Rekenkamerrapport

Informatiebeveiliging en privacy

Bestuurlijke nota

Gepubliceerd op:

7 februari 2023

Rekenkamer
gemeente Doetinchem

Informatiebeveiliging en privacy gemeente Doetinchem

Inleiding

De rekenkamercommissie Doetinchem (hierna 'de rekenkamer') heeft een onderzoek laten uitvoeren naar het informatiebeveiligings- en privacybeleid van de gemeente. Dit onderzoek is uitgevoerd door bureau 'PRAE - advies en onderzoek' te Utrecht. Gekeken is naar het gevoerde beleid, de organisatie, de techniek en het menselijk handelen. In deze inleiding gaat de rekenkamer kort in op de belangrijkste conclusies.

Uit het onderzoek blijkt dat het over het algemeen op orde is, maar dat betekent niet dat de gemeente tevreden achterover kan leunen; er is werk aan de winkel.

De volwassenheid van de organisatie wordt door de gesprekspartners bij de gemeente Doetinchem wisselend ingeschat. Op sommige gebieden, zoals bij DigiD, is die op een hoog niveau aanwezig en op andere applicaties is dat minder het geval. De cultuur is erop gericht om zaken te doen, dingen te regelen zonder alles op papier op orde te hebben.

Een ander punt van aandacht is de bewustwording van de medewerkers. Door ethische hackers is er in het rekenkameronderzoek getest hoe medewerkers reageren op phishing en smishing mails (bij phishing proberen criminelen mensen door e-mails naar een valse website te lokken. Smishing of SMS-phishing is elke vorm van oplichting via sms. Oplichters versturen sms'en met valse links).

Een volgend punt waar de rekenkamer aandacht voor vraagt in deze inleiding is de positie van Doetinchem als gastheer van de omliggende gemeenten op het gebied van ICT en het steeds voldoende afgedekt zijn van actuele risico's daarbinnen.

Het datagedreven werken staat nog in de kinderschoenen. Hiervoor is nog geen beleidskader ontwikkeld. Hierdoor is er nog geen zicht op het waarborgen van de privacy van burgers.

Ten slotte wil de rekenkamer hier wijzen op het feit dat de raad te weinig betrokken wordt bij en te summier geïnformeerd wordt over informatieveiligheid. De rekenkamer benadrukt dat deze conclusie twee kanten heeft. Het college kan meer informatie verschaffen en de raad kan meer vragen stellen.

Het onderzoek

De centrale onderzoeksvraag luidt: “Welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie van de gemeente en op welke wijze gaat de gemeente om met de privacygevoelige gegevens en informatie waarover zij beschikt?”

Dit onderzoek heeft geleid tot een Nota van bevindingen. Deze nota is als bijlage bijgevoegd. Hier volgen de conclusies en de aanbevelingen.

Conclusies

De gemeente Doetinchem onderneemt de stappen om te voldoen aan het beleid op informatiebeveiliging en privacy, samen het informatieveiligheidsbeleid.

Hoofdconclusie

De gemeente Doetinchem heeft nog een ontwikkeling door te maken om ‘in control’ te komen op informatieveiligheid.

Deelconclusies

Deze hoofdconclusie leidt tot de volgende deelconclusies:

1. Het informatiebeveiligings- en privacybeleid, samen in het informatie-veiligheidsbeleid, is actueel.
2. Bewustwording van medewerkers krijgt aandacht en blijft continu punt van aandacht.
3. De strategische formatie op informatieveiligheid moet versterkt worden en los van de lijn in de staf geplaatst worden.
4. Er moet een doelstelling geformuleerd worden om het gemiddelde volwassenheidsniveau op informatieveiligheid te verhogen.
5. De technische kant van informatieveiligheid is conform de normen, maar moet nog beter gemonitord worden.
6. De ICTsamenwerking waarvan Doetinchem gastheer is, kent risico’s die niet afdoende zijn afgedekt in de dienstverleningsovereenkomst.
7. De raad wordt te weinig betrokken bij en te summier geïnformeerd over informatieveiligheid.
8. Er ontbreekt een beleidskader voor de uitdagingen die de transformatie van de digitale dienstverlening van de gemeente biedt.

Aanbevelingen

De conclusies leiden tot de volgende aanbevelingen:

1. Versterk de positie van de strategische functionarissen op informatiebeveiliging en privacy en plaats deze in een staffunctie.

Aan college

- Positioneer de CISO (Chief Information Security Officer) en Functionaris Gegevensbescherming (FG) in een van de lijn onafhankelijk staffunctie.
- Verstevig wat betreft omvang de formatie van deze strategische functies op informatieveiligheid.

1. Formuleer de ambitie om het gemiddelde niveau van de medewerkers van de gemeente te verhogen.
2. Betrek de raad meer bij het formuleren van ambities op informatieveiligheid en informeer de raad meer op de voortgang op deze ambities.
3. Inventariseer de risico's in de samenwerking op ICT, bespreek deze met de partners en richt daarop de vernieuwde samenwerking in.
4. Stel een beleidskader op basis van de Digitale Agenda Gemeenten 2024 van de VNG.

Aan college en raad

Ga samen het gesprek aan om de vrije ruimte in het kader van ENSIA in te vullen, zodat de raad voor zijn controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy. ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit. Het project ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid.

Over het onderzoek

Aanpak

Voor het onderzoek zijn beleidsdocumenten en rapportages op informatiebeveiliging en privacy bestudeerd. Daarnaast zijn in opdracht van de rekenkamercommissie enkele testen uitgevoerd op de systemen en is een phishing/smishing campagne uitgezet onder de medewerkers van de gemeente. Interviews zijn gehouden met een aantal sleutelpersonen. Ook zijn casestudies naar de praktijk van gegevensverwerking uitgevoerd in de teams Sociaal Domein

en Toezicht en Handhaving. Hieronder volgt de beantwoording van de onderzoeksvragen, gevolgd door conclusies en aanbevelingen.

Beantwoording onderzoeksvragen

1. Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?
2. Beschikt de gemeente over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?
3. Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?
4. Hoe is de informatievoorziening aan de gemeenteraad?
5. Wat zijn de toekomstige opgaven?

Onderzoeksvraag 1: Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?

Informatiebeveiligingsbeleid

De gemeente Doetinchem heeft een actueel informatiebeveiligings- en privacybeleid dat in april 2020 door het college van burgemeester en wethouders is vastgesteld. Doel is te voldoen aan de BIO- en AVG-richtlijnen (BIO is Baseline Informatiebeveiliging Overheid en AVG is Algemene Verordening Gegevens-bescherming). Het informatieveiligheidsbeleid maakt onderdeel uit van de Informatievisie 2020-2022, samen met de dienstverlenings- en communicatievisie. In het strategisch beleid zijn de verantwoordelijkheden, functies en rollen belegd op basis van het RASCI-model (R(esponsible), A(ccountable), C(onsulted), S(upportive), I(nformed)). Jaarlijks wordt het informatieveiligheidsplan opgesteld door de CISO (Chief Information Security Officer), met activiteiten voor dat jaar en waarin ook wordt teruggeblikt. Het jaarplan wordt geaccordeerd door het MT.

Protocollen en richtlijnen

De meeste protocollen en richtlijnen zoals voorgeschreven door de BIO, het basisnormenkader, zijn aanwezig bij de gemeente. Een aantal wordt nog gemist, zoals protocollen op mobiele datadragers, cryptografie, leveranciersmanagement en op onderdelen logging/monitoring. Een compleet en integraal bedrijfscontinuïteitsplan staat voor 2022 op de rol. Onderdelen daarvan, zoals het opschalingsmodel cybercrisis, zijn recent gereed gekomen.

Functies

De teamleiders zijn integraal verantwoordelijk voor informatieveiligheid.
De informatieveiligheidsbeheerders en de informatieveiligheidscoördinator zijn respectievelijk op operationeel en tactisch niveau op informatiebeveiliging actief. Op strategisch niveau opereert de CISO op informatiebeveiliging. Deze is sinds eind 2021 'dedicated' voor 16 uur bij het team Informatiemanagement gepositioneerd. Idealiter moet deze functie apart van de lijnorganisatie gepositioneerd zijn.

Daarnaast kent het team ter ondersteuning op operationeel niveau drie informatieadviseurs. Vanwege de gemeentegrootte zijn veel functies duo-functies, ook op informatieveiligheid, en is het lastig capaciteit uit de markt te halen.

Overleggen

In Doetinchem is intern een vierwekelijks overleg tussen de portefeuillehouder, teamleider ICTsamenwerking en manager bedrijfsvoering, onder andere over informatieveiligheid. De CISO kan zelfstandig naar de gemeentesecretaris, portefeuillehouder of burgemeester schakelen. De gemeentelijke partners in de samenwerking participeren in de werkgroep informatiebeveiliging, met een adviesrol. De informatieveiligheidscoördinator van Doetinchem neemt daaraan deel. Daarnaast is er alleen een ambtelijk overleg tussen de gemeentesecretarissen van de deelnemende gemeenten.

Rapportages

Het jaarlijkse informatieveiligheidsplan gaat vanaf 2022 naast het MT ook naar de teamleiders. Elk kwartaal worden de incidenten, datalekken en de verbeterpunten aan het MT gerapporteerd. De informatieveiligheidscoördinator verzorgt ook de ENSIA-rapportage voor de verticale verantwoording richting landelijke toezichthouders en de horizontale verantwoording richting de gemeenteraad. Daarvoor gebruikt de gemeente geen informatiemanagementsysteem, wat een van de voorwaarden in de BIO is.
Tot slot gaat de accountant ook nog in op informatiebeveiliging in de jaarlijkse managementletters.

Onderzoeksvraag 2: Beschikt de gemeente over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?

Privacybeleid

Vanaf 2020 heeft de gemeente in informatieveiligheid het privacybeleid gekoppeld aan informatiebeveiligingsbeleid. De verantwoordelijkheden met betrekking tot privacybeleid zijn belegd. Net zoals bij informatiebeveiliging is de uitvoering van het privacybeleid belegd bij de teamleiders.

Elementen

De voor de AVG verplichte elementen en instrumenten zijn aanwezig, zoals het verwerkingsregister, privacystatement, verwerkersovereenkomsten, een procedure voor datalekken en risicobeoordeling met behulp van dataprotection impact assessments (dpia's).

Functies

De Functionaris Gegevensbescherming (FG) is voor 36 uur bij de gemeente Doetinchem aangesteld en vult deze functie in voor meerdere gemeenten en instellingen. In totaal is de FG voor 170 uur per jaar beschikbaar op strategisch niveau voor Doetinchem. Op tactisch niveau is een privacycoördinator aanwezig en op operationeel gebeid zijn privacybeheerders in de teams aangewezen.

Overleggen

De FG is betrokken bij de werkgroep informatiebeveiliging in het ICT samenwerkingsverband. De FG en CISO hebben maandelijks een overleg over informatieveiligheid. De privacy- en informatiebeveiligingscoördinator hebben wekelijks onderling overleg. Daarnaast heeft de FG een regionaal overleg met de privacycoördinatoren van de gemeenten en instellingen waar deze de FG-functie vervult. Aanvullend is er een overleg met FG'en uit de Achterhoek.

Rapportages

De FG stelt jaarlijks een rapportage op met een toetsing aan de AVG, met aandacht voor de wisselende focusgebieden van de Autoriteit Persoonsgegevens (AP). Net als voor informatiebeveiliging wordt geen gebruikgemaakt van een informatiemanagementsysteem om de rapportages op te stellen.

Onderzoeksvraag 3: Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?

Hieronder gaan we in op vijf punten: bewustwording, uitvoering van de AVG, ICTsamenwerking, autorisatieproces, monitoring en pentesten.

Bewustwording

Bewustwording van medewerkers op de risico's met betrekking tot informatiebeveiliging en privacy is groeiende, zoals het melden van incidenten en datalekken. Maar bewustwording blijft continu inspanningen vragen. Daarop stelt de gemeente jaarlijks een apart bewustwordingsplan op met verschillende activiteiten. Daarbij wordt bewustwording organisatiebreed onder de aandacht gebracht en onderdeel van functioneringsgesprekken. Het proces van bewustwording verloopt traag en niet alle geledingen worden even doeltreffend met activiteiten en verbeterplannen bereikt.

De bewustwordingsactiviteiten worden ook gericht op MT en college. Het draagvlak bij management en bestuur voor informatiebeveiliging en privacy is groeiende. In het MT worden de rapportages en verbeterplannen op beide onderwerpen doorgesproken en vastgesteld. De rekenkamer heeft de indruk dat onderwerpen als investeringen op informatiebeveiliging en privacy in het college niet de hoogste prioriteit hebben.

Het kennisniveau in de organisatie bij de proceseigenaren blijft op het gebied van informatiebeveiliging achter op privacy en is met name aanwezig bij de medewerkers die met cruciale applicaties werken, zoals financiën, DigiD en Suwinet. Informatiebeveiliging is dan ook meer technisch van aard. Het gemiddelde volwassenheidsniveau conform de NOREA-index, is weliswaar niet gemeten, maar wordt niet heel hoog ingeschat (NOREA is de beroepsorganisatie van IT-auditors, die in de NOREA-index normen heeft vastgelegd. Dat heeft onder andere te maken met de cultuur om zaken te regelen zonder alles op papier te documenteren. Het beeld is dan ook dat de gemeente niet volledig in control is op gebied van informatiebeveiliging en privacy.

AVG (Algemene verordening gegevensbescherming)

Vanaf 2017 is de gemeente met medewerkers aan de slag gegaan op het gebied van privacy. De verplichte elementen en instrumenten op gegevensbescherming zijn aanwezig. De (pre)dataprotection impact assessments ([pre-]dpia's) worden door de proceseigenaren gehouden, maar vergen nog veel ondersteuning door de privacycoördinator. Ook hierbij wordt geconstateerd dat het

volwassenheidsniveau op naleving van de processen en vastlegging van activiteiten omhoog kan.

De FG rapporteert jaarlijks aan MT en college over de voortgang op de AVG-maatregelen. En monitort daarbij de activiteiten op onder andere beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking beveiliging en verantwoording. De positie van de FG mist een zekere strategische inbedding, daar MT en bestuur met name contact heeft met de privacycoördinator. In de bestuurlijke processen wordt het privacy aspect vaak te laat betrokken.

ICTsamenwerking

De gemeente Doetinchem is sinds 2015 gastheer van het samenwerkingsverband op ICT met omliggende gemeenten en regionale instellingen. In 2018 is het samenwerkingsverband herbevestigd. Het is een verband met een lichte structuur, zonder uitgebreide dienstverleningsovereenkomsten. Er is geen bestuurlijk overleg binnen de samenwerking, wel hebben de gemeentesecretarissen een overleg.

Inhoudelijk is er op informatiebeveiliging een werkgroep die adviezen geeft. Vanwege de vele verschillende functieniveaus van de participanten is het nog een zoektocht waarover op informatiebeveiliging en privacy overlegd kan worden. De werkgroep kan bij crisissituaties optreden, zoals bij de Log4J-dreiging in december 2021 (Log4J-dreiging wordt uitgebreid beschreven op pagina 23 van het rapport in de bijlage). Een interdisciplinair actieteam is in Doetinchem opgezet, waarbij in samenspraak met de deelnemende partners naar tevredenheid is gecommuniceerd en geacteerd.

Doetinchem is als gastheer verantwoordelijk voor de continue en veilige werking van de ICT. Technische maatregelen zijn en worden daartoe genomen. En de gemeente voert periodiek technische testen uit op de beveiliging van de systemen, zoals uitwijk- en pentesten (zie over pentesten ook hierna).

Betwijfeld kan worden of de governance op het samenwerkingsverband toekomstbestendig is ingeregeld.

Autorisaties

Met het autorisatieproces wordt geregeld dat medewerkers toegang krijgen tot de applicaties en gegevens die ze nodig hebben voor de uitoefening van hun functie. Het autorisatiebeleid ziet er dan ook op toe dat medewerkers niet bij

gegevens kunnen die zij niet nodig hebben. Bij door- of uitstroom van de medewerker moeten de autorisaties worden aangepast. Dat is afhankelijk van de melding door de leidinggevende en de tijdigheid daarvan blijkt niet altijd gegarandeerd. Het autorisatieproces verdient nog meer aandacht en controle. Ook de accountant adviseerde het college begin 2022 om onder andere hieraan aandacht te besteden.

Casestudies

Uit de casestudies bij het Sociaal Domein en Toezicht en Handhaving werd duidelijk dat beide teams al langere tijd ervaring hebben met de verwerking van persoonsgegevens. Dat is met de Algemene Verordening Gegevensbescherming (AVG) sinds 2018 en recenter de Wet politiegegevens (Wpg) sinds 2020 nog strikter geworden. De teams gaan consciëntieus met de richtlijnen hierin om. Op de meeste gegevensverwerkingsprocessen in het sociaal domein zijn (pre)dpia's gehouden, bij toezicht en handhaving nog geen.

In het sociaal domein wordt enige hinder ervaren in de preventiesfeer doordat de AVG drempels opwerpt bij het onderling delen van gegevens met andere instanties. En uit de casus bij toezicht en handhaving kwam naar voren dat het beveiligd mailverkeer met behulp van de applicatie Zivver nog niet voor alle medewerkers is geïmplementeerd.

Monitoring

Monitoring van de uitvoering van het beleid op informatiebeveiliging en privacy geschiedt op verschillende manieren. De implementatie van de BIO-maatregelen gebeurt via op basis van een GAP- en risicoanalyse, die input voor de activiteiten voor de jaarplannen opleveren. Zoals aangegeven is, door het vastleggen van de controleactiviteiten en de checks een aandachtspunt. Daardoor is in de organisatie zicht in bestaan en opzet van beleid en maatregelen, maar ontbreekt een volledig zicht op de werking ervan in de praktijk. Dat is niet het geval bij de applicaties DigiD en Suwinet, daar hierbij de vastlegging van activiteiten, logging en monitoring in het kader van ENSIA landelijk wordt afgedwongen.

Pentesten

De gemeente Doetinchem laat door externen pentesten uitvoeren op de systemen die de gemeente voor de ICTsamenwerking als gastheer beheert. Daar komen verbeterpunten uit die door de ICTsamenwerking worden opgepakt. In het kader van het rekenkameronderzoek zijn ook pentesten uitgevoerd. Om de scope van de testen te bepalen, zijn de recentste externe en interne

netwerkpentesten van de gemeente door de ethische hackers die de rekenkamer heeft ingehuurd bekeken. Op basis van die analyse is door de rekenkamer besloten de wifi-netwerk pentest, AD audit (AD staat voor Active Directory en geeft beheerders de mogelijkheid om de rechten van medewerkers te beheren) en een phishing/smishing test uit te voeren, en niet een externe en interne netwerk pentest over te doen. Ook is afgezien van een in eerste instantie voorgenomen mystery guest bezoek. Omdat veel medewerkers thuis werkten gedurende de coronamaatregelen had zo'n test weinig zin.

De testen leverden laag tot gemiddelde risico's op, geen hoog kritieke risico's. De resultaten van deze testen zijn vertrouwelijk gedeeld met de gemeentesecretaris, zodat de gemeente aan de slag kan met de verbeter- en aandachtspunten uit de testen. Deze verbeterpunten hadden onder andere te maken met bewustzijn van de medewerkers, wat een continu aandachtspunt is.

Onderzoeksvraag 4: Hoe is de informatievoorziening aan de gemeenteraad?

Summier geïnformeerd

De raad heeft volgens het informatieveiligheidsbeleid geen kaderstellende maar alleen een controlerende rol. Het college en management vat het beleid als onderdeel van bedrijfsvoering op. De onderwerpen worden incidenteel geadresseerd in de raad. De gemeenteraad wordt in het kader van de P&C-cyclus over informatiebeveiliging en privacy summier geïnformeerd. In de jaarstukken van de gemeente wordt over het informatiebeveiligingsbeleid gerapporteerd en worden de resultaten van de ENSIA-rapportage behandeld. Kort worden activiteiten op informatiebeveiliging en privacy belicht.

Op privacy krijgt de raad een infographic en samenvatting van de jaarrapportage van de FG. De raad krijgt apart in het kader van de horizontale verantwoording, waarvoor ENSIA is bedoeld, de college- en assuranceverklaring over de audits op DigiD en Suwinet. Het college heeft de ENSIA-stukken geheim verklaard en deze ter inzage gelegd voor raadsleden.

De informatievoorziening op informatieveiligheid aan de raad voldoet in principe aan de gestelde eisen, maar is als summier te beoordelen. Ook al is het voor veel raadsleden een technisch onderwerp, gelet op de risico's die de gemeente hierop loopt, kan de raad hierin meegenomen worden. Naast de rapportages die via het college komen, geeft de accountant in de controles ook op onderdelen van informatiebeveiligingsbeleid oordelen over de werking ervan.

Onderzoeksvraag 5: Wat zijn de toekomstige opgaven?

Risico's en kansen

De verwachting is dat door verdergaande digitalisering de risico's op en de investeringen in informatieveiligheid alleen maar zullen toenemen. Daarentegen gebeurt digitalisering niet zomaar, het biedt ook kansen en de mogelijkheid tot verbetering van de efficiëntie en effectiviteit van het door de gemeente gevoerde beleid. Digitalisering is niet alleen meer van de afdeling ICT, maar doordesemt alle takken van de gemeentelijke werkzaamheden. De Digitale Agenda Gemeenten 2024 van de VNG heeft drie doelstellingen geformuleerd voor de transitie van de digitale gemeentelijke dienstverlening: mogelijk maken – kansen benutten – duiden en reflecteren.

Datagedreven werken

In Doetinchem staat datagedreven werken en koppelen van gegevens nog in de kinderschoenen. De gemeente participeert sinds 2020 in Datalab GO, een project van gemeenten in Oost Gelderland waarvan Bronckhorst de penvoerder is. Vooralsnog gaat het daarbij om koppeling van gegevens in het fysieke domein. Maar het wordt niet uitgesloten dat ook andere gegevens gebruikt gaan worden. In het sociaal domein experimenteert de gemeente met koppeling van gegevens, en dat gebeurt geanonimiseerd en niet tot personen herleidbaar.

Algemene landelijke kaders zijn er slechts ten dele of in ontwikkeling. De gemeente heeft geen eigen visie of beleid geformuleerd om de kansen te benutten die de nieuwe technologieën bieden, of om de risico's met betrekking tot gegevensverwerking te duiden. Daardoor ontbreekt het kader om de transformatie van de digitale dienstverlening van de gemeente optimaal vorm te geven.

Nota van bevindingen Informatiebeveiliging en privacy gemeente Doetinchem

In opdracht van en bewerkt door de rekenkamercommissie Doetinchem

Drs. E. Lemmens, Prae Advies en onderzoek, Utrecht

Januari 2023

Inhoudsopgave

Inleiding

Aanleiding

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonlijke en gevoelige data. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder andere blijkt uit de recente voorbeelden die de Rekenkamer Doetinchem in de directe omgeving signaleert (Hof van Twente en Lochem) en datalekken (zoals belastingsamenwerking West-Brabant). Onderzoeken van rekenkamer(commissie)s wijzen op de risico's op het gebied van informatie-beveiliging en privacy, zoals zeer recent de Rekenkamer Utrecht aantoonde dat de kwetsbaarheid met name intern is.

Wat gebeurt er bijvoorbeeld als die informatie op straat komt te liggen? Of als de digitale dienstverlening aan burgers niet meer mogelijk is? Naast grote financiële, juridische en technische gevolgen kunnen deze crises het imago van de gemeente en de privacy van burgers aantasten.

De Rekenkamer Doetinchem heeft in 2021 informatiebeveiliging en privacy als onderzoeksonderwerpen geagendeerd. Het onderzoek is uitgevoerd door Prae Advies en onderzoek.

Leeswijzer

In hoofdstuk 1 zijn de onderzoeksvragen opgenomen en in hoofdstuk 2 is de onderzoeksaanpak verantwoord. Hoofdstuk 3 gaat in op het informatie-beveiligingsbeleid en hoofdstuk 4 op het privacybeleid. Over de uitvoering van het beleid wordt in hoofdstuk 5 gerapporteerd, met een samenvatting van de 2 cases die in de bijlagen 3 en 4 zijn opgenomen. In hoofdstuk 6 komt de informatievoorziening aan de raad aan bod. Hoofdstuk 7 gaat over de toekomstige opgaven.

Bijlagen

In bijlage 1 zijn de geraadpleegde documenten opgenomen en de geïnterviewde functionarissen. In bijlage 2 is een verklarende woordenlijst opgenomen van termen en afkortingen die in het ICT-jargon worden gebruikt. In de bijlagen 3 en 4 zijn respectievelijk de casestudies naar gegevensgebruik in het Sociaal Domein en bij Toezicht en handhaving opgenomen. Samenvattingen daarvan zijn in hoofdstuk 5 weergegeven. In bijlage 5 zijn de normen, zoals gehanteerd in dit onderzoek, opgenomen en gerangschikt naar de onderzoeksvragen. In bijlage 6 zijn Richtlijnen/procedures Informatiebeveiliging en privacy van de IBD opgenomen. Bijlage 7 bevat het nomenkader van de volwassenheidsmeting van NOREA opgenomen.

1 Onderzoeksvragen

Centrale onderzoeksvraag

De Rekenkamer wil met het onderzoek de volgende centrale vraag beantwoorden:

"Welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie van de gemeente en op welke wijze gaat de gemeente om met de privacygevoelige gegevens en informatie waarover zij beschikt?"

Onderzoeksvragen

Deze centrale vraagstelling wordt uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

1.	Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?
2.	Beschikt de gemeente over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?
3.	Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?
4.	Hoe is de informatievoorziening aan de gemeenteraad?
5.	Wat zijn de toekomstige opgaven?

De onderzoeksvragen worden in de hoofdstukken 3 tot en met 7 beantwoord. In het volgende hoofdstuk gaan we in op de onderzoeksaanpak.

2 Onderzoeksaanpak

Het onderzoek bestaat uit vier verschillende onderdelen, nl. deskresearch, interviews, pentesten en casestudies.

Deskresearch, interviews

Met betrekking tot beleid en de protocollen is deskresearch gepleegd. Een overzicht van de geraadpleegde documenten is in bijlage 1 opgenomen. Met vier bestuurlijke en ambtelijke sleutelfiguren is een interview afgenomen. De lijst met geïnterviewde functionarissen is ook in bijlage 1 opgenomen.

Casestudies

Om de organisatorische en menskant van de uitvoering van het informatie-beveiliging- en privacybeleid in de gemeente te onderzoeken, zijn twee casestudies uitgevoerd. Het gaat daarbij om inzichtelijk te maken hoe het beleid in de praktijk daadwerkelijk wordt uitgevoerd. Voor inzicht in de uitvoering wordt ook gebruikgemaakt van de bevindingen uit de interviews. De voor de casestudies geïnterviewde functionarissen zijn in bijlage 1 opgenomen.

Pentesten

Een ander onderdeel om de uitvoering te onderzoeken, bestaat uit het uitvoeren van pentesten. De pentesten zijn grotendeels gericht op de technische kant van informatiebeveiliging, maar ook deels op de naleving van beleid en procedures. Deze zijn uitgevoerd door ethische hackers van Awaretrain en IP4Sure.

Vooraf aan de pentesten is door het college aangegeven dat ICTsamen-werking, het samenwerkingsverband op basis van gastheerschap van de

gemeente Doetinchem, ook testen uitvoert op de systemen. Die testen bestonden onder andere uit een externe en interne netwerkpentest. Deze waren recent uitgevoerd en op de verbeterpunten die daaruit naar voren kwamen zijn maatregelen getroffen. De pentesten zijn door de onderzoekers gecheckt en als adequaat beoordeeld. De rekenkamer-commissie heeft daarop besloten geen interne en externe netwerkpentest uit te laten voeren.

Besloten is in het kader van het rekenkameronderzoek aanvullend een Active Directory (AD) audit [1], wifi-netwerk pentest [2], phishing [3] en smishing [4] test en een mystery guest [5] uit te voeren. Voor een nadere uitleg van de testen zie §6.2. Gedurende de looptijd van de pentesten werd vanwege de coronapandemie het thuiswerkadvies ingevoerd. Een mystery guest onderzoek heeft weinig zin als geen medewerkers aanwezig zijn op het stadhuis. Vandaar dat is besloten deze test niet uit te voeren.

Hoor en wederhoor

Op 10 mei 2022 is de nota van bevindingen voor de feitencheck in het kader van de ambtelijke hoor en wederhoor aangeboden aan de gemeentesecretaris. De nota van bevindingen is daarna aangevuld met conclusies en aanbevelingen en als rekenkamerrapport op 16 februari 2023 aangeboden aan de gemeenteraad.

1 De Active Directory (AD) staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren. De AD bevat een database waarin onder andere accounts en inloggegevens zijn opgenomen. Een AD audit test onder andere het wachtwoordenbeleid en inactieve accounts.

2 De wifi netwerk pentest is bedoeld om de beveiliging van de draadloze netwerken te toetsen en mogelijke kwetsbaarheden in kaart te brengen. Gesimuleerd wordt of een kwaadwillende baat kan hebben bij een aanvalsscenario op het draadloze netwerk van de gemeente.

3 Phishing is een vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens.

4 Smishing is dezelfde vorm van internet oplichting en fraude als phishing via valse sms-berichten op mobiele telefoons.

5 Tijdens een mystery guest bezoek probeert een onderzoeker onder valse voorwendselen fysiek binnen te dringen in de gemeentelijke organisatie. Doel is inzicht te krijgen in kwetsbaarheden als ongeautoriseerde toegang mogelijk is tot kantoren en werkruimtes, tot werkstations, informatie of dossiers op bureaus, printers of afvalcontainers.

3 Informatiebeveiliging

Onderzoeksvraag 1	In dit hoofdstuk beantwoorden we de eerste onderzoeksvraag: *Beschikt de gemeente Doetinchem over een adequaat informatie-beveiligingsbeleid?*

ICTsamenwerking

Op ICT werkt de gemeente Doetinchem sinds 2015 samen met de gemeenten Bronckhorst, Aalten, Oude IJsselstreek en Doesburg en verschillende regionale instellingen zoals Laborijn, Regio Achterhoek, Streekarchief, BuHa en de Omgevingsdienst Achterhoek (ODA). Doetinchem voert het gastheerschap uit in het samenwerkingsverband. In 2018 is het convenant dat onder de samenwerking en het gastheerschap ligt vernieuwd. In totaal bedient de ICT-dienstverlening ongeveer 2.300 gebruikers.

De gemeente is zich ervan bewust dat de gemeente zelfstandig niet in staat is de ICT-vraagstukken aan te kunnen. Door schaalvergroting, de toenemende vraag naar kwaliteit en risico's wordt samenwerking op ICT noodzakelijk geacht. De samenwerking op ICT is met name gericht op automatisering en standaardisering. Voor het beleid op informatiebeveiliging, privacy en de verschillenden domeinen zijn de gemeenten zelf verantwoordelijk.

3.1 Beleid

Informatiebeveiligingsbeleid

In april 2020 heeft het college van B&W het Informatieveiligheidsbeleid 2020-2022 vastgesteld. Dit beleid verving het Informatiebeveiligingsbeleid 2015-2019 en is in 2022 gelden. Het informatiebeveiligingsbeleid wordt gepositioneerd als onderdeel van de Informatievisie 2020-2022. Samen met de dienstverleningsvisie en communicatievisie vormt deze de basis voor de dienstverlening. In 2018 zijn de drie visies op elkaar afgestemd.

In 2020 is besloten het beleid voor informatiebeveiliging en privacy samen te voegen. Het kader van dit beleid wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO, gebaseerd op ISO-27002) en de Algemene Verordening Gegevensbescherming (AVG). De doelen zoals in het informatiebeveiligingsbeleid opgenomen zijn:

- Het beschermen en op behoorlijke en zorgvuldige wijze omgaan met informatie zodat de beschikbaarheid, integriteit, vertrouwelijkheid behouden blijft;
- Het waarborgen van de bescherming van persoonsgegevens (privacy);
- Het minimaliseren van informatieveiligheidsrisico’s tot een acceptabel niveau.

De gebruikelijke aandachtsgebieden op informatiebeveiliging worden in het beleid geadresseerd: mens-organisatie-techniek.

GAP-analyse

Voor het informatiebeveiligingsbeleid is een GAP-analyse [6] uitgevoerd op basis van de BIO-maatregelen. Daaruit komen in principe de maatregelen voort die de gemeente moet nemen om te voldoen aan de BIO. Niet alle maatregelen kunnen meteen of volledig worden uitgevoerd of geïmplementeerd. Op basis van een risicoanalyse worden risico's al dan niet geaccepteerd, en indien nodig beheersmaatregelen genomen (zie ook §6.1.3.)

Vakgebieden

Het beleid geldt voor de vakgebieden:

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Paspoorten en Nederlandse identiteitskaarten (PNIK)
- Digitale persoonsidentificatie (DigiD)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)

Handboeken, beveiligingsplan

Voor Suwinet en DigiD, Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN)en Paspoorten en Nederlandse identiteitskaarten (PNIK) worden apart handboeken opgesteld. Deze worden jaarlijks gecontroleerd en indien nodig geüpdatet. Deze applicaties maken onderdeel uit van audits die landelijke toezichthouders streng controleren. Dat gebeurt mede in het kader van Eenduidige Normatief Single Information Audit (ENSIA) [7], de rapportage die de verticale en horizontale verantwoording vorm geeft (zie §4.3.)

RASCI-model

In het informatieveiligheidsbeleid zijn de taken en verantwoordelijkheden belegd, waarbij vijf functies/rollen zijn benoemd op basis van het zogenoemde RASCI-model, zie hieronder:

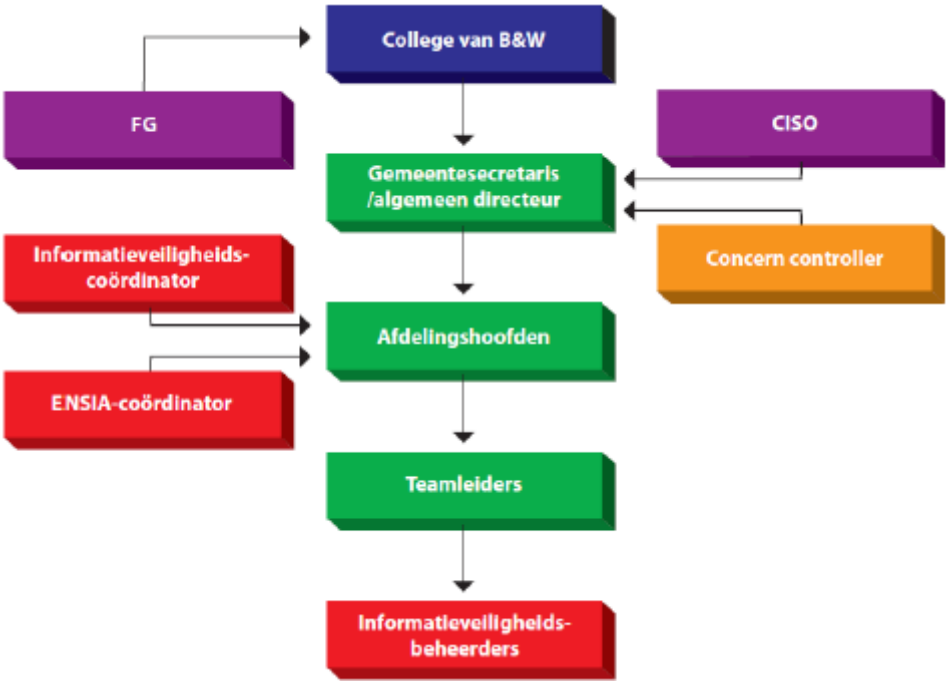
- Responsible (R): die verantwoordelijk is voor de uitvoering van werk, taak en activiteit (teamleiders, managers en gemeentesecretaris)
- Accountable (A): die is uiteindelijk verantwoordelijk dat R de werk, taak en activiteit uitvoert (college van B&W);
- Consulted (C): degene die door R voor advies wordt geraadpleegd (Chief Information Security Officer [CISO] en Functionaris Gegevensbescherming [FG]);
- Supportive (S): levert op verzoek van R ondersteuning (informatieveiligheidscoördinator, ENSIA-coördinator en informatieveiligheidsbeheerders);
- Informed (I): degene die over de status en het resultaat geïnformeerd moet worden (concerncontroller).

---

6 Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie. Het verschil tussen beide is de te overbruggen gap (kloof).

7 Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders).

Afbeelding 1. Rollen op basis van RASCI-model



Verantwoordelijkheden

De teamleiders zijn integraal verantwoordelijk voor informatiebeveiliging en privacy, kortom informatieveiligheid. De teamleiders organiseren op operationeel niveau dat de medewerkers in de teams en aan de beleidseisen kunnen voldoen. De informatieveiligheidsbeheerders zijn op operationeel niveau verantwoordelijk voor de inrichting en implementatie van informatiebeveiliging. Dat zijn de functioneel applicatiebeheerders in de verschillende afdelingen/domeinen. De managers faciliteren de teamleiders en worden daarbij op tactisch operationeel niveau ondersteund door de informatieveiligheidscoördinator. Op strategisch terrein controleert de CISO het informatiebeveiligingsbeleid en adviseert de gemeentesecretaris. De ENSIA-coördinator is verantwoordelijk voor de rapportage in het kader van de horizontale en verticale verantwoording (zie §4.3.)

Functies

Om de strategische rol te kunnen vervullen, heeft de CISO een onafhankelijke positie. Deze heeft een eigen verantwoordelijkheid en kan in principe zelfstandig schakelen met de gemeentesecretaris en de portefeuillehouder. Organisatorisch is de functie vanaf 1 november 2021 ondergebracht bij het team informatiemanagement. Voorheen vervulde een van managementleden de rol van CISO. Deze ging met pensioen en toen is besloten middelen vrij te maken voor een 'dedicated' CISO voor 16 uur. Afhankelijk van wat zich voordoet, kunnen dat meer uren zijn, zoals recent bleek bij de ontdekking van de kwetsbaarheid in verband met Log4J [8] (zie §6.1.3.)

[8] Log4J is een stuk software dat veel gebruikt wordt in webapplicaties en andere systemen, dat in december 2021 bleek kwetsbaar te zijn voor aanvallen van hackers.

Daarnaast zijn drie informatieadviseurs bij het team Informatie-management voor de operationele ondersteuning. Voor het tactische/operationele aspect is er een informatiebeveiligingscoördinator (en privacycoördinator, zie §5.1) bij het team Informatiemanagement ondergebracht.[9]

Uit de interviews blijkt dat het lastig is de juiste capaciteit op ICT binnen te halen, zoals bij veel andere gemeenten. Zo is er al een vacature IT-securityspecialist voor ICTsamenwerking die al maanden open staat. Vanwege de schaalgrootte van de gemeente zijn er op de verschillende niveaus duo-functies.

Procedures/protocollen

Het informatiebeveiligingsbeleid benoemt op specifieke onderdelen de ondersteunende procedures en protocollen die nodig zijn voor de inrichting van het beleid. Zoals gemeld, zijn er op vakgebieden handboeken, die jaarlijks geüpdatet worden. Verder zijn aangetroffen procedures en richtlijnen voor:

- Afvoer ICT-middelen
- Autorisatieprocedure
- Back-up proces
- Configuratiebeheer
- Functiewijziging
- Gedragscode – ambtenaren gemeente Doetinchem
- Gedragscode - nieuwe medewerkers bewustwording – eerste hulp bij privacy
- Gedragscode - nieuwe medewerkers bewustwording – Gouden regels informatieveiligheid
- Handleiding datalekken
- Incidentmanagement en responsebeleid ICT [10]
- Patchmanagement [11]
- Procedure beveiligingsincidenten
- Procedure gegevensdragers opschonen
- Procedure malware voorzieningen [12]
- Procedure voor toegang tot ruimten
- Recovery proces [13]
- Richtlijn clear desk en clear screen
- Richtlijn wachtwoorden
- Richtlijnen voor mobiele devices en mobiele informatie
- Starterspakket Informatieveiligheidsbeheerders
- Thuiswerken – intranetpagina

---

9 Informatiebeveiligingscoördinatoren en privacycoördinatoren zijn gezamenlijk bekend als informatieveiligheidscoördinatoren, bij het team Informatiemanagement.

10 Beleid om incidenten effectief en efficiënt aan te kunnen pakken, bepalend voor het beperken van schade van beveiligingsincidenten.

11 Patchmanagement gaat om het gecontroleerd en planmatig identificeren van kwetsbaarheden en het testen en uitrollen van patches en updates van software. Een patch is een installatiebestand dat een kwetsbaarheid of fout in een programma herstelt.

12 Malware is de verkorte term voor malicious software (schadelijke software), onder andere virussen en ransomware (software die [delen van] computersystemen gijzelt in ruil voor losgeld).

13 Recovery in het kader van data is het weer beschikbaar stellen of 'terughalen' van verloren data van opslagmedia zoals servers, harde schijven, usb-sticks, sd-cards, tablets en smartphones.

- Uitwijkprocedures [14]
- Wijzigingsbeheer [15]

Gemist

Gemist worden nog protocollen op mobiele datadragers, cryptografie [16], leveranciersmanagement. Wat betreft de mobiele datadragers wordt momenteel niet meer gewerkt met overeenkomsten als medewerkers of bestuurders mobiele devices van de gemeente gebruiken. Uit de interviews blijkt dat dit wel weer wordt opgepakt. Ook wordt een richtlijn voor de logging [17] gemist, zo blijkt uit de GAP-analyse, nodig voor de vaststelling van het informatiebeveiligingsbeleid en -plannen. Op een aantal systemen wordt wel al het dataverkeer gemonitord, omdat dat wordt afgedwongen door de landelijke toezichthouders, zoals op Suwinet. Maar de logging/monitoring is nog niet op alle systemen doorgevoerd. Het streven was om in 2021 een Security Information & Event Management (SIEM), Security Operations Center (SOC) [18] in te richten, om zo te voldoen aan de eisen van de BIO. Dat is niet gelukt vanwege issues bij de landelijke aanbesteding van SIEM/SOC. Daarnaast moeten de loggings die al worden bijgehouden consequent en actief worden gecontroleerd, breder dan een SIEM/SOC dat kan uitvoeren.

Bedrijfscontinuïteitsplan

Er is ook nog geen integraal bedrijfscontinuïteitsplan, met instructies hoe de dienstverlening van de gemeente na een crisis hervat kan worden. De gemeente is er wel mee bezig en verschillende documenten vormen een draaiboek of continuïteitsplan. Eind 2021 is een nieuw onderdeel van het continuïteitsplan in het managementteam vastgesteld, namelijk het opschalingsmodel cybercrisis. Het opschalingsmodel of scenariokaart cybersecurity is naar aanleiding van de hack met ransomware bij Hof van Twente tot stand gekomen. Daarmee worden de lijnen geschetst wie waarvoor verantwoordelijk is, wie wanneer acteert en wanneer en waarheen opgeschaald wordt bij een crisis op het terrein van de ICT. Daarmee is de GRIP-structuur [19] vertaald naar een ICT-crisis. De uiteindelijke verantwoordelijkheid ligt dan bij de burgemeester, zoals in andere crisissituaties. Het opschalingsmodel is vooralsnog alleen gericht op de situatie in Doetinchem en niet op de samenwerking op ICT.

Uit de interviews blijkt dat het de intentie is het integrale plan in 2022 op te stellen, mede op basis van de verschillende deelplannen die er al zijn, en deze in het college te laten vaststellen en uiteindelijk ook te testen.

Middelen

De afweging voor middelen voor ICT en informatiebeveiliging gebeurt mede op basis van de capaciteit die er is. Uit de interviews blijkt dat de gemeente de investeringen doet die volgens de functionarissen op informatie-

14 Uitwijkprocedures regelen het zo snel mogelijk herstel van de dienstverlening na een calamiteit.
15 Wijzigingsbeheer is het planmatig en gecontroleerd uitvoeren van wijzigingen in soft- en hardware in een organisatie.
16 Cryptografie is het versleuteld versturen en delen van informatie die voor derden onleesbaar is.
17 Logging is het in een logbestand vastleggen van alle inzagen, aanpassingen, toevoegingen en verwijderingen, die door medewerkers in een systeem of databestand worden gedaan.
18 Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.
19 De GRIP structuur regelt de opschaling van de hulpverleningsdiensten van de veiligheidsregio bij rampenbestrijding en crisisbeheersing.

beveiliging en privacy nodig zijn. De laatste drie jaren zijn bij elke begroting extra investeringen gevraagd voor middelen en formatie. Daar is de raad van Doetinchem in mee gegaan. Er is nog geen politiek-bestuurlijke agenda voor de langere termijn waarbij op basis van visie en risicobewustzijn, (landelijke) afspraken over kwaliteit van de dienstverlening een raming van de benodigde middelen en formatie mogelijk maakt.

3.2 Overleggen

Intern

Intern tussen portefeuillehouder, teamleider ICTsamenwerking en manager bedrijfsvoering werd 1 keer in de 6 weken en wordt sinds eind 2021 eens in de vier weken overlegd. Daarin worden de technische en financiële aspecten van informatieveiligheid besproken.

De CISO en FG kunnen in principe eigenstandig naar de gemeentesecretaris, portefeuillehouder of burgemeester stappen als er zich een acuut issue voordoet op informatiebeveiliging en privacy. Daarvoor hoeven ze niet eerst langs de manager Informatiemanagement.

Werkgroep informatie-beveiliging

In Doetinchem is in ICTsamenwerking-verband de werkgroep informatiebeveiliging opgezet. Daarin zijn de gemeenten vertegenwoordigd, niet de andere partijen die in ICTsamenwerking deelnemen. De werkgroep geeft adviezen op ICT-gebied die de samenwerking aangaat, op tactisch en operationeel niveau.
Vanuit Doetinchem neemt de informatieveiligheidscoördinator deel aan het overleg.

Overleg gemeente-secretarissen

Naast de werkgroep informatiebeveiliging in ICTsamenwerking is er op ambtelijk niveau de stuurgroep met de secretarissen van de deelnemende gemeenten. De andere deelnemende partijen zijn ook niet hierin vertegenwoordigd. In dat overleg is onder andere plaats voor vragen over de risico's in verband met informatiebeveiliging en privacy. De CISO's van de deelnemende partijen hebben geen overleg.

3.3 Rapportages

Informatieveiligheidsplan

Het jaarlijkse informatieveiligheidsplan wordt opgesteld met activiteiten voor dat jaar, bedoeld om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). In april 2021 is het laatste Informatieveiligheidsplan 2021 vastgesteld. Daarin wordt ook teruggeblikt op wat in het jaar daarvoor van de geplande activiteiten op informatiebeveiliging is uitgevoerd. Het plan wordt ter accordering aan het managementteam voorgelegd. Eind 2021 is afgesproken dat de rapportage van de CISO ook naar de teamleiders gaat, zodat ze daar op teamniveau besproken kunnen worden.

Incidenten

In Topdesk worden incidenten op informatieveiligheid gemeld en bijgehouden. De meldingen van datalekken gaan naar de informatie-veiligheidscoördinatoren. Deze maken elke drie maanden een rapportage van de incidenten en datalekken voor het MT. De rapportage bevat het aantal incidenten, het aantal datalekken dat aan de AP is gerapporteerd,

wat ervan geleerd kan worden
en welke verbetermaatregelen genomen kunnen worden.

ENSIA

Een andere belangrijke rapportage is ENSIA. De informatieveiligheidscoördinator coördineert de informatiestroom voor deze rapportage die bedoeld is voor de verticale verantwoording van de gemeente naar landelijk toezichthouders over de applicaties die de gemeente gebruikt, zoals Suwinet en DigiD. Over de belangrijkste moet het college een in control statement geven, waarover een externe auditor een assuranceverklaring moet afgeven. Deze gaat naar de raad toe, met een rapportage waarin het college aangeeft in hoeverre de BIO-maatregelen zijn geïmplementeerd.

Geen echt ISMS

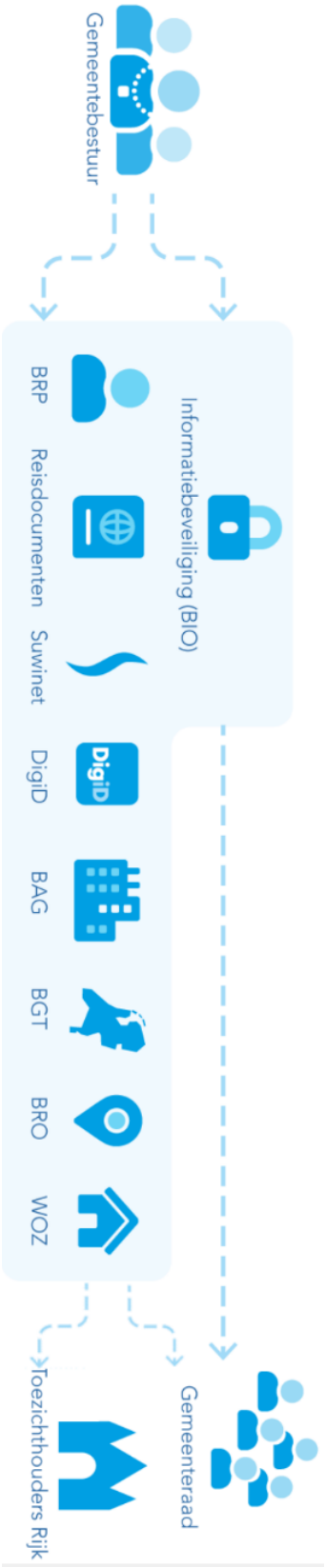
Veel organisaties gebruiken hiervoor een managementtool, een zogenoemd Information Security Management System (ISMS) [20], waar een PDCA-cyclus [21]aan gekoppeld is. Dat is een beleids- of leercyclus waarin activiteiten kunnen worden gepland en bijgehouden.

De gemeente Doetinchem gebruikt geen ISMS. Dat is een van de Geaccepteerde risico's onder het kopje Naleving in de BIO. Doetinchem gebruikt een ander soort applicatie, waar niet alle functionaliteiten van een echt ISMS in aanwezig zijn. Voor 2022 staat de aanschaf van een ISMS op de planning. Daarbij wordt gekeken naar een koppeling met de financiële rechtmatigheidscyclus, met de bedoeling een vergelijkbaar product voor de gehele organisatie te gaan gebruiken.

PDCA-cyclus

De PDCA-cyclus is ingericht op basis van het informatieveiligheidsbeleid. Daarvoor wordt het Informatieveiligheidsplan en de activiteiten die daarin opgenomen zijn gebruikt. In de ENSIA-rapportage wordt de stand van zaken gecontroleerd. En de

Afb. 2 ENSIA-model 2021



[20] ISMS = Information securitymanagement system, is een managementinstrument om de informatiebeveiliging te waarborgen en besturen. Met het instrument kunnen onder andere de veiligheidsrisico's in kaart gebracht worden, beleid en rapportages opgesteld worden en taken en verantwoordelijkheden verdeeld worden.

[21] PDCA = Plan-Do-Check-Act, de beleidsleercyclus.

verbeterpunten die daaruit voortkomen, worden opgenomen in de activiteiten voor het daaropvolgende jaar. Eventueel niet afgeronde activiteiten verhuizen mee naar het volgende jaar.

Accountant

Daarnaast wordt de gemeentelijke top, namelijk raad, college en MT, geïnformeerd over de stand van zaken op informatieveiligheid via de managementletters van de accountants. De laatste jaren voeren deze IT-audits uit als onderdeel van de (interim)controle. Over het algemeen zijn deze audits niet heel uitgebreid, en gericht op de rechtmatigheid van de financiële en administratieve organisatie (zie §5.1 en hoofdstuk 6.)

4 Privacy

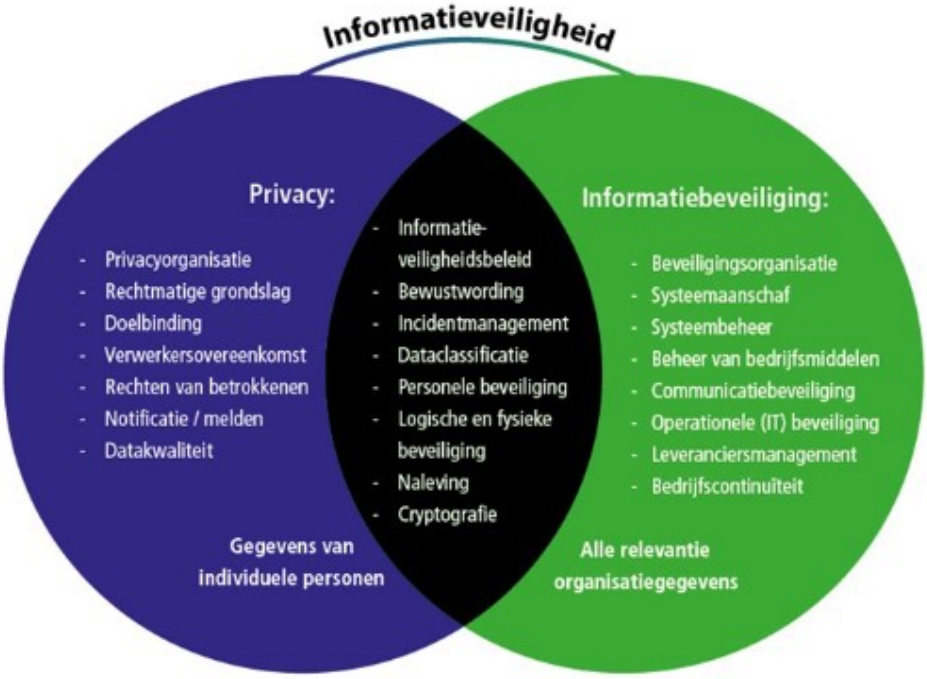
Onderzoeksvraag 2	In dit hoofdstuk beantwoorden we de tweede onderzoeksvraag: *Beschikt de gemeente Doetinchem over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?*

4.1 Beleid

Geen apart beleid

Op privacy/gegevensbescherming is vanaf 2020 geen apart beleid meer geformuleerd. Er is namelijk veel overlap tussen de twee gebieden. En uit de interviews blijkt dat de gemeente het onnodig acht wat al in de Algemene Verordening Gegevensbescherming (AVG) is opgenomen nog een keer in gemeentelijk beleid op te nemen. Informatiebeveiliging en privacy gaan beide om veiligheid, weliswaar met eigen accenten (zie afbeelding 3), en zijn samengevoegd in het Informatieveiligheidsbeleid 2020-2022. Dat beleid verving het Privacybeleid 2017.

Afbeelding 3. Informatieveiligheid met privacy en informatiebeveiliging.



Net als bij informatiebeveiliging zijn de teamleiders uiteindelijk verantwoordelijk voor de uitvoering van het privacybeleid. In het kader van de AVG moet een aantal zaken gerealiseerd zijn. Zoals de functie van de FG die ingevuld moet zijn en aangemeld bij de Autoriteit Persoonsgegevens (AP). Een privacystatement moet gepubliceerd zijn over hoe de gemeente omgaat met persoonsgegevens. Ook moet een procedure zijn opgesteld hoe de rechten van betrokkenen kunnen worden uitgeoefend en een procedure hoe om te gaan met datalekken. En een verwerkingsregister moet zijn opgesteld, waarin alle verwerkingen van persoonsgegevens door

of namens de gemeente zijn opgenomen. Onder contracten die de gemeente sluit met derden, waarin sprake is van verwerking van persoonsgegevens, moet een verwerkersovereenkomst afgesloten worden. Ook moet op een nieuwe verwerking van persoonsgegevens de risico's op privacy zijn beoordeeld. Dat gebeurt met behulp van een data protection impact assessment (dpia). [22]

Functies

Sinds juni 2018 is de FG voor 36 uur in dienst van de gemeente Doetinchem. De FG vervult deze functie voor de gemeente Doetinchem en 7 andere organisaties, in regionaal privacy verband (gemeente Doesburg, Aalten, Oude IJsselstreek, Oost Gelre en Buha, Buurtplein en Laborijn). Die deelnemers participeren niet allemaal in de ICTsamenwerking. Dat betekent dat de FG voor Doetinchem feitelijk 170 uur per jaar beschikbaar is.

De FG is strategisch onafhankelijk als controleur en adviseur gepositioneerd, maar is net als de CISO organisatorisch ondergebracht bij het team Informatiemanagement. Uit de interviews blijkt dat er ooit sprake van was de functies onder te brengen bij de afdeling Control. Dat is niet gerealiseerd.

Privacycoördinator

Naast de FG is op tactisch niveau een privacycoördinator aanwezig. Deze is ook ondergebracht bij het team Informatiemanagement en moet zorgen voor de verbinding van strategisch onderwerpen naar tactisch-operationeel niveau. Deze functionaris vormt op privacy veelal het aanspreekpunt voor medewerkers en lijnmanagement.

Privacybeheerders

Uiteindelijk zijn voor de operationele borging privacybeheerders aangewezen. Dat is een rol die meestal belegd is bij de functioneel applicatiebeheerders.

4.2 Overleggen

Overleg secretaris en portefeuillehouder

In principe heeft de FG als onafhankelijk controleur en adviseur een directe lijn met de secretaris en de portefeuillehouder. Deze wordt niet vaak gebruikt. De secretaris en portefeuillehouder hebben wel regelmatig contact met de informatieveiligheidscoördinatoren. De informatieveiligheidscoördinatoren hebben onderling wekelijks een overleg.

De FG is betrokken bij de overleggen van de werkgroep informatiebeveiliging. Met de relatief nieuwe CISO heeft de FG de afspraak om 1x per maand te overleggen.

Regionale overleggen

Met de privacycoördinatoren van de gemeenten Aalten, Doesburg, Oost Gelre, Oude IJsselstreek en ODA, BUHA en Buurtplein is maandelijks overleg met de FG. De privacycoördinatoren van de gemeenten die in ICTsamenwerking participeren. hebben onderling een overleg. En tot slot is er nog een overleg met de FG'en uit de Achterhoek.

[22] Dpia = data protection impact assessment. Die houdt een analyse in op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG is een dpia verplicht bij gegevensverwerking met een waarschijnlijk hoog privacy risico.

4.3 Rapportages

Jaarlijkse rapportage

De FG stelt jaarlijks een rapportage aan het college op naar aanleiding van de interne toetsing op de AVG. Vanaf 2019 gebeurt dat aan de hand van een toetsingsdocument 'Borging AVG' en interview met de privacycoördinator. In de jaarlijkse rapportage wordt verslag gedaan van de elementen waarop voldaan is aan de AVG, en waarop nog niet of niet helemaal voldaan is. Die elementen bevatten beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking beveiliging en verantwoording. In het toetsingsdocument wordt aangegeven in hoeverre de organisatie voldoet aan de artikelen uit de AVG, met ja/gedeeltelijk/nee/niet van toepassing.

Ook besteedt de FG aandacht aan periodiek wisselende focusgebieden van de Autoriteit Persoonsgegevens (AP). In 2020-2023 wordt door de AP specifiek aandacht besteed aan de focusgebieden datahandel, digitale overheid en artificiële intelligentie en algoritmes.

Incidenten en datalekken

Zoals in §4.3 al is gemeld, krijgt de gemeentesecretaris elke drie maanden een overzicht van de incidenten, opgesteld door de privacycoördinator en informatiebeveiligingscoördinator.

ENSIA en ISMS/PMS

Over privacy wordt ook in het kader van ENSIA aan de raad gerapporteerd. Net als voor informatiebeveiliging is er geen Privacy Management informatiesysteem (PMS). [23] Er wordt wel met de applicatie SafeHarbour/IC Content gewerkt, dat een privacy module bevat. Maar dat wordt niet als een ISMS of PMS gebruikt door de betrokken medewerkers.

[23] PMS = Privacy management systeem, vergelijkbaar met een ISMS voor informatieveiligheid. Het PMS biedt een gestructureerd overzicht van de registers, DPIA's en uitstaande verbeteracties.

5 Uitvoering en monitoring

Onderzoeksvraag 3	In dit hoofdstuk beantwoorden we de derde onderzoeksvraag: *Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?*

Inleiding

In dit hoofdstuk gaan we na hoe het informatiebeveiligings- en privacybeleid wordt uitgevoerd en op welke wijze de gemeente de uitvoering checkt. In eerste instantie benaderen we de onderzoeksvraag op basis van wat er in de rapportages en evaluaties over wordt gemeld. Dat beeld vullen aan met de bevindingen uit interviews. Dat vindt zijn neerslag in §5.1.

We hebben twee onderzoeksmethoden toegepast om het beeld verder in te vullen en de uitvoering van het beleid te testen. De medewerkers van twee teams zijn geïnterviewd op de verwerking van persoonsgegevens. De bedoeling is een beeld te schetsen van de gegevens die het team in- en uitgaan en wat er ondertussen met de informatie gebeurt. Daarvoor zijn het Sociaal Domein en Toezicht en handhaving uitgekozen. Deze komen in de bijlagen 3 en 4 aan bod. Samenvattingen van de cases zijn na §5.1.4 in 2 aparte kaders opgenomen.

Tot slot heeft de rekenkamercommissie door ethische hackers een aantal pentesten laten uitvoeren. Dat zijn een active directory audit, een wifi-netwerk test, een phishingmail en smishing-test. Uitleg over en uitkomsten uit deze testen volgen in §5.2.

5.1 Uitvoering

In deze paragraaf behandelen we achtereenvolgens wat goed gaat op het gebied van informatiebeveiliging en privacy, bewustwording, Algemene Verordening Gegevensbescherming, ICTsamenwerking, het autorisatieproces en contracten met derden.

Wat goed gaat

Respondenten geven aan dat beleidsstukken in opzet en bestaan aanwezig zijn en veel goed gaat zonder dat alles 100% op papier verantwoord wordt. De BIO-normen worden gehanteerd en via de audits kan gecheckt worden in welke mate aan de normen wordt voldaan. Uit de ENSIA over 2019 kwamen geen verbeterpunten. Uit de ENSIA over 2020, met enkele aangescherpte normen, kwamen voornamelijk voor partners van de gemeente verbeterpunten naar voren. Begin 2021 werd voor 82% aan de BIO-normen voldaan. In het Informatieveiligheidsplan 2021 waren 16 activiteiten opgenomen, daarvan waren eind 2021 acht activiteiten uitgevoerd, drie gedeeltelijk of nog in uitvoering en vijf niet uitgevoerd. Als actiepunten voor 2022 zijn onder andere de volgende opgenomen: bewustwording via applicatie; inrichten SIEM/SOC en verbeteringen logging; een nieuw Information Security Management Systeem (ISMS) (zie ook §4.3.)

De aandacht voor informatiebeveiliging en privacy in de ambtelijke organisatie en bij het bestuur neemt toe, zien de geïnterviewden.

Tegelijkertijd wordt gemeld dat dat nog niet op het gewenste niveau is en dat daarop blijvend actie nodig is (zie ook §6.1.1.)

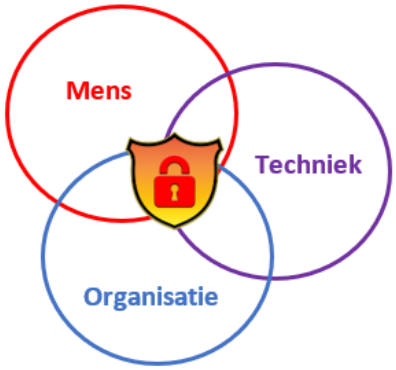
In control

Op basis van de stukken en audits die management en bestuur aangereikt krijgen concluderen respondenten dat de gemeente 'in control' is. In de zin dat 100% in control op informatiebeveiliging niet mogelijk wordt geacht, kwaadwillenden zullen zich blijven ontwikkelen op manieren om schade aan re richten. Maar geïnterviewden geven aan dat de landelijke richtlijnen worden gehanteerd, de risico's in beeld zijn en de benodigde maatregelen worden genomen. De gespecialiseerde kennis is bij het bestuur niet aanwezig om de stukken en audits op de ICT-merites te waarderen. Daarbij moet vertrouwd worden op de kennis en expertise bij de ambtenaren. De in het beleid afgesproken functies zijn aanwezig, zoals de FG, CISO, informatieveiligheids- en privacycoördinator. Respondenten geven aan dat de organisatie alert is op incidenten in de gemeentelijke omgeving. Daarnaast zijn er de landelijke toezichthouders en de IBD die voor acute en permanente dreigingen en risico's waarschuwt. En in gevallen kan de veiligheidsregio de gemeente ondersteunen.

5.1.1 Bewustwording

Meer aandacht

Bewustwording wordt gezien als belangrijk, de menselijke factor in de trits voor informatiebeveiliging en privacy bepalende factoren: techniek-organisatie-mens. Zeker na de gebeurtenissen in de gemeente Hof van Twente. Bewustwording staat vaak bovenaan bij de prioriteiten om op in te zetten en informatieveiligheids- en privacycoördinator geven aan veel aandacht eraan te besteden. Door corona is een aantal fysieke activiteiten hierop vanaf begin 2020 niet door kunnen gaan.



In 2019/2020 is een aanbesteding geweest voor een applicatie voor awareness of bewustwording, samen met de gemeenten waarmee regionaal samengewerkt wordt. De aanbestedingsprocedure mislukte. Op dit moment is er geen applicatie. Daardoor moest de gemeente zelf aan de slag met activiteiten hierop.

Bewustwordingsplan informatieveiligheid 2021

Op bewustwording is voor 2021 een activiteitenplan opgesteld, met de onderstaande uitgangspunten:

1. Aansluiten bij landelijke acties (28-1 Dag van de Privacy, Oktober maand van Cybersecurity, November Integriteitsmaand)
2. Jaarlijks minimaal één speciale bewustwordingsactie organisatiebreed organiseren
3. Via intranet, e-mail en werkoverleggen medewerkers, leidinggevenden en bestuurders informeren over actuele onderwerpen binnen informatieveiligheid
4. Onderdeel van functioneringsgesprek

5. Planning bewustwording december 2020 en heel 2021

   In onderstaand overzicht zijn de activiteiten opgenomen, zoals een phishing mail activiteit, elke drie maanden bijeenkomsten voor nieuwe medewerkers, teams- en opleidingssessies enz. Er zijn cursussen en trainingen, die niet verplicht zijn voor de al langer in dienst zijnde medewerkers. Het zijn met name de privacy- en informatieveiligheidscoördinator die activiteiten oppakken met de teams. De activiteiten worden met de CISO en FG afgestemd.

Tabel 2. Omschrijving bewustwordingsactiviteiten dec 2020-2021, gemeente Doetinchem.

Omschrijving	dec	jan	feb	mrt	apr	mei	juni	juli	aug	sept	okt	nov	dec
Phishing e-mail actie	x												
Starterspakket applicatiebeheerders delen	x												
Intranetbericht Dag van de privacy		x											
Nieuwe medewerkers bijeenkomsten	x			x			x			x			x
Rapportages datalekken en beveiligingsincidenten		x			x			x			x		
Teams en opleidingssessies applicatiebeheerders starterspakket					x	x					x	x	
Themakaarten sessie college en raad					x	x							
Themakaarten sessies per team					x	x	x	x	x	x	x	x	x
Uitrol beveiligd mailen binnen gehele organisatie				x	x	x							
Functioneringsgesprekken						x	x	x	x	x			
Maand van de cybersecurity											x		
Actualiseren dataclassificatie en DPIA's			x	x	x	x	x	x	x	x	x		

Aandacht bij management en bestuur

Hiervoor is geconstateerd dat in de organisatie meer en meer aandacht is voor de onderwerpen informatiebeveiliging en privacy. De bewustwordingssessie voor de teams met themakaarten is ook met het MT en de collegeleden gedaan, waarna een gesprek daarover vanuit een niet-technische invalshoek kan plaatsvinden. Voorbeelden van incidenten brengen het onderwerp heel dicht bij de aanwezigen. Aangegeven wordt dat informatiebeveiliging en privacy als onderwerpen vaak op de agenda van het managementteam staan. ENSIA en plan van aanpak met verbetermaatregelen worden met de ambtenaren en met het managementteam doorgesproken. Daarna wordt het, zonder al te veel vragen, door het college vastgesteld.

Draagvlak voor informatiebeveiliging en privacy bij bestuur is groeiende, blijkt uit de interviews. Het onderwerp komt niet structureel bij het college langs, bijvoorbeeld geen halfjaarlijkse sessie over informatiebeveiliging. Het college bespreekt de jaarlijkse rapportages van de CISO en FG en de jaarlijkse ENSIA-rapportage. De nodige investeringen worden gedaan. Niet

zonder discussie, daar uit de interviews blijkt dat het college kritisch is over extra middelen voor ICT. Aangegeven wordt dat ICT geen populair onderwerp is om publiek geld aan uit te geven. Toch is er bijvoorbeeld geld voor de CISO-functie vrijgemaakt na de pensionering van het MT-lid die die rol vervulde. De portefeuillehouder bedrijfsvoering en de burgemeester zijn op het onderwerp betrokken, meer dan de andere collegeleden. Geen van de collegeleden is inhoudelijk deskundig op informatiebeveiliging of ICT, maar geven aan voldoende meegenomen te zijn in het besluitstuk dat in het college wordt behandeld.

Draagvlak bij alle geledingen

Het draagvlak voor informatiebeveiliging is aanwezig en groeit bij alle geledingen, volgens de respondenten. Zo kon eind 2021 de maatregel om in verband met het Log4J (zie §6.1.3) de dienstverlening stop te zetten op begrip van medewerkers rekenen. Uit de interviews blijkt dat er sinds de organisatieontwikkeling minder lagen in de organisatie zijn, waardoor alle geledingen directer betrokken zijn op informatiebeveiliging en privacy.

Uit de AVG-toetsingen, ten behoeve van de jaarlijkse rapportgage van de FG, blijkt dat de aandacht voor privacy weliswaar toeneemt, maar langzaam en dat er nog groepen medewerkers zijn die moeilijk te bereiken zijn voor verbetermaatregelen. Elkaar onderling aanspreken op gedrag gebeurt weinig. Geconstateerd wordt door respondenten dat uitvoering van beleid niet geheel doorleefd is en dat het vastleggen van activiteiten voor de verantwoording weinig wordt gedaan (zie ook kopje 'Accountant' in hoofdstuk 7.) Er moeten nog forse stappen gezet worden, met name op bewustwording.

Kennisniveau

Een van de aandachtsgebieden van de bewustwordingsactiviteiten is het kennisniveau op het gebied van informatiebeveiliging en privacy in de organisatie. Respondenten geven aan dat dat met name op informatiebeveiliging lastiger is dan op privacy. Uit de interviews blijkt dat een basisniveau niet overal aanwezig is in de organisatie en dat risicobewustzijn en gevoel voor techniek breder kan. De aandacht ging vooral uit naar de belangrijkste applicaties, zoals de financiële applicaties en de applicaties die door de landelijke toezichthouders worden gemonitord. Voor de gehele organisatie is daar nog geen ambitieniveau op vastgelegd. Gedacht wordt dat het kennisniveau het best dicht bij de uitvoering op peil gebracht moet worden, zoals bij de informatieveiligheids-beheerders. Voor hun ondersteuning is een starterpakket met aandacht voor BIO-maatregelen en sjablonen die zij in hun werk kunnen toepassen.

Volwassenheid

De Nederlandse Beroepsorganisatie van Accountants (NBA) heeft een model gemaakt om de volwassenheid op informatieveiligheid van organisaties te meten, zie bijlage 7. Deze wordt toegepast door NOREA, de beroepsorganisatie van IT-auditors in Nederland. Een meting op basis van dat model is niet door accountants of in het kader van dit rekenkamer-onderzoek uitgevoerd. De volwassenheid van de organisatie wordt door respondenten wisselend ingeschat. Op DigiD en Suwinet lijkt die op een hoog niveau aanwezig te zijn en wordt bijvoorbeeld de vastlegging en controle van activiteiten door de landelijke toezichthouders afgedwongen.

Daarmee kan namelijk aangetoond worden wat gedaan is en wat er mogelijk mis is gegaan, zodat geleerd kan worden.[24] Op de andere applicaties is dat minder geval. De cultuur is volgens respondenten erop gericht om zaken te doen, dingen te regelen zonder alles op papier op orde te hebben.

Accountant

In de interimcontrole over 2020 komt de accountant tot eenzelfde conclusie. De accountant merkt op dat binnen de automatiseringsomgeving weliswaar controles plaatsvinden, maar dat deze veelal niet reproduceerbaar en gestructureerd worden uitgevoerd. Het advies hierop is de aanwezige controles gestructureerd uit te laten voeren en te laten documenteren.

5.1.2 AVG

Privacybeleid 2017

Vanaf 2017, met een zelfstandig privacybeleid, is vooral hard gewerkt om de gemeentelijke organisatie op privacyaspecten en richtlijnen in te richten, volgens respondenten. Veel aandacht is ernaar uitgegaan om in de organisatie met de medewerkers aan de slag te gaan. Daarbij lopen een aantal zaken goed, zoals de melding van datalekken. Daarvoor is een procedure opgesteld (zie §5.1) en het aantal gemelde datalekken neemt toe. Dat wordt over het algemeen opgevat als een goed teken, want het is een signaal dat het bewustzijn toeneemt van wat bijvoorbeeld een datalek is en de bereidheid om er op de juiste manier melding van te maken.

Toetsing AVG

De FG rapporteert jaarlijks aan het managementteam en college over de voortgang op de AVG-maatregelen. De raad krijgt hierop op hoofdlijnen gerapporteerd, met een samenvatting door het college en een infographic (zie §5.3 en hoofdstuk 7). De FG rapporteert over 2020 op 133 punten dat deze gerealiseerd zijn, 33 gedeeltelijk, 13 niet en 12 zijn niet van toepassing of worden op een andere wijze gemonitord. De aandachtsgebieden die de FG voor 2021 aanwijst zijn samenwerking (waaronder inzicht in samenwerking en vastleggen van afspraken), processen (met verwerkingsregister en data protection impact assessments [dpia's]) en inbedding in de organisatie (waaronder doorlopende aandacht voor bewustwording.)

Dpia's

Het aantal dpia's dat op kritieke processen en applicaties wordt uitgevoerd waarin persoonsgegevens worden verwerkt, neemt toe. In interviews wordt aangegeven dat een incident zoals Hof van Twente helpt in de aandacht daarvoor, waar de coördinatoren op kunnen aanhaken. De lijn is als proceseigenaar aan zet om een dpia of risicoanalyse uit te voeren. Uit de interviews blijkt dat dpia's worden uitgevoerd, maar dat het proces niet vlekkeloos verloopt. Op operationeel niveau moet door de privacycoördinator nog veel ondersteuning geboden worden.

Checklist pre-dpia

Bij een nieuw informatiesysteem of een gewijzigde werkwijze wordt een van de drie informatieadviseurs van het team informatiemanagement betrokken. De gegevens kunnen anders door de organisatie lopen of andere

[24] Uit de ambtelijke reactie blijkt dat op privacy een toets heeft plaatsgevonden, waarbij het volwassenheidsniveau is inzichtelijk is gemaakt. Die toetsing was nog niet bij de rekenkamer bekend gedurende de onderzoeksfase.

gegevens zijn nodig. Zij voeren een pre-dpia uit, met de zogenoemde Integrale Risico- en Privacy-analyse (IRPA) tool. [25] Aan de hand van een checklist/aandachtspunten checken zij, in overleg met de privacy-coördinator, of een dpia nodig is.

Hieronder is een lijst van de onderwerpen/thema's/applicatie waarop de gemeente Doetinchem vanaf het begin van de AVG in 2018 tot en met januari 2022 een dpia of een pre-dpia op is uitgevoerd:

1. JVS
2. Motion
3. Cocoon
4. AFAS
5. Omgevingswet website
6. Schulddienstverlening
7. Vroegsignalering
8. Tabula
9. WGGZ
10. Zivver
11. AV systeem raad
12. Motion—BW oost
13. Regionale Samenwerking Leerplicht
14. SVH Allegro

ICTsamenwerking

Bij ICTsamenwerking zijn ook dpia's opgestart, zoals op Microsoft365, Intune en een SIEM/SOC-applicatie. Deze zijn nog niet geheel afgerond.

Nieuwe wetgeving

De verwachting is dat er nog veel nieuwe dpia's uitgevoerd moeten worden, daar veel nieuwe wetgeving op stapel staat waarbij gemeentelijke processen herzien moeten worden.

Vastleggen

Uit de interviews blijkt dat de richtlijnen en protocollen op de AVG aanwezig zijn en dat het bewustzijn om ermee om te gaan is gegroeid, maar dat deze nog niet overal goed nageleefd worden. De administratieve vastlegging van activiteiten en verbeteracties kan beter. Dat is cruciaal voor de bewijslast als er een datalek is. Zoals aangegeven, is het volwassenheidsniveau niet gemeten, maar dat lijkt op de NOREA-schaal van 5 tegen de twee te scoren (zie bijlage 7). Groeiend bewustzijn is geconstateerd en medewerkers komen met vragen bij de FG of de privacycoördinator of een verwerkingswijze al dan niet van de AVG mag.

Derden

De inkoop en contracten met leveranciers verloopt via de inkoop-medewerkers. De aanbesteding wordt vanuit die afdeling uitgevoerd of begeleid. De medewerkers werken met een checklist waarin privacy een rol heeft. Gecheckt wordt of persoonsgegevens worden verwerkt en er bij het afsluiten van contracten een verwerkersovereenkomst afgesloten moet worden. Ook wordt gecheckt of een applicatie inpasbaar is in de ICT-omgeving en of een dpia nodig is.

[25] De Integrale risico- en privacy-analyse (IRPA) is een instrument van de Informatiebeveiligingsdienst (IBD) voor een integrale GAP- en risicoanalyse op informatiebeveiliging en privacy.

Positionering FG

Uit de interviews komt de indruk dat de functie van de FG beter strategisch ingebed moet worden richting gemeentesecretaris, portefeuillehouder en burgemeester. De meeste contacten hebben zij met de privacycoördinator, en krijgen via dat kanaal de meeste informatie, zoals over datalekken en dergelijke. De FG is weliswaar aangesteld bij de gemeente Doetinchem, maar is 'slechts' voor 170 uur voor de gemeente beschikbaar. Privacy als aspect wordt niet of vaak te laat betrokken bij strategische keuzen. Dan wordt het moeizamer privacyaspecten in het proces mee te nemen.

De doorleving op privacy bij medewerkers kan nog verbeteren, zoals hierboven opgemerkt. Privacy wordt nog vaak als lastig en belemmerend ervaren en medewerkers zijn al druk met hun reguliere werkzaamheden.

5.1.3 ICTsamenwerking

ICTsamenwerking

Doetinchem werkt op ICT samen met de gemeenten Bronckhorst, Aalten, Oude IJsselstreek en Doesburg en de regionale instellingen Laborijn, Regio Achterhoek, Streekarchief, BuHa en de ODA. Daartoe is uit efficiency-overwegingen besloten in 2015. In 2018 is de samenwerking herbevestigd. Het samenwerkingsverband heeft een lichte structuur, met Doetinchem als gastheer. Onder de samenwerking liggen geen uitgebreide dienst-verleningsovereenkomsten.

Overleg ICTsamenwerking

Met betrekking tot de samenwerking is geen regulier bestuurlijk overleg geregeld. De secretarissen van de deelnemende gemeenten hebben mini-maal 2x per jaar overleg, over governance en ICT. Daarin zijn de andere partners in ICTsamenwerking niet vertegenwoordigd. Ambtelijk is er de werkgroep informatiebeveiliging, dat over de afstemming op automatisering gaat en het delen van elkaars kennis. Daarin werd onder andere gezamenlijk geacteerd op het Log4J veiligheidslek dat in december 2021 werd geconstateerd (zie hierna). Er wordt over nagedacht om in de toekomst de niet-gemeenten bij de overleggen te betrekken.

Werkgroep informatiebeveiliging

De werkgroep informatiebeveiliging geeft adviezen, kan bij crises acteren en wordt waardevol ervaren om onderling kennis te delen. Uit de interviews blijkt dat er soms nog gezocht wordt naar het juiste niveau waarop de onderwerpen in de werkgroep geadresseerd worden. Strategisch, tactisch en operationeel kan het door elkaar heen lopen en sommige deelnemers combineren de functie op informatieveiligheid met taken op privacy.

Crisis: Log4J

Vlak voor kerst 2021 kwam de melding vanuit de IBD over de zogenoemde Log4J-dreiging. Er is toen een app-groep opgezet, zodat alle betrokkenen in ICTsamenwerking snel met elkaar konden communiceren. In Doetinchem is een actieteam opgezet, met daarin de manager dienstverlening, teamleider ICTsamenwerking, CISO, FG, en interne en externe communicatie. Het Gemeentelijk Beleidsteam (GBT) is daarbij steeds geïnformeerd over de stappen. Over Log4J is geschakeld met burgemeesters, portefeuillehouders en secretarissen van de deelnemers in de samenwerking. De medewerkers in de samenwerking hebben tijdens de kerstperiode van 2021 24-uurs-

diensten gedraaid. Uit de interviews blijkt de mening dat de gemeente Doetinchem zijn verantwoordelijkheid heeft gepakt op dit gebied, in samenspraak met de deelnemers in ICTsamenwerking.

Mede naar aanleiding van de crisis bij Hof van Twente heeft Doetinchem recent een opschalingsmodel opgesteld voor dit soort crises, als onderdeel van een nog vast te stellen integraal bedrijfscontinuïteitsplan (zie ook §4.1). Dat model geldt alleen voor Doetinchem. Het Doetinchemse model is gedeeld met de op ICT samenwerkende partijen, maar zij moeten daar zelf actie op ondernemen.

ICT

Doetinchem is verantwoordelijk voor de continue en veilige werking van de ICT. Hiervoor tracht de gemeente in het kader van het Informatie-beveiligingsbeleid 2020-2022 te voldoen aan de BIO- en AVG-richtlijnen. Daarvoor is in 2020 een GAP-analyse uitgevoerd waaruit onder andere bleek dat de gemeente op 29 BIO-maatregelen gedeeltelijk en op 7 nog niet scoorde. Daarop wordt op basis van een risicoafweging prioriteiten gesteld en zijn heeft de gemeente 18 risico's geaccepteerd.

Uitwijk- en pentesten ICTsamenwerking

In ICTsamenwerking wordt de beveiliging van de systemen periodiek getest met behulp van pentesten op de technische systemen. Er is er een uitwijkplan dat jaarlijks getest wordt als een calamiteit zich voordoet en de dienstverlening van kritieke systemen uitvalt en binnen een zekere tijd weer opgestart moet worden. Er is segmentatie op de systemen zodat kwaadwillenden niet overal bij kunnen komen als het eenmaal lukt binnen te komen. De inrichting van een SIEM/SOC en ISMS staan voor 2022 op de planning. Om aan de BIO-eisen te voldoen, voert de gemeente pentesten uit op de systemen. De meest recente interne en externe netwerk pentest zijn in maart 2021 gehouden, zie ook §6.4.

Governance

In interviews wordt eraan getwijfeld of de inrichting van het samen-werkingsverband op ICT tussen gemeenten en andere partijen toekomst-bestendig is. De incidenten nemen toe en navenant de risico's die gemeenten en andere partners lopen. De deelnemers zijn nu nog zelf verantwoordelijk voor opzet, bestaan en werking van het informatie-beveiligings- en privacybeleid in de eigen organisatie. Vanuit ICTsamenwerking wordt momenteel hierop niets tot weinig afgedwongen en geen harmonisering geëist.

In het service level agreement dat in 2018 is afgesloten, wordt heel kort de aansprakelijkheid van de gastheer geadresseerd. Er is weliswaar netwerk-segmentatie op de systemen aangebracht, maar de vraag is of de systemen voldoende afgeschermd zijn als bij de ene partner problemen ontstaan. Kan de gemeente Doetinchem aansprakelijk gesteld worden als leverancier van ondeugdelijke dienstverlening, of kan de ene partner een andere aansprakelijk stellen als deze last ondervindt van diens problemen? Kortom, er is geen sprake van een duidelijke klant-leverancier-relatie in ICTsamenwerking. Bij dit vraagstuk gaat het om een forse formatie en navenante financieel belang. Bestuurlijk worden de risico's op governance erkend maar nog niet geadresseerd.

5.1.4 Autorisatie

Autorisaties

Een van de meest cruciale aspecten op informatiebeveiliging en privacy is het autorisatiebeleid. Bij autorisaties gaat het om het verlenen van toegangsrechten tot informatie die de gemeente verwerkt, meestal in diverse applicaties. Een van de uitgangspunten is dat niemand mag beschikken over autorisaties tot handelingen die het gehele informatiesysteem kunnen beheersen. En er moet sprake zijn van functiescheiding tussen beheer- en andere gebruikstaken. De gemeente heeft daar procedures voor. Voor de ENSIA-applicaties als Suwinet en DigID worden die aan degelijke audits onderwerpen door de landelijke auditoren.

Casus Sociaal domein (voor de volledige beschrijving zie bijlage 3)

Gesproken is met verschillende functionarissen uit het team Sociaal Domein (zie bijlage 1)

Voor deze casus is ingezoomd op de omgang van persoonsgegevens bij de uitvoering van de maatregelen in het kader van financiële ondersteuning van inwoners van de gemeente. Het team was al van oudsher gewend zorgvuldig met persoonsgegevens om te gaan en in verband met de AVG is een aantal procedures aangescherpt. De aandacht voor en bewustwording op informatie-beveiliging en privacy zijn daarmee toegenomen, mede in de teamoverleggen.

Op de meeste processen in het sociaal domein zijn (pre-)dpia's gehouden. Bij nieuwe processen en activiteiten met persoonsgegevens worden de privacyofficer en informatieveiligheidscoördinator betrokken.

Verwerking van de gegevens en opvragen bij andere instanties wordt gedaan op basis van vooraf gegeven toestemming van de klant. Enige hinder van de AVG wordt ervaren in de preventiesfeer door drempels bij het delen van gegevens met andere instanties. Dat is deels ondervangen doordat de gemeente zelf alle minimaregelingen uitvoert. Door de Wet gemeentelijke schuldhulpverlening (Wgs) is de vroegsignalering van schulden al verbeterd. En er ligt een wetsvoorstel om onderling delen van gegevens tussen samenwerkingsverbanden te vergemakkelijken.

Via verschillende kanalen kan een inwoner in aanmerking komen voor een financiële regeling. Via een keukentafelgesprek met een consulent, buurtcoaches of zelf melden. Dan vindt er een intake plaats op het stadhuis en wordt een plan van aanpak opgesteld en in het zaaksysteem Onegov opgeslagen. Voor schuldhulpverlening wordt een andere applicatie in gebruik genomen. Daarin wordt de problematiek geschetst en eventueel relevante bijzondere persoonsgegevens opgenomen. De lopende dossiers zijn op papier, de rest is digitaal. De autorisaties voor toegang van medewerkers tot de gegevens in de applicaties wordt regulier opgehangen aan profielen (zie ook§5.1.4).

Aparte regelingen zijn de bijzondere bijstand en het Meedoenarrangement. Een verkorte aanvraag voor de bijzondere bijstand is er voor de inwoners die al bekend zijn via een uitkering in het kader van Participatiewet. Als de financiële gegevens niet bekend zijn, volgt een draagkrachtberekening die via Suites sociaal domein in het zaaksysteem Onegov wordt geregistreerd. Voor de maatschappelijke participatie komen gezinnen met lage inkomens in aanmerking. De aanvraag daarvoor verloopt via een website die daarvoor is opgezet, die een koppeling legt met Onegov. De aanvragers vullen de NAW-gegevens aan met inkomensgegevens.

Controle op de dossiers vindt plaats door de kwaliteitsmedewerker. Externe audits worden uitgevoerd door de brancheorganisatie van financiële hulpverleners (NVVK), de rechtbank en de accountant. Gedeeld worden gegevens met de rechtbank, in het kader van bewindvoering, en met de Stichting Kredietbank Nederland, in het kader van een schuldhulpverleningstraject. Geaggregeerde gegevens worden gedeeld met CBS voor statistische doeleinden.

Casus Handhaving (voor de volledige beschrijving zie bijlage 4)

Gesproken is met verschillende functionarissen uit het team Toezicht en handhaving (zie bijlage 1.)

De AVG heeft volgens de respondenten geen ingrijpende gevolgen gehad voor de werkwijzen bij toezicht en handhaving. Wel heeft de AVG gezorgd voor meer bewustwording bij de medewerkers bij het zorgvuldig omgaan met persoonsgegevens. De Wpg, de AVG voor de verwerking van politiegegevens, heeft sinds 2020 invloed. De verplichte audit bij de gemeente is nog niet verricht voor de gemeente Doetinchem.

Net als bij het sociaal domein wordt het zaaksysteem Onegov gebruikt, zie het kader op de vorige pagina. Voor de meeste vergunningen worden applicaties van Centric gebruikt, op Squit XO na dat voor bouwvergunningen wordt gebruikt. Er wordt zo min mogelijk op basis van persoonsgegevens geregistreerd. De autorisaties voor toegang tot de applicaties en de gegevens gaat regulier aan de hand van profielen van medewerkers, zie §5.1.4.

Van de aanvragen in het kader van de Horeca- en drankwet worden alleen locatiegegevens geregistreerd binnen een afgeschermd deel van Onegov. Bij de publicatie van de vergunningen worden alleen locatiegegevens gebruikt.

Gegevens worden gedeeld met de politie, maar de politie is zelf terughoudend in delen van gegevens. Via een speciaal beveiligde applicatie, CityControl, kunnen Boa's politiegegevens inzien. Boa's slaan er zelf geen persoonsgegevens in op. Met de GGD worden handhavingsrapporten op de kinderopvang grotendeels gepseudonimiseerd in een aparte digitale inspectieruimte gedeeld. Voorts worden gegevens beveiligd uitgewisseld via het omgevingsloket met de Omgevingsdienst Achterhoek (ODA) en de Veiligheidsregio Noord- en Oost-Gelderland.

Voor het veilig uitwisselen van gegevens kan Zivver gebruikt worden, alleen geven respondenten aan niet allemaal de beschikking daarover te hebben. Aangegeven wordt dat nagedacht wordt om Zivver standaard in het mailprogramma op te nemen.

Bij toezicht en handhaving zijn nog geen dataprotection assessments uitgevoerd. Wel zijn er vanuit het team gesprekken met de privacyofficer en informatieveiligheidscoördinator over op te pakken dpia's en met derden af te sluiten verwerkersovereenkomsten. In de teamoverleggen komen de onderwerpen wel aan bod. Een enkele medewerker vindt dat er meer en meer passende ondersteuning geboden kan worden bij het zorgvuldig omgaan met de eisen op het gebied van informatiebeveiliging en privacy.

Rol/functie

Op basis van de rol/functie krijgt een medewerker toegangsrechten tot een applicatie en de informatie die daarin wordt verwerkt. Het autorisatiebeleid ziet er op toe dat medewerkers niet bij gegevens kunnen komen die zij niet voor hun functie of rol nodig hebben. De bevoegdheidsprofielen waarin is opgenomen welke rollen/functies toegang krijgen tot welke applicaties en informatie zijn vastgesteld in een autorisatietabel of mandatenlijst. De autorisaties worden beheerd door de applicatiebeheerders binnen het team systeembeheer. Naar aanleiding van een melding van de leidinggevende met behulp van een autorisatieformulier, wordt een account aangemaakt en worden rechten toegekend. Ontslag of functiewisseling van de medewerker dient de leidinggevende meteen aan de applicatiebeheerder door te geven; dat signaal kan ook vanuit team HR komen. Uit de interviews blijkt dat wisseling van functie relatief weinig voorkomt. En wanneer wel wordt een account opgeheven en komt een nieuw account daarvoor in de plaats op basis van een nieuw functieprofiel.

Controle

De applicatiebeheerder stuurt elk halfjaar een overzicht van de autorisaties voor een controle aan de betreffende leidinggevende. Deze geeft eventuele nog niet doorgevoerde aanpassingen door aan de applicatiebeheerder. Voor de autorisatietabellen op de BRP is een separaat traject in het beleid opgenomen. Omdat de Rijksdienst voor Identiteitsgegevens (RvIG) toezicht houdt op de autorisatietabellen en daarop halfjaarlijks de leidinggevende, via de privacybeheerder op de BRP, de autorisaties laat controleren.

Elke wijziging wordt door systeembeheer in Topdesk, de incidenten-applicatie, bijgehouden. De accounts worden in de Active Directory (AD) opgenomen. De actuele status van de AD hangt in principe af van de bereidwilligheid van leidinggevenden mutaties door te geven. Uit interviews blijkt niet dat daar garanties op worden gegeven, met name bij functiewijzigingen. Er blijken weinig functiewisselingen te zijn en wat de meldingsbereidheid stimuleert, is dat elk account in rekening wordt gebracht. Een check op de Active Directory kan ook daarbij helpen (zie §6.4.)

Accountant

In het kader van de interim controle over 2021 heeft de accountant zich onder andere gericht op toegangsbeveiliging en wijzigingsbeheer. De accountant merkt in de boardletter van 28 januari 2022 op dat op de authenticatie en autorisatie, alsook het wijzigingsbeheer, verbeteringen noodzakelijk zijn. Gelet op de risico's, maar ook het faciliteren van de bedrijfsvoering, adviseert de accountant het college aan de bevindingen uit de interim-controle voorrang te geven.

5.2 Pentesten

Inleiding

Zoals eerder aangegeven, zijn in het kader van het rekenkameronderzoek pentesten uitgevoerd, door ethische hackers. Uitgevoerd zijn een wifi-netwerk pentest, een Active directory audit, een phishing- en smishing mail aanval, zie hierna voor de resultaten. In eerste instantie was de rekenkamercommissie van plan ook een interne en externe netwerk pentest en mystery guest test uit te laten voeren. ICTsamenwerking heeft

maart 2021 een externe en interne netwerk pentest laten uitvoeren op het gezamenlijke netwerk. ICTsamenwerking gaf aan met de verbeteracties naar aanleiding van deze pentesten aan de slag te zijn. De ethische hackers die de rekenkamercommissie heeft ingehuurd, hebben de testrapportages bekeken. Zij hebben geadviseerd dat het niet efficiënt zou zijn om die testen in het kader van het rekenkameronderzoek uit te voeren, daar ze allicht dezelfde bevindingen zouden opleveren. Ook is afgezien van een mystery guest test, vanwege de thuiswerkadviezen in verband met de coronapandemie gedurende de looptijd van het onderzoek. Als er weinig tot geen medewerkers op kantoor zijn, heeft een dergelijke test geen meerwaarde.

Afgesproken is dat kritieke risico's meteen gemeld zouden worden aan de CISO en gemeentesecretaris. Dat is niet aan de orde geweest. Bij de ambtelijke hoor en wederhoorfase worden de rapporten van de pentesten aan de gemeentesecretaris overhandigd, zodat de gemeente op de geconstateerde risico's verbetermaatregelen kan treffen. Gelet op de gevoelige inhoud van de rapporten worden deze niet breed verspreid.

Hieronder gaan we nader in op de bij de pentesten gesignaleerde risico's.

Wifi-netwerk pentest

Op 8-11-2021 is een wifi-penetratietest bij de gemeente Doetinchem uitgevoerd. Deze test is bedoeld om de beveiliging van de draadloze netwerken te toetsen en mogelijke kwetsbaarheden in kaart te brengen. Gesimuleerd wordt of een kwaadwillende baat kan hebben bij een aanvalsscenario op het draadloze netwerk van de gemeente. De effectiviteit van de genomen beveiligingsmaatregelen wordt daarmee geverifieerd.

De mogelijkheid tot toegang verkrijgen tot het beveiligde draadloze netwerk heeft een hoge impact, en dat doel is gedeeltelijk behaald in de test. Er zijn twee aandachtspunten gesignaleerd, een is een ongeautoriseerde toegang tot een draadloos netwerk die geen directe toegang tot het interne netwerk zou kunnen verschaffen, en twee is de mogelijkheid dat bezoekers op het gastnetwerk elkaars computer of telefoon kunnen zien.

Op basis van de uitgevoerde pentest wordt het risico op laag ingeschat. Wel zijn op basis van de aandachtspunten verbetermaatregelen aanbevolen in het rapport over de wifi-pentest.

AD audit

De Active Directory (AD) audit is op 8-11-2021 uitgevoerd. Een AD staat beheerders toe om het beleid met betrekking tot rechten van medewerkers en instellingen in het netwerk van een organisatie te beheren. De AD audit is dan ook in samenwerking met IT-beheer van de gemeente Doetinchem uitgevoerd. ICTsamenwerking beheert de AD van alle partners in de samenwerking, maar deze audit beperkt zich tot 689 accounts van de gemeente Doetinchem, en 624 met andere deelnemers in ICTsamenwerking gedeelde accounts. Dat zijn beheerderaccounts en enkele algemene serviceaccounts. Niet alle serviceaccounts zijn in gebruik bij de gemeente Doetinchem, maar konden voor de test niet uitgefilterd worden.

De AD audit checkt op zwakke en gekraakte wachtwoorden. Zwakke wachtwoorden worden gecheckt op complexiteitsgraad, gekraakte wachtwoorden worden vergeleken met een lijst op internet met wachtwoorden die in relatie gebracht kunnen worden met de gemeente.

Er zijn kwetsbaarheden gevonden die voornamelijk voort lijken te komen uit het niet consequent toepassen van het wachtwoordbeleid.

Relatief los van wat in de AD audit is getest, is geconstateerd dat de mailadresbestanden van de deelnemers in ICTsamenwerking door alle partners in de samenwerking worden gedeeld. Daarmee is het makkelijker en sneller mailadressen van medewerkers binnen het samenwerkingsverband in de adresbalk op te geven. Het risico snel een verkeerd adres op te geven, neemt evenwel ook toe. De Autoriteit Persoonsgegevens gaf in het jaarverslag over 2021 aan dat het bij het grootste deel van de datalekken gaat om verkeerd geadresseerde brieven en e-mails.

Phishingmail

Kwaadwillenden proberen vaak via e-mails mensen naar een valse website te lokken, om inlog- of andere gegevens buit te maken. Ook kunnen daarmee ransomware of virussen geïnstalleerd worden, of datalekken ontstaan. Om de alertheid en bewustzijn van medewerkers van de gemeente Doetinchem op dat soort e-mails te testen is op 24-11-2021 een phishing mail uitgezet. De e-mail is door Awaretrain verstuurd vanaf een extern mailadres en bevatte een uitnodiging voor een werkoverleg. Als een medewerker op een van de links klikte, kwam deze op een landingspagina waarop gemeld werd dat dit onderdeel was van een test in opdracht van de rekenkamercommissie. En werd uitleg gegeven over phishing mails en hoe deze te herkennen.

Smishing

Criminelen proberen tegenwoordig steeds vaker via sms op een smartphone aan persoonsgegevens te komen of malware te installeren. De rekenkamercommissie heeft op 7-12-2021 door Awaretrain een smishing aanval op de zakelijke 06-nummers van medewerkers van de gemeente laten uitvoeren. De sms werd door Awaretrain verstuurd en bevatte een nep 'bank alert' over een verdachte incasso. De medewerkers werd gevraagd op een link te klikken om het bedrag te storneren. Als een medewerker daarop klikte, kwam deze, net als bij de phishing mail op een landingspagina waarop gemeld werd dat dit onderdeel was van een test in opdracht van de rekenkamercommissie. En werd uitleg gegeven over smishing en hoe deze te herkennen.

Techniek en thuiswerken

Thuiswerken speelt een rol bij de resultaten van de tests op phishing en smishing. Medewerkers zien elkaar niet bij het koffiezetapparaat of lunchtafel om elkaar te waarschuwen. Daarnaast speelt techniek ook een rol bij een aanval met phishingmails. Over het algemeen bereiken veel phishing mails de geadresseerden niet omdat ze worden afgevangen door zwarte lijsten die mailservers van afzenders bijhouden. Om de test mogelijk te maken, wordt van tevoren het verzendadres en domein 'gewhitelist', zodat de mailservers de testmail niet tegenhouden. Ondanks de whitelisting kwam de phishing mail maar moeizaam door, maar uiteindelijk lukte het

alle geadresseerden te bereiken. Het kan dus zijn dat medewerkers weinig met phishingmails worden geconfronteerd, door de technische maatregelen die kwaadwillende mails afvangen. En wellicht vertrouwen zij op de techniek bij het reageren op mails. De testen laten zien dat alertheid altijd geboden blijft.

6 Informatievoorziening aan de gemeenteraad

Onderzoeksvraag 4	In dit hoofdstuk beantwoorden we de vierde onderzoeksvraag: *Hoe is de informatievoorziening aan de gemeenteraad?*

P&C-cyclus

In de Baseline Informatiebeveiliging Overheid (BIO) is opgenomen dat de raad minimaal 1x per jaar in het kader van de P&C-cyclus geïnformeerd wordt over informatieveiligheid en privacy. In Doetinchem wordt over informatieveiligheid gerapporteerd in het hoofdstuk Rechtmatigheid in de jaarstukken van de gemeente. In het informatiebeveiligingsbeleid 2020-2022 wordt de raad benoemd met betrekking tot de controlerende rol, met name in het kader van de horizontale verantwoording waarvoor ENSIA is opgezet (zie hierna). Er is geen kaderstellende rol voor de raad op informatieveiligheid opgenomen, behalve uiteraard in algemene zin het budgetrecht voor de financiële kaders. Uit interviews komt naar voren dat ICT, informatiebeveiliging en privacy door college en management vooral als onderdeel van bedrijfsvoering worden opgevat, waar de raad bestuurlijk gezien meer op afstand van staat.

In het jaarverslag over 2020 wordt kort ingegaan op het gecombineerde informatiebeveiligings- en privacybeleid dat in 2020 is vastgesteld. Gemeld wordt dat de verticale verantwoording richting landelijke toezichthouders via de ENSIA-rapportage (zie hierna) is geschied. De resultaten uit de ENSIA-rapportage met betrekking tot de verbeterpunten en vooruitgang op de BIO-maatregelen zijn opgenomen. Ook wordt een aantal activiteiten op de privacy belicht, zoals het verwerkingsregister, bewustwording en de spelregels voor de thuiswerksituatie in verband met corona.

Het samenwerkingsverband op ICT wordt uiteraard ook behandeld in het jaarverslag, ook financieel. Het lijkt lastig voor raadsleden om de precieze kosten voor de gemeente uit de rapportage te halen. ICT zit in verschillende posten verwerkt en de partners betalen mee aan de uitvoering.

ENSIA

Zoals hiervoor gemeld, wordt ENSIA in de jaarstukken op hoofdlijnen meegenomen. In maart 2021 is de gemeenteraad geïnformeerd over de ENSIA in het kader van de horizontale verantwoording. De raad neemt kennis van de collegeverklaring over de informatiebeveiliging van DigiD en Suwinet, het assurancerapport van de externe auditor over de collegeverklaring en de verbeterplannen naar aanleiding van de audits op Suwinet en DigiD en van Laborijn. Deze stukken zijn geheim verklaard. Daarnaast kan de raad kennis nemen van de verantwoordingsrapportages over de BAG, BGT en BRO.

In 2019 voldeed de gemeente volledig aan de normen en hoefde geen verbeterplan naar aanleiding van ENSIA te worden opgesteld. De normen zijn in 2020 deels aangescherpt. De kernboodschap van ENSIA over 2020 is dat op vier normen na de gemeente voldoet aan de gestelde normen. Deels omdat leveranciers niet aan alle normen voldeden, op Suwinet en DigiD. De

raad kon zich vertrouwelijk op de hoogte stellen van de verbeterplannen hierop door de gemeente en Laborijn. Op de basisregistraties BAG, BGT en BRO werd in 2020 voor respectievelijk 75%, 75% en 60% voldaan de uitvoeringsnormen. Daarop zijn ook verbeterplannen geformuleerd.

Jaarrapportages

De jaarlijkse rapportage van de FG over de uitvoering van het beleid zijn aan MT en/of college gericht. In juni 2021 is de raad op privacy en het voldoen aan de AVG door het college geïnformeerd, met behulp van een infographic en een samenvatting op hoofdlijnen. Weergegeven wordt in hoeverre de gemeente voldoet aan de eisen van de AVG, op beleid, processen, samenwerking met derden, rechten van betrokkenen, beveiliging en organisatorische inbedding. Die meting wordt uitgevoerd op basis van het toetsingsdocument 'Borging AVG'. Ook worden de ontwikkelpunten aangegeven en drie focusgebieden voor 2021. Dat is op samenwerking, processen en inbedding in de organisatie. Aantal datalekken/incidenten dat bij de privacycoördinator is gemeld, aantal datalekken dat aan de AP is gemeld en aantal datalekken waarbij betrokkenen op de hoogte zijn gebracht. Er hebben zich geen dusdanig ernstige incidenten voorgedaan dat de noodzaak werd gevoeld de raad separaat te informeren, zoals bijvoorbeeld het geval was in Lochem en Hof van Twente.

Accountant

De raad krijgt uiteraard de managementletters van de accountant. De accountant controleert de rechtmatigheid van de jaarrekening van de gemeente. Steeds meer en meer richten accountants zich ook op controle van de uitvoering van informatiebeveiliging bij gemeenten. In Doetinchem is automatisering een jaarlijks terugkerend onderwerp in de management-letters en -verslagen. Zo constateert de accountant in 2017 verbeter-mogelijkheden op ICT. In 2018 ziet de accountant deze verbeter-mogelijkheden specifiek op functiescheiding en toegangsbeveiliging. In 2020 doet de accountant naar aanleiding van de controle over 2019 aanbevelingen over de reproduceerbaarheid en structuur van controles. De accountant ziet dat daarvoor ook aandacht bij de ICT-afdeling aanwezig is. In 2021 constateert de accountant in de boardletter over 2020 dat Doetinchem meer in het algemeen nog forse stappen moet zetten op het gebied van het planning- en control instrumentarium en het interne beheersingssysteem.

Lastig onderwerp

Voor de raadsleden zijn informatiebeveiliging en privacy lastige onderwerpen. Informatiebeveiliging is een redelijk technisch onderwerp, wat niet meteen in het middelpunt van de aandacht ligt. Een deel van raad heeft affiniteit op het terrein, maar een groot deel ook niet. Informatie-beveiliging en privacy komen incidenteel langs bij de raad, zo blijkt uit interviews. Uit de interviews komt naar voren dat er uit de raad weinig tot geen vragen komen over deze onderwerpen, behalve een enkele keer naar aanleiding van incidenten elders. In 2019 zijn er vanuit de raad vragen gesteld en zijn er gesprekken over informatiebeveiliging gehouden met raadsleden. Er zijn ook bewustwordingssessies met de raad gehouden, maar minder vaak dan met het college. Na 2019 zien respondenten weinig aandacht meer, wat bij hen de indruk geeft dat het onderwerp bestuurlijk

niet als een urgent thema wordt ervaren. Het gevaar dreigt dat het onderwerp iets is voor de liefhebber en dat de complexiteit van de onderwerpen moeilijk vertaald worden naar de politiek-bestuurlijke realiteit.

7 Toekomstige opgaven

Onderzoeksvraag 5	In dit hoofdstuk beantwoorden we de vijfde onderzoeksvraag: *Wat zijn de toekomstige opgaven?*

De overheid is voor een groot deel een digitale dienstverlener geworden. Dat brengt risico's met zich mee op het gebied van informatiebeveiliging en privacy, zoals uit de vorige hoofdstukken blijkt. De digitale dienstverlening biedt ook kansen, zoals verrijking van data door koppeling van gegevens of datagedreven werken met behulp van algoritmes. Bij de toepassing van nieuwe technologieën hebben overheden een verantwoordelijkheid om een transparante en controleerbare afweging te maken bij het gebruik van data en systemen enerzijds en het beschermen van privacy.

Digitale agenda Gemeenten 2024

De VNG heeft een digitale agenda opgesteld die de digitale transitie ondersteunt. Daarbij worden drie doelstellingen benoemd voor gemeenten voor de komende jaren in de informatiesamenleving:

- Mogelijk maken
- Kansen benutten
- Duiden en reflecteren

Mogelijk maken

Mogelijk maken gaat erover dat de basis op orde is met betrekking tot digitale veiligheid, een betrouwbare overheid die inclusief is en een solide digitale dienstverlening kan bieden.

Kansen benutten

Het benutten van kansen betreft het integraal verbinden van verschillende beleidsdomeinen in het lokaal bestuur ten behoeve van de dienstverlening aan de samenleving en onder andere verbinden met de economie.

Duiden en reflecteren

Duiden en reflecteren betekent dat nieuwe technologie met ethiek verbonden moet worden en met respect voor publieke waarden van de democratische rechtsstaat.

Wat de digitale agenda duidelijk maakt, is dat digitalisering niet meer een ding voor de ICT-afdeling is. In het kader van dit onderzoek wordt al duidelijk dat de verantwoordelijkheid voor informatieveiligheid en privacy al in de lijn is belegd en niet alleen bij ICT-ers of de CISO. We zien ook dat deze onderwerpen ook niet meer alleen de gemeentelijke dienstverlening betreffen, maar ook het functioneren van de overheid in de kern van de samenleving. Door de ethische vraagstukken en publieke waarden die met verdergaande digitalisering gemoeid zijn, en de verwoestende effecten van grootschalige incidenten, zoals Hof van Twente, komt de informatiesamenleving steeds meer op de politieke voorgrond. Het stelt gemeenten voor grote opgaven.

Middelen

De incidenten laten zien dat de kwaadwillenden steeds geraffineerder worden. Ook spelen geopolitieke ontwikkelingen waarin door buitenlandse staten gesteunde groepen de overheid en samenleving proberen te ontregelen. Om zich daartegen te wapenen, zijn middelen en expertise

nodig. De verwachting is dan ook dat de vraag naar middelen en formatie voor ICT en informatiebeveiliging zal toenemen. Het is al lastig om expertise op ICT uit de markt te halen en de moeite daarop zal alleen maar toenemen, zeker voor de kleinere en middelgrote gemeenten. In de vorige hoofdstukken is opzet, bestaan en werking van informatiebeveiligings- en privacybeleid bij de gemeente Doetinchem geschetst.

Datalab GO

Het benutten van kansen staat volgens de geïnterviewden nog in de kinderschoenen. De gemeente Doetinchem participeert samen met gemeenten in de Achterhoek in Datalab Gelderland Oost (Datalab GO). Datalab GO is gestart in 2020 en nog een pril project. Het gaat daarbij vooralsnog om de koppeling van basale gegevens die al aanwezig zijn in het fysieke domein. Er is vooralsnog geen sprake van een koppeling van persoonsgegevens, maar uit de interviews blijkt dat het ook niet wordt uitgesloten.

Bronckhorst is de penvoerder van het project Datalab GO, de projectleider heeft daar een aanstelling. De FG van de gemeente Doetinchem is op strategisch niveau niet aangehaakt bij het project.

Gegevens koppelen, camera's

Binnen de gemeente wordt geëxperimenteerd met koppelen van gegevens in het sociaal domein. Voor de financiële monitoring en de analyse van de voorzieningen worden gegevens uit verschillende databestanden gekoppeld en geanalyseerd. Respondenten geven aan dat dat geanonimiseerd en niet naar personen herleidbaar wordt uitgevoerd. Aangegeven wordt dat geleerd is van landelijke schandalen, zoals de toeslagenaffaire. En duidelijk is dat de gemeente wel van plan is de kansen te benutten die big data en de koppeling van gegevens bieden. Voor de veiligheid rondom het stadhuis zijn camera's aangeschaft en opgehangen. Deze kunnen medewerkers en anderen die binnenkomen registreren.

Duiden en reflecteren

Voor het ophangen van camera's is overleg geweest met de OR en is een protocol opgesteld. Maar er is van tevoren geen risicoanalyse opgesteld en er wordt getwijfeld of over het gebruik en de mogelijke consequenties bestuurlijk een overwogen besluit is genomen, blijkt uit de interviews. Ook wordt in interviews aangegeven dat het koppelen van gegevens kwetsbaar is, zoals in het sociaal domein en zonder nadere afspraken over de wijze waarop. En dat het ook bestuurlijk ingekaderd moet worden.

Kaders

Privacy is geen absoluut recht en kan bij een zorgvuldige en transparante afweging opzij geschoven worden voor een prevalerend publiek belang. Zo kunnen camera's niet zomaar opgehangen worden op willekeurige plekken, maar wel waar veiligheid als publiek belang in het geding is. De ontwikkeling van datagedreven werken is nieuw en er zijn hierop nog weinig specifieke kaders. Boetes van de AP kunnen een toetsingskader bieden en uiteraard de landelijke kaders uit de BIO en AVG. Op onderdelen zijn ook al kaders, zoals in het sociaal domein of de omgevingswet, hoewel die laatste nog geïmplementeerd moet worden. De gemeente heeft zelf noch visie of kader op datagedreven werken ontwikkeld.

Bijlage 1. Geraadpleegde documenten en respondenten

Geraadpleegde documenten

- Aandachtspunten t.b.v. software-aanvraag
- B14 Opschaalmodel cybercrisis – Advies
- Back-up proces
- Bewustwordingsplan Informatieveiligheid 2021
- Bijlage DigiD bij Collegeverklaring ENSIA 2019 - gewaarmerkt
- Bijlage Suwinet bij Collegeverklaring ENSIA 2019 - gewaarmerkt
- Boardletters accountants, 2017-2020
- ENSIA 2020 verantwoording, mededeling van het college aan de gemeenteraad (2021-45)
- GAP analyse BIO
- Getekende collegeverklaring ENSIA 2019 - gewaarmerkt
- Gewaarmerkte bijlage DigiD bij Collegeverklaring ENSIA 2020
- Gewaarmerkte bijlage Suwinet bij Collegeverklaring ENSIA 2020
- Gewaarmerkte en ondertekende Collegeverklaring ENSIA 2020
- Informatieveiligheidsbeleid gD 2020-2022
- Informatieveiligheidsplan 2021 (IVP)
- Jaarstukken 2020, gemeente Doetinchem
- Opschaalmodel Cybercrisis - B Model
- Protocollen
    - Afvoer ICT-middelen
    - Autoriseren van gebruikers voor toegang tot applicaties procedure
    - Beveiligingsincidenten en datalekken procedure
    - Configuratiebeheer
    - Datalek melden handleiding
    - Functiewijziging
    - Gedragscode - Nieuwe medewerkers bewustwording - Eerste hulp bij privacy
    - Gedragscode - Nieuwe medewerkers bewustwording - Gouden regels Informatieveiligheid
    - Gedragscode ambtenaren gemeente Doetinchem
    - Gegevensdragers opschonen procedure
    - Incidentmanagement en Responsebeleid ICT
    - Intranetpagina thuiswerken
    - Malware voorzieningen procedure
    - Patchmanagement
    - Recovery proces
    - Richtlijn clear desk en clear screen
    - Richtlijnen voor mobiele devices en mobiele informatie
    - Starterspakket Informatieveiligheidsbeheerders
    - Toegang tot ruimten procedure
    - Wachtwoorden richtlijn
    - Wijzigingsbeheer
- Rapportage Interne toetsing AVG 2019
- Register van verwerkersovereenkomsten AVG
- Toelichting-uitwijkvoorziening-datacenters
- Verbeterplan ENSIA 2020 Suwinet en DigiD

- Verbeterplan informatiebeveiliging Suwinet Laborijn
- Verwerkersovereenkomst gemeente Doetinchem v2.4
- Voorwaarden inpasbaarheid ICT-infrastructuur
- Vragenlijst inpasbaarheid webapplicatie ICT-infrastructuur

Geïnterviewde functionarissen

- Burgemeester
- Gemeentesecretaris
- Chief Information Security Officer
- Functionaris Gegevensbescherming
- Informatieveiligheidscoördinator
- Teamleider informatiemanagement
- Teamleider ICTsamenwerking

Geïnterviewden cases

Casus 1. Sociaal domein

- Applicatiebeheerder sociaal domein (Suites schuldhulpverlening, Suwinet)
- Beleidsmedewerker armoedebeleid en schuldhulpverlening
- Bewindvoerder
- Kwaliteitsmedewerker financiële ondersteuning
- Teamleider minimabeleid

Casus 2. Handhaving

- Beleidsmedewerker juridische procedures
- Secretaresse en handhaver kinderopvang
- Handhaver, bouwen en ruimtelijke ordening
- Afdelingsmanager
- Applicatiebeheerder

Bijlage 2. Veel gebruikte 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
2-staps-verificatie	zie 2FA
Active Directory (AD)	De Active Directory (AD) staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren. De AD bevat een database waarin onder andere accounts en inloggegevens zijn opgenomen
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 beveiligingsrisico's van de informatie/applicaties zijn geënt
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
BRO	De Basisregistratie Ondergrond (BRO) bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond
CISO	Chief Information Security Officer
Cryptografie	Cryptografie is het versleuteld versturen en delen van informatie die voor derden onleesbaar is
Data Recovery	Data Recovery is het weer beschikbaar stellen of ’terughalen’ van verloren data van opslagmedia zoals servers, harde schijven, usb-sticks, sd-cards, tablets en smartphones
Dataminimalisatie	Houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.
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 een waarschijnlijk 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.
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
GRIP	De GRIP structuur regelt de opschaling van de hulpverleningsdiensten van de veiligheidsregio bij rampenbestrijding en crisisbeheersing
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
Incidentmanagement en responsebeleid	Beleid om incidenten effectief en efficiënt aan te kunnen pakken, bepalend voor het beperken van schade van beveiligingsincidenten
IRPA	integrale risico- en privacy-analyse, instrument van IBD voor een integrale GAP- en risicoanalyse
ISMS	Information security management system, is een managementinstrument om de informatiebeveiliging te waarborgen en besturen. Met het instrument kunnen onder andere de veiligheidsrisico's in kaart gebracht worden, beleid en rapportages opgesteld worden en taken en verantwoordelijkheden verdeeld worden.
Log4J	Log4J is een stuk software dat veel gebruikt wordt in webapplicaties en andere systemen, dat in december 2021 bleek kwetsbaar te zijn
Logging	Logging is het in een logbestand vastleggen van alle inzagen, aanpassingen, toevoegingen en verwijderingen, die door medewerkers in een systeem of databestand worden gedaan
Malware	Malware is de verkorte term voor 'malicious software' (schadelijke software), daaronder vallen onder andere virussen en ransomware.
Patchmanagement	Patchmanagement gaat om het gecontroleerd en planmatig identificeren van kwetsbaarheden en het testen en uitrollen van patches en updates van software. Het doel is om up to date te zijn en tegelijk de dienstverlening zo min mogelijk te verstoren
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA	Zie bij DPIA
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
Proportionaliteit	Een verwerking van persoonsgegevens waarbij de vraag gesteld wordt of de verwerking in evenredigheid is met de inbreuk die gepleegd wordt op de persoonlijke levenssfeer van de betrokkenen
Ransomware	Software (malware) die (delen van) computersystemen gijzelt in ruil voor losgeld
Recovery	Zie Data Recovery
RI&E	Risico inventarisatie en evaluatie
SIEM/SOC	Security Information & Event Management (SIEM) en Security Operations Center (SOC) software die computerdreigingen monitort
Smishing	Smishing is dezelfde vorm van internet oplichting en fraude als phishing via valse sms-berichten op mobiele telefoons
Spoofing	Het verzenden van e-mails waarbij het e-mailadres van de afzender vervalst is
TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen over informatiebeveiliging
Uitwijkprocedures	Uitwijkprocedures regelen het zo snel mogelijk herstel van de dienstverlening na een verstoring of calamiteit
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt

Wifi-netwerk pentest	Deze test is bedoeld om de beveiliging van de draadloze netwerken te toetsen en mogelijke kwetsbaarheden in kaart te brengen. Gesimuleerd wordt of een kwaadwillende baat kan hebben bij een aanvalsscenario op het draadloze netwerk van de gemeente
Wijzigingsbeheer	Wijzigingsbeheer is het planmatig en gecontroleerd uitvoeren van wijzigingen in soft- en hardware in een organisatie
Wpg	Wet politiegegevens, vanaf 2020 van kracht

Bijlage 3. Casus 1. Sociaal Domein

In deze casus gaan we na hoe het team in het sociaal domein omgaat met persoonsgegevens. Met verschillende functionarissen is gesproken, zie ook bijlage 1.[26] Hierna behandelen we achtereenvolgens de AVG, hoe gegevens gedeeld worden, de intake, Plan van aanpak, applicaties en de toegang tot de gegevens, controle, bijzondere bijstand en het meedoenarrangement.

Bureau financiële ondersteuning

Het sociaal domein is breed, specifiek voor deze casus is gesproken met medewerkers van Bureau financiële ondersteuning. Het Bureau financiële ondersteuning voert de minimaregelingen, schuldhulpverlening, bijzondere bijstand, en het meedoenarrangement uit. Beleidsmatig is het bureau ook verantwoordelijk voor de regeling voor kwijtschelding, de uitvoering van deze regeling ligt bij bedrijfsvoering.

AVG

AVG

De werkwijzen van het bureau zijn vanaf 2018, vanaf het moment dat de AVG gehandhaafd werd, onder de loep genomen. Gecontroleerd is of deze AVG-proof zijn. Het merendeel van de werkwijzen was dat al wel, maar de AVG heeft volgens de respondenten de uitvoering aangescherpt. De AVG heeft volgens de respondenten geleid tot meer bewustwording op gegevensbescherming bij de medewerkers. Cursussen en e-learning worden aangeboden en kunnen medewerkers volgen om bewustwording op informatiebeveiliging en privacy te bevorderen.

Verwerkingsregister, dpia's

De verschillende verwerkingen van het bureau zijn opgenomen in het verwerkingsregister. Bij de verschillende nieuwe activiteiten en processen wordt de FG, privacyofficer en informatieveiligheidscoördinator betrokken, geven de respondenten aan. Mede om te bepalen of er een dpia uitgevoerd moet worden op de nieuwe verwerking. In 2019 zijn meteen dpia's op de bestaande verwerkingsprocessen uitgevoerd. Daaruit bleken volgens de respondenten geen risico's op privacy.

De medewerkers van het team geven aan veel onderzoeken op informatiebeveiliging en privacy te hebben en te hebben gehad. Zoals dataclassificatie, risicoanalyse op de processen, dpia's, rapportages van de beveiligingsincidenten en datalekken, actueel houden van het verwerkingsregister, BIO-maatregelen, ENSIA audit, enzovoorts.

In de teamoverleggen wordt regelmatig aandacht besteed aan aspecten op informatiebeveiliging en privacy. De applicatiebeheerder heeft structureel overleg met de informatieveiligheidscoördinator. Bij de uitvoering van de bijzondere bijstand is elk half jaar overleg over informatiebeveiliging.

Spanningsveld

Beleid en regels op informatiebeveiliging en privacy ondersteunen het zorgvuldig omgaan met persoonsgegevens. Het gaat daarbij om data-

[26] Voor deze casus is gesproken met de applicatiebeheerder sociaal domein (Suites schuldhulpverlening, Suwinet), beleidsmedewerker armoedebeleid en schuldhulpverlening, bewindvoerder, kwaliteitsmedewerker financiële ondersteuning en teamleider minimabeleid.

minimalisatie (niet meer gegevens verzamelen of verwerken dan strikt noodzakelijk is voor het doel waarvoor de gegevens worden gebruikt) en proportionaliteit (is de verwerking in evenredigheid met de inbreuk op de persoonlijke levenssfeer van de betrokkene.).

Het beperkte in de financiële dienstverlening volgens de respondenten de dienstverlening aan de inwoners. De medewerkers willen graag financiële diensten verlenen aan inwoners die het hard nodig hebben, maar ervaren dat zij soms teruggefloten worden door de AVG. Met name de dienstverlening in de preventiesfeer, omdat het niet makkelijk mogelijk is gegevens van inwoners met instanties onderling te delen.

Zelf regelingen uitvoeren

Voor een deel is dat door Doetinchem verholpen. De gemeente voert alle minimaregelingen zelf uit, op Werk en inkomen na. De gemeente is dan al zelf in bezit van de NAW-gegevens van een mogelijk nader te bepalen doelgroep die recht heeft op een nieuwe regeling en aangeschreven kan worden. Zo is bijvoorbeeld recent in het kader van de tegemoetkoming energiekosten de doelgroep aangeschreven, met inachtneming van de AVG.

Respondenten geven aan dat de inwoners die het betreft vaak zelf weinig problemen ermee hebben als hun gegevens gedeeld worden. Als ze maar worden geholpen met hun problemen. Daarnaast worden de verschillende instanties die zich met armoedebeleid bezig houden vaak als van een en dezelfde gemeente gezien. Dan hebben ze bijvoorbeeld al gegevens aangeleverd aan Laborijn, en dan moeten de medewerkers van de gemeenten nog een keer dezelfde gegevens uitvragen.

Gegevens delen

Toestemming

De gemeente vraagt tegenwoordig vooraf toestemming of gegevens bij andere instanties kunnen worden opgevraagd of met andere instanties gedeeld kunnen worden. De klanten worden ervan bewust gemaakt om welke gegevens dat gaat, en dat het ten behoeve van de dienstverlening is. Daar zijn de aanvraagformulieren die de klanten krijgen op aangepast.

Schuldhulpverlening (Wgs)

In de Wet gemeentelijke schuldhulpverlening (Wgs) is geregeld welke gegevens gemeenten mogen verwerken om inwoners toegang te geven tot de schuldhulpverlening. In de wet is ook vastgelegd dat vroegsignalering een regietaak van de gemeente is. De gemeente maakt ter voorkoming van ernstige schulden bij inwoners afspraken met woningverhuurders, zorgverzekeraars en drinkwater- en energiebedrijven om gegevens te delen. Dat zijn NAW-gegevens, mailadres en de achterstand van betaling. Naar aanleiding van die melding wordt actief door de gemeente contact opgenomen met de betrokken inwoners. Tot aan de voordeur als er door de inwoner geen contact wordt opgenomen.

Als de inwoner zelf actief een aanvraag doet, mag de gemeente op basis van de Wgs gegevens bij de betrokken partijen opvragen. Als de gemeente de betrokken inwoner een schuldhulpverleningstraject heeft aangeboden, en deze geaccepteerd heeft, kunnen alle schulden in een plan van aanpak worden meegenomen. Niet alleen de schulden van woningverhuurders,

zorgverzekeraars en drinkwater- en energiebedrijven, waarmee het traject wordt opgestart.

Een wet, zoals de Wgs, om gegevens te delen in het brede sociale domein, dus inclusief Wmo en Jeugdwet, is er nog niet. Wel ligt bij de Eerste Kamer het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden voor. Daardoor wordt het voor de uitvoering van de Wmo en Jeugdwet voor gemeenten makkelijker gegevens tussen partijen onderling met elkaar te delen.

Intake

Keukentafelgesprek, buurtcoaches

Er zijn verschillende kanalen waarop een inwoner van Doetinchem bij een voorziening in het kader van financiële ondersteuning in aanmerking kan komen. Een is er via een consulent als deze bij een inwoner komt voor een keukentafelgesprek, bijvoorbeeld in verband met een Wmo-aanvraag. Als de consulent constateert dat er tijdens dat gesprek een schulden-problematiek speelt, kan deze doorverwijzen naar de financiële dienstverlening. Een ander kanaal loopt via het Buurtplein en de buurtcoaches. Huisartsen kunnen patiënten doorverwijzen naar het Buurtplein. De buurtcoaches hebben zicht op de vele leefgebieden van de inwoners en als er een financieel probleem speelt, verwijzen zij ook door naar het Bureau financiële ondersteuning. De buurtcoaches sturen een meldverslag, met NAW-gegevens, gezinssituatie en omschrijving van de hulpvraag. Degenen die doorverwezen worden, krijgen nog een aparte intake, op het gemeentekantoor, voordat een traject wordt opgestart.

Met de introductie van de Wgs in 2020 kunnen inwoners zich ook rechtstreeks melden bij de gemeente met een financiële hulpvraag. Dan krijgen zij ook een intake op het gemeentekantoor. De respondenten geven aan dat In 90% van de gevallen door wordt verwezen naar de buurtcoach voor de vraagstukken op niet-financieel terrein op.

Plan van aanpak

Plan

Na de intake en controles wordt een plan van aanpak opgesteld. In het Plan van aanpak worden de NAW-gegevens en een probleembeschrijving opgenomen. Er wordt alleen een medische problematiek geregistreerd als die van invloed is op de financiële problematiek. Dat betekent dat er bijzondere persoonsgegevens van klanten in een schuldhulpverlening-traject geregistreerd kunnen worden bij de gemeente.

Applicaties en toegang tot de gegevens

Applicatie

De gemeente gebruikt verschillende applicaties om Plan van aanpak en dossiergegevens op te slaan. Onegov is het zaaksysteem van de gemeente. Voor schuldhulpverlening wordt een aparte vakapplicatie gebruikt, namelijk Key2 schuldhulpverlening. Daaruit kunnen de klantgegevens worden opgehaald, gekoppeld aan de basisadministratie van de gemeente. Daarmee wordt de actualiteit gecheckt van de persoonsgegevens. Als een werkproces wordt opgestart of een document wordt aangeraakt, wordt het

gekoppeld aan Onegov, het zaaksysteem. Om onder andere te voorkomen dat dubbel wordt opgevraagd of gedigitaliseerd.

Nieuwe applicatie

In het eerste kwartaal van 2022 wordt Key2 schuldhulpverlening vervangen door nieuwe applicatie, Allegro. Dat wordt de nieuwe actieve applicatie. In de aanbestedingsfase is daarop een dpia uitgevoerd.

Digitaal/papier

De bestanden van Key2 schuldhulpverlening staan in Onegov en worden gescand. Alleen de lopende werkvoorraad is nog op papier, via de scanstraat. Daarnaast wordt voor de bijzondere bijstand, Wmo en Jeugdwet de vakapplicatie Suite sociaal domein gebruikt (zie hierna bij bijzondere bijstand). Ook via Suite worden bestanden automatisch doorgezet naar zaaksysteem Onegov. De lopende werkvoorraad aan dossiers is nog op papier, de rest van de dossiers is via de scanstraat gescand en digitaal.

Toegang

Onegov, het zaaksysteem, werkt met autorisatieprofielen die aangeven tot waar de als medewerker geautoriseerd is om gegevens in te zien en te verwerken. Deze profielen worden bepaald door het team waar de medewerker werkt. Er wordt een typering aan de casus in het zaaksysteem gehangen die bepaalt welk medewerkersprofiel toegang heeft tot de gegevens.

Bewindvoering

De rechter kan, als iemand niet geheel zelfstandig in staat is zorg te dragen voor de financiën, bewindvoering opleggen. De gemeente kan in het kader van schuldsanering ook de bewindvoering uitvoeren. De bewindvoerder mag op basis van de beschikking van de rechtbank alle gegevens opvragen. Niet alleen de gegevens die bij de gemeente aanwezig zijn, maar uitkeringsgegevens van het UWV, huur bij de woningbouwvereniging, de bankrekening enzovoorts.

Deze gegevens worden in het zaaksysteem opgeslagen, met een klantnummer en BSN. Dit laatste om te kunnen koppelen aan de gemeentelijke basisadministratie, zodat de persoonsgegevens actueel zijn. Alleen de bewindvoerder heeft toegang tot het dossier in het zaaksysteem. Deze deelt de gegevens met de rechtbank, via een formulier dat beveiligd via Zivver wordt verzonden.

Kredietbank

In het kader van de schuldhulpverlening kan een krediet verstrekt worden. Voor de gemeente voert de Stichting Kredietbank Nederland deze dienstverlening uit. Als er sprake is van een krediet gaat een aanvraag met NAW-gegevens en het bedrag naar de kredietbank. Het mailverkeer hierover gaat beveiligd via Zivver.

Controle

Zoals aangegeven heeft in principe niemand die niet aan een bepaald medewerkersprofiel voldoet toegang tot de dossiers. Enkele uitzonderingen voor de controle daargelaten.

Kwaliteitsmedewerker

Intervisie en controle op de werkprocessen vindt in eerste instantie plaats bij de casusbespreking door de medecollega's. Daarnaast kan de kwaliteitsmedewerker in Key2 schuldhulpverlening bij het dossier om te

toetsen of de juiste procedures worden gevolgd en of het dossier compleet is. Verder kan in principe niemand bij de dossiers, behalve een bewindvoerder als de klant onder bewindstelling is geplaatst.

Schuldhulpverlening

Vanuit de brancheorganisatie schuldhulpverlening (NVVK) wordt een audit op de schuldhulpverlening gehouden. Dat werd tot voor kort jaarlijks op dossierniveau gedaan. In 2022 heeft de NVVK voor een nieuwe methodiek gekozen. In plaats van de check op de dossiers gaat de nieuwe audit over de visie van de gemeente op schuldhulpverlening. De audit van 2022 zou over de afgelopen drie jaar gaan, maar is vertraagd.

Rechtbank

Er vindt een jaarlijkse handhavingscontrole op beschermingsbewind plaats door het kwaliteitsbureau van de rechtbank. Per dossier moet de gemeente verantwoorden waaraan geld is uitgegeven en hoe de processen op bewindvoering zijn ingeregeld bij de gemeente. Dat zijn volgens de respondenten zware kwaliteitseisen waaraan de gemeente moet voldoen om als bewindvoerder benoembaar te zijn en te blijven.

Accountant

Tot slot voert de accountant controles uit op de bedrijfsmatige uitvoering van het beschermingsbewind. Dat gebeurt steekproefsgewijs op de dossiers.

Bijzondere bijstand

Laborijn en gemeente

Laborijn voert de regelingen van de Participatiewet uit in verband met het levensonderhoud, zoals de bijstandsuitkering. De onbelaste bijzondere bijstand wordt door de gemeente uitgevoerd. De medewerkers van het team zijn ook betrokken bij deze aanvragen voor bijzondere bijstand. Bij een aanvraag zijn gegevens nodig om de cliënt te identificeren, zoals NAW-gegevens en BSN, en de reden voor de aanvraag van de voorziening.

Als iemand al bekend is via een Participatiewet-uitkering dan is er sprake van een verkorte aanvraag, want de financiële gegevens zijn bekend. Dan komen de inwoners sowieso voor bijzondere bijstand in aanmerking. Als de financiële gegevens niet bekend zijn bij de gemeente, bijvoorbeeld als ze een eigen ander inkomen hebben, dan worden financiële gegevens op-gevraagd. De inwoner levert die gegevens zelf aan, dus de verstrekking van die gegevens gebeurt altijd met instemming van de cliënt.

Draagkrachtmeting

Mede op basis van een vermogenstoets maakt de consulent op basis van de gegevens een draagkrachtberekening om te controleren of de cliënt in aanmerking komt voor bijzondere bijstand. En of hij/zij een eigen bijdrage moet betalen. Voor de controle op de aangeleverde gegevens kan 'Suwinet inkijk' gebruikt worden.

Dossier Suites

Sommige uitkeringen zijn incidenteel op basis van een beschikking, andere uitkeringen zijn periodiek, die ook periodiek worden geregistreerd. Het dossier wordt opgenomen in de applicatie voor het sociaal domein dat de gemeente gebruikt, Suites sociaal domein. Deze is gekoppeld aan het zaaksysteem Onegov. In het dossier zitten de aanvraag en aanvullende bewijsstukken zoals aankoopbonnen facturen enzovoorts. De verwerking is

opgenomen in het verwerkingsregister en in 2019 met een dpia gecheckt. De toegang tot de dossiers is ook geregeld via de rollen/functies van de medewerkers.

CBS

De gegevens over de bijzondere bijstand worden verplicht maandelijks gedeeld met het CBS. Dat gebeurt op basis van geaggregeerde en geanonimiseerde gegevens en via speciaal daartoe opgezette en beveiligde communicatiekanalen.

Meedoenarrangement

Participeren

Het meedoenarrangement is bedoeld voor mensen die door gebrek aan geld niet kunnen deelnemen aan het maatschappelijk verkeer. Bedoeld voor gezinnen met een inkomen tot netto 120% van de bijstandsnorm en kinderen en jongeren t/m 17 jaar uit een gezin met een inkomen tot 130% van de bijstandsnorm. Bij een aanvraag bijzondere bijstand of schuldhulp-verlening wordt meteen de link gelegd met het meedoenarrangement.

Aanvraag

De aanvraag kan via buurtcoaches, consulenten, via allerlei andere kanalen van het netwerk in het sociaal domein. Inwoners kunnen de aanvraag ook zelf doen. Daarvoor is een apart systeem opgezet, met behulp van een website of 'software as a service' (SAAS). Daarin worden alleen NAW-gegevens opgevraagd, die inwoners digitaal aanleveren via DigiD. Het aanvraagformulier is gekoppeld aan het zaaksysteem Onegov. Daar vullen de inwoners de NAW-gegevens aan met inkomensgegevens, als die niet bekend zijn via een Participatiewet-uitkering. Deze gegevens zijn ook weer rol- en functieafhankelijk toegankelijk en worden niet gedeeld met anderen, of derden. Met de verschillende uitvoerders van de regeling worden NAW-gegevens gedeeld. Ook op dit verwerkingsproces is een dpia uitgevoerd.

Bijlage 4. Casus 2. Toezicht en handhaving

In deze casus gaan we na hoe het team handhaving omgaat met persoonsgegevens. Met verschillende functionarissen is gesproken, zie ook bijlage 1.[27] Hierna behandelen we achtereenvolgens de AVG en Wpg, de werkwijze in het team, de gebruikte applicaties, de toegang tot de gegevens (autorisaties), communicatie en tot slot overleg en bewustwording.

AVG en Wpg

AVG

Volgens de respondenten heeft de AVG geen ingrijpende wijzigingen in de werkwijzen bij toezicht en handhaving teweeg gebracht. Er werd onder de voorganger, de Wet bescherming persoonsgegevens (Wbp), rekening gehouden zorgvuldig omgaan met gegevens van inwoners. De AVG heeft zeker invloed gehad op de bewustwording en het strikter houden aan regels hoe met persoonsgegevens wordt omgegaan. Het proces van autoriseren is zorgvuldiger vormgegeven en niet iedereen heeft toegang tot dossiers met BSN-nummer van de betrokkenen. Zoveel als mogelijk vermelding van namen in applicaties vermeden, door te pseudonimiseren of te anonimiseren door de term 'bezwaarder' te gebruiken.

Wpg

De Wet politiegegevens (Wpg) is vanaf 2020 in werking getreden. Die wet regelt vanuit het kader van de politiewet en de AVG hoe de gemeente om moet gaan met informatie uit de systemen waar de Boa's toegang toe

Wpg

Een gemeente moet volgens de Wet politiegegevens (Wpg) aan een aantal vereisten voldoen bij de verwerking van gegevens. Die moet plaatsvinden in afzonderlijke systemen en door aangewezen medewerkers. De reden voor deze strenge eisen ligt in de aard van de bevoegdheden. Hiermee kan diep op de privacy van burgers worden ingegrepen en dit vraagt om strenge regels om de privacy van burgers te beschermen.

Voor de verwerking van politiegegevens stelt de Wpg net als de AVG een aantal algemene criteria. Dit betreft criteria over noodzakelijkheid, rechtmatigheid, juistheid, proportionaliteit, subsidiariteit en volledigheid. Daarnaast moet de verwerkingsverantwoordelijke gemeente een aantal technische en organisatorische maatregelen nemen:

1. Inspanningsverplichting verwerkingsverantwoordelijke
2. Beveiliging
3. Gegevensbeschermingseffectbeoordeling (GEB)/dpia
4. Rechten betrokken burgers
5. Registerplicht
6. Meldplicht datalekken
7. Documentatieplicht
8. Voorwaarden ICT-systeem

[27] Beleidsmedewerker juridische procedures, secretaresse en handhaver kinderopvang, handhaver bouwen en ruimtelijke ordening, applicatiebeheerder en afdelingsmanager.

hebben. Daarop zijn tweejaarlijkse audits verplicht en deze is nog niet gehouden voor de gemeente Doetinchem.

Systemen/applicaties

Zaaksysteem

Als digitaal zaaksysteem gebruiken de medewerkers Onegov, die de meeste medewerkers van de gemeente gebruiken. De gegevens kunnen gekoppeld worden met de basisregistraties en zijn in principe open voor de medewerkers die daarop kunnen inloggen. In Onegov kunnen gehele of gedeelten van dossiers afgeschermd worden.

Key2 Vergunningen

Voor toekenning en registratie van vergunningen wordt Key2 Vergunningen van Centric of Centric Leefomgeving gebruikt. Als iemand een vergunning aanvraagt, dan kunnen daarbij alle geregistreerde gegevens worden opgevraagd en ingezien worden. Als de vergunning is verleend, worden alleen de locatiegegevens naar een externe applicatie van Arcadis geëxporteerd, niet naam of andere persoonsgegevens. Daarmee kunnen op locatie met behulp van een mobiel apparaat checklists worden ingevuld.

Squit XO

Specifiek voor gegevens in verband met bouwvergunningen wordt Squit XO gebruikt. Dat is een extern systeem waar geen persoonsgegevens in aanwezig zijn, alleen locatiegegevens. Daar kunnen bovendien alleen medewerkers met een bepaald profiel en toegangsrechten bij. In verband met handhaving bij een overtreding moeten dan wel de persoonsgegevens nagetrokken worden.

Medische gegevens

In de systemen en applicaties zijn geen bijzondere persoonsgegevens aanwezig, volgens de respondenten. Bijvoorbeeld, bij de toetsing van het plaatsen van een vergunningsvrije mantelzorgwoning, waar geen omgevingsvergunning meer voor nodig is, worden geen medische gegevens geregistreerd. In de systemen wordt alleen op basis van een verklaring van een huisarts of wijkverpleegkundige of aan de voorwaarden voor mantelzorg is voldaan. Verder wordt alleen getoetst op de voorwaarden in het Bouwbesluit, zoals de regels op het gebied van veiligheid, gezondheid en milieu.

Wob-verzoeken

De medewerkers gebruikten een applicatie voor het aflakken van persoonsgegevens, en beleidsopvattingen van personen bij de publicatie van Wob-dossiers. Die wijze van zwart maken van passages in documenten kon door speciale software weer ongedaan gemaakt worden. Vandaar dat medewerkers het aflakken handmatig uitvoeren.

Autorisaties

Autorisaties

De toegang tot applicaties en gegevens daarbinnen, de autorisaties, worden toegekend op basis van de rol/functie die een medewerker heeft. Respondenten geven aan dat dat op minimale basis gebeurt, zodat het voorkomt dat medewerkers vaak verzoeken moeten doen om tot meer gegevens toegang te krijgen. De leidinggevende doet de melding voor de toekenning van een autorisatie van de leidinggevende via Topdesk, waarna

de applicatiebeheerder in de applicatie de rechten voor die rol/functie toekent.

Aanvraag vergunning

Werkprocessen

De huidige werkprocessen zijn niet grafisch weergegeven en op papier gezet. Ze zijn wel opgenomen in de systemen. Met de komst van de Omgevingswet moeten alle processen opnieuw ingericht en uitgeschreven worden. Daarvoor worden wel nieuwe processen op papier uitgeschreven.

Aanvraag

Een aanvraag voor een vergunning komt binnen met NAW-gegevens en BSN-nummer. Het gaat bij de registratie in principe om de vergunning en niet meer om de naam van de aanvrager. Voor de aanvraag van vergunningen, zoals horeca- en drankvergunningen, is in de systemen een aparte procedure en bestandssysteem binnen Onegov opgezet. Daarbij kan gedacht worden aan vergunningen voor seksinrichtingen, coffeeshops, speelautomaten. Vanaf de binnenkomst worden die aanvragen apart doorgeleid. De namen en BSN-nummers zijn afgeschermd. Bij die bestanden mogen alleen vanwege hun functie geautoriseerde medewerkers. Ook de dossiers met gegevens die met ondermijning te maken hebben, worden op die manier verwerkt. Deze zijn gelinkt met de APV-applicatie.

In de applicatie zijn de BSN-nummers afgeschermd, maar vergunningen zijn openbare gegevens. De vergunningen worden gepubliceerd met locatiegegevens en de persoonsgegevens worden afgeschermd.

Gegevens delen en ontvangen

Politie

De politie deelt met de gemeente over en weer gegevens, maar is daar zeer terughoudend in. Op last van de politie kunnen Boa's panden verzegelen, zoals drugspanden. Die melding komt via de burgemeester, als onderdeel van de driehoek, binnen. De afdeling krijgt dan alleen te horen dat er op een bepaald moment op een bepaalde locatie een inval wordt gedaan. Daarbij worden geen persoonsgegevens verstrekt. De voorbereiding van de Boa's die daarbij betrokken zijn, is miniem. Uit de interviews blijkt dat dat met de juridische en strafrechtelijke context te maken heeft waarin de politie werkt.

Voor constateringsrapporten gebruiken de Boa's een app op het mobiele apparaat. Daarin mogen geen politiegegevens verwerkt worden. Via een vraag of er politiegegevens verwerkt worden, kan een speciaal beveiligde applicatie gebruikt worden. CityControl, waarbij politiegegevens ingezien kunnen worden en alleen die gegevens die voor de actie die de Boa moet ondernemen. Daarin worden door de Boa's geen (persoons)gegevens opgeslagen.

Zivver

Met veel partijen worden gegevens en (bijzondere) persoonsgegevens gedeeld. Als er persoonsgegevens worden uitgewisseld, moet dat via beveiligd verkeer gebeuren. De gemeente gebruikt daarvoor de applicatie Zivver, waarmee beveiligd (grote) bestanden verstuurd kunnen worden. Zo

gebruikt de afdelingsmanager Zivver voor de mailcommunicatie met de bedrijfsarts over verzuim van medewerkers.

Respondenten geven aan dat niet iedereen rechten heeft om Zivver te gebruiken. Een van de respondenten verstuurt (grote) bestanden met het als onveilig aangemerkte Wetransfer. Persoonsgegevens in pdf-bestanden kunnen dan vervaagd, 'geblurd', worden. Een andere respondent wist niet van het bestaan van Zivver. Wel dat er een programma voor veilig versturen was en dat erover wordt nagedacht dat standaard in het mailprogramma te verwerken, maar de naam was niet gecommuniceerd.

GGD-rapporten kinderopvang

De GGD en de gemeente delen de inspectierapporten over kinderopvang in de landelijke inspectieruimte van de rijksoverheid. Dat is een beveiligd systeem waar alleen de GGD, gemeenten en de Inspectie onderwijs toegang toe hebben. De gemeente kan het stuk met de persoonsgegevens in een pdf-format ophalen en in Onegov in het betreffende handhavingstraject registreren.

In deze GGD-inspectierapporten zijn de naam en functie van de betreffende inspecteur opgenomen. De opvangadressen en de persoonsgegevens van gastouders zijn opgenomen in de rapporten. Waarom de persoonsgegevens van de gastouders zijn opgenomen, wordt verklaard door het feit dat deze als bedrijfsgegevens worden gezien. Gastouders willen als 'bedrijfszaak' gevonden worden. Andere persoonsgegevens zijn gepseudonimiseerd met behulp van een nummer waaronder zij bekend zijn bij het Landelijk Register Kinderopvang (LRK). De GGD en gemeenten reconstrueren zelf op basis van dat nummer uit het Landelijk Register Kinderopvang de betreffende namen.

Omgevingsdienst

De gemeente wisselt gegevens met de Omgevingsdienst Achterhoek (ODA) via het omgevingsloket. Dat is een gezamenlijk initiatief van ministerie van BZK, Interprovinciaal Overleg (IPO), Unie van Waterschappen (UvW) en de Vereniging Nederlandse Gemeenten (VNG). Daarmee wordt over en weer via beveiligde verbindingen gecommuniceerd. Via het omgevingsloket wordt ook beveiligd gecommuniceerd met de Veiligheidsregio Noord- en Oost-Gelderland (VNOG), bijvoorbeeld in geval van een melding van de brandweer.

Aanvraag vergunningen

Over de vergunningen voor horeca en drank (zie hiervoor) en ondermijnende zaken wordt op een beveiligde manier gecommuniceerd met het Regionale Informatie- en Expertise Centra (RIEC).

Bezwarencommissie

Met de bezwarencommissie worden persoonsgegevens gedeeld, in een pdf-bestand via de mail en niet geanonimiseerd. De verklaring die daarvoor wordt gegeven is dat de leden van deze commissie over deze gegevens moeten beschikken om tot een goed oordeel te komen.

DPIA's, verwerkersovereenkomsten, verzoeken om inzage

AVG

In het kader van de AVG worden onder andere dataprotection impact assessments op privacygevoelige verwerkingsprocessen, verwerkersovereenkomsten gesloten met derden als er persoonsgegevens

worden verwerkt en kunnen betrokkenen om inzage verzoeken in de gegevens die van hen door de gemeente worden verwerkt.

Dpia's

Bij toezicht en handhaving zijn nog geen dataprotection impact assessments gehouden, zie ook de lijst met dpia's in §5.1.2. De gesproken medewerkers zijn er niet mee bekend. Gepland staan gesprekken met de privacyofficer en informatieveiligheidscoördinator om een pre-dpia te doen. De accountant heeft daar ook opmerkingen over gemaakt en risico's gesignaleerd. Die constateringen gingen overigens verder dan alleen de persoonsgegevens en betroffen ook de rechtmatigheid van de bedrijfsvoering en informatiebeveiliging.

Verwerkersovereenkomsten

Wel is er contact met de privacyofficer en ICT over verwerkersovereenkomsten die gesloten moeten worden. Zoals bij het ontvangen en delen van informatie van gegevens met betrekking tot de beoordeling over de vergunningsvrije zorgwoningen of de gehandicapten parkeerkaart. Voor de verwerkersovereenkomst is gekeken naar het portaal waarop de gegevens gedeeld worden.

Verzoeken om inzage

Er worden bij vergunningen regelmatig verzoeken gedaan om inzage van eigen of andermans gegevens. Vanwege de procedure bij omgevingsvergunningen moeten gegevens ter inzage liggen. Dan gebeurt het bijvoorbeeld dat buren vragen om inzage in de stukken. Ook in het kader van een Wob-verzoek is een keer om inzage in de eigen persoonsgegevens verzocht. Maar dat zijn andere verzoeken om inzage in de eigen persoonsgegevens dan bedoeld in verband met de AVG. Er zijn in dat kader twee verzoeken binnengekomen om inzage in de persoonsgegevens die bij het team worden verwerkt. Deze komen via de privacyofficer en het zaaksysteem Onegov bij het team binnen. Daar volgden geen verzoeken uit tot verwijdering van de verwerkte gegevens.

Team

Alertheid toegenomen

Respondenten geven aan dat de alertheid met de zorgvuldige omgang met persoonsgegevens is toegenomen. Vanuit het bestuur en management wordt aandacht voor informatiebeveiliging en privacy gestimuleerd. In het MT worden regelmatig rapportages over datalekken van de privacyofficer besproken en verbeteracties opgenomen. Er worden trainingen en cursussen op gebied van informatiebeveiliging en privacy aangeboden. De privacyofficer, FG en CISO zijn bekend bij de medewerkers en men weet ze ook te vinden. Veel van de procedures en informatie op informatiebeveiliging en privacy is voorhanden op intranet. Tegelijk wordt aangegeven dat dat niet door alle medewerkers even goed wordt gelezen en bijgehouden.

Teamoverleggen

Aangegeven wordt dat in de teamoverleggen praktijksituaties worden besproken en hoe in het kader van de AVG hiermee om te gaan. Daarbij krijgt het team ondersteuning van de privacyofficer en informatieveiligheidscoördinator. De handvatten om in overeenstemming met de AVG te handelen, zijn er. Een enkele respondent geeft aan het lastig te vinden,

niet goed ondersteund te worden en met de insteek van de privacyofficer en informatieveiligheidscoördinator te worstelen.

Vragen raadsleden

Richtlijn

Tijdens de gesprekken werpen respondenten het vraagstuk op over informatie delen met raadsleden. De vraag is welke informatie zij als ambtenaren kunnen delen naar aanleiding van een vraag van een raadslid. Een artikel-38 vraag heeft een formele procedure voor de beantwoording, maar soms worden zij ook direct benaderd door raadsleden. Voor zover bekend is daar geen richtlijn voor.

Bijlage 5. Onderzoeksvragen en normen

De onderstaande normen zijn grotendeels overgenomen uit het offerteverzoek van de Rekenkamercommissie Doetinchem. De normen zijn opgesteld vanuit de uitgangspunten van de BIO en AVG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van het informatiebeveiligings- en privacybeleid getoetst wordt.

Onderzoeksvragen	Normen
1. Beschikt de gemeente Doetinchem over een adequaat informatie-beveiligingsbeleid?	- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast. - Er vindt sturing plaats op basis van de BIO. - Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld. De gemeente neemt maatregelen om risico's te verlagen. - Op onderdelen van informatiebeveiliging en privacy is beleid geformuleerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, protocol datalekken, wijzigingsbeleid enz. - De Chief Information Security Officer is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren. - Gegevens zijn goed beschermd tegen ongewenste invloeden van buitenaf.
2. Beschikt de gemeente Doetinchem over een beleid voor het gebruik van belangrijke en gevoelige (privacy)informatie?	- De gemeente werkt volgens/in overeenstemming met de regels van de AVG. - Het bestuur en medewerkers dragen het beleid ten aanzien van privacy actief uit. - Medewerkers krijgen cursussen, trainingen en dergelijke hoe zij moeten werken volgens/in overeenstemming met AVG. - De gemeente heeft in beeld met welke partners (bijzondere) persoonsgegevens worden gedeeld met behulp van het verwerkingsregister. - De gemeente maakt met partners en leveranciers afspraken over het veilig uitwisselen en verwerken van persoonsgegevens en de daarvoor te nemen maatregelen, bij voorkeur op basis van 'privacy by design'. - Partners en leveranciers rapporteren jaarlijks over het verwerken van persoonsgegevens. - De Functionaris Gegevensbescherming is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.
3. Hoe wordt dat beleid uitgevoerd en wordt het gemonitord?	- Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging actief uit. - De gemeente heeft procedures om te leren van beveiligings-meldingen met als doel beheersmaatregelen te verbeteren. - Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens en herkennen incidenten en rapporteren deze ook daadwerkelijk. - Het ISMS, indien aanwezig, is gekoppeld aan de PDCA-cyclus. - Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System). - Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren.

	- Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd.
4. Hoe is de informatievoorziening aan de gemeenteraad?	- Over het functioneren van informatiebeveiliging wordt gerapporteerd aan de raad, in ieder geval jaarlijks in het kader van ENSIA.
5. Wat zijn de eventuele toekomstige opgaven?	- Op basis van de GAP- en risicoanalyse is in beeld welke uitdagingen de gemeente heeft. - De gemeente is zich bewust van de risico's die gepaard gaan met een verdergaande digitale transformatie, zoals met het Internet of Things, kunstmatige intelligentie, big data en machine learning.

Bijlage 6. Richtlijnen/procedures Informatiebeveiliging en privacy

Bron: IBD.

Bijlage 7. Volwassenheidsniveau NOREA

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.