Rekenkamercommissie
gemeente Bronckhorst

prae
Advies & onderzoek

‘Informatiebeveiliging en privacy’ Gemeente Bronckhorst

- Definitieve versie -

In opdracht van de Rekenkamercommissie Bronckhorst

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

Juni 2022

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 recente voorbeelden, zoals de hacks en datalekken bij gemeenten Hof van Twente en Buren en bij de belastingsamenwerking West-Brabant. Onderzoeken van rekenkamer(commissie)s wijzen op de risico's op het gebied van informatiebeveiliging en privacy, zoals zeer recent de Rekenkamer Utrecht aantoonde dat de kwetsbaarheid met name intern is.[1]

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.

Vragen raadsfracties

Mede naar aanleiding van verzoeken van de raadsfracties heeft de Rekenkamercommissie Bronckhorst informatiebeveiliging en privacy als onderzoeksonderwerpen geagendeerd. Het onderzoek is uitgevoerd door Prae Advies en onderzoek.

Leeswijzer

In dit onderzoek komen veel technische termen aan de orde. Daarom volgt na de inleiding eerst een samenvatting, gevolgd door conclusies en aanbevelingen. In hoofdstuk 1 worden de onderzoeksvragen gepresenteerd en in hoofdstuk 2 de onderzoeksaanpak. In hoofdstuk 3 gaan we in op het informatiebeveiligingsbeleid waarop in hoofdstuk 4 het privacybeleid volgt. De uitvoering van het beleid komt in hoofdstuk 5 aan bod, evenals de pentesten die in het kader van het rekenkameronderzoek zijn uitgevoerd. In de marge van dit hoofdstuk wordt gerapporteerd over twee cases over de uitvoering, namelijk het sociaal domein en toezicht en handhaving. De cases worden uitgebreider beschreven in de bijlagen. In hoofdstuk 6 komt de informatievoorziening op informatiebeveiliging en privacy aan de raad aan bod. Hoofdstuk 7 gaat over de toekomstige opgaven.

[1] 'Zo sterk als de zwakste schakel' Een onderzoek naar de informatieveiligheid bij de gemeente Utrecht, Rekenkamer Utrecht, 2021.

Beantwoording onderzoeksvragen, conclusies en aanbevelingen

De hoofdvraag die de rekenkamercommissie Bronckhorst in dit onderzoek stelt 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?"*

Deze hoofdvraag beantwoorden we door middel van de antwoorden op de volgende vijf 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 eventuele toekomstige opgaven?

Onderzoeksvraag 1. Beschikt de gemeente over een adequaat informatiebeveiligings-beleid?

Informatiebeveiligingsbeleid

De gemeente Bronckhorst beschikt niet over een actueel informatie-beveiligingsbeleid dat door het College van B&W is vastgesteld. Het huidige beleid, geldig van 2019-2021, is nog niet op het in VNG-verband landelijk afgesproken basisnormenkader (BIO) geënt. De laatste analyse over de huidige situatie en de gewenste situatie (GAP) en risico's dateren van 2020 en zijn niet actueel. Medio 2021 is voor dat jaar een werkplan voor informatiebeveiliging en privacy opgesteld, met voornamelijk activiteiten op gegevensbescherming. Er is voor 2022 nog geen nieuw jaarplan opgesteld op basis van een nieuwe (risico)analyse.

Protocollen/richtlijnen

De meeste relevante protocollen en richtlijnen zijn voor Bronckhorst aanwezig, inclusief een maatgevend integraal bedrijfscontinuïteitsplan. Een enkel protocol kan nog aangescherpt worden, zoals het beleggen van verantwoordelijkheden bij proceseigenaren in geval van datalekken.

Functies

De posities op informatiebeveiliging, de CISO en privacyofficer zijn ingevuld, in de lijn bij het team I&A. De privacyofficer heeft een rol op informatie-beveiliging en gegevensbescherming. De functies zijn kwetsbaar ingevuld, onder andere door uitval en met variabele uren voor de CISO. Daardoor lopen beleids- en implementatieprocessen vertraging op. Ambassadeurs op informatiebeveiliging en privacy zijn in de teams aanwezig als linking pin tussen operationeel en tactisch/strategisch niveau.

Overleggen en rapportages

Intern zijn er voldoende overleggen met de functionarissen op informatie-beveiliging en privacy en tussen de verschillende niveaus in de organisatie (operationeel, tactisch en strategisch), zoals het informatiebeveiligings-overleg. Ook met de partners in de regionale ICTsamenwerking is overleg op operationeel en tactisch gebied, op strategisch niveau is dat incidenteel en ad hoc. De governance op de ICT-samenwerking is vooral ambtelijk ingericht, onder gastheerschap van de gemeente Doetinchem.

	Over informatiebeveiliging wordt met name in het kader van de Eenduidige Normatiek Single Information Audit (ENSIA) gerapporteerd. Deze is bedoeld voor de verticale verantwoording van gemeenten richting landelijke toezichthouders en voor de horizontale verantwoording richting de gemeenteraad. Deze rapportage wordt niet ondersteund met een managementinformatiesysteem (ISMS), zoals de BIO dat voorschrijft. Verder wordt intern en extern gerapporteerd over incidenten.
Bestuurlijke aandacht	Informatiebeveiliging en privacy zijn niet onderwerpen die bovenaan de bestuurlijke agenda staan. De onderwerpen worden wel besproken en er is bereidheid te investeren, maar de belangstelling is vooral gedreven door incidenten.

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

Privacybeleid	De gemeente Bronckhorst beschikt sinds 2018 over een uitvoeringsbeleid op het gebied van privacy, met de intentie aan de AVG te voldoen. Het uitvoeringsbeleid is operationeel en tactisch gericht. Een strategisch beleid is nog niet geformuleerd en staat voor 2022 op de rol. Zoals hiervoor in het kader van informatiebeveiliging is gemeld is medio 2021 een werkplan informatiebeveiliging en privacy voor dat jaar opgesteld. Het werkplan bevatte voornamelijk elementen op gebied van privacy. Het onderwerp privacy of gegevensbescherming wordt vaak te laat betrokken in het beleids- en besluitvormingsproces. Dat betekent dat privacy niet efficiënt in het beleids- en uitvoeringsproces wordt betrokken en niet effectief geborgd kan worden.
Elementen	De verplichte elementen en instrumenten voor de AVG zijn aanwezig, zoals verwerkingsregister, privacystatement, verwerkersovereenkomsten, procedure voor datalekken. Op gegevensbescherming zijn voor de proces-eigenaren instrumenten ontwikkeld ter ondersteuning van hun taken op privacy, zoals een (pre-)data protection impact assessment ([pre-]dpia). Deze zijn bedoeld om de risico's van kritieke verwerkingsprocessen van persoonsgegevens in kaart te brengen.
Functies	De positie op privacy, de Functionaris Gegevensbescherming (FG) is ingevuld en net als de CISO en privacyofficer in de lijn bij het team I&A gepositioneerd. De FG is grotendeels op gegevensbescherming bezig. Ambassadeurs op informatiebeveiliging en privacy zijn in de teams aanwezig als linking pin tussen operationeel en tactisch/strategisch niveau.
Overleggen en rapportages	Het hiervoor genoemde informatiebeveiligingsoverleg wordt ook gebruikt om zaken met betrekking tot privacy te bespreken. Daarnaast is er het Privacy team, tussen FG, privacyofficer en de ambassadeurs in de teams. In de Jaarrapportage gegevensbescherming rapporteren de FG en privacyofficer over privacy aan het college.

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

Procedures informatiebeveiliging	De meeste procedures op informatiebeveiliging en privacy worden uitgevoerd. Zo worden incidenten geregistreerd, gerapporteerd en besproken in het informatiebeveiligingsoverleg en met de ICTsamen-werking. Indien nodig komen daar verbetermaatregelen uit voort die opgepakt worden. Een enkele procedure, zoals de 2 factor authenticatie, is nog niet voor alle accounts van de gemeente gerealiseerd. Bijvoorbeeld niet voor de bestuurders en raadsleden.
Gegevensbescherming	Op gegevensbescherming zijn voor de proceseigenaren instrumenten ontwikkeld ter ondersteuning van hun taken op privacy, zoals de pre-dpia. In 2020 zijn twee dpia's uitgevoerd, in 2021 zijn er geen uitgevoerd. Op privacyaspecten bij inkoop worden de FG en privacyofficer op basis van een signaal van de proceseigenaar betrokken. De kans is aanwezig dat daarmee contracten zonder de benodigde verwerkersovereenkomst worden gesloten of dat het verwerkingsregister niet up-to-date is. Er is geen regelmatige check op de volledigheid van het verwerkingsregister.
Casestudies	Uit de casestudies bij het Sociaal Domein en Toezicht en Handhaving kwam naar voren dat de twee afdelingen al lange tijd ervaring hebben met de verwerking van persoonsgegevens. Sinds 2018, met de AVG en recenter met de Wet politiegegevens is dat nog sterker onder de aandacht gekomen. Aandachtspunten zijn de nog niet optimale benutting van mogelijkheden van gegevensuitwisseling met derden, het werken met papieren dossiers omdat de systemen in het sociaal domein niet aansluiten en de nog niet volledige dekking van beveiligde mailverkeer.
Bewustwording	Bewustwording bij de medewerkers op de risico's op informatiebeveiliging en gegevensbescherming is groeiende, maar blijft continu aandacht vragen. Dat is terecht een prominent aandachtspunt in de werkplannen van de gemeente.
Vastlegging	Het vastleggen van activiteiten en controles door medewerkers is nog niet op het niveau waarop de gemeente 'in control' is op informatiebeveiliging en privacy. Behalve op de verplichte jaarlijkse rapportages op de ENSIA-onderdelen als DigiD en Suwinet. Daarbij wordt grotendeels voldaan aan de normen die vooral toezien op opzet en bestaan van het beleid en in mindere mate de werking van het beleid in de praktijk. Het volwassenheids-niveau van de organisatie is momenteel op het niveau dat functionarissen op informatiebeveiliging en privacy nog veel van hun tijd kwijt aan operationele taken, ter ondersteuning van de proceseigenaren. Dat beeld werd bevestigd door de casestudies in het teams sociaal domein en handhaving.
Volwassenheid	In het kader van dit onderzoek is het volwassenheidsniveau op informatie-beveiliging bij medewerkers, volgens de methode van NOREA, een beroepsorganisatie van IT-auditors, niet gemeten. Gezien het bovenstaande

is de indruk dat deze op veel werkvelden voor Bronckhorst, net als veel andere gemeenten, tegen de 2 op een schaal van 5 scoort.[2]

Monitoring

De check op de voortgang op de implementatie van de BIO-maatregelen gebeurt via de GAP- en risicoanalyse. Over de audits op de applicaties wordt in het kader van ENSIA gerapporteerd. Uit de laatste GAP-, risico- en impactanalyse kwamen als aandachtspunten het autorisatieproces en de monitoring op incidenten. Het dataverkeer op de systemen kan gevolgd worden via logbestanden, waarin onder andere wordt vastgelegd wie wanneer welke informatie opvraagt. De check op deze logbestanden gebeurde nog niet systematisch, de periodieke monitoring van de logging staat voor 2022 op de rol. Het administratief vastleggen van de controles en de checks is een aandachtspunt, mede door de informele cultuur binnen de gemeentelijke organisatie. Het voordeel van de informele cultuur is dat er korte lijnen zijn wat het werken vergemakkelijkt. Door minder aandacht voor het administratief vastleggen van activiteiten en controles is er niet volledig zicht op de werking van het beleid in de praktijk. Overigens is dat wel 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, de gastheer van de ICTsamenwerking, laat door externen pentesten uitvoeren op de systemen. Daar komen verbeterpunten uit die door de ICT samenwerking worden opgepakt. Uit de pentesten die in het kader van de het rekenkameronderzoek zijn uitgevoerd kwamen wel aandachtspunten naar voren, maar die niet kritiek genoeg waren om direct in te moeten grijpen.

ICTsamenwerking

De governance op de (regionale) ICTsamenwerking is licht ingeregeld. Hiervoor is al geconstateerd dat bestuurlijk geen structureel overleg geregeld is en dat niet alle deelnemende partijen betrokken zijn bij het secretarissenoverleg. Iedere deelnemer is zelf verantwoordelijk voor de inrichting van het informatiebeveiligingsbeleid in de eigen organisatie. Door de samenwerking ontstaat daarop een onderlinge afhankelijkheid en kwetsbaarheid. In de dienstverleningsovereenkomsten zijn geen afspraken over harmonisatie van beleid of onderlinge aansprakelijkheid vastgelegd. Dat kan bestuurlijke, financiële en imago-risico's inhouden voor de deelnemers in de samenwerking op ICT.

Onderzoeksvraag 4. Hoe is de informatievoorziening aan de gemeenteraad?

Summier geïnformeerd

De raad wordt op informatiebeveiliging en privacy summier geïnformeerd via ENSIA en kort in de jaarstukken in het kader van de P&C-cyclus. In de managementletters van de accountant wordt ook aandacht besteed aan informatiebeveiliging, weliswaar niet uitgebreid of uitputtend. Verder worden informatiebeveiliging en privacy incidenteel geadresseerd in de raadscontext. Door de summiere informatievoorziening komt de raad niet

[2] Op de 5 puntenschaal van het Volwassenheidsmodel van NOREA zij de volgende niveaus te onderscheiden: 1: initieel; 2: herhaalbaar; 3: gedefinieerd; 4: beheerst en meetbaar; 5: continu verbeteren. Een organisatie is bij een gemeten volwassenheidsniveau 3 'in control' op informatiebeveiliging. Voor een uitgebreidere uitleg zie bijlage 8.

goed in positie om zijn kaderstellende en controlerende rol op deze terreinen in te kunnen vullen. De raad neemt voor zover we in dit onderzoek hebben kunnen constateren geen proactieve houding aan op deze beleidsterreinen.

Onderzoeksvraag 5.	Wat zijn de eventuele toekomstige opgaven?

Kinderschoenen

De gemeente Bronckhorst zet voorzichtig stappen met betrekking tot datagedreven werken en het koppelen van gegevens, samen met andere gemeenten in de regio. 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.

Conclusies

Hoofdconclusie

Gemeente Bronckhorst zet de nodige stappen om te voldoen aan de basisrichtlijnen voor informatiebeveiliging en privacy. Voor zover de scope van de testen in het kader van het rekenkameronderzoek reikte constateert de rekenkamercommissie dat de technische systemen geen kritieke risico's kennen. Naar aanleiding van de bevindingen uit het rekenkameronderzoek is de conclusie dat er nog veel stappen te zetten zijn voordat de gemeente 'in control' is op informatiebeveiliging en privacy.

Deelconclusies

In algemene zin leidt de hoofdconclusie tot de 6 onderstaande deelconclusies:

1. Het beleid op informatiebeveiliging en privacy is niet actueel en weinig ambitieus;
2. De formatie op informatiebeveiliging en privacy is kwetsbaar;
3. De technische kant van informatiebeveiliging is volgens de normen ingeregeld;
4. Bewustwording is een blijvend aandachtspunt;
5. De regionale samenwerking op ICT kent risico's die niet voldoende worden onderkend;
6. De raad wordt weinig betrokken op en summier geïnformeerd over informatiebeveiliging.

Aansporingen en aanbevelingen

Aansporingen

Zoals gezegd zet de gemeente de nodige stappen, waarbij de rekenkamer-commissie het college wil aansporen verder te gaan met:

- Continue inzet op bewustwording van risico's op informatiebeveiliging en privacy bij de medewerkers;
- Data protection impact assessments uitvoeren op de geselecteerde verwerkingsprocessen;
- Inzet op het gebruik van veilig mailverkeer door medewerkers;

- De koppeling van Civision met het Document management systeem, ter voorkoming van papieren dossiers in het sociaal domein;

Aanbevelingen

De hiervoor gepresenteerde conclusies leiden tot de volgende vijf aanbevelingen:

1. *Actualiseer het beleid op informatiebeveiliging en privacy.*
2. *Verminder de kwetsbaarheid van de formatie op informatiebeveiliging en privacy.*
3. *Houdt de technische kant van informatiebeveiliging op orde;*
4. *Versterk de governance en afspraken op de regionale samenwerking op ICT;*
5. *Informeer de raad meer en inhoudelijker op informatiebeveiliging en bepaal met college en raad het ambitieniveau.*

De aanbevelingen worden hieronder nader uitgewerkt:

1. Actualiseer het beleid op informatiebeveiliging en privacy

Aan de raad

- Geef het college de opdracht om op korte termijn een actueel informatie-beveiligings- en privacybeleid op te stellen.
- Formuleer ambities op informatiebeveiliging en privacy, zoals op het na te streven volwassenheidsniveau.
- Geef het college de opdracht visie en beleid op datagedreven werken te ontwikkelen, hoe om te gaan met verwerking van persoonsgegevens, de ethische vraagstukken die hierop kunnen spelen en binnen die context de benutting van de door de gemeente verzamelde gegevens te optimaliseren.

Aan het college

- Werk het informatiebeveiligings- en privacybeleid uit naar jaarplannen en stel deze tijdig vast, uiterlijk aan het begin van het betreffende jaar.
- Richt de rapportages op informatiebeveiliging en privacy zo in dat ze zicht geven op opzet, bestaan en werking van de maatregelen op informatie-beveiliging en privacy;
- Investeer daarvoor in een informatiemanagementsysteem op informatiebeveiliging (ISMS);
- Betrek het onderwerp gegevensbescherming en de functionarissen op privacy eerder in beleids- en besluitvormingsprocessen.

2. Verminder de kwetsbaarheid van de formatie op informatiebeveiliging en privacy

Aan het college

- Versterk de invulling van de functies op informatiebeveiliging en privacy, door de functies los van de lijn te positioneren en zoveel als mogelijk het vastgestelde aantal uren ingezet kunnen worden.

3. Houdt de technische kant van informatiebeveiliging op orde

Aan het college

- Stel, indien van toepassing in overleg met ICT-samenwerking, een plan van aanpak op naar aanleiding van de verbeterpunten uit de pentesten van het rekenkameronderzoek;
- Draag, indien van toepassing in overleg met ICT-samenwerking, zorg voor:
    - Inregeling van 2 factor authenticatie (2FA) voor alle mailaccounts;
    - Scheiding van de Outlook adresbestanden per partner in de samenwerking.

4. Versterk de governance op de regionale samenwerking op ICT

Aan het college

- Evalueer met de deelnemende partijen de afspraken over de governance op de ICT samenwerking en:
    - Richt de governance en aansturing op bestuurlijk niveau zwaarder in;
    - Sluit service level agreements met aansprakelijkheidsafspraken met betrekking tot de risico's;
    - Spreek af hoe harmonisatie van beleid op informatiebeveiliging en privacy bij de deelnemers uitgevoerd kan worden.

5. Informeer de raad meer en inhoudelijker op informatiebeveiliging en bepaal met hen het ambitieniveau.

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.

Aan de raad

- Neem als raad meer dan nu het geval is de kaderstellende en controlerende rol op informatiebeveiliging en privacy op en pak de regie hierop:
    - Vul eventuele kennislacunes op door te scholen op het stellen van kritische vragen op informatiebeveiliging en privacy;
    - Huur hierbij indien nodig externe expertise in voor een second opinion of pentesten;
    - Geef de accountant de opdracht consistent te rapporteren op aspecten op informatiebeveiliging.

1 Onderzoeksvragen

Centrale onderzoeksvraag

De Rekenkamercommissie wil met het voorliggende onderzoeksrapport 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 eventuele 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

Met betrekking tot beleid en de protocollen is deskresearch gepleegd. Een overzicht van de geraadpleegde documenten is in bijlage 1 opgenomen.

Interviews

Met een viertal bestuurlijke en ambtelijke sleutelfiguren is een interview afgenomen. Een korte lijst met geïnterviewde functionarissen is ook in bijlage 1 opgenomen.

Casestudies

Om de uitvoering van het informatiebeveiliging- 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 gebruik gemaakt 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 pentesten. Pentesten, voluit penetratietesten, worden uitgevoerd door ethisch hackers en geven inzicht in de beveiligingsrisico van de organisatie. De pentesten zijn grotendeels gericht op de technische kant van informatie-beveiliging, 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 ICT-samenwerking, 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 in 2021 uitgevoerd. De pentesten zijn door de onderzoeker en de ethisch hackers gecheckt en als adequaat beoordeeld. Voor de resultaten van de pentesten en de verbetermaatregelen, zie §5.2. De rekenkamercommissie heeft daarop besloten geen interne en externe netwerkpentest uit te laten voeren.

Besloten is in het kader van het rekenkameronderzoek aanvullend een AD-audit, wifi-netwerkpentest, phishing en smishing test en een mystery guest uit te voeren. Voor een uitleg van de testen zie §5.2. 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 gemeentehuis. Vandaar dat is besloten deze test niet uit te voeren.

Hoor en wederhoor

Op 7 april 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 op 27 juni voor een bestuurlijke reactie voorgelegd aan het college van B&W. Daarna is het rapport met een nawoord van de rekenkamercommissie op …. aangeboden aan de gemeenteraad.

3 Informatiebeveiliging

Onderzoeksvraag 1

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

ICT-samenwerking

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

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

Het gemeentebrede integraal informatiebeveiligingsbeleid 2019-2021 is op 4-12-2018 vastgesteld door het college van B&W. Het informatie-beveiligingsbeleid wordt in Bronckhorst 3-jaarlijks vastgesteld. Het nieuwe beleid, dat van 2022-2024 moet gelden was op moment van rapportage nog niet vastgesteld, wat feitelijk betekent dat er geen vigerend beleid is.

In het informatiebeveiligingsbeleid is de ambitie van de gemeente neergelegd en zijn de strategische rollen vastgelegd. Het college stelt de kaders op het beleid en de secretaris is gemandateerd verantwoordelijke. De secretaris stelt met het Ontwikkelingsteam (OT) het gewenste niveau van de informatiebeveiliging op procesniveau vast. De managers (de lijn) zijn verantwoordelijk voor de informatieveiligheid en de betrouwbaarheid van de bedrijfsprocessen. Daarnaast zijn onder andere de rollen van de Chief information security officer of coördinator informatiebeveiliging (CISO), controller, de clusters Informatie en automatisering (I&A), Personeel en organisatie (P&O) en Facilitair met betrekking tot informatiebeveiliging opgenomen. De privacy officer (PO) en Functionaris gegevensbescherming (FG) worden benoemd in relatie tot de Algemene Verordening Gegevensbescherming (AVG), zie daarvoor ook hoofdstuk 5. Tot slot wordt vastgelegd dat alle medewerkers verantwoordelijkheid dragen voor de veiligheid van de activiteiten die tot hun functie en taken behoren.

BIG > BIO

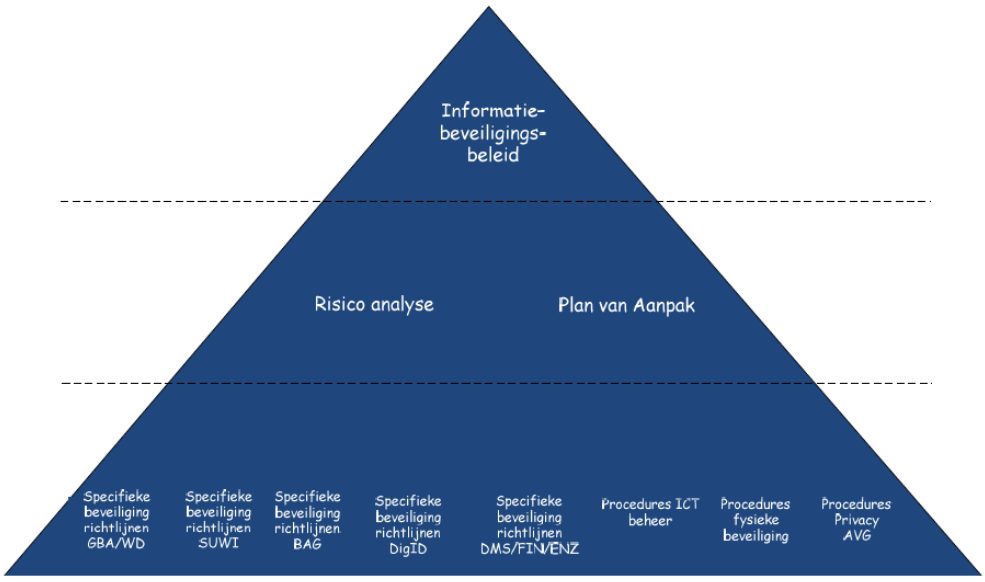
Het informatiebeveiligingsbeleid van de gemeente 2018-2021 is nog gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Deze is gebaseerd op ISO-27002 en bestond uit ruim 300 maatregelen waar gemeenten aan moesten voldoen. Dat was vastgesteld naar aanleiding van een de VNG-resolutie uit 2013. De BIG is in 2019 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO is meer risicogestuurd dan de BIG en bevat minder maatregelen. De gemeente Bronckhorst heeft de ambitie om te voldoen aan de BIO.

Plan van aanpak

Het strategische informatiebeveiligingsbeleid 2018-2021 in het kader van de BIG was ook al grotendeels risicogestuurd. Op tactisch niveau moet jaarlijks een plan van aanpak worden opgesteld met maatregelen op basis van een GAP-analyse en risicoanalyse. De laatste GAP analyse op de BIO-maatregelen is uit 2020. De GAP-analyse was gebaseerd op informatie over informatiebeveiliging (en privacy), zoals een bedrijfsimpactanalyse (BIA), Risico-inventarisatie en evaluatie (RI&E), GAP analyse op ICT-maatregelen en ICT Samenwerking BIO en ENSIA-rapportages. Deze rapportages gingen over de situatie in 2019. Voor een update van het plan van aanpak informatiebeveiliging heeft de organisatie gewacht op een nieuw instrument voor de GAP- en risicoanalyse van de IBD. Dat heet de integrale risico- en privacy-analyse (IRPA) en is recent beschikbaar gekomen. De gemeente is er al voorzichtig mee gestart en verwacht de analyses in de loop van 2022 gereed te hebben. Op basis daarvan kan het plan van aanpak informatiebeveiliging (en privacy) vernieuwd worden. Op 14-6-2021 is een Werkplan informatiebeveiliging en privacy 2021 vastgesteld (zie §3.1), met voornamelijk activiteiten op gegevensbescherming en weinig op informatiebeveiliging.

Op het formuleren van informatiebeveiligingsbeleid en de implementatie van maatregelen op tactisch niveau is vertraging. Gevraagd naar de reden van de vertraging wordt, naast prioriteit gegeven aan onder andere aanpak van incidenten en kwetsbaarheden, gewezen op de kwetsbare invulling van de posities op de CISO en coördinator informatiebeveiliging (zie hierna bij functies informatiebeveiliging).

Afbeelding 1. Pyramide informatiebeveiligingsbeleid gemeente Bronckhorst, 2018.



Richtlijnen en procedures

Onder in de pyramide van het informatiebeveiligingsbeleid (zie afbeelding 1) staan de operationele richtlijnen en procedures. Er zijn specifieke landelijk vastgestelde beveiligingsrichtlijnen voor processen die door de gemeente worden uitgevoerd. Dat zijn onder andere de applicaties Suwinet en DigID, waarvan de uitvoering door landelijke toezichthouders wordt

gecontroleerd. De gemeente moet hierover 'verticaal' naar de betreffende toezichthouders rapporteren. Dat gebeurt in het kader van de eenduidige normatiek single information audit (ENSIA), zie §3.3.

Met betrekking tot de overige procedures en richtlijnen die gemeenten zelf moeten opstellen zijn bij Bronckhorst de volgende aangetroffen:

- Thuiswerken, met behulp van tweefactor authenticatie (2FA)
- Richtlijnen thuiswerken 16 maart 2020
- Richtlijnen digitaal audio/video vergaderen 17 maart 2020
- Afsluiten gebouw en beveiliging
- Gebruik gemeentehuis in het weekend
- Clear-desk- en clear-screen-beleid
- Registratie email- en social media berichten
- Telefonie, privé-toestellen
- Privacyreglement e-mail- en internetgebruik
- Regelgeving automatisering en informatisering (archiefverordening, informatiebeheer enz.)
- Gedragsregels informatiebeveiliging en privacy V3, 4-3-2021
- Veiligheidsincidenten melden
- Meldplicht datalekken
- Protocol noodknop consulenten en handhavers
- Protocol voertuigvolgsysteem (2018)
- Protocol cameratoezicht (2018)
- Handleiding wachtwoord wijzigen
- Bedrijfscontinuïteitsplan

Een aantal procedures die met de ICT op zich te maken hebben wordt uitgevoerd in ICT-samenwerking-verband. Dat geldt bijvoorbeeld voor het back-up en restore beleid en wijzig- en patchbeleid van applicaties op de servers van het samenwerkingsverband. Vandaar dat de gemeente Bronckhorst die procedures niet voor de eigen organisatie heeft.

Werkwijze

Uit de interviews blijkt hoe de gemeente aan de slag gaat met het opstellen van de richtlijnen. Als voorbeeld wordt het bedrijfscontinuïteitsplan genoemd. In 2018-2019 is men ermee begonnen en steeds worden stukken opgepakt. Met onder andere een risico- en business impactanalyse op alle kritieke processen dat breder is dan veel gemeenten vanuit de BIO opzetten. Dat resulteerde uiteindelijk in een volledig plan. Toen de coronapandemie begon kon gemeente de plannen erbij pakken en snel de bevoegdheden, communicatie en besluitvorming regelen. Het plan van de gemeente Bronckhorst is door de VNG opgevraagd en gemeenten komen bij Bronckhorst langs om van het plan te leren.

Functies informatiebeveiliging

In het strategisch beleid zijn de verantwoordelijkheden en functies op informatiebeveiliging belegd. De CISO rol, op strategisch en adviserend niveau, wordt in deeltijd ingevuld. Daarnaast is de CISO ook beleids-medewerker I&A en ENSIA-coördinator. Dat betekent dat de CISO variabele uren heeft voor zijn taak. De gemeente werkt op ICT samen met andere

gemeenten. Uit interviews blijkt dat de nabije beschikbaarheid van een 'eigen' CISO nuttig is en gewaardeerd wordt.

Ook de security/privacy officer (PO) is in deeltijd voor 20 uur werkzaam, en heeft een rol die met name op tactisch niveau ligt. Daarnaast zijn medewerkers in de teams aangewezen als ambassadeur, waarmee het contact tussen CISO en PO op operationeel gebied wordt onderhouden.

De CISO is nog niet lang geleden uitgevallen en is begin 2022 voor halve dagen weer aan het werk. De PO is ook deels uitgevallen. Uit de interviews blijkt dat daarmee de vertraging op informatiebeveiligingsbeleid en plan van aanpak verklaard kan worden. In 2020 kwam het verzoek dat ondersteund werd door directie en college om informatiebeveiliging en privacy robuuster neer te zetten. Daartoe is een beleidsmedewerker I&A geworven die de CISO op de automatiseringswerkzaamheden kan ontlasten. Ook krijgen de functionarissen op informatiebeveiliging op techniek en automatisering ondersteuning vanuit ICT-samenwerking.

In de interviews wordt aangegeven dat als er actie ondernomen moet worden op het gebied van informatiebeveiliging dat voorrang krijgt op andere werkzaamheden. Toch oogt de bezetting van de functies op informatiebeveiliging kwetsbaar, ook in vergelijking met gemeenten van vergelijkbare grootte.

3.2 Overleggen

Intern en extern

Op het gebied van informatiebeveiliging zijn er intern reguliere overleggen in de lijn met de gemeentesecretaris. Verder is er een informatie-beveiligingsoverleg, met een kernteam als er een groot incident is. Extern, met ICT-samenwerking zijn er reguliere overleg met inhoudsdeskundigen op automatisering (ICT-A) en tussen de secretarissen van de deelnemende gemeenten.

Overleg lijnmanager/CISO

De lijnmanager I&A heeft 2-wekelijks overleg met de gemeentesecretaris. Daar komen de informatiebeveiligingsaspecten aan bod, als dat nodig is. De CISO kan in principe ook rechtstreeks naar de gemeentesecretaris of portefeuillehouder in het college stappen. Dat gebeurt bij situaties dat dat door de CISO nodig wordt bevonden, zoals met Log4J of phishing mails. Ook komt de burgemeester wel eens met vragen over informatiebeveiliging bij de CISO langs.

Informatiebeveiligingsoverleg

Op het gebied van informatieveiligheid en privacy is er het formele informatiebeveiligingsoverleg. Dat is een werkgroep die drie keer per jaar bijeen komt en de strategische aangelegenheden op informatiebeveiliging en privacy bespreekt. De werkgroep bestaat uit de CISO als voorzitter, de controller, beveiligingsbeheerders uit de teams van onder andere facilitair, P&O, DIV, SUWI, BRP enz. Verder nemen op het gebied van privacy aan het overleg deel de FG en privacybeheerders uit de teams. Daarmee komen ook de maatregelen met betrekking tot de gegevensbescherming aan bod in de werkgroep. Tot slot kunnen indien nodig of gewenst OT-leden of specialisten aansluiten.

In het informatiebeveiligingsoverleg wordt onder andere de GAP-analyse besproken die uit is gevoerd door de PO. En daar worden activiteiten benoemd die opgenomen worden in het jaarplan. Minimaal wordt 2 keer per jaar een update van de maatregelen uit het plan van aanpak besproken. Die update vindt plaats op basis van een risicoanalyse.

Incidenten

Incidenten op informatiebeveiliging en privacy worden bijgehouden in Topdesk en doorgeleid naar In het informatiebeveiligingsoverleg worden ook veel voorkomende incidenten besproken. Als een incident zich tot een crisis ontwikkelt, wordt een kernteam Informatiebeveiliging opgezet. Daarvan maken deel uit de CISO, de manager van het cluster I&A, een beveiligingsbeheerder ICT, lid van het OT, mogelijke relevante experts en een medewerker Communicatie.

Samenwerking

Er zijn uiteraard ook contacten met ICT-samenwerking in Doetinchem. In de interviews wordt aangegeven dat de contacten steeds beter gaan en meer synergie bieden. Er is een ICT-Automatiseringsoverleg (ICT-A), waar Bronckhorst in vertegenwoordigd. Daar worden besluiten over de inrichting van de ICT besproken en genomen. Dat overleg heeft een officiële status, waartoe besloten is door de deelnemende gemeenten. Op de informatie-kant zijn er werkgroepen waar de deelnemers aan ICT-samenwerking in vertegenwoordigd zijn. Deze zijn informeler dan het ICT-A overleg.

Bij het ICT-A overleg waren altijd de CISO's of security officers aanwezig. Sinds 2019 is met de deelnemers in ICT-samenwerking jaarlijks een vrijdag bestempeld als zogenoemde 'co-locatiedag'. Daarin worden alle veiligheidsissues besproken, zodat de deelnemers één geluid richting het ICT-A overleg kunnen laten horen. In dat overleg is ook ruimte voor vraagstukken op het gebied van privacy. Dat overleg wordt mede als regionaal klankbordgroep op informatiebeveiligings- en privacy issues gebruikt.

Governance ICT-samenwerking

Op ambtelijk niveau vindt er minimaal 2 keer per jaar een overleg tussen de secretarissen van de in ICT-samenwerking deelnemende gemeenten. Opvallend is dat andere deelnemende partijen, zoals Laborijn, niet bij dat overleg betrokken zijn. Zij zijn afnemer van ICT-diensten, terwijl de gemeenten zich positioneren als mede-eigenaar van ICT-samenwerking. Uit de interviews blijkt dat er ook in het bestuurlijk overleg aandacht is voor informatiebeveiliging in het samenwerkingsverband.

3.3 Rapportages

ENSIA

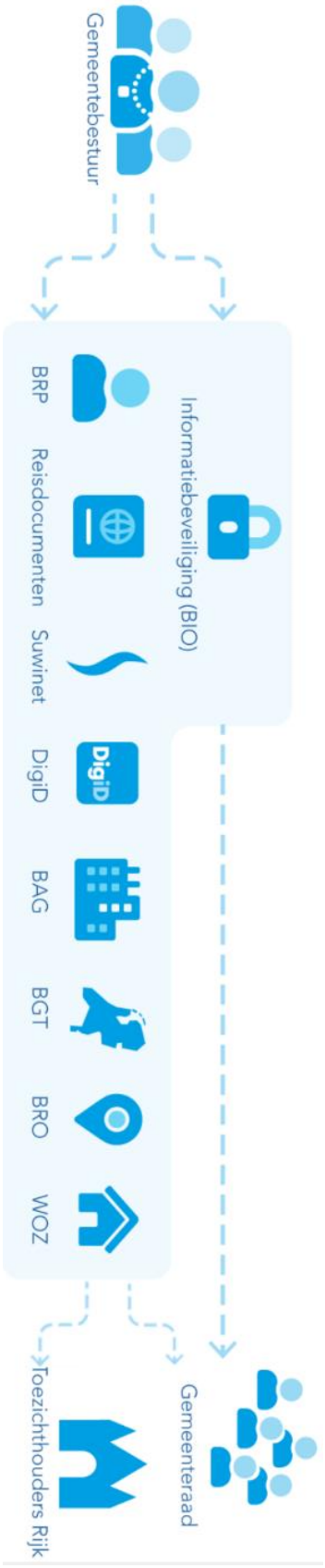
Over informatiebeveiliging worden verschillende rapportages opgesteld. De jaarlijkse ENSIA-rapportage maakt een belangrijk onderdeel uit van de P&C-cyclus. Hierin staat de verticale verantwoording (landelijke toezichthouders) en de horizontale verantwoording (gemeenteraad) centraal. Uit de audits die nodig zijn voor de ENSIA komen verbetermaatregelen op informatie-beveiliging en gegevensbeheer. De CISO is de ENSIA-coördinator. Het lijnmanagement is procesverantwoordelijk en voert elk jaar zelfevaluaties uit, als onderdeel van de ENSIA-rapportage. De zelfevaluaties worden jaarlijks gecheckt door de CISO.

Assuranceverklaring

Het college rapporteert ENSIA ook naar de raad toe, met een onafhankelijke 'assuranceverklaring' over het 'in control'-statement van het college. Het assurance rapport over de ENSIA 2020 kwalificeert de collegeverklaring over het voldoen aan de geselecteerde normen van DigID en Suwinet als juist. Maar geeft ook aan dat de gemeente nog niet aan alle normen van Suwinet voldoet. De maatregelen daartoe zijn in een verbeterplan opgenomen.

Deze rapportages aan de raad vallen onder de passieve informatieplicht van het college. Er zijn geen aanvullingen aangetroffen met betrekking tot de actieve informatieplicht van het college richting raad met betrekking tot informatiebeveiliging. Dat wil zeggen dat door het college geen gebruik wordt gemaakt van de vrije ruimte die de ENSIA biedt om de raad te informeren over informatiebeveiliging.

ENSIA-model, 2021



ISMS

Er wordt geen gebruik gemaakt van een zogenoemd information security management system (ISMS) om rapportages op te stellen en sturingsinformatie te genereren. In de GAP analyse die in 2020 is opgesteld wordt geconstateerd dat informatie over informatiebeveiliging (en privacy) over meerdere documenten is verspreid. Zoals de bedrijfskritische processen die in de business impact analyse (BIA) zijn opgenomen, de risicoanalyse in de RI&E, een GAP-analyse specifiek voor ICT-maatregelen vanuit Doetinchem, GAP-analyse op de BIO-maatregelen van de ICT-samenwerking, de ENSIA-rapportage van ICT-samenwerking, en de ENSIA-rapportages op DigID en Suwinet.

Incidenten

De CISO wordt geïnformeerd over de beveiligingsincidenten en deze worden besproken in het informatiebeveiligingsoverleg. Minimaal eenmaal per jaar rapporteert de CISO over de incidenten aan de gemeentesecretaris. De incidenten worden ook in ICT-samenwerking verband besproken en daarop worden indien nodig maatregelen genomen. Zeer recent is besloten tot de aanschaf

van een applicatie dat de systemen op kwetsbaarheden onderzoekt, mede op basis van een discussie naar aanleiding van de gebeurtenissen van Hof van Twente in 2020.

4 Privacy

Onderzoeksvraag 2

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

4.1 Beleid

Uitvoeringsbeleid privacy

In februari 2018 heeft het college van burgemeester en wethouders het Uitvoeringsbeleid privacy en het privacyreglement van de gemeente Bronckhorst vastgesteld. Daarbij heeft het college vastgelegd dat de gemeente de ambitie heeft de doelstellingen en beginselen uit de Algemene Verordening Gegevensbescherming (AVG) te behalen en te waarborgen.

In het uitvoeringsbeleid is een opsomming van activiteiten en regels op bescherming van persoonsgegevens opgenomen. In het beleid zijn niet de rollen, verantwoordelijkheden en de governance vastgelegd zoals in het strategisch informatiebeveiligingsbeleid wel is gedaan. Het beleid zou na 3 jaar geëvalueerd en op basis daarvan opnieuw opgesteld moeten worden. Dat was op moment van rapportage nog niet gebeurd.

Verplichtingen AVG

Uitgangspunt van de AVG is dat de verantwoordelijkheid voor het opvolgen van de AVG bij de organisatie zelf ligt. Aantoonbaar moet de gemeente voldoen aan de privacyregels van de AVG. Dit betekent dat het college van B&W aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

De AVG schrijft een aantal zaken verplicht voor, zoals het aanstellen van een Functionaris gegevensbescherming (FG), de publicatie van een privacystatement waarin de gemeente aangeeft hoe deze met persoons-gegevens omgaat, een verwerkingsregister waarin de processen zijn opgenomen waarin de gemeente persoonsgegevens verwerkt en een procedure voor het melden van datalekken.

De functie van FG is ingevuld, zie hieronder bij functies privacy. Het privacystatement is vastgesteld en gepubliceerd. In de notitie Datalekken is uitgelegd wanneer een incident met persoonsgegevens een datalek is en hoe gehandeld moet worden bij het vermoeden van een datalek. De verwerkingen die door of namens de gemeente worden verricht met persoonsgegevens zijn opgenomen in het verwerkingsregister. Het lijnmanagement, zijnde de proceseigenaren, geeft deze door aan de FG, die het register bijhoudt. Met derden die voor de gemeente persoonsgegevens verwerken worden verwerkingsovereenkomsten gesloten, op basis van de standaard van de VNG.

Werkplan Informatiebeveiliging en privacy 2021

In het werkplan informatiebeveiliging en privacy 2021 zijn, zoals hiervoor al gemeld voornamelijk activiteiten op privacy opgenomen. In het algemeen is in het werkplan voor 2021 opgenomen dat privacy bewustzijn vergroot moet worden en dat er aandacht is voor privacy in werkprocessen. Voor

2021 staan specifiek privacy protocol thuiswerken en het (laten) opstellen van data protection impact assessments (dpia's). Dpia's worden uitgevoerd om de risico's van de verwerking van persoonsgegevens in kritische processen in kaart te brengen. Om het lijnmanagement daarbij te ondersteunen heeft de FG een pre-dpia ontwikkeld. Dat is een checklist waarmee het lijnmanagement kan checken of uiteindelijk een dpia nodig voor dat specifieke verwerkingsproces.

In het werkplan 2021 is in een vooruitblik op 2022 ook opgenomen dat een nieuw privacybeleid opgesteld moet worden. Verder zijn als activiteiten opgenomen het stellen van regels voor dataminimalisatie, de periodieke monitoring van de logging gegevens en handvatten voor de dpia. En dat in 2022 het proces ingericht moet worden dat rechten van betrokkenen met betrekking tot hun persoonsgegevens vaststelt.

Procedure rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het feit dat gegevens worden verwerkt, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang tot en verwerking van de persoonsgegevens te voorkomen. Actief doet de gemeente dat door onder andere een privacystatement te publiceren waarin de gemeente aangeeft hoe met persoonsgegevens wordt omgegaan. Passief door betrokkenen in staat te stellen vragen te stellen over de verwerking en controle en invloed uit te oefenen over de registratie van hun persoonsgegevens.

Functies privacy

Zoals gemeld is de rol van de FG ingevuld. Deze functie is ondergebracht bij het team I&A. De rol van de FG werd eerst nog in deeltijd ingevuld, naast de functie van applicatiebeheerder vergunningen. Momenteel is de functionaris het grootste deel van de tijd actief als FG. Naast de FG is er de privacy officer/security officer, voor 18 uur aan het team I&A toegevoegd. Zoals eerder gemeld, is deze al een tijd niet actief. Dat betekent dat de strategische functie van FG ook een aantal tactisch/operationele taken moet uitvoeren.

Privacybeheerders

In de teams zijn ambassadeurs of contactpersonen aangewezen die de link tussen de FG en PO enerzijds en de teams anderzijds vormen. Voor de verwerking van gegevens in specifieke domeinen zijn privacybeheerders aangewezen. Zo is er een privacybeheerder voor het sociaal domein en de Basisregistratie Personen (BRP). Zij vormen de contactpersonen voor de FG en PO voor deze domeinen.

4.2 Overleggen

Informatiebeveiligingsoverleg

In het vorige hoofdstuk is het Informatiebeveiligingsoverleg, waarin de FG en PO deelnemen al aan de orde geweest. De FG heeft daarnaast een keer in de zes weken overleg met de gemeentesecretaris, waarin het brede terrein van informatiebeveiliging en privacy wordt besproken.

Privacy team

In het privacy team binnen de gemeente zijn de FG, PO en de ambassadeurs/contactpersonen binnen de teams vertegenwoordigd. Daar worden

de vraagstukken op het gebied van privacy behandeld. In Jaarrapportage gegevensbescherming wordt gemeld dat de dit overleg nog verder ingebed moet worden in de organisatie.

Externe overleggen

Vanwege ICT-samenwerking is tussen de FG'en van Doetinchem en Bronckhorst een rechtstreekse communicatielijn. Met de functionarissen gegevensbescherming van Montferland en Doetinchem heeft de FG van Bronckhorst 1 keer per maand overleg. Met de FG'en van Berkelland, Winterswijk en de ODA worden periodiek bespreekpunten op privacy doorgenomen.

4.3 Rapportages

Jaarrapportage gegevensbescherming

De belangrijkste rapportage op het gebeid van privacy is de door de FG opgestelde jaarrapportage gegevensbescherming. De rapportage is gebaseerd op een format van de VNG, door de FG aangevuld met een aantal aandachtsgebieden. De jaarrapportages worden besproken in het OT en het college. De laatste versie, medio 2021 gereedgekomen, is pas in december in het OT aan de orde geweest, ten tijde van het interview nog niet in het college.

De rapportage bevat een evaluatie van de activiteiten in 2020 en een vooruitblik met adviezen voor 2022. De evaluatie in de jaarrapportage bevat stand van zaken met betrekking tot de AVG en wordt op een aantal onderwerpen weergegeven:

- Beleid
- Samenwerking
- Processen
- Beveiliging
- Organisatorische inbedding
- Verantwoording
- Rechten van betrokkenen
- Totaalbeeld

Het specifieke doel voor 2020 was privacy beter in te bedden in de organisatie. Voor 2021 en verder staat het verder ontwikkelen van bewustzijn bij de medewerkers ten aanzien van risico's en procedures op gegevensbescherming. Het streven is in 2022 om op privacy een meer strategisch governance document op te stellen, waarin de rollen, taken en verantwoordelijkheden zijn vastgelegd.

De rapportage wordt afgesloten met een lijst datalekken, waarin onder andere is opgenomen de aard van het incident, welke persoonsgegevens het betrof, hoeveel personen (betrokkenen) het betrof, of het gemeld is aan de AP en welke verbetermaatregelen zijn aanbevolen.

ENSIA

Met ENSIA (zie §3.3) heeft de FG weinig bemoeienis en levert alleen een actueel verwerkingsregister aan. De PO is wel actief bezig met ENSIA vanwege de dubbelrol als security officer.

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 een tweetal onderzoeksmethoden toegepast om het beeld verder in te vullen en de uitvoering van het beleid te controleren. 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, de casebeschrijvingen zijn respectievelijk in de bijlagen 6 en 7 weergegeven. Een samenvatting van de cases is in dit hoofdstuk in 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, AVG, het samenwerkingsverband ICT-samenwerking, het autorisatieproces, contracten met derden?

Wat goed gaat

Gevraagd naar wat goed gaat op het gebied van informatiebeveiliging en privacy antwoorden de meeste respondenten dat de aandacht voor de onderwerpen de laatste jaren is toegenomen. Mede door de incidenten van de afgelopen jaren is in algemene zin het bewustzijn toegenomen. Gedrag en bewustzijn van medewerkers op de risico's is de menselijke kant van het informatieveiligheidsvraagstuk, de andere zijn organisatorische randvoorwaarden en de techniek.

Bestuurlijke aandacht

Uit de interviews blijkt dat de onderwerpen informatieveiligheid en privacy niet bovenaan de bestuurlijke agenda staan, maar wel onderdeel zijn van debat. Risico's zien en daarop actie (laten) ondernemen is een bestuurlijke aangelegenheid. Daar is de organisatie mee aan de slag en het bestuur in brede zin, college en raad. Zie met betrekking tot de raad hoofdstuk 7. De aandacht is volgens respondenten evenwel grotendeels incident gedreven, vragen komen bestuurlijk op als er zich elders een incident heeft voorgedaan, zoals in Lochem en Hof van Twente. Over het algemeen gaat

het gemeentebestuur ervan uit dat het beleid op orde is en de functies adequaat ingevuld zijn.

Analyses en evaluaties

Dat beeld wordt grotendeels bevestigd in de risicoanalyses en evaluaties die op informatiebeveiliging en privacy worden gehouden. Uit de ENSIA-rapportage (zie ook §3.3) naar de landelijke toezichthouders en de gemeenteraad blijkt dat de gemeente redelijk goed op de BIO-normen scoort. Er wordt voldaan aan geselecteerde normen op DigiD en Suwinet, hoewel nog niet aan alle normen. Dat geeft het gevoel bij de bestuurders dat de gemeente in control is. Alle risico's worden in kaart gebracht en daarop kunnen op basis van een afweging maatregelen genomen worden. Tegelijk geven de bestuurders aan dat een garantie op 100% veiligheid niet te geven is. Het besef is aanwezig dat de gemeente het technisch en organisatorisch/beleidsmatig nog zo goed kan afdichten, het grootste risico blijft menselijk handelen. Daarnaast is de gemeente meer en meer afhankelijk van externe leveranciers, veelal (grote) internationale bedrijven. Dat brengt andere risico's met zich mee (zie §5.1.5).

GAP- en impactanalyse

Uit de GAP-analyse van begin 2020 blijkt dat beleid, organisatie van informatiebeveiliging, fysieke beveiliging en fysieke omgeving, communicatiebeveiliging en beheer van informatiebeveiligingsincidenten op orde zijn. De GAP-analyse is intern opgesteld, en is aangevuld met gegevens uit de GAP-analyse van ICT-samenwerking uit 2019. Van 137 maatregelen uit de BIO, en deels nog BIG, wordt onder andere aangegeven of deze geheel of gedeeltelijk aanwezig is, wie verantwoordelijk is, of er een externe leverancier bij betrokken is. Op 94 van de mogelijke 137 punten wordt door de gemeente gescoord. Verbeteracties zijn nodig op de leveranciersrelaties en naleving van de voorgenomen verbeteracties. Daarnaast zijn als aandachtspunten de toegangsrechten van medewerkers tot gegevens in applicaties en de monitoring van incidenten en bedreigingen (SIEM/SOC) genoemd. Dezelfde aandachtspunten komen in de impact-analyse begin 2020 ook naar voren. Deze impact-analyse meet de mate van control op de diverse gebieden van de BIO.

5.1.1 Bewustwording

Bewustwording

Op bewustwording wordt al enige tijd ingezet door de gemeente, want het is een van de belangrijkste bepalende factoren in informatiebeveiliging. De CISO, FG en PO publiceren regelmatig berichten over informatiebeveiliging en privacy op intranet. Er is een brochure opgesteld voor nieuwe medewerkers in het kader van het inwerkprogramma, met gedragsregels en e-learning onderwerpen. Bij de eedaflegging van ambtenaren wordt stilgestaan bij ambtelijke verantwoordelijkheid en integriteit. Al langer meedraaiende medewerkers krijgen een uitnodiging om deel te nemen aan een cursusaanbod op het leerplatform 'Bronckhorst leert door'.

Door corona is een aantal voorgenomen activiteiten niet doorgegaan. En door een mislukte Europese aanbesteding op bewustwordingsactiviteiten door ICT-samenwerking ligt het initiatief op deze activiteiten bij de gemeente zelf. Daarop heeft de gemeente ook het initiatief genomen, zoals

recent een serious game op informatiebeveiliging en privacy van de IBD, *Spion op je pad*, is met de lijnmanagers en een cursus over veilig mailen met Zivver.

Uit de interviews blijkt dat medewerkers enthousiast zijn om zaken op te pakken en met steeds meer relevante vragen op informatiebeveiliging en privacy bij de functionarissen komen. Bijvoorbeeld op het gebied van privacy niet meer met de vraag "Wat moet ik doen?" maar "Als ik het zo aanpak, ben ik dan op de goede weg?" Het algemene beeld is dat de gemeente op informatiebeveiliging en privacy nog niet op het gewenste niveau is, mede gelet op de risico's en dreigingen op informatiebeveiliging. Maar dat beleid aanwezig is en het bewustzijn door de gehele organisatie een ontwikkeling heeft doorgemaakt. Helder is ook dat alertheid bij de medewerkers op de risico's blijvende aandacht vragen.

Informele sfeer

Uit de interviews komt het beeld naar voren van de gemeente Bronckhorst als een niet zeer formele organisatie. Veel verantwoordelijkheden zijn laag in de organisatie belegd, en niet alles is in procesbeschrijvingen of procedures vastgelegd. Dat geeft ruimte aan medewerkers om vanuit hun gevoel voor verantwoordelijkheid te kunnen werken. De sfeer is meer van aanpakken en handelen en de aandacht gaat niet zozeer uit naar controle op basis van een vooropgezet plan en vastlegging van de activiteiten.

Dat laatste wordt wel door de landelijke toezichthouders afgedwongen op de applicaties Suwinet en DigID, waarover in het kader van ENSIA-verantwoording moet worden afgelegd. Voldoet een gemeente herhaaldelijk niet aan de vastgestelde normen, dan kan deze uiteindelijk van het gebruik van deze applicaties worden afgesloten. Zoals eerder geconstateerd voldoet de gemeente aan de gestelde eisen in het kader van de ENSIA-rapportage.

Taken op informatie-beveiliging & privacy

Uitgangspunt van het beleid is dat de verantwoordelijkheid voor informatiebeveiliging en privacy niet alleen bij de FG, CISO en PO ligt, maar een zaak is van de proceseigenaren. De genoemde functionarissen hebben een toezichthoudende en (strategisch) adviserende taak. De proces-eigenaren moeten de risico's op informatieveiligheid en privacy inventari-seren. Zoals het uitvoeren van een dpia of opstellen van een verwerkings-overeenkomst met een derde partij. Zij zijn ook aan zet bij het opvolgen van aanbevelingen en uitvoeren van verbetermaatregelen naar aanleiding van de rapportages op informatiebeveiliging en privacy. Maar de FG, PO en CISO zijn tot nu toe hierop ook operationeel adviserend bezig geweest en zijn nog niet volledig toegekomen aan de toezichthoudende taak.

Datalek

De datalekprocedure is op papier geregeld en wordt ook grotendeels uitgevoerd. De meldingsbereidheid van beveiligingsincidenten is groot, zo blijkt uit de interviews. Incidenten worden in Topdesk opgenomen, periodiek geanalyseerd door de PO en besproken in het Informatie-beveiligingsoverleg. Als er een vermoeden tot een datalek is gemeld wordt deze geregistreerd in een intern register. In 2021 zijn bij de FG 15

meldingen gedaan waarbij een datalek werd vermoed. Uiteindelijk zijn 6 datalekken gemeld bij de Autoriteit Persoonsgegevens.

Uit de interviews blijkt dat de taken van de proceseigenaren op datalekken niet volledig goed zijn vastgelegd. Zoals bij het informeren van betrokkenen van een datalek en het documenteren van de activiteiten die proces-eigenaren moeten nemen. Bij de meest voorkomende kleine incidenten is dat over het algemeen niet zo'n probleem, maar ook dan kan de gemeente niet aantonen welke stappen zijn gevolgd. Naarmate het incident en lek groter wordt, wordt het risico op een ontbrekende bewijslast navenant groter. In de risicoanalyse 2019 werd al geconstateerd dat het niet goed documenteren een rode draad in de organisatie is. De gewoonte op papier of digitaal vastleggen van procedures, werkinstructies en controleverslagen is gering. Zo werd geconstateerd dat in het geval van bijvoorbeeld controleverslagen het lastig is om aan te tonen dat controles daadwerkelijk zijn uitgevoerd en deze kunnen dan ook niet als naslagwerk worden gebruikt. Dat komt de vereiste zorgvuldigheid niet ten goede, zo werd geconcludeerd.

De meeste (bijna) datalekken ontstaan door onopzettelijk foutief omgaan met informatie, zoals ook in de risicoanalyse van 2019 werd geconstateerd. Bijvoorbeeld door onwetendheid hoe informatie veilig te delen, of verkeerde adressering van een e-mail. Een risico dat in de interviews is geconstateerd is dat in ICT-samenwerking de mailadressen van de medewerkers van alle organisaties voor iedereen binnen ICT-samenwerking toegankelijk zijn. De kans op verkeerd adresseren van mail met persoonsgegevens, doordat het mailprogramma een mailadres vanuit de gedeelde adresbestanden invult, neemt daardoor toe. En daarmee de kans op een datalek.

ENSIA

Daarnaast vergt het coördineren van de ENSIA-rapportages steeds meer tijd van de al kwetsbare capaciteit op de functie van CISO en PO. Bij de gemeente wordt niet gewerkt met een zogenoemd information security managementsysteem (ISMS) om het ENSIA-proces te ondersteunen. Er is ooit een dergelijk managementsysteem aangeschaft, maar dat voldeed uiteindelijk niet. Zoveel mogelijk wordt getracht de medewerkers uit de lijn de benodigde auditlijsten in Excel in te laten vullen.

Er zijn afdelingen die al jarenlang persoonsgegevens verwerken en waar vanuit de medewerkers zelf al veel aandacht wordt besteed aan gegevensbescherming. In de jaarrapportage van de gegevensbescherming wordt geconstateerd dat er ook nog afdelingen zijn waar ervan wordt uitgegaan dat privacy een kwestie van de FG is en informatiebeveiliging van de CISO. Respondenten zien daar wel ontwikkeling op, maar het is nog veel zoeken naar de juiste rol en informatie voor de lijn.

5.1.2 AVG

AVG

Om de proceseigenaren te ondersteunen is een aantal hulpmiddelen ontwikkeld. Zoals een checklist voor verwerking van persoonsgegevens,

zodat keuze gemaakt kan worden of en hoe een proces in het verwerkingsregister opgenomen moet worden. En een zogenoemde pre-dpia, waarmee de proceseigenaren kunnen bepalen of een dpia op een proces uitgevoerd moet worden. De gegevensverwerkingen waarop een dpia verplicht is moeten elke drie jaar geactualiseerd worden, maar een overzicht dat daarbij van nut zou kunnen zijn is er nog niet. De op de AVG ontwikkelde hulpmiddelen worden nog niet overal optimaal gebruikt. Maar geconstateerd wordt dat door steeds vaker het gesprek met proceseigenaren over verwerkingen en dpia's plaatsvindt, gaandeweg de bewustwording op privacy en de kwaliteit van de naleving van de AVG verbetert. Een aantal aanbevelingen uit de laatste rapportage gegevens-bescherming van de FG is daadwerkelijk opgevolgd, tegelijk constateert deze dat een aantal nog uitgevoerd moet worden.

Dpia's

Uit de jaarrapportage gegevensbescherming blijkt dat in 2020 twee dpia's zijn uitgevoerd. Op Office365 applicaties en Zivver, de applicatie om veilig te mailen. FG is daarvoor advies gevraagd, en heeft aanbevelingen gedaan die medio 2021 nog niet waren opgevolgd. In 2021 zijn geen dpia's uitgevoerd. In de jaarrapportage is dan de aanbeveling opgenomen dat de teams de verwerkingen nalopen met de pre-dpia. Het management heeft toegezegd dat te gaan uitvoeren.

Rechten van betrokkenen

In 2020 zijn twee verzoeken om inzage van gegevens op grond van de AVG gedaan. Dat zijn geen Wob-verzoeken, maar verzoeken van betrokkenen om gegevens die de gemeente verwerkt in te zien of te laten verwijderen. In de procedures is nog niet vastgelegd hoe de gemeente met deze verzoeken van betrokkenen omgaat. In de jaarrapportage gegevens-bescherming wordt geconstateerd dat veel gegevens op verschillende decentrale plekken te lang worden bewaard, zoals in de mailboxen van medewerkers waar controle daarop ontbreekt.

Privacy by design

Privacy by design betekent dat het aspect privacy zo vroeg mogelijk bij ontwerp van beleid en processen wordt meegenomen. Als privacy als aspect pas laat in dat proces wordt betrokken en al een aantal design beslissingen zijn genomen, worden eisen op gegevensbescherming vaak als een last ervaren. De ervaring, zo blijkt uit interviews, is dat privacy vaak pas in latere fases van het beleidsproces erbij wordt betrokken. De ambtelijke en bestuurlijke aandacht is hierop groeiende, maar bijvoorbeeld het advies van de FG heeft nog geen standaard plek in het sjabloon van B&W-voorstellen.

5.1.3 ICT-samenwerking

ICT-samenwerking

De gemeente Bronckhorst werkt in ICT-samenwerking met Doetinchem als gastheer samen met andere gemeenten en andere partijen. In 2015 is daartoe besloten, uit efficiencyoverwegingen. In 2018 is de samenwerking herbevestigd. Volgens de bestuurders werkt de samenwerking naar behoren.

Overleg ICT-samenwerking

Met betrekking tot de samenwerking is geen regulier bestuurlijk overleg geregeld. Opgemerkt wordt dat zo'n overleg in een crisissituatie gestart kan worden als bijvoorbeeld delen van de dienstverlening afgekoppeld moeten worden. De CISO is ambtelijk aangesloten op het zogenoemde ICT-A overleg, dat over de afstemming op automatisering gaat. Daarin werd geacteerd op het Log4J veiligheidslek dat in december 2021 werd geconstateerd. Bestuur en ambtelijk apparaat vinden dat ze daarbij goed op de hoogte zijn gehouden door de afdeling I&A van Doetinchem en dat daarop goed geacteerd is door de gemeente, ook in het weekend. De mening is dat de gemeente Doetinchem zijn verantwoordelijkheid pakt op dit gebied, in samenspraak met de deelnemers in ICT-samenwerking.

Governance ICT-samenwerking

Onder de samenwerking met Doetinchem, en andere partijen, liggen zogenoemde service level agreements (sla). Deze overeenkomsten zijn relatief licht ingestoken. De aansprakelijkheid bij calamiteiten lijkt daarin niet goed geregeld. Als zich bijvoorbeeld een calamiteit voordoet, zoals een ransomware aanval bij Hof van Twente, dan is het onduidelijk of en welke partij daarvoor aansprakelijk gesteld kan worden. Dat brengt bestuurlijke, financiële en imago-risico's met zich mee. De accountant adviseerde het college in de interimcontrole 2020 de sla met de gemeente Doetinchem te actualiseren, het informatiebeveiligingsbeleid daarop te actualiseren en de wederzijdse aansprakelijkheden te bespreken. Uit de interviews blijkt dat in Bronckhorst bestuurlijk geen urgentie hierop wordt ervaren.

Uitwijk- en pentesten

In ICT-samenwerking verband wordt de beveiliging van de systemen periodiek getest door pentesten op de technische systemen. De meest recente interne en externe netwerk pentest zijn in maart 2021 gehouden, zie ook §5.2. Ook wordt getest of de ICT-dienstverlening na een calamiteit vanuit een uitwijksituatie binnen een bepaalde termijn weer opgestart kan worden. In 2021 is met goed gevolg de uitwijk getest van de Basisregistratie Personen (BRP) van de gemeente Bronckhorst.

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.

Rol/taak

De toekenning van toegangsrechten gebeurt op basis van rollen en taken. Het autorisatiebeleid ziet erop toe dat medewerkers niet bij gegevens kunnen komen die zij niet voor hun functie of rol nodig hebben. Het autorisatieproces begint te lopen als een manager opdracht geeft voor de aanvraag voor een nieuwe medewerker. De rol van de medewerker bepaalt in welke applicatie en tot welke informatie deze toegangsrechten krijgt. Tot

en met 2020 werd de applicatie Umra gebruikt, daarna werd dat Ivanti. Deze applicatie is gekoppeld aan Topdesk en het personeelssysteem. Vanwege de overgang moest er met de hand van de ene naar de andere applicatie worden overgezet en nog steeds wordt daarop gecontroleerd.

De rol/taak wordt aan een domein gekoppeld en geregistreerd in de Active Directory (AD), dat is een database die onder andere gebruikt wordt om rechten toe te kennen. Via Topdesk krijgen de applicatiebeheerders een signaal dat een medewerker in een rol bij een team zit, en worden de rechten toegekend die daarbij horen. Als er bij personeelszaken iets wijzigt in de functie van een medewerker, dan wijzigt dat automatisch in de Active Directory en de daarbij behorende toegekende autorisaties. Als iemand van het ene team of cluster naar het andere gaat, dan worden de oude rechten ontnomen en nieuwe toegekend.

P&O checkt eens per kwartaal of mensen nog werkzaam zijn bij de gemeente, zodat mogelijk nog lopende autorisaties achterhaald kunnen worden en worden stopgezet. En incidenteel checkt de FG de autorisaties. Een aansporing voor applicatiebeheerders om de autorisaties actueel te houden is dat betaald wordt per actieve licentie. Een onnodige licentie, met bijbehorende autorisaties, kost extra geld als de rol/taak niet meer vervuld wordt.

5.1.5 Derden

Inkoop en contracten met derden

Een gemeente besteedt veel uit en koopt veel in, zoals diensten van derden en applicaties. In het kader van informatiebeveiliging en privacy moeten daar afspraken over worden gemaakt zodat voldaan wordt aan BIO en AVG. Op applicaties van derden is een risicoanalyse uitgevoerd en daar is een lijst van 20 belangrijke softwarepakketten uit naar voren gekomen. Zo is recent een aanvullende module aan het personeelssysteem toegevoegd. Omdat het hierbij om verwerking van persoonsgegevens gaat is daar een dpia op uitgevoerd.

Bij een inkoopproces wordt meestal onderzoek verricht en sinds de AVG zijn de FG en PO daarbij betrokken. Dat is om te bezien of daar een dpia op moet worden uitgevoerd of dat er een verwerkingsovereenkomst gesloten moet worden. Deze aanpak geldt voor de nieuwe inkopen. Contracten in verband met softwarepakketten hebben vaak een korte looptijd, die komen bij vernieuwing dus langs bij de FG en PO. Er zijn ook langlopende contracten, die niet regelmatig langs komen en waarvan onduidelijk is of er een verwerkingsovereenkomst bij afgesloten zou moeten worden. Daar is een inhaalslag te maken volgens de respondenten.

De betrokkenheid van de FG/PO is afhankelijk van het signaal dat de proceseigenaar afgeeft. Bij een omvangrijke of ingewikkelde inkoop-procedure worden zij wel betrokken. Bij kleinere procedures alleen als hen een vraag wordt gesteld, bijvoorbeeld of een verwerkingsovereenkomst nodig is. Als er geen signaal komt dan krijgen de FG/PO soms achteraf ter kennisgeving de verwerkingsovereenkomst toegestuurd. Op basis daarvan

kan dan, indien nodig, het verwerkingsregister aangepast worden. Een check op de compleetheid van het verwerkingsregister wordt niet op regelmatige basis gedaan. Waarmee er een kans bestaat dat, zonder melding aan de FG/PO, het verwerkingsregister achterloopt op de daadwerkelijke verwerkingen die de gemeente verricht.

Casus Sociaal domein (voor de volledige beschrijving zie bijlage 6)

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

Het team was al voor de AVG gewend met het oog op privacy met persoonsgegevens om te gaan. Toch zijn er verschillen, zo worden de klantgegevens tegenwoordig geanonimiseerd met een klantnummer, in plaats van voorheen met het BSN. De verwerkingen van persoonsgegevens zijn opgenomen in het verwerkingsregister en de benodigde dpia's worden uitgevoerd. Bij nieuwe verwerkingsprocessen wordt de FG betrokken en een pre-dpia uitgevoerd, zoals recent de nieuwe inburgeringswet.

Intern wordt in het sociaal domein onder andere voor de Wmo, jeugdzorg en Participatiewet integraal gewerkt. Dat betekent dat gegevens intern indien nodig gedeeld kunnen worden. Er worden spanningen ervaren in relatie tot delen met en verkrijgen van gegevens van derde partijen. Ervaren wordt dat dat niet altijd in het belang van de inwoner is.

Van de werkprocessen zijn geen stroomschema's, die zitten in de systemen verwerkt. Via verschillende kanalen kunnen inwoners zich melden voor ondersteuning, of gemeld worden. Via wijkteam, huisarts of de Raad voor de Kinderbescherming. Bij een aanvraag in het kader van de Participatiewet wordt de intake gedaan op het gemeentehuis, bij andere aanvragen gaat het via een huisbezoek. Bij een huisbezoek worden met behulp van een app gegevens opgenomen en de problematiek in kaart gebracht. Hierbij wordt gestreefd naar dataminimalisatie, opname van relevante, maar zo minimaal mogelijk, informatie om de dienstverlening te kunnen uitvoeren. In de dossiers zijn indien nodig financiële en medische gegevens aanwezig. De toestemming van de klant wordt gevraagd of informatie kan worden gedeeld met dienstverleners of als gegevens opgevraagd moeten worden bij derden.

De dossiers waarmee het team werkt zijn nog niet geheel gedigitaliseerd, omdat de applicatie Civision Samenlevingszaken nog niet is aangesloten op het zaaksysteem Join. De toegang tot de gegevens is, in overeenstemming met de autorisatieprocedure (zie §5.1.4), opgehangen aan rol en functie van de medewerkers. De interne communicatie verloopt via Civision, de externe communicatie beveiligd via Zivver. Voor zorgleveranciers moet dan het anonieme klantnummer omgezet worden in een BSN, en dat wordt gecodeerd en beveiligd verstuurd naar het Gemeentelijk Gegevensknooppunt. De communicatie met betrekking tot gegevens in het kader van de jeugdzorg verloopt op basis van pseudoniemen en zijn alleen toegankelijk voor medewerkers die geautoriseerd zijn door de Stichting Kwaliteitsregister Jeugd.

De kwaliteitsmedewerkers hebben een taak alert te zijn op informatieveiligheid en gegevensbescherming. Applicatiebeheerders van het team sluiten aan bij de informatiebeveiligings-werkgroep. Het team sluit aan bij de reguliere bewustwordingsactiviteiten (zie §5.1.1).

Casus Handhaving (voor de volledige beschrijving zie bijlage 7)

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

De AVG heeft volgens de respondenten weinig gevolgen gehad voor de werkwijzen in het team. De AVG heeft wel geleid tot meer bewustwording op de gegevensbescherming. De verwerkingen zijn opgenomen in het verwerkingsregister en er bleek geen dpia nodig te zijn. Sinds 2020 is Wet politiegegevens (Wpg) ingevoerd, die regelt hoe BOA's met politiegegevens omgaan. Daarop is een audit geweest, uitgevoerd met behulp van de FG en een externe auditor.

Meldingen voor handhaving worden in Topdesk opgenomen, meestal via het KCC. Alleen NAW-gegevens en de strijdigheid worden geregistreerd. Ook via DUO kunnen meldingen binnenkomen, bijvoorbeeld over bewoningssituaties die niet stroken met de basisregistratie. Meldingen over verzegeling van (drugs)panden komen vanuit een bestuurlijke rapportage van de politie, via de burgemeester en het Cluster Openbare Orde en Veiligheid, bij de handhavers terecht. De politie deelt met de BOA's zogenoemde mutatierapporten over vermeldingswaardige incidenten in de gemeente. Deze rapporten zijn alleen bestemd voor de BOA's.

Van de bezoeken van de handhavers worden constateringsrapporten opgesteld, met behulp van een app op de IPad of later op de computer op het kantoor. Alleen NAW-gegevens, de constateringen en de afspraken worden vastgelegd. De rapporten worden in het zaaksysteem Join opgeslagen. Als er door BOA's politiegegevens worden verwerkt dan gebruiken zij een andere applicatie, namelijk Citycontrol. Daarmee kunnen kentekengegevens worden opgevraagd en kan ook verbaliseerd worden. Voor foto's als bewijslast wordt TimeStampFreeCamera gebruikt, omdat daarmee datum, tijd en locatie op de foto vermeld worden.

De dossiers zijn gedigitaliseerd. Mogelijk schriftelijke stukken die opgevraagd worden, worden door DIV gedigitaliseerd en ook in Join opgenomen. De medewerkers van het team hebben toegang tot de dossiers. De communicatie van gegevens in het kader van handhaving gaat vanuit de gemeente in principe beveiligd via Zivver. Voor beveiligde verzending van grote bestanden wordt een oplossing gezocht.

De juridisch medewerker van het team is contactpersoon op privacy voor de FG. Medewerkers van het team nemen deel aan de reguliere activiteiten op bewustwording in het kader van informatie-beveiliging en privacy. Uitdagingen zien de respondenten op het vastleggen van de activiteiten en het informeel delen van persoonsgegevens in een kleine overzichtelijke en gemoedelijke gemeente als Bronckhorst.

5.2 Pentesten

Inleiding

Zoals eerder aangegeven zijn in het kader van het rekenkameronderzoek pentesten uitgevoerd, door ethische hackers. In eerste instantie was de rekenkamercommissie van plan een interne en externe netwerk pentest en mystery guest test uit te laten voeren. ICT-samenwerking heeft maart 2021 een externe en interne netwerk pentest laten uitvoeren op het gezamenlijke netwerk.

Pentesten 2021

De interne en externe pentesten van 2021 leverden een aantal risico's op voor ICT-samenwerking (2 gekwalificeerd als zeer laag risico, 1 laag, 14 gemiddeld, 20 hoog en 13 kritisch) en de interne pentest voor Bronckhorst apart (2 gemiddeld, 7 hoog en 5 kritisch). Naar aanleiding van de risico's is een verbeterplan opgesteld. Stand van zaken begin 2022 is dat de kritische punten grotendeels zijn afgehandeld en van de andere punten zijn in Topdesk meldingen opgenomen die van daaruit bewaakt en afgehandeld worden. Ook is een applicatie aangeschaft die regelmatig de systemen scant en de verbeterpunten die daaruit naar voren kwamen zijn maatregelen getroffen.

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.

In het kader van het rekenkameronderzoek zijn een wifi-netwerk pentest, een Active directory audit, een phishing- en smishing mail aanval uitgevoerd. Zie hierna voor de resultaten op deze testen. 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 is een wifi-penetratietest bij de gemeente Bronckhorst 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 dat iemand

ongeautoriseerde toegang tot een losstaand draadloos netwerk kan krijgen die in principe niet direct toegang zou mogen geven tot het interne netwerk, en twee is de mogelijkheid dat iemand via het gastnetwerk iemand anders computer of telefoon zou 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 van de accounts van de medewerkers van de gemeente Bronckhorst is in het kader van ICT-samenwerking in beheer bij de gemeente Doetinchem. De AD-audit is dan ook in samenwerking met IT-beheer van de gemeente Doetinchem uitgevoerd. ICT-samenwerking beheert de AD van alle partners in de samenwerking, maar deze audit beperkt zicht tot 638 accounts van de gemeente Bronckhorst, en 624 met andere deelnemers in ICT-samenwerking gedeelde accounts. Dat zijn beheerderaccounts en enkele algemene serviceaccounts. Niet alle serviceaccounts zijn in gebruik bij de gemeente Bronckhorst, 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.

Van de in totaal 638 accounts van de gemeente Bronckhorst zijn 12 zwakke wachtwoorden gevonden, 128 wachtwoorden die vaker gebruikt worden en 177 accounts zonder AES-sleutel (beveiligingssleutel). Daarnaast zijn 624 gedeelde accounts gescand waarbij 13 zwakke wachtwoorden zijn gevonden, 142 niet unieke wachtwoorden, 587 accounts waarvan het wachtwoord nooit verloopt, 36 accounts die gebruik maken van een kwetsbare beveiliging, 36 accounts zonder AES-sleutel en 1 account zonder pre-authenticatie. Er zijn geen gekraakte wachtwoorden in combinatie met gebruikersnamen van de gemeente aangetroffen.

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

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 Bronckhorst op dat soort e-mails te testen is op 24-11 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. Het resultaat van de phishingmail aanval is in bijlage 4 opgenomen.

De medewerkers van de gemeente Bronckhorst bleken meer dan gemiddeld vatbaar voor een phishingaanval. Dit was een standaard phishing mail, die vaker is uitgezet bij vergelijkbare organisaties zodat de scores vergeleken kunnen worden. Iets meer dan de helft van de medewerkers, 50,3% van de 459 uitgezette e-mails, heeft op een van de links in de mail geklikt. Het gemiddelde is ca. 35%. Positief is dat een deel van de medewerkers die niet op een van de links van de phishing mail heeft geklikt dat via de reguliere weg bij de CISO en PO heeft gemeld.

Smishing

Criminelen proberen tegenwoordig steeds vaker via sms op een smart-phone 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. Het sms-bericht is in bijlage 5 opgenomen.

Hierbij bleken medewerkers van de gemeente Bronckhorst minder dan gemiddeld vatbaar om op de link te klikken. Ook deze smishing aanval is vaker uitgezet bij vergelijkbare organisaties zodat de scores vergeleken kunnen worden. Iets meer dan 16% van de medewerkers, op 356 uitgezette sms'en, heeft op de link mail geklikt. Het gemiddelde is ca. 19%. Desalniettemin is toch nog een deel van de medewerkers voor de sms-link gevallen.

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?*

Jaarstukken

In de BIO is opgenomen dat de raad minimaal 1x per jaar in het kader van de P&C-cyclus geïnformeerd wordt over informatieveiligheid en privacy. Zoals in veel gemeenten wordt daarbij in Bronckhorst gebruik gemaakt van de dienstverleningsparagraaf in de jaarstukken van de gemeente. In de jaarstukken over 2020, behandeld in de raadsvergadering van 24 juni 2021, wordt gemeld dat digitalisering toeneemt waardoor de onderwerpen informatiebeveiliging en privacy belangrijker en urgenter worden. Voorts worden in het jaarverslag 4 onderwerpen kort toegelicht: vergroten van bewustwording, bedrijfscontinuïteitsmanagement (BCM), ENSIA en de privacy jaarrapportage.

ENSIA

In de jaarstukken 2020 wordt een korte toelichting gegeven over de verantwoording over informatieveiligheid over het jaar 2019 op basis van ENSIA. Gemeld wordt dat de landelijke toezichthouders over 2020 zijn geïnformeerd over de audits op DigID-aansluitingen en Suwinet en de zelfevaluaties in het kader van ENSIA op paspoort- en reisdocumenten en de basisregistraties BAG, BGT en BRO.

De ENSIA-rapportage over 2020 stond als ingekomen stuk op de raads-vergadering van 1 juli 2021, in het kader van de Actieve informatie-voorziening van het college. Hierin wordt kort ingegaan op de zelfevaluaties uitgevoerd in de 2e helft van 2020 op de BRP, Reisdocumenten, 3 DigID-aansluitingen, Suwinet, BAG, BGT en BRO. Gemeld wordt dat de evaluaties voldoende waren, op die van de BRO na, omdat de administratie daarvan nog in opbouw was.

Vermeld wordt de collegeverklaring op de ENSIA over DigID en Suwinet. Specifiek dat de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de normen over Suwinet. En dat bij één van de DigID-aansluitingen niet aan alle normen is voldaan. Daarop is actie ondernomen richting de leverancier. De collegeverklaring is door een onafhankelijk auditor beoordeeld door middel van een assurance rapport. Er zijn bij het ingekomen stuk over de ENSIA geen onderliggende stukken over de zelfevaluaties of de college- en assurance verklaring.

Zoals eerder gemeld is ENSIA bedoeld voor de verantwoording van de uitvoering van informatiebeveiliging en privacy naar de landelijke toezichthouders (verticale verantwoording) en naar de gemeenteraad (horizontale verantwoording.) In ENSIA worden gemeenten een vrije ruimte geboden om de raad nader te informeren op informatiebeveiliging en privacy. Van deze vrije ruimte wordt in Bronckhorst geen gebruik gemaakt.

Auditcommissie

Voor zover we hebben kunnen constateren is de ENSIA-rapportage noch de onderliggende stukken geagendeerd geweest in de auditcommissie. Ook

andere rapportages, zoals de Jaarrapportage gegevensbescherming, bereiken niet de raad. De jaarrapportage is expliciet gericht aan College van B&W en wordt ook besproken in het OT.

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 en privacy bij gemeenten. In de boardletter van de interimcontrole 2021 bij Bronckhorst gaat de accountant niet zeer uitgebreid in op informatiebeveiliging. Maar doet, zoals hiervoor gemeld, aanbevelingen ten aanzien van de actualiteit van het informatie-beveiligingsbeleid in relatie tot ICT-samenwerking, en de service level agreements daaronder. Ten aanzien van de AVG adviseert de accountant een integrale analyse uit te voeren op privacy en de verwerking van persoonsgegevens.

Lastig onderwerp

Voor de raadsleden zijn informatiebeveiliging en privacy lastige onder-werpen. Informatiebeveiliging is een redelijk technisch onderwerp, wat niet meteen in het voorfront van de aandacht ligt. Een deel van raad heeft affiniteit op het terrein, maar een groot deel ook niet. Informatiebeveiliging en privacy komen incidenteel langs bij de raad, zo blijkt uit interviews. Bijvoorbeeld in het presidium als een nieuw privacybeleid moet worden vastgesteld of de audit in het kader van de Wet politiegegevens (Wpg) die eens in de 4 jaar verplicht is als Boa's persoonsgegevens verwerken.

Een deel van de respondenten ziet de raad incidenteel vragen stellen over informatiebeveiliging en privacy. Een ander deel ziet daarop weinig van de raad. Wat als een wake-up-call werd ervaren was de phishing via Whatsapp gericht op de raadsleden. De ambtelijke organisatie kwam daarbij in actie om raadsleden te ondersteunen, ook in de avonduren.

Kaders stellen

In het informatiebeveiligingsbeleid is opgenomen dat het college de kaders stelt. De financiële kaders worden uiteindelijk door de raad gesteld. Respondenten ervaren dat de raad het gevoel heeft dat het allemaal veel kost, en dat voor dat geld ook heel veel andere goede dingen voor de inwoners gedaan kunnen worden. Maar zij zien ook dat het besef aanwezig is dat de investeringen nu eenmaal moeten en dat anders de risico's groter worden.

De raad en informatie-beveiliging en privacy

De raadsleden beschikken zelf ook over persoonsgegevens. De raad is zelf verantwoordelijk voor de eigen bewerkingen, en dat wordt via de griffie opgepakt. Uit de interviews blijkt dat het een open vraagstuk is dat de reguliere email toegankelijk is zonder 2-factor authenticatie (2FA). Daarbij wordt verwezen naar het feit dat in ICT-samenwerking honderden mobiele devices niet onder beheer zijn van I&A van de gemeente Doetinchem, de gastheer van het samenwerkingsverband. Probleem is dat met 2FA raadsleden, bestuurders en ambtenaren buiten de Citrix-omgeving niet meer hun mail kunnen lezen. Bestuurlijk is bekend dat dit een risico is.

7 Toekomstige opgaven

Onderzoeksvraag 5

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

Risico's en kansen

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. Die risico's gelden de gemeentelijke dienstverlening aan inwoners en bedrijven/instellingen, en schept ook een verantwoordelijkheid van de overheid hen te beschermen tegen digitale criminaliteit. 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 tevens 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.

Koppeling van gegevens

Overheden beschikken over een grote hoeveelheid data van hun inwoners en zij zijn enkele jaren geleden enthousiast aan de slag gegaan met de mogelijkheden die big data-methoden bieden. Het gaat daarbij vaak om het koppelen van data uit verschillende bronnen, waarmee data verrijkt wordt en sturingsinformatie gegenereerd kan worden. Soms gaat het om een koppeling van data waarmee groepen geprofileerd konden worden, wat in geval van de Afdeling Toeslagen van de Belastingdienst tot een affaire van ongekende omvang leidde. De AP beoordeelde de jarenlange verwerking van de (dubbele) nationaliteit van aanvragers van kinderopvangtoeslag als onrechtmatig, discriminerend en als een zware overtreding van de AVG. Overheden zijn hierdoor kopschuw geworden voor de koppeling van gegevens, terwijl er ook kansen liggen voor de dienstverlening die ten dienste staat van de inwoners.

Algoritmes

Algoritmes zijn hulpmiddelen op basis van kunstmatige intelligentie, die grote hoeveelheden data kunnen analyseren. Voorbeeld daarvan is machine learning. Kunstmatige intelligentie kan op basis van programmering patronen herkennen in big data, zoals een menselijk brein dat ook zou kunnen. Machine learning kan daarbovenop zelfstandig patronen leren herkennen zoals een menselijk brein zou kunnen leren, maar dan zonder daartoe geprogrammeerd te zijn. Hier hoeft aldus geen mens aan te pas te komen en de wijze waarop de patronen tot stand zijn gekomen is niet altijd herleidbaar. Ook op dit terrein liggen kansen om op basis van big data sturingsinformatie te genereren. Maar ook uitdagingen voor een overheid die transparant besluiten moet nemen.

Datagedreven werken

In Bronckhorst lopen twee trajecten op de digitale agenda. Het programma 'Datagedreven werken in Bronckhorst', dat door respondenten een organisatieveranderprogramma wordt genoemd. Het is de intentie om een proces in te richten waarbij een medewerker die een voorstel moet opstellen ondersteund wordt door big data. Deze intentie is vastgelegd in het collegeprogramma van de periode 2018-2022. Daartoe is een werkgroep ingericht waar de CISO bij betrokken is.

Datalab GO

Daarnaast is er in de Achterhoek de samenwerking met een aantal gemeenten en het CBS in Datalab GO (Gelderland Oost). Bronckhorst is de penvoerder van dit project en de FG en CISO zijn daarbij betrokken. 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. Dus vooralsnog is er geen sprake van een koppeling van persoonsgegevens. Volgens de respondenten is het project nu nog in de fase van verkenning van de mogelijkheden om uit de aanwezige data verrijkte informatie te halen. En is het nog te vroeg om te bepalen of en welke kaders met betrekking tot privacy en informatiebeveiliging nodig zijn.

Het college van B&W is van het jaarprogramma van Datalab GO op de hoogte gesteld en volgens de respondenten is ook de raad daarop geïnformeerd. In het regionale FG-overleg wordt de werkwijze toegelicht, zodat naast Bronckhorst alle deelnemende partijen op de hoogte zijn van

de intentie en de werkwijze van het project. Daarna zijn de partijen aan zet om de afweging te maken of en hoe de informatie ingezet kan worden.

FG betrokken

Bij dit soort projecten en voornemens is de FG op privacy en de CISO op informatieveiligheid betrokken. Zo kon de FG bij een voorstel van een externe partij om te participeren in een pilot voor tekstanalyses op dossiers in het sociaal domein waarschuwen voor de risico's op profilering van inwoners.

Ook is de FG betrokken geweest bij het overleg met de OR bij het opstellen van een protocol over biometrische gegevens bij de entree. De gemeente werkt met vingerafdrukken bij de toegangspoorten en de lockers in het gemeentehuis. Uit de Jaarrapportage Gegevensbescherming blijkt dat een toetsingskader hiervoor werd aangereikt door de boete die een bedrijf kreeg opgelegd door de AP vanwege het ongeoorloofd gebruik van biometrische gegevens.

Ook is er overleg tussen de OR en de FG geweest over de registratie van gegevens op basis van de track&trace op de voertuigen van de gemeente. Hetzelfde geldt voor de logging van de toegang tot gegevens in de applicaties. Niet altijd zijn medewerkers zich bewust van het feit dat hun bewegingen binnen de systemen van de gemeente worden geregistreerd.

Kaders

Privacy is geen absoluut recht en kan bij een zorgvuldige en transparante afweging opzijgeschoven 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 nog geen visie of kader op datagedreven werken ontwikkeld.

Bijlage 1. Geraadpleegde documenten en respondenten

Geraadpleegde documenten

- Gemeentebreed Informatiebeveiligingsbeleid 2019-2021 definitief, 4-12-2018
- Gedragsregels informatiebeveiliging en privacy V3
- Boardletter 2021 Bronckhorst
- Spion op je pad, vragen Bronckhorst
- Datalekregister 2021
- ENSIA assurance-rapport 2020 Gemeente Bronckhorst
- ENSIA assurance-rapport 2019 Gemeente Bronckhorst
- GAP-analyse-BIO-v2.11_Bronckhorst_V0.1
- Jaarrapportage Gegevensbescherming 2020, Aan College van Burgemeester en wethouders, augustus 2021
- Risicoanalyse informatieveiligheid gemeente Bronckhorst 2019
- Protocol noodknop consulenten en handhavers
- Protocol voertuigvolgsysteem
- Protocol cameratoezicht
- Handleiding wachtwoord wijzigen
- Thuiswerken Gemeente Bronckhorst
- Privacyreglement e-mail- en internetgebruik
- Gedragsregels informatiebeveiliging en privacy V3
- Veiligheidsincidenten melden
- Meldplicht datalekken
- Werkplan_IBP_2021_140621
- Zelfevaluaties
- BCM_BCP_Continuiteitsplan-gemeente_Bronckhorst_v1
- BCM_BIA_Bronckhorst_def_aangepast_voor_derden
- IZRM-BRP-Uitwijktest_2021
- Samenwerking ICT Bronckh-Doetin -1
- Samenwerking ICT Bronckh-Doetin -5

Geïnterviewde functionarissen

- Burgemeester
- Gemeentesecretaris
- CISO
- FG

Geïnterviewden cases

Casus 1. Sociaal domein

- Teamleider
- Applicatiebeheerder
- Kwaliteitsmedewerker

Casus 2. Handhaving

- Teamleider
- Applicatiebeheerder
- Juridisch beleidsmedewerker
- Administratief medewerker
- Bouw- en woningtoezichthouder
- BOA

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
BIA	Bedrijfsimpactanalyse, deze wordt gebruikt om inzicht te krijgen in de kritieke processen en om deze te onderscheiden van de niet kritieke processen
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
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 waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
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
IBD	Informatiebeveiligingsdienst voor gemeenten

ICT	Informatie- en communicatietechnologie
IRPA	integrale risico- en privacy-analyse, instrument van IBD voor een integrale GAP- en risicoanalyse
ISMS	Information securitymanagement system
Log4J	Stuk software dat veel gebruikt wordt in webapplicaties en andere systemen, die in december 2021 bleek kwetsbaar te zijn
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 (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
PO	Privacy officer
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.
RI&E	Risico inventarisatie en evaluatie
SIEM/SOC	Security Information & Event Management (SIEM) en Security Operations Center (SOC) software die computerdreigingen monitort
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
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
Wpg	Wet politiegegevens, vanaf 2020 van kracht

Bijlage 3. Onderzoeksvragen en normen

De onderstaande normen zijn grotendeels overgenomen uit het offerteverzoek van de Rekenkamercommissie Bronckhorst. 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 Bronckhorst 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 CISO is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren. - Gegevens zijn goed beschermd tegen ongewenste invloeden van buitenaf.
2. Beschikt de gemeente Bronckhorst 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 e.d. 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 FG 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 4.

Bijlage 5.

Bijlage 6. 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.[3] Hierna behandelen we achtereenvolgens de AVG, de werkwijze in het team, de gebruikte applicaties en dossiers, de toegang tot de gegevens (autorisaties), communicatie, overleg en bewustwording en tot slot datagedreven werken.

AVG

AVG

De AVG vanaf 2016, die vanaf 2018 werd gehandhaafd, heeft de werkwijze volgens de respondenten niet grondig veranderd. De AVG heeft wel voor meer bewustwording gezorgd. De medewerkers en management zijn kritischer naar de werkprocessen gaan kijken. Er is nagedacht over welke informatie echt nodig is voor het werkproces. Daarbij gaat het om data-minimalisatie (niet meer gegevens verzamelen of verwerken strikt noodzakelijk 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.) Dat betekent ook voor het contact met de klant dat transparant uitgelegd moet kunnen worden welke informatie van welke partij nodig is en dat die informatie op basis van persoonlijke toestemming verkregen moet worden. Klanten mogen natuurlijk weigeren, maar dat betekent dat het mogelijk is dat de gemeente hen niet volledig kan helpen. Er moet bijv. een indicatie zijn om huishoudelijke hulp te bieden. Daarvoor zijn gegevens nodig en de zorgaanbieder moet dat ook weten.

Spanningsveld

Beleid op informatiebeveiliging en privacy ondersteunt het werk, maar respondenten constateren een spanning tussen voldoen aan de eisen van de AVG en efficiency in de zin van doorlooptijden. Daarbij gaat het bijvoorbeeld over het verkrijgen van gegevens van een uitkerings-gerechtigde die van de ene gemeente verhuist naar de andere gemeente. Dat gaat niet vanzelfsprekend in het kader van de AVG. Respondenten ervaren daarbij de spanning tussen de dienstverlening aan de inwoner en de beperkende eisen van de AVG.

Verwerkingsregister

De verwerkingen van persoonsgegevens in het sociaal domein zijn opgenomen in het verwerkingsregister. Met betrekking tot het sociaal domein zijn veel regels in het verwerkingsregister opgenomen. Als er een nieuwe verwerking aan de orde is wordt de FG geraadpleegd, mede om te bepalen of een dpia uitgevoerd moet worden. De nieuwe inburgeringswet, per 1-1-2022 ingevoerd, heeft dat proces recent doorlopen. Daar is de regio bij betrokken en het sociaal domein, omdat de gezinnen vaak vraagstukken hebben op meerdere leefgebieden. Daar is een projectgroep voor opgezet

[3] Manager, applicatiebeheerder, kwaliteitsmedewerker (aanspreekpunt/aandachtsfunctionaris voor sociaal domein op het gebied van privacy).

waarbij een van de applicatiebeheerders op onderdelen betrokken is. Daarbij is het pre-dpia format van de FG bij gebruikt.

Werkwijze Sociaal Domein

Vanaf 2014-2015 werkt de gemeente Bronckhorst integraal in het team Sociaal Domein, met wijkteams. Dat wil zeggen overkoepelend voor de Wmo, jeugdzorg en Participatiewet. Daar concentreren we ons in deze casus op, maar ook de Wsw, schuldhulpverlening, leerplicht en leerlingenvervoer vallen onder het sociaal domein. Gevraagd naar (stroom)schema's van werkprocessen merkten de respondenten op dat deze niet op papier staan maar in het systeem.

Wijkteam

Als iemand zich bij wijkteam meldt worden naam, woongegevens en geboortedatum geregistreerd en wordt een afspraak gemaakt. Er wordt gevraagd wat het probleem of vraagstuk is, bijvoorbeeld of er schulden zijn. Dat gegeven wordt niet geregistreerd, maar wordt mondeling gedeeld met de consulent. Pas bij een huisbezoek aan de keukentafel wordt dieper op het probleem of vraagstuk ingegaan door de consulent.

Huisbezoek

Bij het huisbezoek wordt een app gebruikt die vragen naloopt die relevant zijn voor de casus. Tijdens het huisbezoek kan daarmee de problematiek in kaart gebracht worden. In de app zitten vragen op financieel gebied, zorggebied (als het om jeugdproblematiek gaat) en medische gegevens (als het om een Wmo-aanvraag gaat). De consulent vraagt op het eind van het gesprek of de gegevens gedeeld mogen worden met een derde partij, als van die partij dienstverlening afgenomen moet worden.

Van het huisbezoek wordt een gespreksverslag opgesteld. De klanten krijgen dat in te zien en moeten ook voor akkoord tekenen. In het verslag is een vrij veld opgenomen waarin consulenten zaken die opvallen kunnen noteren. Aangezien de klant het verslag ondertekent kan daar niet een persoonlijke observatie in opgenomen worden. Tenminste niet een die de klant niet ook kan zien.

Buitengewone zaken

Wanneer tijdens een huisbezoek buitengewone of criminele zaken worden geconstateerd, zoals een hennepkwekerij, kan daarop bij het cluster Openbare Orde en Veiligheid een melding worden gedaan. Deze kunnen, weer in geval van een hennepkwekerij, de melding doorgeleiden naar de woningbouwvereniging.

Aanvraag Participatiewet

Als het gaat om aanvraag van een uitkering op grond van de Participatiewet vindt de intake niet plaats tijdens een huisbezoek. De klanten worden eerst uitgenodigd op het gemeentehuis en wordt onder andere gevraagd naar scholing, werkervaring en financiële gegevens.

Huisartsen, Raad voor de Kinderbescherming

Er zijn ook andere partijen, zoals huisartsen en Raad voor de kinder-bescherming die jeugdzorg kunnen opstarten. Dat gebeurt op basis van productcodes die voor bepaalde zorg staat, de zogenoemde 30- of 50-codes. Over de medische gegevens die daaronder liggen, zoals de diagnose, beschikt de gemeente niet. Er valt natuurlijk wel wat uit deze categorie af

te leiden, maar niet heel specifiek. Op basis van de code wordt een bij de gemeente bekende zorgleverancier aan de casus gekoppeld. Soms wijzen huisartsen een specifieke zorgverlener aan. Dan krijgt de gemeente alleen een bericht dat de zorg is gestart en periodiek wordt de zorg gefactureerd.

Applicaties en Dossiers

Civision Samenlevingszaken

Het sociaal domein werkt met de applicatie Civision Samenlevingszaken van PinkRoccade, waarin de gegevens van klanten in het kader van de Participatiewet, Wmo en jeugdwet worden verwerkt. Door het integrale werken moesten en konden persoonsgegevens uit meerdere processen verwerkt en gedeeld worden.

De gemeente voert taken in het kader van de Participatiewet zelf uit. De uitkeringsadministratie binnen Civision Samenlevingszaken bevat gegevens over uitkeringen of terugvorderingen, bijzondere bijstand enzovoort. De controle op de gegevens en de registratie verloopt via Suwinet. In de dossiers kunnen ook medische gegevens zitten. Met toestemming van de klant wordt bijvoorbeeld een medisch rapport van een verzekeringsarts opgevraagd. Dat maakt dan onderdeel uit van het dossier in Civision.

Dossiers

Niet alle gegevens worden digitaal verwerkt. Er zijn nog papieren dossiers aanwezig daar niet alle historische en ondertekende dossierbescheiden in Civision aanwezig zijn, zoals beschikkingen. Civision is nog niet aangesloten op het document management systeem (DMS.) De papieren dossiers worden bewaard bij de afdeling DIV. De medewerkers moeten voor inzage in de dossiers deze digitaal aanvragen. De papieren dossiers kunnen in de postvakjes of kluisjes van de medewerkers worden bewaard. Na een mystery guest bezoek is besloten de postvakjes overdag en 's avonds met een rolluik af te sluiten. Afspraak is dat de dossiers op gemeentehuis moeten blijven, maar het is feitelijk mogelijk om ze mee naar buiten te nemen.

Civision Samenlevingszaken van PinkRoccade is niet aangesloten op het zaaksysteem Join van Decos, waar het grootste deel van medewerkers mee werkt. Jaren geleden is tevergeefs geprobeerd de twee systemen te koppelen en het sociaal domein is het enige cluster waar de medewerkers zelf moeten printen, versturen en opbergen. Er waren tijdens corona drie ondersteuners op het gemeentehuis om te kunnen printen voor de consulenten die niet naar het gemeentehuis mochten komen. De dossiers met betrekking tot de leerplicht zijn wel digitaal in Decos aanwezig. Op basis van rollen en functies kunnen binnen Decos documenten afgeschermd worden van toegang door onbevoegden.

Toegang tot gegevens

Rollen

In Civision wordt afhankelijk van de rol en functie toegang gegeven tot gegevens. Het afdelingshoofd en teamleiders bepalen de rollen en de autorisaties, in het centrale zaaksysteem. De drie applicatiebeheerders op Civision maken de toegang mogelijk op basis van die autorisatie door. Andere rollen/functies kunnen niet bij de gegevens komen. De

kwaliteitsmedewerker checkt met regelmaat de autorisaties op personele wijzigingen.

Toegang door derden

De burgerbalie kan de basisgegevens (NAW-gegevens) inzien, maar verder niet verwerken of aanpassen of inhoudelijk inzien. Het komt voor dat een zorgleverancier om inzage in dossiers verzoekt, of een sociaal rechercheur of Boa die bevoegd is in het sociaal domein opsporingen te doen, of een medewerker van het ROC in verband met de leerplicht. Dat kan alleen onder begeleiding van een consulent. Voor de uiteindelijke controle gaat een sociaal rechercheur het gesprek met de klant aan, zonder de consulent daarbij te betrekken. Om de vertrouwensband tussen klant en consulent niet te bezwaren.

Communicatie

Uniek klantnummer

Vóór de AVG werd het BSN gebruikt om klanten in dossiers te identificeren. Nu worden de klantgegevens geanonimiseerd met een uniek klantnummer, op basis waarvan intern gecommuniceerd wordt. Als een consulent op huisbezoek gaat krijgt hij/zij het dossier met een klantnummer en adres. Het adres is in de afsprakenlijst van de consulent bekend. Dat is zo geregeld opdat als er iets gebeurt de gemeente weet waar de consulent naar toe is gegaan. De consulenten hebben ook een noodknop waarop ze bij nood kunnen drukken. Dat is nog nooit gebeurd.

Communicatie en rapportage

Communicatie en rapportage intern over de cases in de Wmo en Participatiewet gaan direct vanuit Civision, zodat niet ergens apart lijsten of gegevens opgeslagen hoeven te worden. Daardoor blijven de raadpleegbare gegevens actueel.

Zorgleveranciers

Als met zorgleveranciers wordt gecommuniceerd, dan worden BSN-nummers gebruikt. Het klantnummer moet dan weer omgezet worden naar een BSN-nummer. Er gaat een bestand met gecodeerde gegevens naar het Gemeentelijk Gegevensknooppunt. De zorgverleners hebben aan hun kant een eigen knooppunt. Dat bestand met gecodeerde gegevens wordt beveiligd verstuurd via Zivver waardoor de zorg geïnitieerd, gestart, gefactureerd en betaald kan worden. In het kader van de PGB's deelt de gemeente ook gegevens met de Sociale verzekeringsbank (SVB.)

Jeugdzorg

De inkoop op jeugdzorg is regionaal georganiseerd. De communicatie daarover verloopt via het documentmanagementsysteem (DMS). Dat is ten behoeve van maandelijkse rapportages met sturingsinformatie over hoeveel en welke zorg geleverd is, de kosten enz. Ook hier zijn BSN-nummers opgenomen, die met een speciaal programma, Pseudo8, de gegevens pseudonomiseert. Het gedeelte met die rapportages, met verslagen van de zorgleverancier, zijn alleen inzichtelijk voor de medewerkers die daartoe geautoriseerd zijn en gecertificeerd zijn door de Stichting Kwaliteitsregister Jeugd (SKJ).

Leerplicht

Via een beveiligde koppeling deelt de gemeente onderwijsgegevens met DUO. Bijvoorbeeld over welke leerlingen bij welke onderwijsinstelling zijn ingeschreven. Die gegevens komen automatisch terecht in de gemeente-

lijke applicatie. In het kader van de inburgeringswet hebben de statushouders uitkeringen nodig en moeten kinderen onderwijs volgen, inburgeringscursussen volgen enz. Daarvoor worden gegevens met DUO en COA uitgewisseld.

Beveiligd verkeer

Beveiligd mailverkeer wordt afgedwongen, o.a. Zivver en de bovengenoemde beveiligde omgevingen. In de regionale aanbesteding voor WMO en Jeugdzorg, wordt daarop gestuurd. De leveranciers moeten aan voorwaarden voldoen, systeemtechnisch, financieel, veiligheid, vakinhoudelijk enz. Onder de contracten liggen verwerkersovereenkomsten, met eisen op informatiebeveiliging. De inkoop is gezamenlijk op 1 volume, afsluiten van contracten gebeurt per individuele gemeente. Controle op de naleving van de contracten wordt gezamenlijk uitgevoerd.

Overleg en bewustwording

Activiteiten en overleg

De algemene activiteiten op bewustwording op informatiebeveiliging en privacy zijn in §5.1.1 langs gekomen, zoals het introductiepakket voor nieuwe medewerkers en serious game *Spion op je pad*. In het Participatieoverleg, het sociaal domein brede overleg, worden de onderwerpen besproken en periodiek komt de FG langs om door te nemen wat er speelt op gegevensbescherming. De kwaliteitsmedewerkers hebben een taak om alert te zijn op kwesties in verband met informatiebeveiliging. Periodiek is er een applicatiebeheerdersoverleg waarin informatiebeveiliging aan bod komt. En er is een informatiebeveiligingswerkgroep waar de applicatiebeheerders in vertegenwoordigd zijn, waarin onder andere incidenten worden besproken.

Onderling wijzen de medewerkers elkaar op gedrag, zoals op een clean desk en clear screen. Het cluster sociaal domein zit dicht bij de ingang en er zijn veel nieuwe collega's in coronatijd bijgekomen. Het voelt voor de medewerkers vervelend om elk nieuw gezicht te vragen wie ze zijn als blijkt dat ze al een tijd voor de gemeente werken. Respondenten geven aan dat ze dat toch doen.

Datalek

Respondenten geven ook aan dat de meldingsbereidheid van datalekken aanwezig is. Zij melden dat recent een mail met persoonsgegevens verkeerd geadresseerd verstuurd werd. Melding daarvan is bij de FG gedaan, het lek is hersteld en de betrokkene is op de hoogte gesteld. In 2021 zijn er 12 datalekken geweest, waarvan uiteindelijk drie gemeld zijn aan de AP.

Datagedreven werken

Dashboards

Respondenten geven aan dat gebruik wordt gemaakt van de mogelijkheden van big data. Zo worden maatwerk overzichten gemaakt om inkoop op jeugdzorg te voorspellen. Er zijn dashboards waar management en teamleiders in kunnen om sturingsinformatie te genereren, op geanonimiseerd en geaggregeerd niveau. Zo viel bijvoorbeeld op dat uit 1 gebied veel aanvragen voor dyslexietesten kwamen. Dat vraagstuk is met

beleidsmakers opgepakt en besproken is wat de redenen daarvan zouden zijn.

Tegelijk geven de respondenten aan dat de gemeente een bulk aan gegevens heeft die beter uitgenut kan worden. Heel gedetailleerd en tot op huishoudensniveau. Respondenten geven aan dat je dan eerst ethische vraagstukken zou moeten beantwoorden.

Bijlage 7. 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.[4] 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

De AVG heeft de werkwijze bij Toezicht en handhaving niet veel gewijzigd. Met persoonsgegevens werd al langer bewust omgegaan, onder de WBP, de voorloper van de AVG. Respondenten geven aan dat de AVG wel heeft aangezet tot bewustwording op een aantal punten, zoals: welke software pakketten worden gebruikt; zijn daarbij de juiste verwerkersovereen-komsten afgesloten; hoe wordt informatie onderling en met derden gedeeld.

De verwerkingen van persoonsgegevens zijn opgenomen in het verwerkingsregister. Door de afdeling is, met hulp van de FG, gecheckt of een risicoanalyse of dpia uitgevoerd moest worden. Dat was niet het geval.

Wpg

De nieuwe 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

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

[4] Gesproken is met de teamleider, applicatiebeheerder, juridisch beleidsmedewerker, administratief medewerker, bouw- en woningtoezichthouder en een van de BOA's.

toegang toe hebben. De gemeente heeft daarop een audit gedaan, met behulp van de FG en een externe auditor. Terwijl dat nog niet verplicht was, zie hierna over de audit.

Corona

De coronapandemie heeft invloed gehad op handhaving. Veel mensen zaten thuis, met de kinderen, en irriteerden zich onderling en in hun omgeving aan kleine dingen. Daarvan kwamen veel meldingen binnen. Waar de afdeling niet op hoefde te acteren was op handhaving van de quarantaineplicht. Dat is regionaal vanuit de GGD en de gemeente Apeldoorn uitgevoerd. Boa's van Apeldoorn controleerden of inwoners van Bronckhorst zich aan de quarantaineplicht hielden. Het cluster Openbare Orde en Veiligheid van de gemeente Bronckhorst kreeg maandelijks een overzicht van de resultaten van die handhavingstaak.

Werkwijze

Meldingen

Bij handhaving gaat het meestal om partijen die het onderling niet eens zijn, of om inwoners die het niet eens zijn met de gemeente. Dat gaat bijna altijd om vertrouwelijkheid en vraagt om zorgvuldige communicatie. Een melding kan telefonisch bij het Klantcontactcentrum (KCC) binnen komen. Dan wordt gevraagd naar het de inhoud van de melding en de contact-gegevens. Dat wordt geregistreerd in Topdesk, software voor helpdesk en registratie. Inwoners kunnen ook via internet zelf een melding doen, dan zijn ze zelf aan zet welke gegevens ze kenbaar maken. Meestal gaat het om naam, telefoonnummer, locatie en de inhoud van de melding (strijdigheid met vergunning, wet- en regelgeving.)

Huisbezoeken

De afdeling verricht ook controles, huisbezoeken, in het kader van de Basisregistratie Personen. Dat betreft bewoningssituaties die niet als zodanig in de basisregistratie zijn opgenomen. Mensen die er wonen maar niet ingeschreven staan en mensen die ingeschreven staan maar niet op dat adres wonen.

Vergunningen

De handhaving strekt zich ook uit tot het toezicht op de verschillende vergunningen. De woningtoezichthouder controleert of hetgeen gebouwd of aangepast wordt in overeenstemming met de afspraken wordt uitgevoerd. Ook houdt de toezichthouder toezicht op de uitvoering van evenementen en alcoholvergunningen.

Verzegeling

Op basis van een bestuurlijke maatregel kunnen Boa's panden verzegelen, bijvoorbeeld als het gaat om drugspanden. Die melding gaat via het Cluster Openbare Orde en Veiligheid naar de toezichthouder/Boa. Deze krijgt de adresgegevens en de strijdigheid en gaat op pad om het pand te verzegelen.

Constateringsrapport

Van het bezoek ter plaatse wordt een constateringsrapport opgemaakt. In constateringsrapport worden locatiegegevens en strijdigheid en de wetgeving opgenomen, bijvoorbeeld aangetroffen elementen die in strijd zijn met het bestemmingsplan. Als er iemand gesproken is en diegene wil daarover teruggekoppeld krijgen, worden ook de inhoud van het gesprek en de contactgegevens opgenomen. Er wordt geregistreerd wat met wie

besproken is. Het constateringsrapport wordt in het zaaksysteem Join opgeslagen, na een digitale handtekening van de toezichthouder.

Niet juridische brief

Vaak wordt in een brief aan de betrokkenen gemeld wat de handhaver heeft geconstateerd en wat er is afgesproken. Met een termijn waarop de eventuele strijdigheid opgelost moet zijn. Na afloop van de termijn wordt gecontroleerd of de strijdigheid is opgelost. Zo ja, dan wordt daar een rapport van opgemaakt en de zaak afgedaan. Zo nee, dan wordt een nieuw constateringsrapport opgemaakt en een vooraankondiging last onder dwangsom of bestuursdwang verstuurd.

Applicaties

Bronnen

De gegevens die de toezichthouders nodig hebben komen uit verschillende bronnen. Inwoners kunnen meldingen via de website doen, of meldingen van burgers bereiken de afdeling via Topdesk vanuit het KCC. Meldingen kunnen ook van andere clusters komen, of van derden, zoals ODA. De gegevens in verband met toezicht op een bouwvergunning komen uit Squit XO. Daar zitten geen verdere persoonsgegevens bij dan de NAW-gegevens. Meldingen over verzegelingen komen van het cluster Openbare Orde en Veiligheid, ook alleen met de benodigde NAW-gegevens.

App

Voor het opmaken van een constateringsrapport gebruiken de toezichthouders een app op het mobiele device. Dat is een SharePoint applicatie. Daarin mogen geen gevoelige politiegegevens verwerkt worden. De app vraagt aan te geven of er politiegegevens worden verwerkt. Zo ja, dan meldt de app om Citycontrol van Sigmax te gebruiken. Dat is een systeem om online te verbaliseren, een beveiligde omgeving waarmee politiegegevens verwerkt mogen worden. Daarin kan onder andere bij een foutparkeerder op basis van het kenteken de gegevens van de kentekenhouder ingezien worden. Citycontrol heeft zelf ook al een eigen check op het verwerken van politiegegevens.

Foto's

Voor de bewijslast is het vaak nuttig situaties vast te leggen door middel van een foto. Daarvoor wordt de app TimeStampFreeCamera gebruikt. Daarmee worden tijd, datum en locatie bij de foto vastgelegd. De foto's worden bij het constateringsrapport gevoegd.

Dossiers

In principe zijn alle dossiers gedigitaliseerd. De Sharepoint app voor de constateringsrapporten is uiteraard al digitaal en alle stukken die worden opgevraagd en bijgehouden worden door DIV gescand in het zaaksysteem Join.

Toegang tot gegevens

Join en Citycontrol

De medewerkers van het team hebben toegang tot de dossiers in Join. De handhavers hebben toegang tot Citycontrol, om onder andere gegevens van kentekenhouders op te halen en politiegegevens te delen. De gemeente deelt geen gegevens met de politie, wel andersom. Er is een keer in de twee weken overleg met de BOA-coördinator van de politie. Daar

worden zaken die de gemeente aangaan besproken. Van die bijeenkomsten worden geen verslagen van gemaakt.

Mutatierapporten

De BOA-coördinator deelt informatie uit zogenoemde mutatierapporten van de politie. Dat zijn over het algemeen kleine zaken die vermeldenswaard zijn. Bijvoorbeeld een kort verslag van wat zij hebben gezien of meegemaakt met betrekking tot jeugdoverlast. Daar wordt in algemene termen over gesproken. Die rapporten worden verder niet gedeeld, alleen BOA's en politie mogen die van elkaar inzien.

Wpg-audit

Op de registratie en verwerking van politiegegevens heeft de gemeente een Wpg-Audit uitgevoerd. Het uiteindelijke resultaat van de audit is nog niet bekend. Gedurende de audit kwam naar voren dat de afdeling al een heleboel procedures goed uitvoert, maar nog niet alles is goed beschreven of wordt goed vastgelegd. Daar komen de meeste verbeterpunten uit naar voren: werkprocessen opstellen en zaken vastleggen.

Communicatie

Beveiligd mailverkeer

Het mailverkeer met persoonsgegevens vanuit en naar de gemeente gebeurt standaard op een beveiligde manier. Vanuit de gemeente met behulp van Zivver. Respondenten geven aan dat dat over het algemeen goed gaat, maar dat Zivver niet altijd goed overweg kan met grote bestanden. Dan wordt wel eens gebruik gemaakt van een oplossing die niet geheel AVG-proof is.

Zo is recent een bulk aan informatie via Wetransfer verstuurd. Dat is niet beveiligd en de gemeente heeft geen verwerkersovereenkomst met bijvoorbeeld Wetransfer om beveiligd te versturen. Het lek is hersteld en hoefde niet aan de AP gemeld te worden. De verbetermaatregel is dat contact gezocht wordt met ICT om een oplossing voor het veilig versturen van grote databestanden.

Gegevens delen

Gegevens op juridisch gebied kunnen worden gedeeld met het Openbaar Ministerie. Dat wordt gedaan door 1 of 2 mensen van het team, in samenspraak met Juridische Zaken. Met opsporingsdiensten als FIOD of SIOD wordt niet gecommuniceerd.

Mutatieformulieren

De gemeente deelt geen gegevens met de politie, wel andersom. De mutatieformulieren krijgt de gemeente via de mail en niet beveiligd. De formulieren mogen verder niet gedeeld worden.

Bestuurlijke rapportage

In opdracht kunnen Boa's panden verzegelen, als het bijvoorbeeld gaat om drugspanden. De Boa's verwerken daarvoor alleen NAW-gegevens. De burgemeester krijgt daarvoor een bestuurlijke rapportage van de politie binnen. In die rapportage kunnen (bijzondere) persoonsgegevens aanwezig zijn. De melding met NAW-gegevens en de strijdigheid gaat naar het cluster Openbare Orde en Veiligheid en vervolgens naar Handhaving. Dat onderlinge mailverkeer gaat beveiligd via Zivver. De juridisch medewerker stelt daarop een besluit op waarna de melding en het besluit in de Zivver-

Join wordt opgeslagen. De toezichthouder gaat op pad om het pand te verzegelen.

Overleg en bewustwording

Contactpersoon

De juridisch medewerker van team Handhaving is het contactpersoon voor privacy, en onderhoudt contact met de FG. De medewerker neemt ook deel aan het privacy team.

Nieuwe medewerkers

Nieuwe medewerkers krijgen een inwerkprogramma. Ter informatie krijgen zij de werkinstructies en het inwerkplan van het team Toezicht en handhaving. De nieuwe medewerkers nemen kennis van de gedragsregels op informatiebeveiliging en privacy, zoals de algemene regels van clean desk/clear screen-beleid. Zij moeten cursussen en trainingen volgen op aspecten als integriteit en privacy. Ook de zittende medewerkers krijgen reminders voor dit soort cursussen, maar deelname is geen verplichting.

Uitdaging

In het inwerkprogramma zijn een aantal werkprocessen geschetst, en zijn werkafspraken gemaakt hoe de zaken gedaan worden en hoe dat wordt vastgelegd. De grootste uitdaging, blijkt uit de interviews, wordt gezien op het vastleggen van de activiteiten en het aantonen van de werking van het beleid. Respondenten vinden dat de aandacht voor protocollen en vastlegging kan doorschieten.

Op teamdagen worden de onderwerpen informatiebeveiliging en privacy besproken. Een van de items was gegevensbeheer en hoe dat verbeterd kan worden. Naar aanleiding daarvan is vorig jaar overgestapt naar Citycontrol, zodat gegevens gekoppeld kunnen worden en minder fouten gemaakt worden.

Risico gegevens delen

Respondenten zien een risico dat persoonsgegevens, ook bijzondere persoonsgegevens, onderling informeel gedeeld worden. Bronckhorst is een kleine overzichtelijke en gemoedelijke samenleving waar iedereen elkaar kent. Met een kleine ambtelijke organisatie, met korte lijnen waarin informatie makkelijk informeel wordt uitgewisseld. Het blijft daarop alert zijn en elkaar bij de les en de spelregels vanuit de AVG proberen te houden.

Wpg audit

Door de uitvoering van de Wpg audit is aandacht voor het onderwerp weer toegenomen. Daardoor is FG beter bekend geworden bij de medewerkers en makkelijker toegankelijk.

Bijlage 8. Volwassenheidsniveau NOREA

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, NBA.

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.