoor zijn een aantal taken op privacy en de implementatie van de AVG blijven liggen. Beschikbaarheid van middelen en menskracht op informatiebeveiliging en privacy is vaak nog wel een discussiepunt in management en bestuur. Hierop moet binnen DD geconcurreerd worden met andere projecten op het beleidsterrein van I&A. Dat betekent dat er vaak een keuze gemaakt moet worden tussen investeren in enerzijds

applicaties die nodig zijn voor informatiebeveiliging en anderzijds applicaties die een randvoorwaarde zijn voor de continuïteit van de dienstverlening.

Wet – en regelgeving, in hoeverre wordt er aan voldaan?

De gemeente stuurt op de BIO en AVG. Vanaf 2018 wordt gehandhaafd op de AVG en vanaf 1 januari 2020 geldt de BIO. Begin 2020 is in DD-verband het strategisch informatiebeveiligingsbeleid op basis van BIO opgesteld. Op basis daarvan is vervolgens de GAP-analyse opgesteld, met behulp van het lijnmanagement. Er is nog geen risicoanalyse en (nog) geen jaarplan opgesteld met geprioriteerde maatregelen voor 2020. De bedoeling dat deze nog wordt opgesteld in het 2e kwartaal van 2020, met behulp van externe ondersteuning. Het kader voor verbetermaatregelen komt uit de audits en assessments die mede in het kader van ENSIA worden gehouden. Een gestructureerde aanpak op informatiebeveiliging is met de formulering van het strategische beleid in eerste aanzet aanwezig, maar nog niet in de volle breedte. Op onderdelen zijn protocollen en procesbeschrijvingen aangetroffen, maar er ontbreken op cruciale onderdelen van het beleid protocollen/procedures, zoals de invoer van 2 factor authenticatie en het beheer van mobiele apparaten.

De conclusies is dat de gemeente Son en Breugel deels aan de wet- en regelgeving voldoet. De gemeente voldoet aan de verplichte audits (bij het niet voldoen volgen sancties). Verder is de rekenkamercommissie van oordeel dat de processen effectiever en efficiënter kunnen worden ingericht, zoals bijvoorbeeld tijdig een risicoanalyse en jaarplan opstellen.

Privacybeleid

De rekenkamercommissie heeft geen integraal privacybeleid aangetroffen. Implementatie van vereisten in het kader van de AVG is nog niet helemaal gereed. Veel is er al, zoals een op de website gepubliceerde privacyverklaring, aanwezigheid van verwerkingsovereenkomsten en een verwerkingsregister e.d. Het verwerkingsregisters is echter (nog) niet compleet. Nieuwe verwerkingsovereenkomsten worden AVG-proof opgesteld, op basis van het model van de IBD (Onderdeel van de VNG). De bestaande verwerkingsovereenkomsten zijn echter nog niet up-to-date gemaakt. Een aantal processen waarin persoonsgegevens worden verwerkt zijn met een DPIA op privacy risico's zijn door de organisatie doorgenomen. Er moeten nog meer processen volgen, daar is (nog) geen tijdschema voor opgesteld. Deze processen lopen achter, mede vanwege vertrek van de privacybeheerder.

Rol gemeenteraad

De gemeenteraad wordt in het kader van de P&C-cyclus geïnformeerd over de informatiebeveiliging en privacy. Dat is een kort verslag in de jaarrapportages. De raadscommissie AZ wordt vaker en meer in detail geïnformeerd. Ook beveiligingsincidenten worden daar besproken. Vanaf 2017 krijgt de raad informatie op basis van ENSIA, over de assessments, evaluaties en beheersmaatregelen op informatiebeveiliging en privacy. De ENSIA-rapportage over 2018 was niet volledig. Deze bestond alleen uit de audits op DigID en Suwinet, een college-verklaring en de assuranceverklaring van een derde onafhankelijke partij op de collegeverklaring. Over andere zaken, zoals te nemen maatregelen en andere assessments, dan de verplichte audits op DigID en Suwinet is niet gerapporteerd. Ook is het vormvrije deel van ENSIA niet gevuld om de raad te informeren over specifieke aspecten op informatiebeveiliging en privacy. Dat komt mede door het ontbreken van een ISMS/PMS (integraal management informatiesysteem op informatiebeveiliging en privacy). Daardoor is het voor de CISO te tijdrovend om de voor ENSIA benodigde informatie, die versnipperd in de organisatie aanwezig is,

te vergaren. Ook heeft de rekenkamercommissie geen aparte rapportage aangetroffen over de maatregelen in het kader van privacy. Verwachting is dat over 2018-2019 medio 2020 wordt gerapporteerd.

Autorisatiebeleid en uitvoering: aandachtspunt!

Verlenen en wijzigen van autorisaties op de toegang tot informatie in de verschillende applicaties en de controle daarop is een punt van aandacht. Voor DigID en Suwinet is dat verplicht en grondig geregeld, met eventuele sancties als de gemeente niet aan de eisen voldoet. Dit is dan ook op orde in de gemeente. Voor de andere applicaties is een structurele jaarlijkse controle zeer recent opgestart en nog niet geheel goed functionerend. Daar ligt een risico op ongeautoriseerde toegang tot onder andere (bijzondere) persoonsinformatie, met name bij functiewisselingen en uitdiensttredingen. Een ander punt met risico's op het gebied van rechtmatigheid betreft de logging van de toegang tot de applicaties. Ook hierop is het voor DigID en Suwinet verplicht geregeld de gemeente voldoet aan deze eisen. Op andere onderdelen van de systemen is automatische logging niet geïmplementeerd. Dat aspect wordt wel meegenomen in de implementatie van het nieuwe zaaksysteem. Een vraagstuk dat daarbij speelt is de capaciteit om de met logging verzamelde gegevens te analyseren en interpreteren, gelet op de beperkte capaciteit van de CISO. Met andere woorden: het is raadzaam om tevoren te bedenken in hoeverre er mensen beschikbaar zijn om analyses te maken van de sturings- en controle-informatie die systemen genereren. Alleen met het implementeren van een systeem is het probleem niet ondervangen.

Continuïteitsplan en beelden uit de interviews.

De rekenkamercommissie heeft geen integraal continuïteitsplan voor de gemeentelijke dienst-verlening aangetroffen. Door de corona-crisis zijn in korte tijd een aantal zaken opgepakt, zoals de identificatie van vitale werk- en dienstverleningsprocessen en de verdere inrichting van digitale werkplekken. Dat kunnen elementen vormen voor een op te stellen continuïteitsplan. Op onderdelen bestaan crisisteams op regionaal en lokaal niveau, maar een specifiek op informatiebeveiliging en ICT gericht team, zoals een zogenoemd CERT, is er niet.

De meeste respondenten geven aan dat het bewustzijn van de risico's op informatiebeveiliging en privacy steeds verder toeneemt. De FG en CISO komen langs bij afdelingen als er vragen komen, en die komen er steeds meer. Ook de corona-crisis en de uitvoering van bijvoorbeeld de Tozo-regeling, gaf aanleiding tot vragen van medewerkers over behandeling van persoonsgegevens. Geconstateerd kan worden dat het bewustzijn toeneemt, maar nog niet bij alle afdelingen even goed landt. Het onaangekondigde bezoek in 2019 van een 'mystery guest' heeft bij bestuur, management en medewerkers voor de nodige opschudding gezorgd. Bewustzijn op risico's blijft continu een punt van aandacht, want die kan ook weer snel wegebben. Dat dit een continu aandachtspunt is blijkt uit het beveiligingsincident met een zogenoemde ceo-mail, begin 2020. Ook uit de verschillende interviews blijkt dat respondenten flink zijn geschrokken en dat het veel geld heeft gekost (€ 40.000).

De rekenkamercommissie heeft de robuustheid van de ICT-systemen en het bewustzijn van de medewerkers niet aan een diepgravend onderzoek onderworpen. Verschillende soorten pen-testen geven daar over het algemeen inzicht in. DD heeft met de mystery guest al een test laten uitvoeren. Maar andere pen-testen liggen nog niet in het verschiet. Hierbij wordt aangevoerd dat zulke testen begeleid, geanalyseerd en geïnterpreteerd moeten worden. En verbetermaatregelen naar aanleiding daarvan moeten worden geïmplementeerd. Daarvoor ontbreekt de capaciteit bij de CISO.

Aansporingen die de rekenkamercommissie aan Dienst Dommelvallei heeft gegeven in 2019, opvolging?

De rekenkamercommissie van de gemeente Geldrop Mierlo heeft begin 2019 een onderzoek uitgevoerd naar de informatiebeveiliging en privacy. Net zoals bij de gemeente Son en Breugel heeft Geldrop-Mierlo ook delen van informatiebeveiliging en privacy ondergebracht bij Dienst Dommelvallei. Een aantal zaken die de rekenkamercommissie Geldrop-Mierlo vorig jaar constateerde bij Dienst Dommelvallei zijn ook van belang om in deze conclusies mee te nemen. Weliswaar in volgelvlucht om na te gaan wat er met de aansporingen die de rekenkamercommissie aan Dienst Dommelvallei heeft gegeven een jaar geleden is gebeurd. De voorbereiding op BIO is ter hand genomen. Deels zijn de volgende aandachtpunten opgepakt: de implementatie van de AVG-maatregelen, bewustwordingscampagnes en maatregelen op autorisaties. Nog niet opgepakt zijn de aanschaf van een ISMS/PMS, de koppeling daarvan aan de PDCA-cyclus en de implementatie van een procesmatig wijzigingsbeheer.

9.2 Aansporingen en aanbevelingen

De rekenkamercommissie doet naar aanleiding van bovenstaande conclusies de volgende aansporingen en aanbevelingen. De rekenkamercommissie geeft aansporingen aan zowel de gemeente Son en Breugel als Dienst Dommelvallei. 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 gemeente de aansporingen om:

- een risicoanalyse en een Jaarplan informatiebeveiliging voor en in 2020 op te stellen, met maatregelen en aangeven van de prioriteiten;
- het verwerkingsregister heeft de gemeente Son en Breugel in die zin voldoet is de gemeente AVG-proof. Het verdient de aandacht om op korte termijn de verwerkingsovereenkomsten te completeren;
- het instellen van automatische logging in de systemen en dit meenemen bij de aanbesteding van nieuwe systemen te implementeren;
- in te blijven zetten op vergroting van risicobewustzijn bij medewerkers, management en bestuur;
- verder te gaan met implementatie AVG-maatregelen;
- aan de slag te gaan met de verbetermaatregelen uit de evaluatie van het autorisatieproces.

De rekenkamercommissie beveelt het college aan om:

- integraal privacybeleid vast te stellen;
- door te gaan met het uitvoeren van pen-testendoor externe ethische hackers en daarmee het interne en externe beveiligingsniveau op het gewenste peil te brengen;
- zorg te dragen dat er een ISMS/PMS wordt geïmplementeerd, mogelijk als aanvullende module op al bestaande applicatie en deze te koppelen aan de PDCA-cyclus;
- het wijzigingsbeheer procesmatig aan te laten pakken;
- de positie en capaciteit van de CISO-functie te versterken. Enerzijds door een uitbreiding van de functie van de CISO bij Dienst Dommelvallei, anderzijds door snel een privacy beheerder voorde gemeente Son en Breugel aan te stellen;

- een integraal continuïteitsplan op te stellen, mede op basis van de ervaringen uit de corona-crisis, en informatiebeveiliging- en privacyaspecten daarin mee te nemen;
- zorg te dragen voor logging op de cruciale applicaties en systemen.

De rekenkamercommissie beveelt de gemeenteraad aan:

- met het 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 aan de gemeenteraad te rapporteren over de bovenstaande aansporingen en aanbevelingen.

Bijlage 1. Geraadpleegde stukken en geïnterviewde respondenten

Geraadpleegde stukken Son en Breugel (01-04-2020)

- Strategisch Beleid Dienst Dommelvallei september 2019.
- Meerjarenbegroting 2020 -2023 Son en Breugel: Paragraaf bedrijfsvoering: onderdeel Informatiebeveiliging en Privacy
- Aanpak invoering BIO 1e concept 26-08-2019
- Checklist DPIA 03-03-2020
- Ensia verantwoording gemeente Son en Breugel 15-08-2018
- Ensia assurance rapport DigID en Suwinet verantwoording 2018 Son en Breugel door BKBO 04-04-2019
- Collegeverklaring ENSIA 2018 Informatiebeveiliging DigID en Suwinet, 17-04-2019
- Social enginering test Dommelvallei organisaties 29-10-2019
- Beheer informatie beveiligingsincidenten. Procesbeschrijving 28-06-2017
- Verwerkersovereenkomst bestemd voor de aangesloten gemeenten Dienst Dommelvallei, ongedateerd
- Verwerkersovereenkomst Son en Breugel versie november 2019
- Internetbericht telefoonfraude door Irene Kuipers, 26-02-2020
- Intranet, bewustwordingstegel, schermbeveiliging, nep e-mails en nep telefoontjes, ongedateerd
- Intranet, bewustwordingstegel Informatiebeveiliging en Privacy, ongedateerd
- Format verwerkersovereenkomst Dienst Dommelvallei en de drie aangesloten gemeenten, besluit B&W Son en Breugel 18-09-2019
- Privacy statement en Proclaimer Son en Breugel 17-03-2020
- Son en Breugel Openbaar register verwerking persoonsgegevens (format, ongedateerd)
- Datalekken, Dienst Dommelvallei door CISO, intranetbericht voor de periode na 25-05-2018
- Procesbeschrijving Beveiligingsincidenten en datalekken (stroomschema ongedateerd)
- Stappenplan: Kom in actie bij een datalek (afkomstig van de Autoriteit Persoonsgegevens, ongedateerd)
- Jaarstukken Son en Breugel 2018 onderdeel bedrijfsvoering, betreffende plannen voor de periode 2018 – 2020. Publicatie in 2018.
- Kritische processen Dienst Dommelvallei, bijgewerkt tot 12-03-2020
- Spelregels Son en Breugel coronavirus (nummer 20.0003346 ongedateerd)
- Werkconcept nieuwe gemeentehuis (17.0004741 ongedateerd)
- Service level agreement ICT Dienst Dommelvallei, december 2017
- Procedure Autorisatie toegang tot informatiesysteem gemeente Son en Breugel (behorend bij plan informatiebeveiliging)
- Visitatie VNG Dienst Dommelvallei en de aangesloten gemeenten 23-03-2016 (laatste versie)
- DPIA light t.b.v. inrichting van het zaaksysteem Sprint 2, 03-04-2020
- DPIA Zaaksysteem Vergunningen, Sprint 1, 06-02-2020
- DPIA Zaaksysteem Vergunningen, KCS, 29-10-2019
- DPIA Registratie ondersteuningsvragen CMD, 05-06-2019
- Chatfunctionaliteit Nuenen – Son en Breugel (versie 3 ongedateerd)
- Nieuwjaarstocht def (ongedateerd)
- DPIA Intergrip Son en Breugel (ongedateerd)
- Richtlijnen gebruik Circuit (ongedateerd)
- Richtlijnen aanvragen nieuw wachtwoord (ongedateerd)
- Eisen aan wachtwoord en schermbeveiliging (ongedateerd)

- Hoe kan ik extern werken, (Dienst Dommelvallei en de drie aangesloten gemeenten) 07-11-2019
- B&W adviesnota Ensia 2018 en DigID en Suwinet, 05-04-2019

Bijlage 2 Functies van geïnterviewde respondenten

Contactpersoon: Business Controller

- Chief Information Security Officer (CISO)/ENSIA-coördinator, Dienst Dommelvallei
- Controller, Dienst Dommelvallei
- Functionaris Gegevensbescherming, Dienst Dommelvallei
- Afdelingshoofd Dienstverlening, *gemeente Son en Breugel* moet zijn Dienst Dommelvallei
- Afdelingshoofd Personeel, Organisatie en Informatievoorziening, Dienst Dommelvallei
- Burgemeester (portefeuille houder) gemeente Son en Breugel

Bijlage 3. Normen

Om de onderzoeksvragen te beantwoorden hanteren we de onderstaande normen, per onderzoeksvraag gerangschikt.

1. Vraag: 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 Overheid (BIO). Hoe is het commitment en draagvlak op dit onderwerp bij bestuur en management van de gemeente? Dragen zij het informatiebeveiligingsbeleid uit?

   Norm: 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. Vraag: 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?

   Norm: Het management stelt naar aanleiding van een GAP-analyse het informatiebeveiligingsbeleid op. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld.

3. Vraag: 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?

   Norm: 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 Gegevens-bescherming (FG), opstellen van een privacystatement en opstellen van een register van verwerkingsactiviteiten.

4. Vraag: Kent de gemeente de leveranciers en partners waarmee deze samenwerkt en toetst deze hen op informatieveiligheidsaspecten, en zo ja hoe?

   Norm: 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.

5. Vraag: Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatie-veiligheid 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?

Norm: 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.

6. Vraag: Rapporteert en bespreekt de organisatie het functioneren van informatie-veiligheidsbeleid op management- en bestuursniveau (college en raad)? Zo ja, hoe?

   Norm: Gemeenten hebben afgesproken dat over het functioneren van de informatiebeveiliging aan het management en bestuur (colleges en raden) wordt gerapporteerd.

7. Vraag: 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?

   Norm: Voorwaarde voor informatiebeveiliging is onder andere dat dit een verantwoordelijk-heid 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.

8. Vraag: Welke opvolging heeft Dienst Dommelvallei gegeven aan de aansporingen en aanbevelingen van het onderzoek naar IB en privacy (mei 2019) van de Rekenkamercommissie Geldrop-Mierlo en wat betekent dit voor de gemeente Son en Breugel?

   Norm: Dienst Dommelvallei heeft adequaat gevolg gegeven aan de aansporingen en aanbevelingen van de Rekenkamercommissie Geldrop-Mierlo en heeft de inzichten ook geïmplementeerd bij de gemeente Son en Breugel.

Bijlage 4 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.
Assuranceverklaring	Een rapport van een onafhankelijke externe auditor, die een betrouwbaarheidsoordeel geeft over cijfers of processen.
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
Ceo-mail	Criminelen sturen, uit naam van de CEO van een organisatie, een mail naar een financiële medewerker van het bedrijf, met het dringende verzoek per ommegaande geld over te maken.
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/PMS	Information security management system/privacy 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 over 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 5 Bestuurlijke reactie

M E M O

Onderwerp : Bestuurlijke reactie op rapport Informatiebeveiliging en privacy

Aan : Rekenkamercommissie Son en Breugel

Van : College Son en Breugel

D.D. : 9 juni 2020 Kenmerk : 20.0006948

Geachte mevrouw Van Breugel, geachte heer Lemmens,

Wij spreken onze waardering uit voor het rapport, waarin u blijk geeft ook in deze bijzondere tijd een gedegen onderzoek te kunnen uitvoeren. Zoals in het Presidium is besproken, is informatiebeveiliging een onderwerp dat blijvend onze aandacht zal vragen, mede gelet op het toenemend belang van ict en data voor het functioneren van de gemeentelijke overheid. Dit onderzoek van de rekenkamercommissie beschouwen wij als een belangrijke informatiebron om een beeld te krijgen waar we nu staan.

De conclusies die u trekt kunnen wij volgen en grotendeels onderschrijven. Op basis van de getrokken conclusies geeft u een aantal waardevolle aanbevelingen en aansporingen. Echter zoals u zelf ook al concludeert, zijn wij continue bezig met nieuw beleid. Dat doen wij op dit terrein stapsgewijs. Momenteel bereiden wij samen met de beide andere gemeenten in de Dienst Dommelvallei een nieuw ict-beleidsplan voor. Informatieveiligheid zal daarvan integraal onderdeel uitmaken en als het ware het spoorboekje bieden voor achtereenvolgens te zetten stappen. Een aantal zaken is al in gang gezet. Zo start per 1 juli aanstaande de nieuwe privacy beheerder, waarbij wij hebben gekozen om gezamenlijk met de Dommelvallei gemeenten Nuenen en Geldrop Mierlo iemand aan te stellen. Deze zal ook een deel van uw aanbevelingen oppakken. Daarnaast richten we voor het zaakgericht werken dubbele autorisaties in op devices. We zijn voornemens om dit in de gehele organisatie door te voeren. Ook zijn wij in overleg met de collega Dommelvallei gemeenten over een verbetering van de fysieke (toegangs-)beveiliging van onze gebouwen. Deze maakt onderdeel uit van de tweede fase van het nieuwe gemeentehuis. Terecht wijst u in het rapport op het belang van bewustwording bij medewerkers. Ook dat heeft onze aandacht.

Ondanks dat we een aantal aanbevelingen zeer waardevol achten, maken wij op onderdelen een afweging tussen beschikbare middelen, menskracht en andere prioriteiten. Dit doen wij steeds weloverwogen en met oog voor praktische oplossingen.

Tot slot plaatsen wij nog enkele kanttekeningen. Wat ons opvalt is dat u naast de portefeuillehouder, de burgemeester, geen interviews heeft afgenomen met personen uit de organisatie Son en Breugel en u zich heeft beperkt tot interviews met werknemers van Dienst Dommelvallei. Deze collega's zijn van veel op de hoogte, maar we kunnen ons goed voorstellen dat organisatie specifieke kennis niet altijd aanwezig is bij de geïnterviewden. Een voorbeeld daarvan is dat u in uw rapport diverse keren verwijst naar (lijn)management, terwijl wij nu de omslag maken naar zelforganiserende teams. Daarnaast missen wij in uw stuk hoe u tot de normeringen bent gekomen. In bijlage 3 geeft u per onderzoeksvraag de norm aan. Wij zijn benieuwd waarop u deze heeft gebaseerd en hadden graag een toelichting daarop gezien in het rapport.

Wij danken u voor uw inspanningen.

Met vriendelijke groet, Burgemeester en wethouders van Son en Breugel,

De secretaris, De burgemeester,

Rien Schalkx Hans Gaillard

Bijlage 6. Nawoord Rekenkamercommissie

De rekenkamercommissie bedankt het college van B&W voor de bestuurlijke reactie en de waardering voor het onderzoek.

Informatiebeveiliging en privacy zijn terreinen die sterk in beweging (moeten) zijn, dat erkent de rekenkamercommissie. Vandaar het onderscheid dat wij maken tussen aansporingen, op de initiatieven die al door de gemeente en de Dienst Dommelvallei worden opgepakt, en de aanbevelingen met een hogere urgentiewaarde.

De rekenkamercommissie is verheugd om te vernemen dat het beleidsplan wordt c.q. inmiddels is opgepakt, in de veronderstelling dat daarmee ook het Jaarplan Informatiebeveiliging en integraal privacybeleid onder begrepen worden. Tevens is het goed te vernemen dat de functie van privacybeheerder per 1 juli 2020 wordt ingevuld, samen met de Dienst Dommelvallei en de gemeente Nuenen. Ook is het goed te lezen dat de gemeente aandacht schenkt aan dubbele verificatie (2FA) op zaakgericht werken, de fysieke en beveiliging en de bewustwording van medewerkers.

Het college heeft twee vragen in haar bestuurlijke reactie. Waarom de rekenkamercommissie naast de portefeuillehouder niet met personen uit de gemeentelijke organisatie heeft gesproken en waar de door de rekenkamercommissie gehanteerde normen in dit rapport op zijn gebaseerd.

De rekenkamercommissie deelt de opvatting van het college dat het altijd goed is om ook medewerkers uit de organisatie in dit geval de gemeente Son en Breugel te interviewen. De rekenkamercommissie was tot aan het bestuurlijke hoor en wederhoor in de veronderstelling dat het afdelingshoofd Dienstverlening, die geïnterviewd is, werkzaam is voor de gemeente Son en Breugel. Zo is de functie ook opgenomen in de oorspronkelijke concept respondentenlijst in bijlage 2 en is verbeterd bij de huidige definitieve versie. Dat deze veronderstelling niet klopte is de rekenkamercommissie niet gebleken uit het ambtelijk hoor en wederhoor. In een volgend onderzoek zal de rekenkamercommissie hierop extra alert zijn.

Met betrekking tot de normen die de rekenkamercommissie heeft gehanteerd het volgende. De normen zoals gesteld in dit rapport zijn gebaseerd op de regels uit de AVG en de BIO. Deze gelden als kader voor zowel privacy- en informatiebeveiliging. De rekenkamercommissie is ervan uit gegaan dat dit bekend is.

Naar aanleiding van de ambtelijk reactie wenst de rekenkamercommissie opmerken dat zelfsturende teams enige mate van lijnmanagement niet is uit te sluiten, de gemeentesecretaris blijft immers ambtelijk eindverantwoordelijk voor de organisatie.

Tot slot geeft het college aan een aantal aanbevelingen zeer waardevol te achten, maar op onderdelen een afweging te maken tussen beschikbare middelen, menskracht en andere prioriteiten. Die redenering kan de rekenkamercommissie goed volgen. De afweging is uiteraard binnen de kaders die de gemeenteraad stelt. Het ligt voor de hand de raad te informeren over de gemaakte keuzen, in het kader van ENSIA of op andere informatiemomenten met de raad of raadscommissie.