Eindrapport

Onderzoek naar informatiebeveiliging en bescherming persoonsgegevens

Een onderzoek van de rekenkamers van de gemeenten Elburg, Hattem, Nunspeet, Oldebroek en Putten

PARTNERS+PRÖPPER
DENKERS EN DOENERS VOOR DE PUBLIEKE ZAAK

IB&P
Dat gaat je niets aan

Leeswijzer

Rapport A	
Deel 1 De kern	**Deel 1 is voor de lezer die snel de kern tot zich wil nemen.** Het richt zich op de centrale vragen van het onderzoek en kan eigenstandig gelezen worden. Het bevat de inleiding, de conclusies en aanbevelingen. > In het hoofdstuk 'conclusies' wordt de centrale vraag van het onderzoek beantwoord; > In het hoofdstuk 'aanbevelingen' worden aanbevelingen aan de raden en de colleges gedaan; > Het laatste hoofdstuk bevat kernbevindingen per gemeente.
Deel 2 De bevindingen	**Deel 2 is voor de lezer die meer details tot zich wil nemen.** Het bevat een beantwoording van alle deelvragen.
Bijlagen	**Deel 3 bevat de bijlagen.** > Basisbeveiligingsniveaus van de BIO; > Lijst van veel gebruikte termen en afkortingen; > Respondenten en bronnenlijst.

Op het gebied van Informatievoorziening en Automatisering (I&A) werken de gemeenten **Hattem en Oldebroek** per 1 juli 2017 samen in een gemeenschappelijke regeling **H2O** (waarin ook Heerde). Dit is een gemeenschappelijke bedrijfsvoeringorganisatie. H2O biedt automatiseringsdiensten aan en de gemeente Oldebroek fungeert als centrumgemeente voor de informatievoorziening.
In het rapport zullen we de I&A van de gemeenten Hattem en Oldebroek dan ook als één organisatie beschouwen en bevindingen niet apart per gemeente presenteren.

De gemeente Putten werkt samen met de gemeenten Bunschoten, Leusden en Nijkerk op het terrein van I&A. Deze gemeenten behoren echter niet tot de scope van het onderzoek en daarom zal in dit rapport de gemeente **Putten** apart worden behandeld. Dit geldt ook voor de gemeente **Elburg** en **Nunspeet.** De gemeenten Elburg en Nunspeet hebben weliswaar een onderzoek gestart naar samenwerking met de H2O-gemeenten, maar deze samenwerking is nog niet tot stand gekomen.

Colofon

Dit rapportage is opgesteld voor de rekenkamers van de gemeenten Elburg, Hattem, Nunspeet, Oldebroek en Putten. Het is opgesteld door:

> Onderzoekers van het bestuurskundig onderzoeks- en adviesbureau Partners+Pröpper: Ing. Peter Struik MBA en Hilda Sietsema.
> Het adviesbureau IB&P: Erna Havinga MBA CISSP CISM CISA.

Noordwijk, 5 juli 2024

Inhoudsopgave

Deel 1 De kern 4

1 Inleiding 5
2 Vraagstelling 6
3 Evaluatiemodel en afbakening 7
4 Conclusies 8
5 Aanbevelingen 12
6 Algemene kernbevindingen 14
5.1 Algemene kernbevindingen voor alle gemeenten 14
5.2 Kernbevindingen per gemeente 17

Deel 2 De bevindingen 22

1 Ambities en beleid van de gemeenten 23
1.1 Landelijke kaders 26
1.2 Lokale ambities en beleid 27
1.2.1 H2O-gemeenten Hattem en Oldebroek 27
1.2.2 Elburg 31
1.2.3 Nunspeet 32
1.2.4 Putten 33
2 Uitvoering 35
2.1 Vertaling van beleid naar uitvoering 38
2.2 Kwaliteit van het proces 40
2.3 Regie op samenwerking 40
2.4 Financiële middelen 41
2.5 Actuele ontwikkelingen en trends 41
3 Sturing door de raad 44
3.1 Bevoegdheden van de raad en het college 44
3.2 Rolinvulling door de raden in de praktijk 44

Bijlage 1: De basisbeveiligingsniveaus 46
Bijlage 2: Lijst van veel gebruikte termen en afkortingen 47
Bijlage 3: Respondenten en schriftelijke bronnen 48

1

De kern

1 Inleiding

Waarom dit onderzoek?

De samenwerkende rekenkamers van de gemeenten Elburg, Hattem, Nunspeet, Oldebroek en Putten (hierna: de rekenkamer) voerden een gezamenlijk onderzoek uit naar de informatiehuishouding, -veiligheid en bescherming van persoonsgegevens in de vijf gemeenten. Met het onderzoek wil de rekenkamer zicht krijgen op wat de gemeenten willen bereiken met informatiehuishouding en in hoeverre de staat van de informatiebeveiliging en waarborging van privacy voldoet. Dit onderwerp is namelijk van groot belang. De digitalisering neemt alleen maar toe en als de informatiebeveiliging niet op orde is heeft dit grote negatieve gevolgen. Digitalisering heeft natuurlijk ook grote voordelen. Inwoners en bedrijven kunnen online diensten afnemen bij hun gemeenten en informatie raadplegen. Dat levert een gemak voor zowel inwoners en bedrijven. Het heeft ook voordelen voor het gemeentebestuur en de ambtelijke organisatie. Door digitalisering kan in no-time de juiste informatie, op de juiste plek en op het juiste moment beschikbaar zijn voor beleidsontwikkeling, besluitvorming, uitvoering en voor publieke verantwoording. Tegelijkertijd maakt het de overheid ook kwetsbaar. Onbevoegde personen kunnen er namelijk ook misbruik van maken. Dat gebeurt ook in de praktijk en door allerlei incidenten is de aandacht voor informatie-beveiliging en waarborging van privacy dan ook toegenomen, zie het onderstaande kader.

De dreiging neemt ook toe, er is een toename van ransomware-aanvallen (gijzelsoftware).[1] Steeds vaker proberen kwaadwillenden een ingang te vinden en de (potentiële) gevolgen van een aanval worden ook ernstiger. Kwaadwillenden versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken. De Informatiebeveiligingsdienst van de VNG ontving de afgelopen twee jaar steeds meer meldingen van situaties waar gemeentelijke processen langdurig(er) verstoord zijn als gevolg van destructieve gijzelsoftware. Criminelen aarzelen niet om privacygevoelige gegevens van inwoners, bedrijven en medewerkers online te publiceren. Er rust dus een grote verantwoordelijkheid op de schouders van gemeenten. Inwoners en bedrijven verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Informatiebeveiliging en de waarborging van privacy gaan daarbij hand in hand. Zo kan het gevolg van een datalek een inbreuk op de privacy van personen betekenen. Het kan niet alleen schade opleveren voor personen, maar kan ook de reputatie schaden van de overheid.

Cyberaanval

De gemeente Hof van Twente is in 2020 getroffen door een cyberaanval. Medewerkers konden niet langer inloggen op de computersystemen. Bij de aanval is mogelijk 'zeer privacygevoelige informatie' buitgemaakt door de daders. Het datalek is gemeld bij de Autoriteit Persoonsgegevens en andere relevante instanties. *Bron: Hof van Twente in een persverklaring op haar website.*
De gemeente Buren werd in 2022 getroffen door een ransomware-aanval. Bij de hack zijn gegevens van de gemeente gestolen. Vervolgens is een grote hoeveelheid data gepubliceerd op het darkweb. *Bron: Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023-2024, Informatiebeveiligings-dienst (IBD) van de VNG.*
De MIVD en AIVD troffen tijdens een incident response onderzoek een nieuwe Remote Access Trojan (RAT) malware aan. Deze RAT is een gerichte persistente malware die buiten het zicht van traditionele detectiemaatregelen opereert en specifiek voor FortiGate-apparaten is ontwikkeld. *Bron: Nationaal Cyber Security Centrum, 6 februari 2024*

---

[1] Bron: Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023-2024, Informatiebeveiligingsdienst (IBD) van de VNG.

2 Vraagstelling

Centrale vraagstelling

> Wat willen de gemeenten met de informatiehuishouding, in relatie tot informatiebeveiliging en waarborging van privacy, bereiken en wat is of wordt bereikt?
> Voldoet de staat van de informatiebeveiliging en waarborging van privacy?

Deelvragen

Om de centrale vraag te kunnen beantwoorden zijn verschillende deelvragen geformuleerd.

Ambities en beleid

1 Wat zijn de ambities, de doelen en het beleid van de gemeenten ten aanzien van de informatie-huishouding in relatie tot informatiebeveiliging en waarborging van privacy?
   > In hoeverre kent het beleid evalueerbare en/of meetbare ambities en doelen?
2 In welke mate sluit het beleid aan op wet- en regelgeving en op landelijke richtlijnen?

Uitvoering

3 Hoe is het beleid vertaald naar de uitvoering?
4 Wat is de kwaliteit van het proces van informatiehuishouding in relatie tot informatie-beveiliging en waarborging van privacy?
   > Hoe is het risicomanagement vormgegeven?
   > Wordt de kwaliteit van het proces gemonitord, waaronder tenminste de verplichte ENSIA audit?
   > Wordt daarover gerapporteerd, aan wie en hoe wordt indien nodig bijgestuurd?
5 Hoe voeren de gemeenten regie op die zaken waarbij de gemeenten samenwerken met anderen op het terrein van informatiehuishouding, informatiebeveiliging en waarborging van privacy?
6 Hoe wordt het beleid vertaald naar structurele en incidentele financiële lasten die gemoeid zijn met de informatiehuishouding, de informatiebeveiliging en de waarborging van privacy?
7 Wat zijn actuele ontwikkelingen met betrekking tot informatietechnologie, wet- en regelgeving en in hoeverre spelen de gemeenten daarop in?

Resultaten

8 Zijn de beoogde beleids- en uitvoeringsdoelen van de gemeenten, waaronder het voldoen aan landelijk wet- en regelgeving, gehaald en wat zijn verklarende factoren voor het wel of niet realiseren van deze doelen?

Rol van de raad

9 Hoe en met welke informatie worden de raden door het college in positie gebracht om hun kaderstellende rol uit te kunnen oefenen?
10 Hoe en met welke informatie worden de raden door de colleges in positie gebracht om hun controlerende rol uit te kunnen oefenen?

3 Evaluatiemodel en afbakening

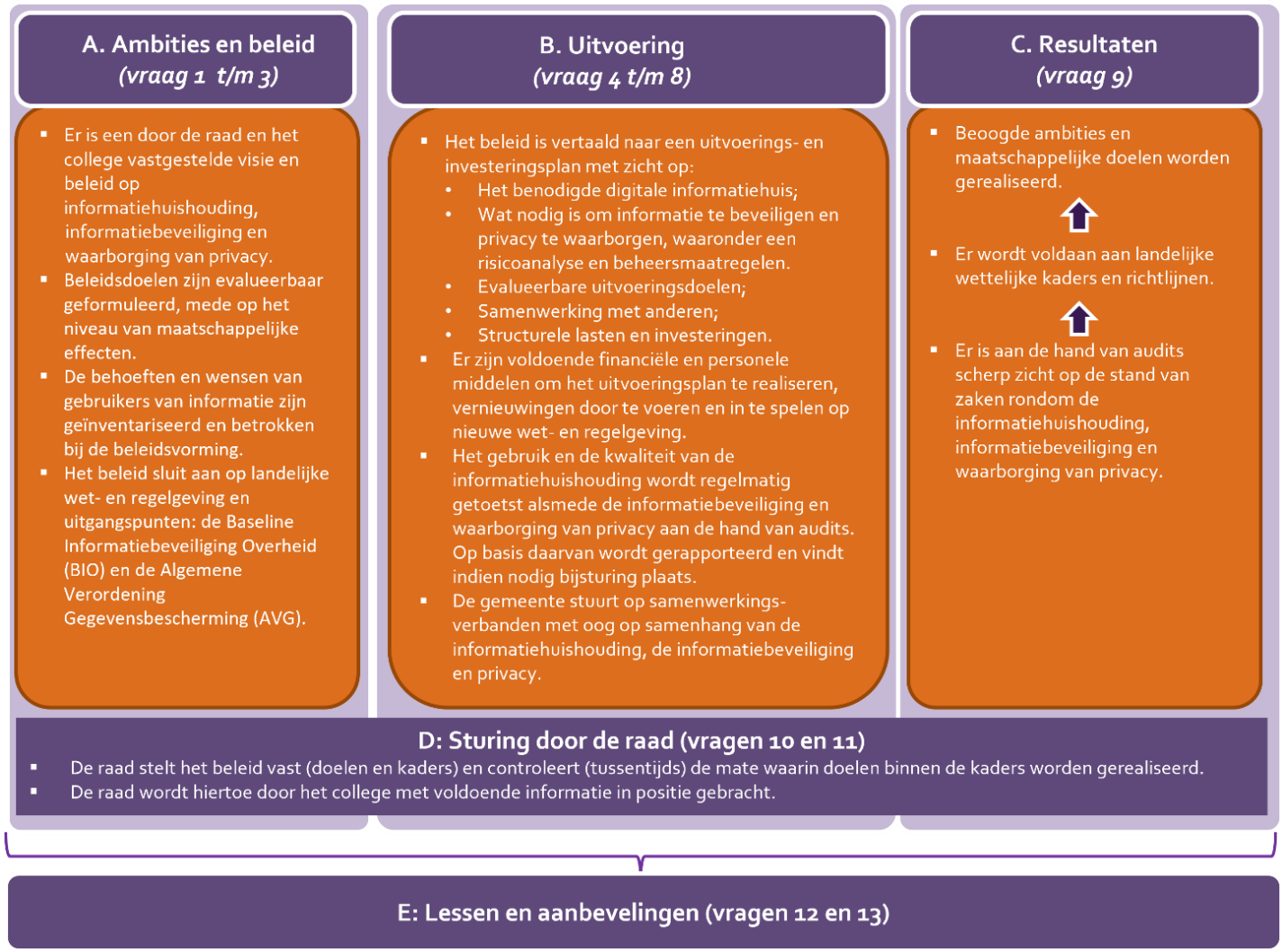
Afbakening

Dit rekenkameronderzoek richt zich op de bestuurlijke- en organisatorische voorwaarden die de gemeente moet invullen om zoveel als mogelijk te waarborgen dat informatie bij de gemeente in goede handen is. Het biedt daarmee geen antwoord op de vraag of de gemeente daadwerkelijk informatie op een veilige wijze verwerkt en opslaat. Dit onderzoek is namelijk geen externe audit op de werking en effecten van informatiebeveiligingsmaatregelen. In dit onderzoek is de gemeente ook niet getest met een stresstest of is geprobeerd de informatiebeveiliging te breken.

Het onderzoek spitst zich toe op de informatiehuishouding van de gemeenten zelf in relatie tot de beveiliging van informatie en de bescherming van persoonsgegevens. Tegelijkertijd verwerken ook verbonden partijen, en andere relevante samenwerkingsverbanden, gegevens voor de gemeenten. De informatiehuishouding van deze partijen valt buiten de reikwijdte van het onderzoek. Wel is bestudeerd in hoeverre de gemeenten regie voeren of sturing geven aan deze partijen rondom eisen met betrekking tot informatiebeveiliging.

Evaluatiemodel

Als 'roer' op het onderzoek is het onderstaande evaluatiemodel gebruikt. Het evaluatiemodel sluit aan op de deelvragen en bevat eveneens de hoofdnormen die gebruikt worden in het onderzoek.



Figuur 3.1: Evaluatiemodel en hoofdnormen.

4 Conclusies

In dit hoofdstuk beantwoorden we de twee centrale vragen:

> Wat willen de gemeenten met de informatiehuishouding, in relatie tot informatiebeveiliging en waarborging van privacy, bereiken en wat is of wordt bereikt?

> Voldoet de staat van de informatiebeveiliging en waarborging van privacy?

Kernconclusie

Beleidsmatig (op papier) is de informatiebeveiliging en waarborging van privacy op orde. Alle vijf gemeenten hebben een identiek informatiebeveiligings- en privacybeleid. Zij streven dezelfde doelen en normen na die zijn ontleend van de landelijke landelijke richtlijn 'Baseline Informatiebeveiliging Overheid (BIO)'.

Ten aanzien van de uitvoering is er nog veel ruimte voor verbetering:

1. De maatschappelijk doelen raken uit het zicht: leveren alle inspanningen daadwerkelijk informatieveiligheid voor inwoners en bedrijven?
2. Er is een landelijk een stelsel van sturings- en controlemechanismen opgetuigd. Dat stelsel is dermate complex dat het in de uitvoering veel onduidelijkheid geeft over rollen, taken en verantwoordelijkheden. Het vraagt heel wat van gemeenten en voor kleinere gemeenten is de uitvoering moeilijk.
3. De raden zijn niet in staat om met de huidige informatie hun controlerende rol op een zinvolle wijze in te vullen.
4. De gemeenten werken in meer of mindere mate samen. De gemeenten Hattem en Oldebroek doen dit het meest intensief met de samenwerking in de gemeenschappelijke regeling H2O. Hoewel niet diepgaand onderzocht, zijn er signalen dat intensieve samenwerking kansen biedt voor gemeenten die dat nog niet doen.
5. Er bestaan tussen de gemeenten verschillende beelden over hoe zij zich verhouden tot verbonden partijen.
6. Tot slot zijn er kansen voor de gemeenten om best-practices over en weer te benutten. Een aantal best-practices zijn in dit onderzoek naar boven gekomen.

We werken de bovenstaande punten verder uit in de onderstaande deelconclusies.

Deelconclusie 1: maatschappelijke doelen geraken uit zicht.

Deze deelconclusie sluit aan op kernbevinding 1 uit paragraaf 6.1 van deel 1 van dit rapport.

De gemeenten richten zich op het inrichten van sturings- en controlmechanismen om te kunnen voldoen aan de normen zoals die gesteld zijn in de Baseline Informatiebeveiliging Overheid (BIO). Zij noemen dit ook wel 'de basis of het huis op orde hebben'. Dat is begrijpelijk maar het zijn in feite voorwaarden die gemeenten moeten invullen om de maatschappelijke doelen op het terrein van informatiebeveiliging te realiseren. Uiteindelijk draait het om de betekenis voor de samenleving; de beoogde maatschappelijke doelen voor inwoners en bedrijven, te weten: beschikbaarheid (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit).

Alle sturings- en controlmechanismen ten spijt, geen van de gemeenten geeft in de jaarrapportages over informatiebeveiliging een helder oordeel over in welke mate deze drie maatschappelijke doelen worden gerealiseerd. De maatschappelijke doelen, en de mate waarin deze worden gerealiseerd, raken uit het zicht. Dit wordt overigens ook landelijk onderkend, zie het onderstaande kader.

Meer aandacht voor informatieveiligheid

Op de VNG-ledenvergadering van juni 2022 namen de leden een motie aan voor meer structurele aandacht en financiering voor informatieveiligheid op lokaal niveau. Ondertekenaars van de motie vroegen de VNG ook zo spoedig mogelijk in gesprek te gaan met BZK over de processen rondom de BIO– en ENSIA-veiligheidsaudits. Die toetsen nu of het vereiste instrumentarium aanwezig is voor beveiliging, maar niet of het ook wordt gebruikt en **in hoeverre het structureel bijdraagt aan daadwerkelijke informatieveiligheid voor inwoners, ondernemers en (gemeentelijke) processen**.
Bron: https://ibestuur.nl/artikel/vng/ensia-verantwoordingsmethodiek-viert-eerste-lustrum/

Deelconclusie 2: in de uitvoering is er - door het complexe stelsel van sturings- en controlemechanismen - nog veel onduidelijkheid over rollen, taken en verantwoordelijkheden.
Deze deelconclusie sluit aan op kernbevindingen 1 en 2 uit paragraaf 6.1 van deel 1 van dit rapport.

Dat er sprake is van een complex stelsel wordt geïllustreerd in het onderstaande kader. Zoals genoemd is dit stelsel in het beleid van de gemeenten verankerd maar is ons inziens voor (kleinere) gemeenten niet eenvoudig uit te voeren.

Een complex stelsel van sturings- en controlemechanismen

Alle gemeenten hebben in hun informatiebeveiligings- en privacybeleid de verschillende functionarissen en rollen beschreven, aansluitend op landelijke regelgeving, waarin deze rollen worden voorgeschreven. Het gaat om de rollen van het College van B&W, de gemeentesecretaris, de Chief Information Officer (CIO), Chief Information Security Officer (CISO), de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG) en de Proceseigenaren.

Het college legt jaarlijks verantwoording af ten aanzien van de informatieveiligheid op basis van de Eenduidige Normatiek Single Information Audit systematiek (ENSIA). De gedachte hierachter is dat met ENSIA het gemeentebestuur met een zelfevaluatie overzicht heeft over de informatieveiligheid van de gemeente en verantwoording kan afleggen aan de gemeenteraad (horizontale verantwoording) en aan de rijksoverheid (verticale verantwoording). Dit met één systematiek dat onder meer uitgaat van de Baseline Informatiebeveiliging Overheid (BIO) en het volgende bundelt: verantwoording over Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Woz, Algemene verordening gegevensbescherming (AVG) en de Gezamenlijke Elektronische Voorzieningen Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Voor de informatiebeveiligingsnormen inzake DigiD en Suwinet bestaat een verantwoordingsplicht aan het rijk door middel van een Assurance van een onafhankelijke IT auditor. Hierover leg het college een collegeverklaring af. De collegeverklaring omvat het voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 3.0 (de Norm v3.0) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.0). De collegeverklaring wordt opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet.

Het complexe stelsel is in de kern gericht op risicomanagement en het afleggen van verantwoording. Alle gemeenten in dit onderzoek zien een cyclus van risicomanagement als belangrijk. Zij hebben echter moeite met het daadwerkelijk implementeren van zo'n cyclus. De eerste stappen van deze cyclus worden uitgevoerd, namelijk het in beeld krijgen van risico's en het formuleren van benodigde maatregelen om risico's weg te nemen of te minimaliseren. De stap

daarna, het uitvoeren van maatregelen en de controle daarop, gaat moeizamer. Beleidsmatig zijn hiertoe proceseigenaren benoemd maar in de praktijk komt deze rol onvoldoende uit de verf. Proceseigenaren zijn managers van afdelingen of teams binnen de primaire processen. Zij hebben de handen al vol hebben aan het managen van de productie en het werkproces waar zij leiding aan geven. Ook is het voor hen niet altijd duidelijk wat hun taak en mandaat is ten aanzien van het nemen van maatregelen, en hoe dit zich verhoudt tot alle andere rollen zoals die van de CIO, CISO, PO en FG. De verdergaande taakdifferentiatie, als gevolg van het onderscheiden van al deze rollen, werkt in de hand dat er juist onduidelijkheid over rolverdeling bestaat en het stimuleert in onvoldoende mate gedeeld eigenaarschap binnen de organisatie.

Deelconclusie 3: de raden zijn niet in staat om met de huidige informatie hun controlerende rol op een zinvolle wijze in te vullen.

Deze deelconclusie sluit aan op kernbevinding 3 uit paragraaf 6.1 van deel 1 van dit rapport.

De raden zien informatiebeveiliging vooral als een randvoorwaardelijke zaak, waarbij geen politieke keuzes spelen. Zij houden zich niet bezig met het controleren van het college of de gemeente aan alle normen van de Baseline Informatiebeveiliging Overheid (BIO) voldoet. Zij vinden het maatschappelijke effect belangrijker. Kernpunten voor raadsleden zijn:[2]

> Dat de essentiële processen van de gemeente altijd door kunnen gaan en de gemeentelijke dienstverlening altijd beschikbaar is voor inwoners en bedrijven;
> Dat informatie niet in de verkeerde handen valt.

De raden ontvangen van het college jaarlijks de rapportages uit ENSIA zelfevaluaties en externe audits rondom informatiebeveiliging en privacy. Deze informatie is bedoeld voor zowel verantwoording naar de raden (horizontale verantwoording) als naar de rijksoverheid (verticale verantwoording). Met deze informatie zijn de raden echter niet in staat om op een eenvoudige wijze een eenduidig oordeel te vormen over de bovenstaande kernpunten.

Deelconclusie 4: intensieve samenwerking biedt kansen.

Deze deelconclusie sluit aan op kernbevinding 4 uit paragraaf 6.1 van deel 1 van dit rapport.

De gemeenten Hattem en Oldebroek gaan een stap verder in de samenwerking dan de andere gemeenten. Hattem en Oldebroek werken samen in de gemeenschappelijke regeling H2O op het gebied van Informatievoorziening en Automatisering. In dit onderzoek hebben we de doelen en resultaten van deze samenwerking niet diepgaand onderzocht. Wel zijn er signalen uit interviews dat er synergievoordelen zijn en het de continuïteit ten goede komt. De organisatie is minder kwetsbaar. Kennis en ervaring kan worden behouden waardoor er kan worden voortgebouwd.

Deelconclusie 5: er bestaan tussen de gemeenten verschillende beelden over hoe zij zich verhouden tot verbonden partijen.

Deze deelconclusie sluit aan op kernbevinding 5 uit paragraaf 6.1 van deel 1 van dit rapport.

In het geval de gemeenten een verbonden partij beschouwen als gegevensverwerker, en de gemeenten als verwerkersverantwoordelijken, dan sluiten de gemeenten een verwerkersovereenkomst af. Ten aanzien van de Omgevingsdienst Noord-Veluwe hebben de gemeenten hierbij niet een gezamenlijke lijn getrokken. Met de Omgevingsdienst Noord-Veluwe is door de H2O gemeenten een verwerkersovereenkomst afgesloten. De gemeenten Nunspeet en Elburg hebben dit niet gedaan.

---

[2] Bron: werkatelier met raadsleden.

Tot slot deelconclusie 6: kansen om best-practices te benutten.

Deze deelconclusie sluit aan op kernbevinding 6 uit paragraaf 6.1 van deel 1 van dit rapport.

De gemeenten kunnen van elkaar leren want er zijn in dit onderzoek best-practices per gemeente naar voren gekomen die over en weer kunnen worden benut. Om herhaling te voorkomen verwijzen we naar de tabel van kernbevinding 6 uit paragraaf 6.1 van deel 1 van dit rapport. In deze tabel zijn de best-practices per gemeente opgenomen.

5 Aanbevelingen

De onderstaande aanbevelingen doet de Rekenkamer. Om het in één stuk te houden nemen we de aanbevelingen van de Rekenkamer in dit rapport integraal over.

Naar aanleiding van de conclusies doet de Rekenkamer 5 aanbevelingen, waarvan 2 aan de gemeenteraden en 3 aan de colleges van B&W.

Aanbevelingen aan de gemeenteraden

Aanbeveling 1: Verbeter het inzicht in de maatschappelijke effecten van het informatieveiligheidsbeleid
Het ontbreekt aan inzicht in de daadwerkelijke effecten van het informatieveiligheidsbeleid. Hoewel de beleidsmatige basis op orde is, kan niet worden beoordeeld hoe effectief het beleid daadwerkelijk is. Door in samenwerking met het college te investeren in rapportages die inzicht geven in de maatschappelijke effecten kan dit inzicht worden verbeterd. Mogelijke instrumenten hiervoor zijn audits op diverse onderdelen van het beleid, maar ook het concreet testen van de veiligheidsmechanismen door bijvoorbeeld de inzet van ethische hackers, mystery guests of het uitvoeren van (technische) pentesten.

Aanbeveling 2: Stuur vervolgens zo nodig op het vergroten van de maatschappelijke effecten
Zodra inzicht ontstaat in de daadwerkelijke effecten, kan worden beoordeeld waar eventuele verbeteringen nodig zijn en welke kosten en inspanningen daarbij acceptabel zijn. Bovendien schrijdt de techniek continu voort, en ook kwaadwillenden ontwikkelen hun werkmethoden continu. Absolute veiligheid kan nooit worden gegarandeerd, maar het bepalen van het juiste ambitieniveau (wat willen we bereiken) en welke inspanningen daarvoor acceptabel zijn (wat gaan we daarvoor doen, wat mag het kosten) lenen zich wel degelijk voor politieke discussie.

Aanbevelingen aan de colleges van B&W

Aanbeveling 3: Investeer in de kwaliteit van uitvoering van het informatieveiligheidsbeleid
Zoals in de conclusies is beschreven, is de uitvoering kwetsbaar. Bij proceseigenaren, die doorgaans geen expert zijn op het gebeid van IT en informatieveiligheid, ontbreekt veelal de kennis om het beleid adequaat uit te voeren. Hierdoor ontstaat een (te) grote druk op de sleutelfunctionarissen en inhoudelijke experts zoals de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO).

Een manier om te zorgen voor een evenwichtiger taakverdeling en vooral beter bewustzijn bij proceseigenaren, is de vorming van een integraal 'opgaveteam' of andere organisatorische vorm. Hierin komen en werken de proceseigenaren en inhoudelijke experts samen en richten zij zich, voorvloeiende uit de periodieke risicoanalyses, op het implementeren van multidisciplinaire maatregelen om de informatiebeveiliging en waarborging van privacy voortdurend op een hoger niveau te brengen.

Een multidisciplinair team is in deze visie verantwoordelijk voor informatiebeveiliging en privacy, en rapporteert aan college en managementteam. De proceseigenaren van de afdelingen staan dus niet alleen, er is sprake van gedeeld eigenaarschap in plaats van individueel eigenaarschap. Aan een dergelijk team kunnen ook, afhankelijk van de aard van een vraagstuk, tijdelijk anderen worden toegevoegd. Bijvoorbeeld als het vraagstuk impact heeft op de processen van samenwerkingspartners zoals verbonden partijen.

Aanbeveling 4: Versterk de regie op samenwerkingspartners en verbonden partijen
De gemeenten hebben qua beleid de basis op orde, maar vertalen dit nog niet altijd naar andere partijen die processen uitvoeren waarvoor de gemeenten wel mede- of eindverantwoordelijk zijn. Door in contracten, gemeenschappelijke regelingen, subsidierelaties etc. dezelfde waarborgen voor informatieveiligheid vast te leggen, kunnen de gemeenten hun beleid ook vertalen naar alle taken die niet door de gemeente alleen worden uitgevoerd.

Aanbeveling 5: Verken de mogelijkheden tot samenwerking
Voor kleinere gemeenten is het een grote uitdaging om voldoende technische beveiligingsmaatregelen te treffen. Schaalvergroting kan daarbij helpend zijn. De H2O samenwerking is hiervan een voorbeeld. Het verdient aanbeveling voor alle 5 gemeenten om de winstkansen van samenwerking te onderzoeken.

6 Algemene kernbevindingen

De bronnen voor dit hoofdstuk bestaan uit:
> De jaarrapportages Informatiebeveiliging van de gemeenten, waarin de resultaten van de jaarlijkse ENSIA-evaluatie zijn verwerkt (bij voorkeur die van 2023, anders die van 2022);
> Interviews met sleutelpersonen.

De ENSIA-evaluatie is een zelfevaluatie waarin vijf onderwerpen aan de orde komen. Wij nemen de uitkomst in hoofdlijnen op (zie de tabellen paragraaf 5.2 per gemeente, kolom Resultaat ENSIA). Wij voegen daar verbeterpunten aan toe, die uit gesprekken in het kader van het onderzoek van de rekenkamers naar voren zijn gekomen (zie de tabellen per gemeente, kolom Verbeterpunten uit gesprekken). Wij voegen tevens toe of de gemeenten maatschappelijke doelen hebben gesteld en of er zicht is op realisatie van deze doelen. Dit is namelijk de hoogste laag waarop de raad kan sturen. ENSIA richt zich op een laag daaronder, namelijk op de uitvoeringsdoelen en -prestaties.

Verder is dit hoofdstuk opgesteld met het oog op de controlerende rol van de raad. Daarmee is zoveel als mogelijk geprobeerd het toegankelijk te maken voor raadsleden, door op hoofdlijnen zaken te benoemen, (technisch) jargon te vermijden en niet perse langs het format te werken van de ENSIA.

6.1 Algemene kernbevindingen voor alle gemeenten

Er zijn een aantal algemene kernbevindingen die voor alle vijf de gemeenten gelden.

1 Alle gemeenten hebben de ENSIA opgenomen in hun beleid als instrument, om periodiek de stand van zaken rondom informatiebeveiliging te evalueren. Met de ENSIA leggen de gemeenten verantwoording af over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, waaronder de vragenlijsten met betrekking tot de BIO, BAG, BRO, DigiD, BGT en Suwinet. Met een verklaring geven de colleges aan in hoeverre de gemeenten voldoen aan de normen en waar nog verbeterpunten zijn. Wat de daadwerkelijke maatschappelijke effecten zijn van het wel of niet realiseren van de normen en de gerapporteerde incidenten is echter niet helder. Is bijvoorbeeld door een of meer incidenten - of het niet voldoen aan een bepaalde norm- de beschikbaarheid van de dienstverlening van de gemeente onder de maat geweest, of is informatie in verkeerde handen gevallen of is de informatie niet meer juist en volledig? Deze vragen worden met de rapportages niet beantwoord.

   Als laatste geven de gemeenten aan dat eerst het huis of de basis op orde moet zijn om verder te kunnen doorgroeien naar een hoger volwassenheidsniveau rondom informatiebeveiliging en waarborging van privacy. Tegelijkertijd geven zij ook aan dat het huis of de basis voortdurend aan verandering onderhevig zal zijn. Ontwikkeling op het terrein van wet- en regelgeving, technologie en cyberaanvallen zullen voortdurend aan de orde zijn.

2 Alle gemeenten zien een cyclus van risicomanagement als belangrijk, maar hebben moeite met het daadwerkelijk implementeren van zo'n cyclus op het gebied van informatiebeveiliging en privacy. In grove lijnen gaat het om het in beeld krijgen van risico's, het inschatten van de zwaarte van een risico, het maken van een plan met maatregelen om de grootste risico's te minimaliseren en het uitvoeren van de maatregelen. De eerste stappen van deze cyclus worden uitgevoerd, namelijk het formuleren en vaststellen van beleid, het uitvoeren van dat beleid, het

regelmatig in beeld krijgen van risico's en het formuleren van benodigde maatregelen om risico's weg te nemen of te minimaliseren.
Hiertoe spelen verschillende organen en functionarissen een rol. Alle gemeenten hebben in hun informatiebeveiligings- en privacybeleid de verschillende rollen beschreven, aansluitend op landelijke regelgeving, waarin deze rollen worden voorgeschreven. Het gaat om de rollen van het College van B&W, de gemeentesecretaris, de Chief Information Officer (CIO), Chief Information Security Officer (CISO), de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG) en de Proceseigenaren.

Bij de aangewezen proceseigenaren is hiertoe de eigen rol binnen de gemeenten echter nog onvoldoende helder. Dit is een belangrijk sluitstuk van de cyclus van risicomanagement. Maatregelen die volgen uit risicoanalyses (en die niet bij de ICT-afdeling liggen) moeten immers ook worden geïdentificeerd, geïmplementeerd en de planning hiervan moet worden bewaakt. In alle gemeenten is de invulling van de rol van de proceseigenaren, weliswaar in verschillende mate, een zorgpunt.

3 De raden hebben geen kaderstellende rol ten aanzien van informatiebeveiliging en privacy. Dit valt geheel binnen de bevoegdheid van het college, waarbij de speelruimte voor het college zeer gering is. Het beleid wordt voornamelijk bepaald door Nationale en Europese wet- en regelgeving. Over het algemeen geven de raden aan de invulling van de controlerende rol moeilijk te vinden. Zij zien informatiebeveiliging en privacy vooral als een randvoorwaardelijke zaak, waarbij geen politieke keuzes spelen. Er is dan ook nauwelijks raadsaandacht voor deze onderwerpen. Het hangt sterk af van de kennis en interesse van individuele raadsleden of er vragen aan het college worden gesteld.

4 Uit de gesprekken blijkt dat samenwerking met andere gemeenten als positief wordt beschouwd. Er wordt kennis en ervaring gedeeld rondom informatiebeveiliging en privacy.

De gemeenten Hattem en Oldebroek gaan daarbij nog een stap verder door samen te werken in een gemeenschappelijke regeling H2O op het gebied van Informatievoorziening en Automatisering. In dit onderzoek hebben we niet diepgaand onderzocht wat de voordelen zijn van deze verdergaande samenwerking. Wel zijn er signalen dat er voordelen zijn. Die worden genoemd in interviews in het kader van dit onderzoek, te weten:

> De samenwerking in H2O verband bieden de betrokken gemeenten kansen voor synergie zoals een gezamenlijke inkoop of gezamenlijke ontwikkelingen van oplossingen die bijdragen aan het verbeteren van informatiebeveiliging en privacybescherming.
> Ook biedt het voordelen ten aanzien van de continuïteit. Kleinere gemeenten zijn kwetsbaar voor personeelsverloop in combinatie met een krappe arbeidsmarkt. Kennis en ervaring dat wordt opgebouwd kan onvoldoende worden vastgehouden en daarop kan onvoldoende worden voortgebouwd. Er is dan veelal sprake van voortdurend achter de feiten aanlopen en brandjes blussen.

Echter, zoals bij elke vorm van samenwerking, kunnen er ook uitdagingen zijn. Enkele uitdagingen die in interviews worden genoemd zijn:

> Verschillen van volwassenheidsniveau van informatiebeveiliging en privacy tussen gemeenten kunnen de samenwerking bemoeilijken.
> Het op één lijn brengen van beleid, procedures en oplossingen tussen verschillende gemeenten kan complex zijn.
> Het gezamenlijk toewijzen van middelen (financieel en personeel) voor samenwerkingsinitiatieven kan een uitdaging vormen, vooral als er concurrerende prioriteiten tussen en binnen de afzonderlijke gemeenten zijn.

> Educatie van het personeel (bewustwording) is nodig maar dat gebeurt nog niet volgens een bewustwordingsplan, dat ook daadwerkelijk getoetst kan worden op doeltreffendheid.

5 Een deel van de taken van gemeenten worden uitgevoerd door verbonden partijen of private partijen. In het geval de gemeenten een verbonden partij beschouwen als gegevensverwerker, en de gemeenten als verwerkersverantwoordelijken, dan sluiten de gemeenten een verwerkersovereenkomst af. Hier bestaan tussen de gemeenten wel verschillende beelden over. Bijvoorbeeld rondom de Omgevingsdienst Noord-Veluwe. De Omgevingsdienst Noord-Veluwe kwalificeert zichzelf, op basis van advies van de landsadvocaat Pels Rijcken, als verwerker.[3] Met de Omgevingsdienst Noord-Veluwe is door de H2O gemeenten reeds in 2017 een verwerkersovereenkomst afgesloten.[4] De gemeenten Nunspeet en Elburg hebben dit niet gedaan.[5] Van de gemeente Putten hebben de onderzoekers hierover geen stukken ontvangen.

Met de verwerkersovereenkomsten is toezicht en controle door de gemeenten mogelijk. Het volgende is daartoe opgenomen in de verwerkersovereenkomsten:
> De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm;
> De toereikendheid van de informatiebeveiliging blijkt uit eigen controles, certificering, en/of uit externe audits.

6 De gemeenten kunnen van elkaar leren. In dit onderzoek zijn best-practices per gemeente naar voren gekomen die over en weer kunnen worden benut, zie onderstaande tabel.

Leerpunt te benutten door de andere gemeenten	
Elburg	> Elburg heeft een uitgebreide continuïteitsstrategie ontwikkeld met evalueerbare doelen voor de beschikbaarheid van informatiesystemen voor kritische bedrijfsprocessen. Andere gemeenten kunnen hiervan leren door duidelijke prioriteiten te stellen voor herstel van bedrijfsprocessen bij uitval. Op basis van beveiligingsincidenten wordt het proces herzien/geëvalueerd. > Er is een procedure vastgesteld waarbij een risicoafweging voor toegang tot informatiesystemen door externe leveranciers deel uitmaakt. Andere gemeenten kunnen deze procedure overnemen/verbeteren om de veiligheid van externe samenwerkingen te waarborgen. > De ambitie leeft bij Elburg om security en privacy-by-design in te voeren. Mogelijk kan dit in samenwerking met de betrokken gemeenten om zo tot een gezamenlijk plan te komen en dit vervolgens binnen de organisatie te implementeren.
Nunspeet	> Nunspeet heeft een notitie opgesteld met betrekking tot bewustwording voor informatiebeveiliging en bescherming van persoonsgegevens. Hoewel nog summier, kan dit als startpunt dienen voor andere gemeenten om vergelijkbare plannen te ontwikkelen. > Nunspeet onderzoekt kansen voor regionale samenwerking op het gebied van informatisering en automatisering. Gemeenten kunnen hiervan leren om samenwerkingsverbanden te versterken en gezamenlijke continuïteitsplannen te ontwikkelen

3 Bron: Opdrachtgeversoverleg Omgevingsdienst Noord-Veluwe, 12 januari 2023.
4 Bron: Verwerkersovereenkomst gemeente Oldebroek met ODNV, tevens bruikbaar in H2O verband, april 2017.
5 Bronnen: e-mail van Elburg d.d. 11 december 2023, e-mail van Nunspeet d.d. 8 december 2023.

Putten	> Putten werkt aan de implementatie van een Informatie Securitymanagement System, een cyclisch proces om informatiebeveiliging te borgen. Dit systeem omvat het opstellen van de PDCA-cyclus, wat als een gedetailleerde blauwdruk kan dienen voor andere gemeenten. > In het beleid van Putten is de werkwijze voor risicomanagement expliciet uitgewerkt in het beleidsplan. Alle gegevensverzamelingen en -applicaties worden toegewezen aan een eigenaar en geclassificeerd op risicoklassen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid en de basisbeveiligingsniveaus worden vastgesteld.
Oldebroek en Hattem (H2O)	> H2O heeft specifieke kernwaarden en een privacybeleid opgesteld, wat richting geeft aan de werkwijze van de gemeente. Deze aanpak kan helpen bij het ontwikkelen van een cultuur van zorgvuldige omgang met persoonsgegevens . > H2O en gemeente Elburg hebben een ENSIA rapportage format gebruikt om te rapporteren over de ENSIA resultaten. Wellicht is dit ook toepasbaar bij gemeente Nunspeet en Putten om meer inzicht in de resultaten te communiceren richting de Raad. > Oldebroek en Hattem werken intensief samen in de gemeenschappelijke regeling H2O. In het geval de andere gemeenten ook een intensievere samenwerking onderzoeken en overwegen is het raadzaam de ervaringen van H2O mee te nemen.

6.2 Kernbevindingen per gemeente

Zie de overzichten op de volgende bladzijde.

2O-gemeenten Hattem en Oldebroek

Maatschappelijke doen en resultaten

Maatschappelijke doelen worden niet expliciet geformuleerd in termen van de betekenis voor inwoners en bedrijven.

Er zijn in 2022 in totaal 22 incidenten geregistreerd. Er is vanuit de rapportages niet op te maken wat de gevolgen zijn geweest van deze incidenten voor inwoners en bedrijven en/of deze acceptabel zijn geweest.

Uitvoeringsdoelen en -prestaties

Onderwerp en conform de richtlijn BIO	Resultaat ENSIA	Verbeterpunten uit de gesprekken
Informatiebeveiligingsbeleid en organisatie Er is een actueel beleid en organisatie van informatiebeveiliging en controle op naleving.		• Steevast wordt nog gesproken over 'het accent ligt op huis op orde'. Tegelijkertijd is er het besef dat het huis permanent aan verandering onderhevig zal zijn. • Aanpak risicomanagement moet nog worden beschreven. • Beleidsmatig is de regie op informatiebeveiliging op orde, de implementatie van regie is nog te verbeteren. • Uitvoering van het beleid is soms moeizaam. Verschillende lagen van de organisatie houden er, vanwege gemak, ook alternatieve werkwijzen erop na. • Meer aandacht voor bewustwording is nodig. Niet alle medewerkers zijn zich bewust van hun rol en verantwoordelijkheden rondom informatiebeveiliging.
Personeel en toegang Juiste toegang voor medewerkers tot systemen en gegevens.		
Continuïteit en incidenten Zorgen voor continuïteit van de gemeentelijke dienstverlening en adequate opvolging incidenten.		• Incidenten hebben tot verhoogde aandacht geleid, maar structurele borging van risicoanalyses en investeringsplannen ontbreekt. • Er is geen structurele monitoring en evaluatie van incidenten en continuïteitsplannen.
Leveranciersmanagement Veilige omgang met informatiesystemen en afspraken hierover met leveranciers.		• Samenwerking met leveranciers biedt kansen maar vereist heldere afspraken en borging van verantwoordelijkheden. • Er is geen volledig overzicht van alle contracten en de beveiligingseisen die aan leveranciers worden gesteld.
Databescherming Veilige omgang met data in de software.		• Bewustzijn en implementatie van databeschermingsmaatregelen varieert. • Specifieke activiteiten voor databescherming zijn aanwezig, maar niet altijd gestructureerd.

Gemeente Elburg

Maatschappelijke doelen en resultaten

Maatschappelijke doelen worden niet expliciet geformuleerd in termen van de betekenis voor inwoners en bedrijven.

Onderzoekers hebben geen specifiek verslag informatieveiligheid over 2022 ontvangen. In de jaarstukken 2022 wordt wel aangegeven dat er minder incidenten zijn gemeld dan in 2021. Er wordt verder niet aangegeven of incidenten gevolgen hadden voor inwoners en bedrijven en/of deze acceptabel zijn geweest.

Uitvoeringsdoelen en -prestaties

Onderwerp en conform de richtlijn BIO	Resultaat ENSIA	Verbeterpunten uit de gesprekken
Informatiebeveiligingsbeleid en organisatie Er is een actueel beleid en organisatie van informatiebeveiliging en controle op naleving.		• Een aanzet tot een bewustwordingsplan is opgesteld, moet nog worden uitgebreid. • Het is wenselijk om met de raad een meerjarig investeringsplan met projecten te kunnen bespreken. • De personele capaciteit en kennis is onvoldoende om zaken op te pakken.
Personeel en toegang Juiste toegang voor medewerkers tot systemen en gegevens.		• De gemeente kampt met verloop aan medewerkers, daarmee is het uitdagend om het beleid te implementeren. Op technisch vlak lukt dit wel omdat maatregelen afgedwongen kunnen worden, op organisatorisch vlak is dit moeilijker. • Bewustwordingsactiviteiten zijn aanwezig, maar niet verplicht en soms onvoldoende.
Continuïteit en incidenten Zorgen voor continuïteit van de gemeentelijke dienstverlening en adequate opvolging incidenten.		• Nog teveel brandjes blussen, hoger volwassenheidsniveau is nodig volgens de organisatie. Daar worden wel stappen gezet bij bijv. verbeteren Incidentmanagement. • Er zijn in het verleden beveiligingsincidenten geweest, op basis hiervan is het proces van incidentenmanagement herzien. Incidentenmanagement- en responsprotocol is opgesteld in 2022.
Leveranciersmanagement Veilige omgang met informatiesystemen en afspraken hierover met leveranciers.		• De ambitie is om informatiebeveiliging en privacy 'by-design' in te richten. De beschikbaarheid van mensen en middelen is hier een barrière. • Nog geen regie op verbonden partijen ten aanzien van informatiebeveiliging.
Databescherming Veilige omgang met data in onze software.		• Privacybeleid is onvoldoende en wordt momenteel herzien. • Privacyfunctionarissen worden te laat of ad hoc betrokken bij projecten. • Dataclassificatie, DPIA's e.d. worden niet consequent uitgevoerd.

Gemeente Nunspeet

Maatschappelijke doelen en resultaten

Maatschappelijke doelen worden niet expliciet geformuleerd in termen van de betekenis voor inwoners en bedrijven.

Er zijn in 2022 43 incidenten geweest. De meeste incidenten hadden geen onacceptabel gevolgen. Eén keer was vanwege te grote kwetsbaarheid de dienstverlening aan burgers enkele dagen niet mogelijk.

Uitvoeringsdoelen en -prestaties

Onderwerp en conform de richtlijn BIO	Resultaat ENSIA	Verbeterpunten uit de gesprekken
Informatiebeveiligingsbeleid en organisatie Er is een actueel beleid en organisatie van informatiebeveiliging en controle op naleving.	ENSIA is wel uitgevoerd. De jaarrapportage bevat geen eindoordeel over de vijf onderwerpen.	• Steevast wordt nog gesproken over 'het accent ligt op basis op orde'. Tegelijkertijd is er het besef dat de basis permanent aan verandering onderhevig zal zijn. • Proceseigenaren zijn druk bezig met processen, nog onvoldoende tijd voor bewustwording
Personeel en toegang Juiste toegang voor medewerkers tot systemen en gegevens.		• Niet alle processen op het gebied van informatiebeveiliging en privacy zijn formeel gedocumenteerd of gestandaardiseerd. • Er is in de uitvoering een gebrek aan duidelijkheid over de rollen en verantwoordelijkheden op het gebied van informatiebeveiliging en privacy zoals deze in het beleid zijn beschreven.
Continuïteit en incidenten Zorgen voor continuïteit van de gemeentelijke dienstverlening en adequate opvolging incidenten.		• Risicoanalyse op het terrein van privacy frequenter uitvoeren en maatregelen monitoren. • Kwetsbaarheid door onvoldoende protocolleren van werkzaamheden. Inhoudelijke kennis over welke (technische) beveiligingsmaatregelen er zijn moet worden vastgelegd. • De mogelijkheid om uit te wijken naar andere IT-omgeving is nog niet gerealiseerd.
Leveranciersmanagement Veilige omgang met informatiesystemen en afspraken hierover met leveranciers.		• Nog geen formeel toezicht op verbonden partijen of controle op leveranciers. • Geen specifieke voorafgaande eisen opgesteld voor samenwerkingsverbanden op het gebied van informatiebeveiliging en privacy
Databescherming Veilige omgang met data in onze software.		• Verwacht wordt dat niet alle datalekken worden herken en/of gemeld. • Verwerkersovereenkomsten worden met derden opgesteld, maar toezicht is nog niet formeel ingericht.

Gemeente Putten

Maatschappelijke doelen en resultaten

Maatschappelijke doelen worden niet expliciet geformuleerd in termen van de betekenis voor inwoners en bedrijven.

Onderzoekers hebben geen specifiek verslag informatieveiligheid over 2022 ontvangen. Er is niet op te maken wat de gevolgen zijn geweest van eventuele deze incidenten voor inwoners en bedrijven en/of deze acceptabel zijn geweest.

Uitvoeringsdoelen en -prestaties

Onderwerp en conform de richtlijn BIO	Resultaat ENSIA	Verbeterpunten uit de gesprekken
Informatiebeveiligingsbeleid en organisatie Er is een actueel beleid en organisatie van informatiebeveiliging en controle op naleving.	ENSIA is wel uitgevoerd. De jaarrapportage bevat geen eindoordeel over de vijf onderwerpen.	• Beleid op het gebied van informatiebeveiliging is verouderd en biedt onvoldoende kaders. • Er is een overkoepelend beleid. Er is nog behoefte aan deelbeleid voor domeinen waar verwerking van bijzondere persoonsgegevens aan de orde is. • Onvoldoende governance en onduidelijke rollen, vooral rondom proceseigenaren.
Personeel en toegang Juiste toegang voor medewerkers tot systemen en gegevens.		• Er is geen scherp zicht op de stand van zaken van de uitvoering van een actieplan op basis van de GAP-analyse. • Nog geen eigen vaste CISO, rol wordt nu a.i. ingevuld voor 20 uur per week.
Continuïteit en incidenten Zorgen voor continuïteit van de gemeentelijke dienstverlening en adequate opvolging incidenten.		• Risicomanagement is nog niet breed geïmplementeerd. Veel zaken worden nog ad hoc opgepakt. Proceseigenaren moeten nog in positie worden gebracht om de eisen met betrekking tot bedrijfscontinuïteit binnen hun eigen processen te inventariseren.
Leveranciersmanagenent Veilige omgang met informatiesystemen en afspraken hierover met leveranciers.		• Er wordt nog niet toegezien op verbonden partijen m.b.t. informatiebeveiliging. • Verwerkersovereenkomsten worden opgesteld, maar onduidelijk of dit bij elk contract is gebeurd en of hier op wordt toegezien.
Databescherming Veilige omgang met data in onze software.		• Privacy-by-design wordt toegepast, maar monitoring en evaluatie ontbreken grotendeels

2

De bevindingen

1 Ambities en beleid van de gemeenten

In dit hoofdstuk worden de deelvragen 1 en 2 beantwoord. De lezer die snel zicht wil krijgen op de antwoorden kan de korte beantwoording lezen direct onder het onderstaande kader. De lezer die meer details tot zich wil nemen kan de daaropvolgende paragrafen raadplegen waarin we uitgebreider ingaan op de verschillende deelvragen.

DEELVRAGEN

1 Wat zijn de ambities, de doelen en het beleid van de gemeenten ten aanzien van de informatiehuishouding in relatie tot informatiebeveiliging en waarborging van privacy?
   > In hoeverre kent het beleid evalueerbare en/of meetbare ambities en doelen?
2 In welke mate sluit het beleid aan op wet- en regelgeving en landelijke richtlijnen?

TOEGEPASTE NORMEN

- Er is een door de raad en/of het college vastgestelde visie en beleid op informatiehuishouding, informatiebeveiliging en waarborging van privacy;
- Beleidsdoelen zijn evalueerbaar geformuleerd, mede op het niveau van maatschappelijke effecten;
- De behoeften en wensen van gebruikers van informatie zijn geïnventariseerd en betrokken bij de beleidsvorming;
- Het beleid sluit aan op Nationale en Europese wet- en regelgeving en uitgangspunten: de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG).

Korte beantwoording van de deelvragen

INFORMATIEBEVEILIGINGSBELEID

1 Alle vijf gemeenten hebben een nagenoeg identiek informatiebeveiligingsbeleid, waarin doelen en processen zijn beschreven voor de beveiliging van informatie. Dat beleid is vastgesteld door de colleges en de raden zijn daarvan in kennis gesteld.

De gemeenten volgen met het beleid de landelijke richtlijn 'Baseline Informatiebeveiliging Overheid (BIO)'. De BIO gaat uit van drie kerncriteria voor informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De BIO biedt de gemeenten keuzes voor verschillende beveiligingsniveaus. Er worden van licht naar zwaar drie niveaus onderscheiden, te weten: BBN1, BBN2 en BBN3. Het niveau is zwaarder in het geval kennisname van informatie door ongeautoriseerde buitenstaanders leidt tot grotere negatieve gevolgen voor het openbaar bestuur en de samenleving. Het gaat daarbij om financiële gevolgen voor de overheid, politieke gevolgen voor het openbaar bestuur, het vertrouwen van burgers in de overheid en ongemak of zelfs schade voor burgers. Als een gemeente een bepaald beveiligingsniveau nastreeft, heeft de gemeente daarmee dus een beleidsdoel op het niveau van bestuurlijke- en maatschappelijke effecten geformuleerd. BBN3 is overigens niet van toepassing voor gemeenten maar voor de ministeries van het rijk. De Informatiebeveiligingsdienst (IBD) van de VNG heeft voor gemeenten hiertoe voor gemeenten een tussenniveau BBN2+ voorgeschreven, dat van toepassing is als systemen aan een zwaardere eis moeten voldoen dan BBN2. Verder heeft de Informatiebeveiligingsdienst van de VNG aangegeven dat BBN2 hoe dan ook het basisniveau is voor de gemeenten.

De gemeenten benoemen in hun beleid wel de mogelijke beveiligingsniveaus, maar niet alle gemeenten stellen expliciet een bepaald beveiligingsniveau als beleidsdoel vast. Dat gebeurd niet in algemene zin maar ook niet per kerncriterium. Hiermee zijn de beleidsdoelen niet evalueerbaar

geformuleerd. Een uitzondering is de gemeente Putten en de gemeente Elburg. Deze gemeenten stellen expliciet in het beleid dat alle informatiesystemen worden geclassificeerd op risicoklassen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. Beveiligingsniveaus worden hierop vastgesteld; Putten en Elburg hanteren gemeentebreed het basisniveau BBN2, dat overigens het landelijk vastgestelde niveau is.

Zoals eerder genoemd is het informatiebeveiligingsbeleid van alle gemeenten verder in de basis nagenoeg identiek. Verschillen zijn er in de mate waarin deelonderwerpen worden belicht en uitgewerkt. We lichten dat hieronder verder toe.

a **De H2O gemeenten (Hattem en Oldebroek)** belichten, naast informatiebeveiliging, de thema's waaraan de gemeenten de komende jaren willen werken. Belangrijke hoofdlijnen zijn gericht op enerzijds standaardisatie en anderzijds voldoende flexibiliteit te behouden om in te kunnen spelen op de behoefte van gebruikers en nieuwe ontwikkelingen. Deze hoofdlijnen zijn:
> Verder bouwen aan een stevige basis rondom het werken onder één architectuur, om meer grip te krijgen. Projecten zijn niet meer vrij om hun 'eigen beste' oplossing te kiezen;
> Digitale dienstverlening zodanig inrichten dat de klant centraal staat en in samenhang en harmonie brengen van behoeften van gebruikers (vraag) en informatiesystemen (aanbod). Dit met oog op het realiseren van de doelen van het bestuur en de organisatie als geheel. Daarmee maakt een inventarisatie van behoeften en wensen van gebruikers deel uit van beleidsvorming;
> Het vergroten van het bewustzijn van bestuurders en medewerkers over informatie veiligheid en privacy.
Uit gesprekken in het kader van dit onderzoek blijkt dat alternatieve werkwijzen worden gekozen. Bijvoorbeeld: Zivver (programma wat zorgt dat e-mails versleuteld worden verstuurd). Verschillende lagen van de organisatie (ook raad en college) vinden het toch moeizaam om hiermee te werken. Hierdoor worden ook alternatieve werkwijzen eropna gehouden om het Zivver-programma te ontwijken. Hierdoor wordt waarschijnlijk nog onveiliger gewerkt en wordt de ambitie/doel vanuit het informatiebeveiligingsbeleid niet gehaald. Het lijkt soms een keurslijf waar je in wordt gedrukt, waar je niet meer aan ontkomt, en dat geeft ook wrijving. Aanvullende bewustwording rondom de noodzaak en de mogelijke gevolgen of risico's van dit gedrag kan het gedrag veranderen.

b **De gemeente Elburg heeft:**
> Een strategie voor continuïteit uitgewerkt met daarbij evalueerbare doelen ten aanzien van de beschikbaarheid van informatiesystemen voor kritische bedrijfsprocessen;
> Het logische toegangsbeleid uitgewerkt dat ingaat op processen en procedures voor het toewijzen van autorisaties en toegangsrechten, inloggen en authenticatie en opschonen van niet gebruikte accounts;
> Een procedure vastgesteld voor externe leveranciers, waar een risicoafweging voor toegang tot informatiesystemen deel van uitmaakt.

c **De gemeente Nunspeet** heeft een korte notitie met betrekking tot bewustwording voor informatiebeveiliging en bescherming van persoonsgegevens opgesteld. Daarbij merken we op dat dit inhoudelijk nog zeer summier is en nog niet voldoet aan de template/handreiking zoals die is opgesteld door de IBD. Alle gemeenten maken overigens gebruik van een Bewustwording Management Systeem. Dat systeem voorziet in basistrainingen voor nieuwe medewerkers en herhalingsmodules, specifieke trainingen voor medewerkers die toegang hebben tot Suwinet of een module Privacy.

d **De gemeente Putten** werkt het zogeheten 'Information Security Management System' verder uit. Dat is een cyclisch proces dat wordt doorlopen om informatiebeveiliging te borgen. Het bestaat uit vier stappen: Opstellen van Informatiebeveiligingsbeleid, Informatieveiligheidsanalyse, Actieplan en als laatste stap Technische en Organisatorische maatregelen.

2 Het beleid van alle vijf gemeenten sluit aan op landelijke wetgeving en -richtlijnen zoals de Baseline Informatiebeveiliging Overheid (BIO), de Algemene Verordening Persoonsgegevens (AVG) en aanvullende beveiligingseisen voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).

Privacybeleid

Alle vijf gemeenten hebben een privacybeleid. Dat beleid is vastgesteld door de colleges en de raden zijn daarvan in kennis gesteld. Rondom het waarborgen van privacy moet rekening worden gehouden met allerlei wet- en regelgeving, wat het complex maakt. Het beleid van de gemeenten sluit hier op aan. De belangrijkste is de Algemene Verordening Gegevensbescherming (AVG). Daarnaast zijn er andere bijzondere wetten die ook iets zeggen over het gebruik van persoonsgegevens. Het gaat om de Wet open overheid (Woo), de Wet basisregistratie personen (Wet BRP), de Wet maatschappelijke ondersteuning (Wmo), de Wet politiegegevens (Wpg), de Jeugdwet en de Archiefwet.

De gemeenten Oldebroek besteedt in het privacybeleid ook aandacht aan de beveiliging van persoons-gegevens en voor het sociaal domein is een apart privacybeleid opgesteld. De gemeente heeft dit gedaan omdat dit domein een aantal specifieke aandachtspunten met zich mee brengt. Het gaat om het gebruik van bijzondere persoonsgegevens en de samenwerking met andere overheidsorganisaties en zorg- en hulpverleners.

Overkoepelend

De gemeenten Hattem, Oldebroek en Putten beschrijven in hun beleid de kernwaarden en principes of uitgangspunten waaruit zij werken. Door kernwaarden en principes te formuleren, wordt het beleid voor bestuurders en medewerkers behapbaar en richt het zich op de bedoeling van het waarborgen van privacy. De gemeenten Nunspeet en Elburg beschrijven geen kernwaarden en principes/uitgangspunten. Het beleid van deze gemeenten is voornamelijk procedureel van aard en gericht op strikte navolging van wet- en regelgeving.

Een in onze ogen interessant punt is de spanning die kan ontstaan tussen strikte navolging van wet- en regelgeving, de taak die de gemeenten hebben en de hulp- of zorgvraag die een inwoner nodig heeft. Deze spanning komt nadrukkelijk tot uiting met het benoemen van kernwaarden en principes. Voorbeelden uit het beleid van de gemeente Hattem. Oldebroek en Putten zijn:

a "We willen voldoen aan alle wetten en dat is een hele uitdaging. We willen ons daarbij flexibel opstellen en denken in mogelijkheden en oplossingen."
b "We voldoen aan wet- en regelgeving, dat is een hele uitdaging. We zoek altijd naar de beste oplossing om zorgvuldig met persoonsgegevens om te gaan en tegelijkertijd onze taak zo goed als mogelijk uit te voeren."
c "Wij hebben daarbij in het bijzonder oog voor kwetsbare groepen. Wij zoeken daarbij de ruimte op binnen de wettelijke kaders, zeker wanneer de zorg voor onze inwoners hierom vraagt."

1.1 Landelijke kaders

De **Baseline Informatiebeveiliging Overheid** (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Het is voor alle overheidsinstanties per 1 januari 2020 het verplichte normenkader. De huidige BIO wordt naar verwachting overigens eind dit jaar vervangen door de BIO 2.0.

De drie basisbeveiligingsniveaus van de BIO

Kerncriteria in de BIO zijn: beschikbaarheid (continuïteit) , integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit) van informatie. Binnen de basisbeveiligingsniveaus worden de drie kerncriteria verder gespecificeerd. Als voorbeeld ten aanzien van vertrouwelijkheid van informatie:

> Het ambitieniveau kan als 'laag' worden gesteld (BBN1) als kennisname van informatie door ongeautoriseerden (buitenstaanders) niet gewenst is, maar niet leidt tot schade van enige omvang. Het kan hoogstens leiden tot financiële gevolgen, die zijn op te vangen binnen de begroting van de gemeente, en irritatie en ongemak bij burgers;

> Het ambitieniveau kan als 'midden' worden gesteld (BBN2) als kennisname van informatie door ongeautoriseerden (buitenstaanders) niet gewenst is en leidt tot politieke schade aan een bestuurder, financiële gevolgen niet zijn op te vangen binnen de gemeentelijke begroting, bindende aanwijzing van de Autoriteit Persoonsgegevens en directe imagoschade door negatieve publiciteit;

> Het ambitieniveau kan als 'hoog' worden gesteld (BBN3) als kennisname van informatie door ongeautoriseerden (buitenstaanders) niet gewenst is en het gaat om vertrouwelijke informatie waarbij het openbaar maken grote impact heeft, waarvan niet is uit te leggen dat deze niet gerubriceerd is en beschermd wordt op BBN3 niveau en geen weerstand is geboden tegen statelijke actoren.

In bijlage 1 van dit rapport worden de drie niveaus nog verder toegelicht.

De **Eenduidige Normatiek Single Information Audit** (ENSIA) is een initiatief van gemeenten en de ministeries van BZK en SZW. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel. ENSIA is ontstaan omdat er veel toezichthouders waren (lees ministeries) die bij wet toezicht moesten houden op bepaalde wetten die door gemeenten werden uitgevoerd. Om te voorkomen dat elk ministerie zijn eigen manier van verantwoorden ging verzinnen en daarmee de gemeenten zouden overvragen, is er gekozen voor een algemeen portaal met vragenlijsten waar de gemeente zich jaarlijks in kan verantwoorden. ENSIA wordt door gemeenten, provincies, waterschappen en de rijksoverheid ook gebruikt om zich te onder andere te verantwoorden over de staat van informatie-beveiliging. Daarin zijn ook de beveiligingsnormen van de Basisregistratie Personen, Reisdocumenten, en Suwinet betrokken.[6] ENSIA is onderdeel is van de jaarlijkse verantwoordingscyclus van gemeenten. Het bestaat uit verschillende vragenlijsten. Gemeenten vullen zelf de vragenlijst in en het is daarmee een zelfevaluatie. Voor de DigiD-koppelingen en Suwinet worden verplichte audits uitgevoerd in het kader van ENSIA. Voor deze audits moeten wel vragenlijsten worden ingevuld maar het is geen zelfevaluatie.

Daarnaast is er de **Algemene Verordening Gegevensbescherming** (AVG). De AVG is een Europese verordening, die de regels voor de verwerking van persoonsgegevens door overheidsinstanties en private organisaties standaardiseert. Dit met als doel om het vrije verkeer van gegevens te waarborgen, maar op een dusdanige wijze dat de bescherming van persoonsgegevens is gegarandeerd. Voor de verantwoor-ding rond de Algemene Verordening Gegevensbescherming (AVG) zijn separate procedures aanwezig. De Functionaris Gegevensbescherming heeft een toezichthoudende rol. De FG is niet verantwoordelijk voor het borgen van de procedures; hij/zij moet controleren of de organisatie de juiste procedures heeft

[6] Via Suwinet kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen.

geïmplementeerd. De FG kan wel advies geven over de te implementeren procedures, maar is niet verantwoordelijk voor het daadwerkelijke gebruik of implementatie hiervan.

1.2 Lokale ambities en beleid

Hieronder beschrijven we de ambities en het beleid van de verschillende gemeenten. We richten ons daarbij voornamelijk op de doelen, de processen en/of de thema's voor doorontwikkeling van de informatiebeveiliging en privacy. De ambtelijke organisatie, rollen en taken van verschillende functionarissen zijn door de gemeenten ook opgenomen in de beleidsplannen. Denk aan de rol van de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en proceseigenaren. Deze bespreken we in het volgende hoofdstuk 2 'Uitvoering'.

1.2.1 H2O-gemeenten Hattem en Oldebroek

De gemeenten Hattem en Oldebroek werken sinds december 2017 samen op het terrein van Informatisering en Automatisering (I&A). De informatisering (CIO) zit bij de gastheergemeente Oldebroek en de automatisering (i-Dienst) in de gemeenschappelijke regeling H2O. Het doel van deze samenwerking is dat het de gemeenten in staat moet stellen om, vanuit gezamenlijke ambities en beleid, te voorzien in een robuuste en betrouwbare informatievoorziening. Door dit samen te doen willen de gemeenten hun kwetsbaarheid verlagen en kwaliteit verhogen. De ambities en het beleid zijn vastgelegd in het 'Strategisch Informatiebeveiligingsbeleid 2023-2025' en zijn in 2023 verder geactualiseerd in de 'Kadernota Strategisch Informatiebeleidsplan 2024-2027'. Tevens is er een door de gemeentesecretaris vastgestelde Strategisch Continuïteitsplan Informatievoorziening H2O. Hiermee zijn de ambities en het beleid met betrekking tot de informatiehuishouding en -beveiliging gemeenschappelijk gemaakt. De uitwerking van dit beleid in concrete maatregelen vindt plaats in een jaarlijks op te stellen informatiebeveiligingsplan, dat we in het volgende hoofdstuk van dit rapport verder belichten.

Strategisch Informatiebeveiligingsbeleid 2023-2025

De gemeenten verstaan onder informatiebeveiliging het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten zijn: beschikbaarheid, integriteit (juiste en volledige informatie) en vertrouwelijkheid van persoonsgegevens en andere informatie.[7] Het treffen van maatregelen beperkt zich niet tot ICT maar heeft betrekking op het openbaar bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.[8]

De gemeenten hanteren de Baseline Informatiebeveiliging Overheid (BIO) als normenkader voor informatiebeveiliging. Dit in algemene zin, want evalueerbare ambities/doelen ten aanzien van de zwaarte van het beveiligingsniveau (BBN1, BBN2, BBN2+ of BBN3) worden niet gesteld. De doelen zijn verder niet gedifferentieerd naar de verschillende drie kerncriteria: beschikbaarheid, integriteit en vertrouwelijkheid. Wel maken aanvullende beveiligingseisen deel uit van het strategische informatie-beleidsplan, te weten eisen voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK) en Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).

Ook hanteren de gemeenten tien principes als bestuurlijke aanvulling op de BIO, zie het onderstaande kader. De tien principes voor informatiebeveiliging zijn een-op-een overgenomen van de VNG. De tien principes zijn gelijk met de BIO van kracht geworden en vastgesteld door de Vereniging van Nederlandse Gemeenten en de Informatiebeveiligingsdienst. Door deze principes als uitgangspunt te nemen zien de gemeenten het onderwerp informatiebeveiliging als een proces van risicomanagement, waarbij het

---

7 Deze definitie sluit aan op artikel 1 sub a Voorschrift Informatiebeveiliging Rijksdienst 2007

8 Bron: Strategisch Informatiebeleidsplan H2O gemeenten 2023-2025

openbaar bestuur een uitdrukkelijke rol heeft doordat het deel uitmaakt van bestuurlijke besluitvorming, controle en evaluatie.

Tien principes voor informatiebeveiliging als bestuurlijke aanvulling op de BIO

1 Bestuurders bevorderen een veilige cultuur
2 Informatiebeveiliging is van iedereen
3 Informatiebeveiliging is risicomanagement
4 Risicomanagement is onderdeel van besluitvorming
5 In (keten)samenwerking is informatiebeveiliging ook van belang
6 Informatiebeveiliging is een proces
7 Informatiebeveiliging kost geld
8 Onzekerheid wordt ingecalculeerd
9 Verbetering komt voort uit leren en ervaring
10 De besturen controleren en evalueren

Bron: Strategisch Informatiebeleidsplan 2023-2025

Als laatste wordt in het strategisch informatiebeveiligingsbeleid 2023-2025 aangegeven dat het plan jaarlijks wordt opgesteld door de Chief Information Security Officer (CISO) onder leiding van de Chief Information Officer (CIO). De CIO is binnen een organisatie de functionaris die verantwoordelijk is voor de informatievoorziening. Om het plan te actualiseren worden de volgende bronnen meegenomen:

> De uitkomsten van de jaarlijkse ENSIA audit;
> Uitkomsten van overige audits;
> Het 'Dreigingsbeeld Nederlandse gemeenten' van de Informatiebeveiligingsdienst (IBD);
> De door procesverantwoordelijke managers ingebrachte onderwerpen.

Kadernota Strategisch Informatiebeleidsplan H2O 2024-2027

In de kadernota wordt gesteld dat de H2O gemeenten stapsgewijs werken aan het voldoen aan de BIO. In dat licht is het een voorzetting van het beleid zoals verwoord in het Strategisch Informatiebeleidsplan.

Er worden verder vijf thema's belicht waar de H2O-gemeenten aan wil werken:

1 **Bouwen aan een stevige basis, de zogeheten 'digitale infrastructuur'.** Dit bestaat uit een aantal componenten die de H2O-gemeenten de komende jaren op orde wil hebben:
   > Gegevensmanagement: processen en producten voor uitwisseling, kwaliteit en beveiliging over de verwerking van gegevens;
   > Informatiebeheer: betrouwbaar en duurzaam bewaren van digitale informatie;
   > Werken onder architectuur: om grip te krijgen op de informatievoorziening willen de gemeenten werken onder één architectuur. Projecten zijn niet meer vrij om hun eigen 'beste' oplossing te kiezen, maar moeten binnen gestelde kaders werken;
   > Centralisatie en professionalisering van functioneel beheer: het functioneel beheer is in de loop de jaren versnipperd waardoor er weinig samenhang is en integratie van systemen;
   > Governance en sturing op projecten: de IT-governance verbeteren. Taken en rollen op strategisch, tactisch en operationeel niveau beter beschrijven en afstemmen.
2 **Datagedreven werken**. Het nemen van beslissingen op basis van data en feiten.
3 **Doorontwikkelen digitale dienstverlening.** Dienstverlening waarbij de klant centraal staat door deze flexibel in te richten en diensten te leveren via de digitale kanalen. Tegelijkertijd wordt gestreefd naar uniformiteit en standaardisatie van processen en informatie.
4 **Doorontwikkelen van de informatievoorzieningsorganisatie.** De gemeenten spreken hier over het verbeteren van 'Business- en IT-alignement'. Om dit Engelse vakjargon nader te verklaren vertalen wij dit verder in het Nederlands.

   Onder de term 'Business- en IT-alignement' wordt verstaan het in samenhang en harmonie brengen van behoeften (vraag) enerzijds en informatiesystemen en -technologie (aanbod) anderzijds, met oog op het realiseren van de doelen van het bestuur en organisatie als geheel. Soms ontstaat er een kloof tussen beiden, dat leidt tot onbegrip tussen gebruikers en IT-professionals. Als deze kloof niet wordt

overbrugd leidt dit tot dure onsamenhangende systemen. Het doel is dit te voorkomen en dat vraag om een goede aansluiting van strategische organisatiedoelen naar benodigde informatiesystemen op tactisch en operationeel niveau.

5 **i-Bewustzijn.** De gemeenten willen werk maken van het vergroten van digitale geletterdheid en het creëren van bewustzijn over digitale veiligheid, informatiebeveiliging en privacy.

Privacybeleid

Op het terrein van de waarborging van privacy is er geen gemeenschappelijk beleid; beide gemeenten hebben hun eigen privacybeleid opgesteld.

De **gemeente Oldebroek** heeft het beleid in twee stukken beschreven: 'Grip op privacy, juni 2021' en 'Grip op privacy in het sociaal domein'. Het is van toepassing op alle processen binnen de gemeente waarin persoonsgegevens worden verwerkt, daarop is de privacywet van toepassing. De belangrijkste is de Algemene Verordening Gegevensbescherming (AVG). Daarnaast zijn er andere bijzondere wetten die ook iets zeggen over het gebruik van persoonsgegevens. Het gaat om de Wet open overheid (Woo), de Wet basisregistratie personen (Wet BRP), de Wet maatschappelijke ondersteuning (Wmo), de Jeugdwet en de Archiefwet. Het beleid beschrijft verder welke persoonsgegevens de gemeente gebruikt en voor welke doelen. Denk aan het uitgeven van identiteitsbewijzen, het bijhouden van basisregistratie personen, het verstrekken van uitkeringen, het heffen van belastingen et cetera. Alle doelen en grondslagen staan in een verwerkingsregister. Het beleid besteedt ook aandacht aan beveiliging van persoonsgegevens:

> De gemeente heeft een datalekprotocol dat beschrijft hoe om te gaan met datalekken. Medewerkers dienen (mogelijke) datalekken te melden en een datalekteam moet dat oppakken en afhandelen.
> Bij een nieuw proces of het inkopen van een dienst of product houdt de gemeente in de ontwerpfase als rekening met privacy, ook wel 'privacy-by-design' genoemd. De standaard werkwijze is zo min mogelijk persoonsgegevens te verwerken.
> Als een gegevensverwerking complex is of een hoog risico heeft, wordt een risicobeoordeling uitgevoerd en maatregelen getroffen om risico's zo klein als mogelijk te houden, ook wel een 'data protection impact assessment (DPIA)' genoemd.

Naast het voldoen aan alle wet- en regelgeving heeft de gemeente Oldebroek vijf kernwaarden en tien privacyregels opgesteld die richtinggevend zijn voor de werkwijze van de gemeente, zie het onderstaande kader.

Vijf kernwaarden Oldebroek

1 **Dienstverlenend:** Gegevens van inwoners worden gebruikt ten dienste van inwoners en alleen als dat echt noodzakelijk is.
2 **Eigenaarschap:** We nemen verantwoordelijkheid voor het werken met persoonsgegevens. Vertrouwelijkheid en zorgvuldig omgaan met gegevens vinden we belangrijk.
3 **Flexibel:** We willen voldoen aan alle wetten en dat is een hele uitdaging. We willen ons daarbij flexibel opstellen en denken in mogelijkheden en oplossingen.
4 **Verbindend:** We verbinden wet- en regelgeving aan de taken die we hebben. Dus aandacht voor hoe we de taak het beste kunnen uitvoeren, maar ook hoe we daarbij de privacy van inwoners kunnen beschermen.
5 **Vakbekwaam:** Alle medewerkers zijn zich bewust van het belang van privacy en medewerkers passen dit ook toe. Daar is aanvullende kennis voor nodig en de gemeente heeft daartoe een Privacy Officer en een Functionaris Gegevensbescherming aangesteld.

Tien privacyregels Oldebroek

1 We verwerken alleen persoonsgegevens als dat nodig is.

2 We gebruiken voor het uitvoeren van taken alleen de echt noodzakelijke persoonsgegevens.
3 We wisselen persoonsgegevens alleen uit als dat nodig is om de taak uit te kunnen voeren.
4 Als we een andere partij vragen om persoonsgegevens te verwerken, dan maken we daar afspraken over.
5 We slaan persoonsgegevens op zo min als mogelijke plekken op.
6 Als we bijzondere persoonsgegevens verwerken zijn we extra alert op hoe we dat doen en met wie we de informatie delen.
7 We zijn transparant over wat we doen met persoonsgegevens.
8 We zorgen voor een goede beveiliging van de persoonsgegevens.
9 Als de bewaartermijn verstreken is, verwijderen we de persoonsgegevens.
10 Als we denken dat persoonsgegevens 'gelekt' zijn melden we dat zo snel als mogelijk.

Bron: Grip op privacy, gemeente Oldebroek, juni 2021

De **gemeente Oldebroek** heeft ervoor gekozen om voor het sociaal domein een apart privacybeleid op te stellen: 'Grip op privacy in het sociaal domein'. De gemeente heeft dit gedaan omdat dit domein een aantal aandachtspunten met zich mee brengt. Het gaat om het gebruik van bijzondere persoonsgegevens en de samenwerking met andere overheidsorganisaties en zorg- en hulpverleners. Als er taken worden overgedragen, al dan niet via een mandaat of delegatie, dan maakt de gemeente afspraken hoe invulling wordt gegeven aan de AVG.

Bijzonder persoonsgegevens betreffen bijvoorbeeld iemands etniciteit of strafrechtelijke gegevens. Bij verwerking van deze gegevens geeft de gemeente aan extra aandacht te schenken aan een aantal specifieke criteria uit de AVG. Het gaat bijvoorbeeld om de vraag of verwerking van de persoonsgegevens van vitaal belang is, het omgaan met rechten en plichten van hulpverleners (beroepsgeheim) en de toestemming die nodig is van cliënten om zijn/haar gegevens te mogen verwerken. Transparantie is daarbij belangrijk. Zo schrijft het beleid voor dat vanaf het eerste contact met een inwoner de gemeente transparant is over hoe persoonsgegevens worden verwerkt, op de website is een privacyverklaring te vinden en ook gedurende een traject worden inwoners geïnformeerd als nieuwe informatie wordt opgevraagd en verwerkt. Daarnaast zijn in de Wmo en Jeugdwet bepalingen opgenomen over het recht van inzage, het recht van correctie en het recht van wissen van gegevens die de gemeente verwerkt.

De **gemeente Hattem** heeft het beleid rondom privacy beschreven in het stuk 'Grip op privacy'. Ook in dit beleid worden de eerder genoemde tien privacyregels gepresenteerd. Het beleid is verder identiek aan die van de gemeente Oldebroek, behalve dat er vier andere kernwaarden worden genoemd en er geen specifiek privacybeleid is opgesteld voor het sociaal domein.

Vier kernwaarden Hattem

1 **Duidelijkheid:** Gegevens van inwoners worden gebruikt ten dienste van inwoners en alleen als dat echt noodzakelijk is. We communiceren hierover naar inwoners.
2 **Samenwerken:** We willen van elkaar leren en elkaar helpen om aandacht te blijven houden voor privacy.
3 **Vertrouwen:** Een zorgvuldige omgang met persoonsgegevens draagt bij aan het vertrouwen in onze organisatie en onze mensen. Om dit vertrouwen te vergroten zijn we transparant over wat we doen met persoonsgegevens en zijn we aanspreekbaar op ons handelen.
4 **Verbeteren:** We voldoen aan wet- en regelgeving, dat is een hele uitdaging. We zoeken altijd naar de beste oplossing om zorgvuldig met persoonsgegevens om te gaan en tegelijkertijd onze taak zo goed als mogelijk uit te voeren.

Bron: Grip op privacy, gemeente Hattem

1.2.2 Elburg

De gemeente Elburg beschikt over een informatiebeveiligingsbeleid 2021-2023, dat recent is geactualiseerd met vaststelling van het 'Strategisch Informatiebeveiligingsbeleid 2024-2026', een continuïteitstrategie 2023 en een logisch toegangsbeveiligingsbeleid 2023-2026.

Strategisch Informatiebeveiligingsbeleid 2024-2026

Dit beleid is een voorzetting van het beleid over de voorgaande jaren 2021-2023, zie hieronder. Het omvat verder geen nieuw beleid.

Informatiebeveiligingsbeleid 2021-2023

Het beleid is identiek aan die van de H2O-gemeenten, zoals besproken in de voorgaande paragraaf. Ook Elburg hanteert de BIO als normenkader en de tien principes als bestuurlijke aanvulling op de BIO. Tevens zijn aanvullende bepalingen opgenomen voor SUWI, BRP en PNIK. Ook hier worden verder geen evalueerbare ambities/doelen ten aanzien van de zwaarte van het beveiligingsniveau (BBN1, BBN2, BBN2+ of BBN3) gesteld. Er wordt ook niet gedifferentieerd naar twee kerncriteria: integriteit en vertrouwelijkheid. Ten aanzien van het kerncriterium beschikbaarheid zijn wel evalueerbare doelen gesteld, zie hieronder de continuïteitstrategie.

Continuïteitstrategie 2023

In dit document besteedt de gemeente bijzondere aandacht aan kritieke bedrijfsprocessen van de gemeente. Het gaat hierbij om het kerncriterium 'beschikbaarheid'. De bedrijfsprocessen zijn hiertoe ingedeeld naar prioriteiten, waarbij nummer 1 de hoogste prioriteit heeft. Het gaat om bedrijfsprocessen die vallen onder: wettelijke bepalingen (bij uitval herstel binnen de door de wet bepaalde tijd), wenselijk herstel binnen 24 uur, 48 uur, of 72 uur . Het document bevat een bijlage waarin alle kritieke bedrijfsprocessen zijn genoemd en zijn verdeeld over de prioriteiten.

Logisch toegangsbeveiligingsbeleid 2023-2026

Het logisch toegangsbeveiligingsbeleid is een onderdeel van de gemeentelijke informatiebeveiliging. Het doel is ervoor te zorgen dat onbevoegden minder makkelijk toegang kunnen krijgen tot de gemeentelijke informatiesystemen en de informatie binnen deze systemen. Het heeft betrekking op zowel de fysieke beveiliging als op het logische toegangsbeheer. Het beschrijft het gebruik van authenticatie en autorisatie:

1. Een procedure om toegangsrechten toe te wijzen, gebaseerd op het instroom-, doorstroom en uitstroom proces van de afdeling Personeel & Organisatie van de gemeente.
2. Een uniforme autorisatiestructuur voor de gehele gemeente: elk systeem heeft een autorisatie-matrix. In deze matrix zijn per systeem functies en rollen van functionarissen beschreven die zijn gekoppeld aan rechten zoals toevoegen, bekijken, wijzigen, verwijderen van gegevens et cetera.
3. Niemand binnen de gemeente mag autorisatie hebben om een gehele cyclus van handelingen in een informatiesysteem of database te beheersen, ook wel 'Segregration of Duties' (SOD) genoemd. SOD is in feite een functiescheiding, bepaalde verantwoordelijkheden worden over meer dan één persoon gespreid.
4. Er wordt gebruik gemaakt van een persoonsgebonden gebruikersnaam, wachtwoord en hardwaretoken of authenticator-app. Door de combinatie wil de gemeente de toegangsbeveiliging versterken, ook wel 'two-factor'of 'multi-factor' authenticatie genoemd.

Een two-factor authenticatie (2FA) is een authenticatiemethode waarbij men twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen. In het Nederlands noemen we dit ook wel een twee stappen authenticatie. De eerste stap is veelal het invoeren van een gebruikersnaam en wachtwoord. De tweede stap is bijvoorbeeld het invoeren van een sms-code die na de eerste stap naar de mobiele telefoon wordt verzonden. Alleen deze combinatie zorgt ervoor dat men toegang krijgt.

Het beleid voorziet verder in een procedure voor het opschonen van niet meer gebruikte accounts. Deze vormen namelijk een risico op ongewenste toegang en worden daarom uitgeschakeld. Indien de laatste inlogdatum meer dan een maand ligt voor de controledatum van een periodieke controle, wordt het account geblokkeerd. Als laatste besteedt de gemeente in het beleid aandacht aan bewustwording van medewerkers. Het beleid schrijft voor dat de CISO daar aandacht aan moet schenken. Tevens is voor externe leveranciers een procedure vastgesteld, waar een risicoafweging voor toegang tot het netwerk deel van uitmaakt.

Privacybeleid

De gemeente Elburg heeft het privacybeleid veel minder omvattend omschreven dan de hiervoor besproken H2O gemeenten. Het is met name ingegeven door wet- en regelgeving en bevat verder geen lokale visie van de gemeente zelf, zoals kernwaarden die richtinggevend zijn. Er is geen specifiek privacybeleid rondom het sociaal domein.

1.2.3 Nunspeet

Strategisch informatiebeveiligingsbeleid 2021-2024

De gemeente Nunspeet beschikt over een 'Strategisch Informatiebeveiligingsbeleid 2021-2024'. Ook hier is het beleid identiek aan die van de andere in dit onderzoek onderzochte gemeenten. Ook Nunspeet hanteert de BIO als normenkader en de tien principes als bestuurlijke aanvulling op de BIO. Tevens zijn aanvullende bepalingen opgenomen voor SUWI, BRP en PNIK. Ook hier worden verder geen evalueerbare ambities/doelen ten aanzien van de zwaarte van het beveiligingsniveau (BBN1, BBN2, BBN2+ of BBN3) gesteld. Verder wordt er niet gedifferentieerd naar de drie kerncriteria: beschikbaarheid, integriteit en vertrouwelijkheid.

De gemeente heeft een traject gestart om een nieuw informatiebeleid op te stellen. In dit nieuwe beleid wil de gemeente de ambities meer integraal beschrijven. Dat wil zeggen dat er gekeken zal worden naar verbindingen tussen verschillende organisatieonderdelen en een gemeentebrede informatie-architectuur.[9] Daarbij onderzoekt Nunspeet de kansen voor mogelijkheden voor regionale samenwerking op het gebied van informatisering en automatisering.

De gemeente Nunspeet beschikt ook over een bewustwordingsplan voor informatiebeveiliging en bescherming van persoonsgegevens. De gemeente beschrijft daarin gebruik te maken van een Bewustwording Management Systeem. Dat systeem omvat:

> Een basistraining met een module voor nieuwe medewerkers, een herhalingsmodule voor medewerkers, specifieke modules voor medewerkers die toegang hebben tot Suwinet of een module Privacy. Omdat de voorgaande modules als belastend werden ervaren is de gemeente overgestapt naar een wekelijkse uitvraag; medewerkers ontvangen iedere woensdag een beveiligingsvraag;
> De gemeente heeft de mogelijkheid om een mysteryguest-onderzoek uit te voeren.

Privacybeleid

Het 'Privacy beleidskader Gemeente Nunspeet 2020-2024' is voornamelijk procedureel van aard, kernwaarden en uitgangspunten worden niet genoemd. Wel worden gedragsnormen voor het bestuur, directie en proceseigenaren beschreven. Zo wordt aangegeven dat het college, de directie en proceseigenaren het belang moeten uitdragen van de uitvoering van het privacy beleid. Zij moeten zelf het goede voorbeeld geven en privacy bespreekbaar maken. Bij dillema's moeten zij de dialoog aangaan met doelgroepen over wie informatie wordt verwerkt. Ook wordt uitgebreid aandacht besteed aan de 'data protection impact assessment (DPIA)' en een auditbeleid. De DPIA wordt ingezet om

[9] Bron: interviews

procesplannen op te stellen en passende beheersmaatregelen te nemen voor verbetering van de waarborging van privacy. Het beleid omschrijft de rol en taak van proceseigenaren in relatie tot de procesplannen en hoe zij moeten rapporteren naar de directie over de voortgang.

In de gemeente Nunspeet is het verder de ambitie om het privacybeleid het komende jaar te evalueren en geleerde lessen mee te nemen in nieuwe beleid.

1.2.4 Putten

Strategisch informatiebeleid

De gemeente Putten werkt sinds begin 2017 onder andere op het terrein van ICT samen met de gemeenten Bunschoten, Leusden en Nijkerk. De gemeente Bunschoten fungeert als gastheergemeente. De gemeente hebben een gezamenlijk informatiebeveiligingsbeleid, het 'Strategisch gemeentebreed Informatieveiligheidsbeleid' van maart 2020. Dat beleid is grotendeels identiek aan die van de andere in dit onderzoek onderzochte gemeenten, want ook Putten hanteert de BIO als normenkader en sluit het aan op specifieke wettelijke kaders voor de BRP, SUWI, AVG en PNIK.

In het beleid wordt aandacht gegeven aan het zogeheten 'Information Security Management System'. Dit is een cyclisch proces dat wordt doorlopen om informatiebeveiliging te borgen. Het bestaat uit vier stappen:

> Stap 1: Informatiebeveiligingsbeleid.
  Eens in de drie jaar wordt een informatiebeveiligingsbeleid opgesteld. Het bevat de uitgangspunten, normen en kaders voor alle gemeentelijke informatieprocessen.
> Stap 2: Informatieveiligheidsanalyse.
  Deze stap richt zich op de implementatie van het beleid, dat start met een veiligheidsanalyse. Alle gegevensverzamelingen en -applicaties worden toegewezen aan een eigenaar en geclassificeerd op risicoklassen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. De basis-beveiligingsniveaus worden vastgesteld. Hierbij geldt dat gemeentebreed het niveau BBN2 wordt gehanteerd, dat ook het landelijke basisniveau is.
  Wij merken op dat de gemeente Putten hiermee in het beleid een evalueerbaar doel stelt en dit ook differentieert naar de drie kerncriteria beschikbaarheid, integriteit en vertrouwelijkheid. De praktijk-situatie wordt getoetst aan de BIO, door het uitvoeren van een risico evaluatie en een GAP-analyse (verschil gewenste en huidige situatie).
> Stap 3: Actieplan.
  Op basis van de veiligheidsanalyse wordt een actieplan opgesteld, waarin geconstateerde risico's worden voorzien van maatregelen en prioriteiten. De informatieveiligheidsorganisatie bewaakt de implementatie.
> Stap 4: Technische en organisatorische maatregelen.
  Het gaat hier om het opstellen van procedures en werkinstructies, of opleveren van technische maatregelen, die voortvloeien uit het actieplan.

In het beleid van Putten is de werkwijze voor risicomanagement expliciet uitgewerkt in het beleidsplan. Alle gegevensverzamelingen en -applicaties worden toegewezen aan een eigenaar en geclassificeerd op risicoklassen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid en de basisbeveiligings-niveaus worden vastgesteld. Hierbij geldt dat gemeentebreed het niveau BBN2 wordt gehanteerd. De praktijksituatie wordt getoetst aan de BIO door het uitvoeren van een risico evaluatie en een GAP-analyse (verschil gewenste en huidige situatie). Op basis van de veiligheidsanalyse wordt een actieplan opgesteld waarin geconstateerde risico's worden voorzien van maatregelen en prioriteiten en de informatieveiligheidsorganisatie bewaakt de implementatie.

Privacybeleid

Het beleid van de gemeente Putten is beschreven in het 'Privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten'. Deze gemeenten hebben dus een gezamenlijk beleid. In het beleid worden zes beginselen en vijf principes beschreven voor het handelen van de gemeente.

Zes beginselen

1. Het is inzichtelijk in hoeverre en op welke manier persoonsgegevens worden gebruikt.
2. Het is duidelijk voor welk doel persoonsgegevens worden gebruikt.
3. Er worden niet te veel maar ook niet te weinig persoonsgegevens verwerkt.
4. De gebruikte persoonsgegevens zijn juist en actueel.
5. Persoonsgegevens worden niet langer bewaard dan nodig.
6. Persoonsgegeven worden op een passende manier beveiligd.

Vijf principes

1. Wij verwerken vooral voor onze inwoners en medewerkers veel persoonsgegevens waaronder ook bijzondere persoonsgegevens.
2. Wij zijn ons bewust van de maatschappelijke verantwoordelijkheid die dit met zich mee brengt.
3. Wij gaan zorgvuldig en vertrouwelijk om met persoonsgegevens en treffen passende beveiligingsmaatregelen.
4. Wij zijn transparant over het verzamelen, gebruik, opslaan en delen van persoonsgegevens.
5. Wij houden voortdurend rekening met de belangen van mensen bij de verwerking van hun persoonsgegevens. Wij hebben daarbij in het bijzonder oog voor kwetsbare groepen. Wij zoeken daarbij de ruimte op binnen de wettelijke kaders, zeker wanneer de zorg voor onze inwoners hierom vraagt. Wij zetten bij dilemma's de belangen van onze inwoners centraal en gaan wij proactief het gesprek met hen aan.

Bron: Privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

2 Uitvoering

In dit hoofdstuk worden de deelvragen 3 t/m 7 beantwoord. De lezer die snel zicht wil krijgen op de antwoorden kan de korte beantwoording lezen direct onder het onderstaande kader. De lezer die meer details tot zich wil nemen kan de daarop volgende paragrafen raadplegen waar we uitgebreider ingaan op de verschillende deelvragen.

DEELVRAGEN

3 Hoe is het beleid vertaald naar de uitvoering?
4 Wat is de kwaliteit van het proces van informatiehuishouding in relatie tot informatie-beveiliging en waarborging van privacy?
   > Hoe is het risicomanagement vorm gegeven?
   > Wordt de kwaliteit van het proces gemonitord, waaronder tenminste de verplichte ENSIA-audit?
   > Wordt daarover gerapporteerd, aan wie en hoe wordt indien nodig bijgestuurd?
5 Hoe voeren de gemeenten regie op die zaken waarbij de gemeenten samenwerken met anderen op het terrein van informatiehuishouding, informatiebeveiliging en waarborging van privacy?
6 Hoe wordt het beleid vertaald naar structurele en incidentele financiële lasten die gemoeid zijn met de informatiehuishouding, informatiebeveiliging en waarborging van privacy?
7 Wat zijn actuele ontwikkelingen met betrekking tot informatietechnologie, wet- en regelgeving en in hoeverre spelen de gemeenten daarop in?

TOEGEPASTE NORMEN

- Het beleid is vertaald naar een uitvoerings- en investeringsplan met zicht op:
  > Het benodigde digitale informatiehuis;
  > Wat nodig is om informatie te beveiligen en privacy te waarborgen, waaronder een risicoanalyse en beheersmaatregelen.
  > Evalueerbare uitvoeringsdoelen;
  > Samenwerking met anderen;
  > Structurele lasten en investeringen.
- Er zijn voldoende financiële en personele middelen om het uitvoeringsplan te realiseren, vernieuwingen door te voeren en in te spelen op nieuwe wet- en regelgeving.
- Het gebruik en de kwaliteit van de informatiehuishouding wordt regelmatig getoetst, alsmede de informatiebeveiliging en waarborging van privacy aan de hand van audits. Op basis daarvan wordt gerapporteerd en vindt indien nodig bijsturing plaats.
- De gemeente stuurt op samenwerkingsverbanden met oog op samenhang van de informatiehuishouding, informatiebeveiliging en privacy.

Korte beantwoording van de deelvragen

3 Alle gemeenten hebben in hun informatiebeveiligings- en privacybeleid de verschillende functionarissen en rollen beschreven die relevant zijn voor dit beleid. Hierbij sluiten de gemeenten aan op de wet- en regelgeving, waarin deze rollen worden voorgeschreven. Het gaat om de rollen van het college van b&w, de gemeentesecretaris, de Chief Information Security Officer (CISO), de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG) en de proceseigenaren.

In alle gemeenten is de invulling van de rol van proceseigenaar echter een zorgpunt. Weliswaar in verschillende mate. Voor proceseigenaren zelf is de rol niet helder en mede door hoge werkdruk komen zij niet toe aan een goede invulling van deze rol.

4 Meerdere keren geven gemeenten aan dat eerst het huis of de basis op orde moet zijn om verder te kunnen doorgroeien naar een hoger volwassenheidsniveau rondom informatiebeveiliging en waarborging van privacy.[10]

Enkel de gemeente Putten heeft daarbij expliciet een uitvoeringsdoel gesteld, namelijk dat gemeentebreed het beveiligingsniveau BBN2 van moet worden gerealiseerd. Zoals eerder beschreven is in het beleid van Putten de werkwijze voor risicomanagement expliciet uitgewerkt in het beleidsplan. Alle gemeente zien een cyclus van risicomanagement als belangrijk, maar hebben echter moeite met het daadwerkelijk implementeren van zo'n cyclus op het gebied van informatie-beveiliging en privacy. In alle gemeenten is de invulling van de rol van proceseigenaar een zorgpunt. Voor proceseigenaren is de rol niet helder en mede door hoge werkdruk komen proceseigenaren niet toe aan een goede invulling van deze rol.

Alle gemeenten hebben de ENSIA opgenomen in hun beleid als instrument, om periodiek de stand van zaken rondom informatiebeveiliging te evalueren en daarover verticale verantwoording af te leggen aan de toezichthouders van de ministeries die een rol hebben in het toezicht op informatieveiligheid. Met de ENSIA leggen de gemeenten verantwoording af over informatie-veiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, waaronder de vragenlijsten met betrekking tot de BIO, BAG, BRO, DigiD, BGT en Suwinet. Met een verklaring geven de colleges aan in hoeverre de gemeenten voldoen aan de normen en waar nog verbeterpunten zijn.

5 Er worden verwerkersovereenkomsten afgesloten met verbonden partijen. Met de verwerkersovereenkomsten is toezicht en controle door de gemeenten mogelijk. Het volgende is daartoe opgenomen in de verwerkersovereenkomsten:
> De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm;
> De toereikendheid van de informatiebeveiliging blijkt uit eigen controles;
Uit de certificering, eigen of externe controles of uit de audits blijkt of kan afgeleid worden dat de beveiliging voldoet.

De Omgevingsdienst Noord-Veluwe kwalificeert zichzelf, op basis van advies van de landsadvocaat Pels Rijcken, als verwerker.[11] Met de Omgevingsdienst Noord-Veluwe is door de H2O gemeenten reeds in 2017 een verwerkersovereenkomst afgesloten.[12] De gemeenten Nunspeet en Elburg hebben dit niet gedaan.[13] Van de gemeente Putten hebben de onderzoekers hierover geen stukken ontvangen.

6 Alle gemeenten begroten de financiële middelen die nodig zijn voor I&A binnen het programma Bestuur van de programmabegroting. Dit is verder niet gedifferentieerd naar financiële middelen die nodig zijn voor informatiebeveiliging en waarborging van privacy. Uit gesprekken in het kader van dit onderzoek blijkt dit ook ingewikkeld en zelfs niet mogelijk. Ook zijn er bedenkingen bij geïnterviewden of dit wel zinvol is. Tegelijkertijd wordt aangegeven dat investeringen en middelen voor de implementatie van beleid wel nodig zijn. Er wordt aangegeven dat het ook zou helpen om deze zichtbaar te maken om concrete acties en noodzakelijke verbeteringen uit te kunnen voeren.

---

[10] Bron: interviews

[11] Bron: Opdrachtgeversoverleg Omgevingsdienst Noord-Veluwe, 12 januari 2023.

[12] Bron: Verwerkersovereenkomst gemeente Oldebroek met ODNV, tevens bruikbaar in H2O verband, april 2017.

[13] Bronnen: e-mail van Elburg d.d. 11 december 2023, e-mail van Nunspeet d.d. 8 december 2023.

7 Alle gemeenten richten zich op wetgeving die al van kracht is. Deze vormen een belangrijk onderdeel van de werkzaamheden van gemeentelijke organisaties, en informatiebeveiliging in het bijzonder. Daar wordt in de beleidsstukken van de gemeenten ook aandacht aan gegeven. Het gaat dan om de impact van de Omgevingswet op de digitale infrastructuur van de gemeenten en de Wet open overheid. Er wordt in beperkte mate ingespeeld op nieuwe ontwikkelingen rondom wetgeving. Geen van de gemeenten kijkt vooruit op de digitale agenda van bijvoorbeeld de Europese Unie, waarvan nog een groot aantal wetten aankomen die ook van toepassing zijn voor de gemeenten. Denk bijvoorbeeld aan NIS2. Hier wordt momenteel nog weinig aandacht aan besteed.

De gemeenten besteden verder nog weinig aandacht aan externe ontwikkelingen, zoals:

> Het Internet of Things (IoT). Er worden steeds meer apparaten met elkaar verbonden via internet, denk bijvoorbeeld aan camera's, sensoren die allerlei zaken meten in onze leef-omgeving, maar ook geautomatiseerde besturingssystemen van verkeerslichten of bruggen et cetera. De diversiteit en alomtegenwoordigheid van IoT-apparaten maakt ze aantrekkelijke doelwitten voor cyberaanvallen. Hun onderling verbonden karakter kan tot wijdverbreide kwetsbaarheden leiden;

> Artificial Intelligence (AI) en Machine Learning (ML) maken de afgelopen jaren een enorme ontwikkeling door en zal daarmee ook een belangrijke rol spelen in informatiebeveiliging

> Tekorten aan ervaren cybersecurity-professionals. Naarmate cyberdreigingen geavanceerder worden, stijgt de vraag naar ervaren cybersecurity-professionals. Er is een groot tekort aan mensen die zijn uitgerust met de noodzakelijke vaardigheden en kennis om deze evoluerende bedreigingen effectief te bestrijden. Dit tekort vormt een risico voor organisaties.

2.1 Vertaling van beleid naar uitvoering

Organisatie algemeen

Alle gemeenten hebben in hun informatiebeveiligings- en privacybeleid de verschillende functionarissen en rollen beschreven die relevant zijn voor dit beleid. Daarmee sluiten de gemeenten aan op de wet- en regelgeving waarin deze rollen worden voorgeschreven. Het gaat om de rollen van het college van b&w, de gemeentesecretaris, de Chief Information Security Officer (CISO), de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG) en de proceseigenaren. De gemeentesecretarissen dragen de ambtelijke eindverantwoordelijkheid voor het functioneren van de bedrijfsvoering van de ambtelijke organisatie als geheel, waaronder de organisatie en processen rondom informatiebeveiliging en waarborging van privacy. Zij rapporteren hiertoe naar de desbetreffende portefeuillehouders van het college, zodat deze politiek en bestuurlijk verantwoording kunnen afleggen aan de raad.

In de onderstaande tabel wordt weergegeven wat de personele formatie per gemeente is voor de CISO, PO en FG.

Rol Formatie in FTE, pijldatum 5 maart 2024	H2O, Hattem en Oldebroek	Elburg	Nunspeet	Putten
Chief Information Security Officer (CISO)	1,50	0,89	0,33	Geen data ontvangen.
Privacy Officer (PO)	1,50	1,00	0,33	
Functionaris Gegevensbescherming (FG)	0,60	0,44	0,50	

Tabel 2.1 Personele formatie per gemeente

Organisatie informatiebeveiliging

Binnen alle gemeenten stellen de gemeentesecretarissen het gewenste beveiligingsniveau vast en zij autoriseren de benodigde procedures en beheersingsmaatregelen die nodig zijn om dat beveiligings-niveau te behouden of te realiseren. Om de ambtelijke eindverantwoordelijkheid waar te kunnen maken worden de gemeentesecretarissen ondersteund door een CISO. Voor de H2O-gemeenten zijn daartoe twee CISO's aangesteld. Dit zijn sleutelfunctionarissen binnen de informatiebeveiligingsorganisatie. In hoofdlijnen bestaat hun rol uit:

> Het ontwikkelen en implementeren van het informatiebeveiligingsbeleid. Dat laatste door het opstellen van beveiligings- en verbeterplannen en projectleiders en proceseigenaren de opdracht geven de plannen uit te voeren;
> Het toezien op de naleving van dat beleid door onder andere het laten uitvoeren van audits, waaronder de ENSIA-evaluatie;
> Het inrichten en voeren van een incidentenregistratiesysteem, oplossen van incidenten en periodieke rapportage over incidenten naar de directie;
> Monitoren van de kwaliteit van de beheersing van het informatiebeveiligingsproces als geheel. Denk aan de kwaliteit van risicoanalyses, eisen die gesteld worden aan de architectuur, maar ook het bewustzijn onder medewerkers;
> Invulling geven aan specifieke rollen: Security Officer Suwinet, Algemeen Contactpersoon InformatieBeveiliging (ACIB), Vertrouwens Contactpersoon InformatieBeveiliging (VCIB), coördinator ENSIA, beveiligingsfunctionaris PNIK.

Proceseigenaren

Managers zijn verantwoordelijk voor de informatiebeveiliging van dat deel van de processen die onder hun sector of afdeling vallen. Dit worden proceseigenaren genoemd. De proceseigenaren rapporteren aan hun gemeentesecretaris over de door hen uitgevoerde informatiebeveiligingsmaatregelen en -activiteiten. In sommige gemeenten zijn proceseigenaren leden van het Management Team (MT), in andere gemeenten zijn het afdelingsmanagers/teamleiders die moeten rapporteren aan het betreffende

MT-lid. Afstemming met de andere organisatorische eenheden over de inhoudelijke aanpak vindt plaats door het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

In alle gemeenten is de invulling van de rol van proceseigenaar een zorgpunt. Voor proceseigenaren zelf is de rol niet altijd helder, of wordt nog niet altijd zo opgepakt, mede door hoge werkdruk komen proceseigenaren niet toe aan een goede invulling van deze rol.

Organisatie privacy

In alle gemeenten is het college bestuurlijk verantwoordelijk voor de verwerking van persoonsgegevens. In bepaalde gevallen ligt de verantwoordelijkheid bij een specifieke portefeuillehouder. Dat is het geval voor de openbare orde en veiligheid; de burgemeester is dan de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke moet zich verantwoorden over de omgang met persoonsgegevens en kunnen aantonen dat de AVG nageleefd wordt. Het college geeft de directie (gemeentesecretaris) opdracht om te voorzien in een team van professionals op het terrein van privacy. Dat team bestaat uit de Functionaris Gegevensbescherming (FG), de Privacy Officer (PO), maar ook de Chief Information Security Officer (CISO). De laatste richt zich niet zozeer op de vraag of persoonsgegevens conform de AVG worden verwerkt, maar wel op de beveiliging van deze gegevens.

De Privacy Officer (PO) maakt de gemeente bewust van het belang van privacy. Hij/zij ontwikkelt en bewaakt het privacybeleid en -procedures en geeft advies aan de proceseigenaren over een privacy-bestendige uitvoering van de processen. De PO kan bij de meer ingewikkelde vraagstukken de Functionaris voor Gegevensbescherming (FG) om advies vragen. De FG is binnen de gemeente de toezichthouder op de naleving van privacywetgeving conform artikel 37-39 AVG en doet in dat kader ook direct verslag aan het college. De FG is tevens aanspreekpunt voor de Autoriteit Persoonsgegevens.

Om te borgen dat de privacywet- en regelgeving in elk proces toegepast wordt, werken de gemeenten met proceseigenaren. Het is de bedoeling dat een proceseigenaar de eisen uit de AVG implementeert en beheersmaatregelen neemt als dat nodig is. De proceseigenaar kan daarbij advies vragen bij de PO en/of FG als dat nodig is. Advies over de veiligheid van de gegevens wordt gevraagd bij de CISO (informatieveiligheid).

Bijzonderheden:

> De H2O-gemeenten en Putten hebben binnen elke organisatorische eenheid een privacy-ambassadeur aangesteld, met uitzondering van de gemeente Hattem.

> Hij/zij vervult deze rol naast zijn/haar andere taken. De privacy-ambassadeur is binnen de eenheid het aanspreekpunt voor vragen over de AVG. Ook stimuleert de privacy-ambassadeur de eenheid om te werken volgens de AVG. Tot slot helpt de privacy-ambassadeur de eenheid bij het uitvoeren van taken die voortkomen uit de AVG, zoals het invullen van het verwerkingsregister en het opstellen van een verwerkersovereenkomst.

2.2 Kwaliteit van het proces

Algemeen

Meerdere keren geven gemeenten aan dat eerst het huis of de basis op orde moet zijn om verder te kunnen doorgroeien naar een hoger volwassenheidsniveau rondom informatiebeveiliging en waarborging van privacy.[14]

Risicomanagement

In het beleid van Putten is de risicoanalyse het meest uitgewerkt, zie het voorgaande hoofdstuk. Alle gemeente vinden een cyclus van risicomanagement belangrijk, maar hebben moeite met het daadwerkelijk implementeren van zo'n cyclus op het gebied van informatiebeveiliging en privacy. In grove lijnen gaat het om het in beeld krijgen van risico's, het inschatten van de zwaarte van risico's, het maken van een plan met maatregelen om de grootste risico's te minimaliseren en het uitvoeren van de maatregelen. De eerste stappen van deze cyclus worden uitgevoerd (beleid), maar de rol van proceseigenaar is binnen de gemeenten nog onvoldoende geborgd en helder bij de aangewezen proceseigenaren.

Control en verantwoording

Alle gemeenten hebben de ENSIA in hun beleid opgenomen. De ENSIA werkt als instrument om periodiek de stand van zaken rondom informatiebeveiliging te evalueren en daarover verticale verantwoording af te leggen aan wettelijke toezichthouders die een rol hebben in het toezicht op informatieveiligheid. Met de ENSIA leggen de gemeenten verantwoording af over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. De verantwoording over de informatiebeveiliging komt onder andere in het jaarverslag en in de Collegeverklaring Informatie-beveiliging tot uitdrukking. Met deze verklaring geven de colleges aan in hoeverre de gemeenten voldoen aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeenten gaanuitvoeren.

2.3 Regie op samenwerking

Tijdens het onderzoek is gevraagd om voorbeelden van verbonden partijen en private partijen waarmee de gemeenten samenwerken, waaruit blijkt dat gemeenten ook toezicht houden op de informatiebeveiliging en waarborging van privacy bij deze partijen. Denk bijvoorbeeld aan verbonden partijen in het geval de desbetreffende gemeenten verwerkingsverantwoordelijk zijn. Er zijn door de onderzoekers stukken ontvangen waaruit de aandacht voor informatiebeveiliging en privacy blijkt:

> De gemeente Oldebroek heeft een verwerkingsovereenkomst afgesloten met de Inclusief Groep NV, ten behoeve van de Wet sociale werkvoorziening.

> De Veiligheidsregio Noord- en Oost Gelderland heeft een Strategisch Informatiebeveiligings-beleid en er is een verwerkersovereenkomst afgesloten.

> De Omgevingsdienst Noord-Veluwe kwalificeert zichzelf, op basis van advies van de landsadvocaat Pels Rijcken, als verwerker.[15] Met de Omgevingsdienst Noord-Veluwe is door de H2O gemeenten reeds in 2017 een verwerkersovereenkomst afgesloten.[16] De gemeenten Nunspeet en Elburg hebben dit niet gedaan.[17]

---

[14] Bron: interviews

[15] Bron: Opdrachtgeversoverleg Omgevingsdienst Noord-Veluwe, 12 januari 2023.

[16] Bron: Verwerkersovereenkomst gemeente Oldebroek met ODNV, tevens bruikbaar in H2O verband, april 2017.

[17] Bronnen: e-mail van Elburg d.d. 11 december 2023, e-mail van Nunspeet d.d. 8 december 2023.

Met de verwerkersovereenkomsten is toezicht en controle door de gemeenten mogelijk. Het volgende is daartoe opgenomen:

> De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm;
> De toereikendheid van de informatiebeveiliging blijkt uit eigen controles of eigen mededelingen;
> Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet.

2.4 Financiële middelen

Alle gemeenten begroten de financiële middelen die nodig zijn voor I&A binnen het programma Bestuur van de programmabegroting. Dit is verder niet gedifferentieerd naar financiële middelen die nodig zijn voor informatiebeveiliging en waarborging van privacy. Enkel van de gemeente Elburg hebben de onderzoekers een verbijzonderd investeringsplan rondom Informatiebeveiliging ontvangen.

Uit gesprekken in het kader van dit onderzoek blijkt het ook ingewikkeld om informatiebeveiliging financieel te verbijzonderen, waarbij bij geïnterviewden ook bedenkingen zijn of dit wel zinvol is. Het probleem ligt niet bij het begroten van de personele lasten. De formatie voor het invullen van de functies - zoals een CISO, PO en GF - is immers bekend, los van de vraag of die formatieomvang voldoende is voor de taken waarvoor de functionarissen zijn aangesteld, dat hebben we in dit onderzoek niet onderzocht. De ingewikkeldheid zit in de infrastructuur, de hardware, de applicaties en de processen. Informatiebeveiliging is daar een integraal onderdeel van. De kosten daarvan zijn dan ook niet eenvoudig te verbijzonderen. Applicaties en softwarelicenties omvatten bijvoorbeeld naast functionaliteit, ook beveiligingseisen. Deze maken onlosmakelijk deel uit van de licentie. Ook maakt informatiebeveiliging integraal en onlosmakelijk onderdeel uit van de inrichting van de informatiearchitectuur en werkprocessen binnen de gemeenten.

2.5 Actuele ontwikkelingen en trends

Wetswijzigingen

De voorbereiding en implementatie van wetswijzigingen vormen een belangrijk onderdeel van de werkzaamheden van gemeentelijke organisaties, en informatiebeveiliging in het bijzonder. Daar wordt in de beleidsstukken van de gemeenten ook aandacht aan gegeven.

> De **Omgevingswet** integreert 26 wetten op het gebied van de fysieke leefomgeving, met als doel de regels voor ruimtelijke ordening te vereenvoudigen en samen te voegen. De wet is recent in werking getreden en heeft een grote impact op de digitale infrastructuur van de gemeenten;
> De **Wet open overheid** (Woo) heeft als doel overheidsorganisaties transparanter te maken. De Woo verplicht gemeenten om de informatiehuishouding op orde te brengen en hun digitale overheids-informatie duurzaam toegankelijk te maken en te houden. Actief openbaar maken van documenten in specifieke informatiecategorieën is een andere vereiste van de Woo. Het is de bedoeling dat alle bestuursorganen en uitvoeringsorganisaties hun openbare informatie koppelen aan het Platform Open Overheidsinformatie (PLOOI), zodat iedere inwoner van Nederland alle overheidsinformatie via die plek kan vinden. Deze verplichting geldt onder andere voor raads- en bestuursstukken en Wob/Woo-verzoeken. PLOOI bevat dan een verwijsindex en een zoekfunctie.
> De **Wet Hergebruik Overheidsinformatie** (Who). Deze wet is bedoeld om de openheid en het hergebruik van gegevens, die door organisaties met een publieke taak worden beheerd, te verbeteren. Personen kunnen, volgens de Who, een verzoek indienen om hergebruik van informatie mogelijk te maken. Als deze informatie vervolgens geleverd wordt, moet deze in een open en machine leesbaar formaat aangeboden worden.
> De **Wet Digitale Overheid**. Deze wet regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen krijgen met een substantiële of hoge mate van betrouwbaarheid.

> De **Wet Elektronische Publicaties**. Met deze wet wil de overheid de toegankelijkheid van (voorgenomen) overheidsbesluiten vergroten door alle wettelijk voorgeschreven bekendmakingen, mededelingen en kennisgevingen van (voorgenomen) besluiten die niet tot een of meer belanghebbenden zijn gericht, te publiceren in de officiële elektronische publicatiebladen van de openbare lichamen waartoe de bestuursorganen behoren. Daarbij dienen deze publicatiebladen op gestandaardiseerde wijze te worden gepubliceerd op www.officielebekendmakingen.nl. Door deze standaardisatie wordt het voor burgers mogelijk om op één website alle algemene bekendmakingen, mededelingen en kennisgevingen van de overheid te raadplegen.
> De **Wet Modernisering Elektronisch en Bestuurlijk Verkeer**. Het wetsvoorstel geeft de burger recht om elektronisch berichten aan een bestuursorgaan te zenden op een door het bestuursorgaan bepaalde wijze.
> De **NIS2-richtlijn** (Network and Information Security directive) is de opvolger van de NIS-richtlijn. Deze is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2 vergroot de reikwijdte van de eerste richtlijn door meer sectoren te omvatten. Daarnaast stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. De NIS2 wordt momenteel naar Nederlandse wetgeving vertaald.

Common Ground[18]

Common Ground is een informatiekundige visie waarmee gemeenten collectief de informatie-voorziening eenvoudiger, flexibeler en slimmer gaan inrichten. Het doel van Common Ground is het sneller en slimmer oplossen van maatschappelijke opgaven en het terugwinnen van de controle over de eigen gegevens. Het is een VNG-initiatief dat is ontstaan vanuit de behoefte aan een nieuwe, moderne en gezamenlijke informatievoorziening voor gemeenten. Dit moet het mogelijk maken om snel en flexibel te vernieuwen, te voldoen aan privacywetgeving en efficiënt om te gaan met data. Het draait om een structurele hervorming van de gemeentelijke informatievoorziening, waarbij gegevens uniform worden gemaakt, gegevens via API's worden opgehaald en er met één gemeenschappelijke integratie-laag wordt gewerkt.

Een API (Application Programming Interface) is een softwareverbinding die het mogelijk maakt dat twee of meer applicaties met elkaar kunnen communiceren.

Dit leidt tot een transitie die grondig moet worden voorbereid en waarvoor een nieuwe visie op gegevensmanagement nodig is. Nieuwe Common Ground-applicaties zullen gaan draaien op een gestandaardiseerd platform genaamd Haven.

Internet of Things (IoT)

In de beleidsstukken van de vijf gemeenten wordt geen aandacht gegeven aan IoT.

Er worden steeds meer apparaten met elkaar verbonden via internet, denk bijvoorbeeld aan camera's, sensoren die allerlei zaken meten in onze leefomgeving maar ook geautomatiseerde besturingssystemen van verkeerslichten of bruggen et cetera. De diversiteit en alomtegenwoordigheid van IoT-apparaten maakt ze aantrekkelijke doelwitten voor cyberaanvallen, en hun onderling verbonden karakter kan tot wijdverbreide kwetsbaarheden leiden.

Kloof in cybersecurityvaardigheden en onderwijs

In de beleidsstukken van de vijf gemeenten wordt geen aandacht gegeven aan het tekort aan cybersecurityprofessionals.

---

[18] Bron: https://vng.nl/artikelen/common-ground

Naarmate cyberdreigingen geavanceerder worden, stijgt de vraag naar ervaren cybersecurity-professionals. Er is echter een groot tekort aan mensen die zijn uitgerust met de noodzakelijke vaardigheden en kennis om deze evoluerende bedreigingen effectief te bestrijden. Deze kloof vormt een risico voor organisaties. Uit de ambtelijke verificatie van het conceptrapport van bevindingen geeft de gemeente Oldebroek overigens aan geen tekort te hebben aan cybersecurityprofessionals.

Kunstmatige intelligentie, Artificial Intelligence (AI)

In het strategisch informatiebeveiligingsbeleid H2O wordt (summier) aandacht gegeven aan AI. In de beleidsstukken van de andere gemeenten niet.

AI en Machine Learning (ML) maken de afgelopen jaren een enorme ontwikkeling door en zal daarmee ook een belangrijke rol spelen in informatiebeveiliging. Bijvoorbeeld:

> Data-analysemogelijkheden van AI kunnen worden gebruikt voor het identificeren en voorspellen van cyberdreigingen;
> ML-algoritmen zullen in staat zijn nieuwe dreigingen te herkennen en erop te reageren, waardoor defensieve maatregelen steeds verder worden verbeterd;
> ML zal waarschijnlijk ook vooruitgang boeken bij het autonoom aanpassen en bijwerken van cybersecurityprotocollen, waardoor de afhankelijkheid van handmatige updates wordt verminderd;
> Mogelijk zullen in de toekomst AI-gestuurde securitybots worden geprogrammeerd om onafhankelijk cyberdreigingen te identificeren en te neutraliseren. Informatiebeveiliging wordt daarmee minder reactief en meer proactief.

3 Sturing door de raad

In dit hoofdstuk worden de deelvragen 8 en 9 beantwoord. In afwijking met de voorgaande hoofdstukken geven we geen korte beantwoording direct onder het onderstaande kader. De deelvragen kunnen namelijk al redelijk kort worden beantwoord in de paragrafen van dit hoofdstuk.

DEELVRAGEN

8 Hoe en met welke informatie worden de raden door het college in positie gebracht om hun kaderstellende rol uit te kunnen oefenen?

9 Hoe en met welke informatie worden de raden door de colleges in positie gebracht om hun controlerende rol uit te kunnen oefenen?

TOEGEPASTE NORMEN

- De raad stelt het beleid vast (doelen en kaders) en controleert (tussentijds) de mate waarin doelen binnen de kaders worden gerealiseerd.
- De raad wordt hiertoe door het college met voldoende informatie in positie gebracht.

3.1 Bevoegdheden van de raad en het college

De raden hebben ten aanzien van informatiebeveiliging en privacy geen kaderstellende rol. Dit valt geheel binnen de bevoegdheid van het college. Het college gaat immers over de bedrijfsvoering van de gemeente. Daarbij is ten aanzien van de onderwerpen informatiebeveiliging en privacy de speelruimte van het college gering. Het beleid wordt namelijk voornamelijk bepaald door Nationale en Europese wet- en regelgeving. Het college is wel bestuurlijk eindverantwoordelijk voor de informatieveiligheid en privacy van haar gemeente. Het college stelt dan ook het informatiebeveiligings- en privacybeleid vast.

Het college legt verantwoording af over het gevoerde beleid. Er is sprake van een verticaal verantwoordingsproces van het college aan toezichthouders die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe toegepast dat alle informatie die noodzakelijk is voor verticale verantwoording ook onderdeel is van het horizontale verantwoordingsproces. Met dat laatste heeft de raad een controlerende rol; we lichten de rolinvulling van de verschillende raden hieronder verder toe.

3.2 Rolinvulling door de raden in de praktijk

Uit gesprekken met een afvaardiging van de raden is een beeld gevormd hoe raden hun controlerende rol in de praktijk invullen. De raden ontvangen van het college jaarlijks de rapportages uit evaluaties en audits rondom informatiebeveiliging en privacy. Hiermee zouden de raden in staat moeten zijn om de controlerende rol richting het college in te vullen. Over het algemeen geven raden aan de invulling van deze rol moeilijk te vinden. Zij zien informatiebeveiliging en privacy vooral als een randvoorwaardelijke zaak waarbij geen politieke keuzes spelen. Er is dan ook nauwelijks raadsaandacht voor deze onderwerpen. Het hang sterk af van de kennis en interesse van individuele raadsleden of er vragen aan het college worden gesteld.

We lichten dit hieronder verder toe per gemeente.

Rol van de raad (Elburg)

De Elburgse gemeenteraad heeft voornamelijk een controlerende en toetsende rol. Deze rol is (op het gebied van informatiebeveiliging) ook concreet vastgelegd in het informatie-beveiligingsbeleid. In de

praktijk blijkt het afhankelijk van de kennis en interesse van een raadslid of ook daadwerkelijk inhoudelijke vragen over dit onderwerp wordt gesteld.

Rol van de raad (Hattem)

Voor de Hattemse raad is het technische gehalte van de informatie, als het gaat over ICT en informatiebeveiliging, te hoog. Hierdoor haken raadsleden af en is er onvoldoende collectieve aandacht vanuit de raad voor informatiebeveiliging. Dat blijkt onder andere ook uit de matige interesse voor informatiebijeenkomsten over dit onderwerp. Zo is er ten behoeve van dit onderzoek een informatie-sessie aangeboden, maar deze is inmiddels vier keer uitgesteld.

Rol van de raad (Nunspeet)

De Nunspeetse raad wordt door het college in ruime mate geïnformeerd. Er worden volgens raadsleden veel stukken ter informatie naar de raad gestuurd. Wanneer een raadslid additionele informatie zou willen over een bepaald onderwerp, dan wordt deze een maand later op de agenda gezet.

De raad vult de controlerende rol in door vragen te stellen aan het college. In een gesprek in het kader van dit onderzoek geven raadsleden aan dat meer bewustwording bij raadsleden over informatie-beveiliging nodig en zinvol is. Zowel in positieve zin (wat levert ICT op en wat zijn de mogelijkheden?) en in negatieve zin (wat zijn de gevaren en belemmeringen?).

Rol van de raad (Putten)

De controlerende rol van de Puttense raad op het gebied van informatiebeveiliging en privacy moet binnen de gemeente nog goed vorm gegeven worden. Dat is ook gaande. Zo is er is een handreiking 'Gemeenten en privacy: wat kunt u als raadslid doen?', dat is gedeeld met de raad. De Functionaris Gegevensbescherming heeft ook contact gehad met de griffiers om te bespreken op welke wijze de raad meer betrokken kan worden.

Sinds vorig jaar is er meer inhoudelijke belangstelling voor informatiebeveiliging en privacy omdat er raadsleden zijn die hier interesse in hebben. Er is aandacht gevraagd voor informatiebeveiliging, een motie hierover is aangenomen en extra budget is beschikbaar gesteld.

Rol van de raad (Oldebroek)

De Oldebroekse gemeenteraad heeft vooral een controlerende rol. De raad doet dit op het niveau van de gemeentelijke begroting en de jaarrekening. De onderwerpen informatievoorziening, -beveiliging en privacy spelen daarbij geen grote rol. Voor de raad zijn dit randvoorwaardelijke zaken en er spelen geen politieke vraagstukken op dit terrein.

Bijlage 1: De basisbeveiligingsniveaus

De drie basisbeveiligingsniveaus van de Baseline Informatiebeveiliging Overheid (BIO)

Basisbeveiligingsniveau 1 (BBN1)
Dit is het niveau waaraan alle overheidssystemen minimaal dienen te voldoen. Hierbij gaat het om het voldoen aan wet- en regelgeving (zoals de AVG) en algemeen geldende beveiligingsprincipes.

Basisbeveiligingsniveau 2 en niveau 2+ (BBN2 en BBN2+)
BBN2 is van toepassing indien er sprake is van verwerking van vertrouwelijke informatie. Mogelijke incidenten leiden tot bestuurlijke commotie en de veiligheid van andere systemen is afhankelijk van de veiligheid van het eigen systeem. Ongewenst openbaren van informatie kan leiden tot politieke schade aan bestuurders, financiële gevolgen die niet meer op te vangen zijn binnen de begroting, verlies van publiek respect en imagoschade en aanwijzingen van de Autoriteit Persoonsgegevens door schending van privacy. Op dit niveau moeten overheden bewust preventieve maatregelen nemen. BBN2+ is in het leven geroepen omdat het voor gemeenten soms noodzakelijk is om aanvullende maatregelen te nemen boven BBN2. Deze set aan maatregelen is opgesteld in samenwerking met gemeenten en dient ter inspiratie waar men aan kunt denken als men extra maatregelen moet implementeren. De maatregelen die erin staan zijn dus niet verplicht en ook niet uitputtend en worden genomen op basis van een eigen risico-inschatting.

Basisbeveiligingsniveau 3 (BBN3), niet van toepassing voor gemeenten
Het gaat hier om de bescherming van gegevens die zijn gerubriceerd als Departementaal Vertrouwelijk. Het verlies van deze gegevens heeft een grote impact waarbij actief weerstand moet worden geboden tegen dreiging van statelijke actoren (andere landen) en beroepscriminelen. We gebruiken hier de term 'actief', dat verder gaat dan preventief. We bedoelen hier dat dreigingen moeten kunnen worden gedetecteerd, waarop vervolgens gereageerd moet worden.

Bijlage 2: Lijst van veel gebruikte termen en afkortingen

AP	Autoriteit Persoonsgegevens: nationale instantie die toezicht houdt op bescherming van persoonsgegevens.
API	Application Programming Interface: softwareverbinding die het mogelijk maakt dat twee of meer applicaties met elkaar kunnen communiceren.
AVG	Algemene Verordening Gegevensbescherming: Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation).
BAG	Basisregistratie Adressen en Gebouwen.
BIO	Baseline Informatiebeveiliging Overheid.
BMS	Bewustwording Management Systeem.
BRO	Basisregistratie Ondergrond.
BRP	Basisregistratie Personen: applicatie met persoonsgegevens van de inwoners.
CIO	Chief Information Officer: functionaris die de algemene verantwoordelijkheid heeft voor de netwerken, systemen, hardware, software en cloudcomputing-activiteiten van de organisatie.
CISO	Chief Information Security Officer: de centrale functionaris voor informatiebeveiliging.
CMM	Capability Maturity Model: geeft aan op welk niveau de software-ontwikkeling van een organisatie zit.
DPIA	Data Protection Impact Assessment: analyse op risico's in verband met privacy en gegevens-bescherming. Onder de AVG verplicht bij gegevensverwerking met een waarschijnlijk hoog privacy-risico.
ENSIA	Eenduidige Normatiek Single Information Audit: eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders).
FG	Functionaris Gegevensbescherming: belast met toepassing en naleving van de AVG.
GAP	Is de Engelse term voor 'kloof'; het verschil tussen bestaande situatie en gewenste situatie.
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn.
I&A	Informatie & Automatisering.
IBD	Informatiebeveiligingsdienst voor gemeenten.
IoT	Internet of Things: apparaten met elkaar verbonden via internet.
ISMS	Informatie Securitymanagement System: om informatiebeveiliging te waarborgen en besturen.
Patch-management	Gecontroleerd en planmatig identificeren van kwetsbaarheden, testen en uitrollen van patches, en updates van software. Het doel is om up-to-date te zijn en tegelijk de dienstverlening zo min mogelijk te verstoren.
PDCA	Plan-Do-Check-Act: de beleidsleercyclus.
PNIK	Paspoorten en Nederlandse Identiteitskaarten: dit is een aanvullende beveiligingseis.
PO	Privacy Officer: maakt de gemeente bewust van het belang van privacy.
Privacy by design	Bij het ontwerp van producten en diensten dient nagedacht te worden over privacy.
Proceseigenaar	Implementeert de eisen uit de AVG en neemt beheersmaatregelen als dat nodig is.
SOD	Segregration of Duties: is een functiescheiding; bepaalde verantwoordelijkheden worden over meer dan één persoon gespreid.
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen: de gemeenten, het UWV en sociaal ontwikkelbedrijven voeren samen een aantal wettelijke taken uit.
Suwinet	Via Suwinet kunnen overheidsorganisaties gegevens van inwoners en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen.
Wmo	Wet maatschappelijke ondersteuning.
Wob	Wet openbaarheid van bestuur.
Woo	Wet open overheid.

Bijlage 3: Respondenten en schriftelijke bronnen

Interviews

Aanhef Dhr./Mw.	Naam	Functie	Organisatie
Interviews met portefeuillehouders en ambtelijke sleutelpersonen			
Dhr. J.N.	Rozendaal	Burgemeester, portefeuille ICT	Gemeente Elburg
Dhr. V.	Petkovic	Adviseur Informatisering	
Mw. B. van	Voorst	Chief Information Security Officer	
Dhr. P.	Baars	Adviseur ICT	
Dhr. J.	Hofstede	Domeinmanager Samenleving/proceseigenaar	
Dhr. J.P. den	Boer	Functioneel beheerder GEO	
Dhr. M.	Degeling	Domeinmanager bedrijfsvoering/proceseigenaar	
Dhr. P.	Band	Privacy Officer	
Dhr. T.	Vroon	Functionaris Gegevensbescherming	
Dhr. E. 't	Jonge	Wethouder, portefeuille ICT	Gemeente Putten
Mw. M.	Udo	Functionaris Gegevensbescherming	
Dhr. GJ.	Fierloos	Chief Information Officer	
Dhr. H.	Timmerman	Chief Information Security Officer	
Dhr. J.	Koning	Privacy Officer	
Mw. D.	Kolder	Concern controller	
Dhr. K.	Castelein	Wethouder, portefeuille ICT	Gemeente Hattem
Dhr. H. van	Dijk	Concern controller	
Dhr. J.	Boorsma	Chief Information Security Officer	
Dhr. G. van	Beek	Beleidsadviseur/proceseigenaar inhuur, KCC en burgerzaken.	
Dhr. H. van	Dijk	Manager Bedrijfsvoering, proceseigenaar ketenondersteuning.	
Dhr. B.	Engberts	Wethouder, portefeuille ICT	Gemeente Oldebroek
Dhr. P.	Lensselink	Gemeentesecretaris	
Dhr. B.	Disco	Concern controller	
Dhr. J.	Boorsma	Chief Information Security Officer	
Mw. G.	Zielhuis	Team Samenleving/proceseigenaar	
Dhr. J.van	Dijk	Team Leefomgeving/proceseigenaar	
Mw. S.	Zandbergen	Team Dienstverlening/proceseigenaar	
Dhr. F.	Beekhuis	Team Ruimte/proceseigenaar	
Mw. P.	Tanahatoe	Team Bedrijfsvoering/proceseigenaar	
Dhr. W.	Stoffer	Wethouder, portefeuille ICT	Gemeente Nunspeet
Dhr. L. van den	Bogaard	Informatiemanager	
Dhr. P.	Baas	Chief Information Security Officer/Privacy Officer (PO)	
Dhr. J.	Gardenbroek	Teammanager Personeel, Organisatie en Communicatie/concerncontroller.	
Dhr. T.	Vroon	Functionaris Gegevensbescherming	
Mw. T.	Rolink	Teammanager Informatie/proceseigenaar	
Dhr. A.	Dickhof	Teammanager RO & Volkshuisvesting/proceseigenaar	
Dhr. P.	Smink	Beleidsmedewerker Vastgoed	
Dhr. J.	Boorsma	Chief Information Security Officer	H2O organisatie
Dhr. R.	Brinkhof	Functionaris Gegevensbescherming	

Aanhef Dhr./Mw.	Naam	Functie	Organisatie
Mw. G.	Kurnaz	Privacy Officer	(Hattem en Oldebroek)
Dhr. H.	Hendriks	Chief Information Security Officer (50%) en Privacy Officer (50%)	
Dhr. H. van	Rooij	Interim Chief Information Officer	
Groepsgesprek met een afvaardiging van de raden			
Dhr. A. van	Dijk	Raadslid	Gemeente Elburg
Dhr. J. van der	Reijden	Burgerraadslid	Gemeente Elburg
Dhr. J.N.	Rozendaal	Burgemeester	Gemeente Elburg
Dhr. G.	Schoots	Burgerraadslid	Gemeente Elburg
Dhr. J. van der	Velde	Burgerraadslid	Gemeente Elburg
Dhr. T.	Juk	Fractievoorzitter	Gemeente Hattem
Dhr. M.	Kers	Raadslid	Gemeente Hattem
Mw. P.	Koortens	Raadslid	Gemeente Hattem
Dhr. E.	Kort	Raadslid	Gemeente Hattem
Dhr. J.J.	Zijlstra	Raadslid	Gemeente Hattem
Dhr. J. van den	Hoorn	Raadslid	Gemeente Nunspeet
Dhr. W.H.	Peggeman	Raadslid	Gemeente Oldebroek
Dhr. H.	Tabak	Griffier	Gemeente Oldebroek

Geraadpleegde schriftelijke stukken

S	Volg-nr.	Jaar	Maand-nr.	Titelbeschrijving
Gemeente Elburg				
SA	1			Gemeente Elburg, *Beschrijving Informatievoorziening en ICT*, datum onbekend
SA	2			Gemeente Elburg, *Verwerkingenregister Elburg concept*, datum onbekend
SA	3	2019	1	Gemeente Elburg, *Collegevoorstel Dienstverleningsconcept 2020*, 29 januari 2019
SA	4	2019	10	Gemeente Elburg, *Privacybeleid gemeente Elburg*, 20 oktober 2019
SA	5	2020	1	Gemeente Elburg, *Cryptografiebeleid gemeente Elburg 2021*, 4 januari 2021
SA	6	2020	7	Gemeente Elburg, *Gedragsregeling voor digitale werkomgeving*, 21 juli 2020
SA	7	2020	11	Gemeente Elburg, *Informatiebeveiligingsbeleid gemeente Elburg 2021-2023*, 9 november 2020
SA	8	2022	4	Gemeente Elburg, *Memo Domeinmanager bedrijfsvoering: Organisatie brede afspraken toegang leveranciers*, 11 april 2022
SA	9	2022	5	Gemeente Elburg, *Collegeprogramma 2022-2026*, mei 2022?
SA	10	2022	6	Gemeente Elburg, *Incidentmanagement- en respons protocol*, 13 juni 2022
SA	11	2023		Gemeente Elburg, *Logisch toegangsbeveiligingsbeleid gemeente Elburg 2023-2026*, datum onbekend.
SA	12	2023		Gemeente Elburg, *Continuïteitstratege gemeente Elburg 2023*, datum onbekend
SA	13	2023	2	Gemeente Elburg, *Procesbeschrijving Logging & Monitoring*, 9 februari 2023
SA	14	2023	4	Gemeente Elburg, *Plan van Aanpak Organisatieontwikkeling 2023*, 20 april 2023
SA	15	2023	5	Gemeente Elburg, *Informatiestrategie (concept)*, mei 2023
SA	16	2020	2	Gemeente Elburg, *Verwerkingenregister Hattem*, 20 februari 2020
SA	17	2020	5	Gemeente Elburg, *Beantwoording vragen raadslid bij kadernota over*

S	Volg-nr.	Jaar	Maand-nr.	Titelbeschrijving
				I-dienst, 25 mei 2020
Gemeente Hattem				
SB	1			Gemeente Hattem, *Bijlage 6: belegging verantwoordelijkheden DigiD-koppelingen, aanvulling op strategisch informatiebeveiligingsbeleid*, datum onbekend
SB	2			Gemeente Hattem, *Privacybeleid gemeente Hattem 'Grip op privacy'*, datum onbekend
SB	3	2021	11	Gemeente Hattem, *Programmabegroting 2022*, november 2021
SB	4	2022	5	Gemeente Hattem, *Bestuursakkoord Hattem 2022-2026 'Inspireren, Verbinden, Versterken'*, mei 2022?
SB	5	2022	11	Gemeente Hattem, *Programmabegroting 2023*, november 2022
Gemeente Nunspeet				
SC	1			Gemeente Nunspeet, *Overzicht uitgevoerde pre-DPIA's en DPI's gemeente Nunspeet*, datum onbekend
SC	2			Gemeente Nunspeet, *Bijlage E bij informatiebeveiligingsbeleid 2021-2024: DigiD-uitwerking norm B.01*, datum onbekend
SC	3	2017		Gemeente Nunspeet, *Informatiebeleidsplan 2017-2020*, datum onbekend
SC	4	2019	9	Gemeente Nunspeet, *Strategisch gemeentelijk Informatie-beveiligingsbeleid Nunspeet 2021-2024*, 1 september 2019?
SC	5	2020		Gemeente Nunspeet, *Aanvullend Gemeentelijk Informatie-beveiligingsbeleid BP en Waardedocumenten 2020*, datum onbekend
SC	6	2020		Gemeente Nunspeet, *Aanvullend Gemeentelijk Informatiebeveiligingsbeleid Suwinet 2020*, datum onbekend
SC	7	2021	1	Gemeente Nunspeet, *Privacybeleidskader gemeente Nunspeet 2020-2024*, 1 januari 2021
SC	8	2022		Gemeente Nunspeet, *Collegeprogramma gemeente Nunspeet 2022-2026 'Samen meer voor elkaar'*, 2022
SC	9	2022		Gemeente Nunspeet, *Visie op dienstverlening 2023-2027*, 2022?
SC	10	2022		Gemeente Nunspeet, *Strategisch HR beleid gemeente Nunspeet 2022-2025*, datum onbekend
SC	11	2022		Gemeente Nunspeet, *Flyer Hybride werken 2022*, datum onbekend
SC	12	2022	1	Gemeente Nunspeet, *Programmabegroting 2023-2026*, november 2022
SC	13	2022	1	Inkoopsamenwerking Noord Veluwe (ISNV), *Inkoopbeleid gemeenten (10), ODNV, GR Meerinzicht en bvo H2O*, 1 januari 2022
SC	14	2022	6	Gemeente Nunspeet, *Jaarstukken 2021*, 30 juni 2022
SC	15	2023		Bakertilly, *Management letter 2022 gemeente Nunspeet*, incl. IT-audit, 2023
SC	16	2023	6	Gemeente Nunspeet, *Jaarstukken 2022*, juni 2023. Inclusief bijlagenboek
SC	17	2023	6	Gemeente Nunspeet, *Excelbestand-jaarcijfers I&A 2023 e.v.*, juni 2023
Gemeente Putten				
SD	1			Gemeente Putten, *Overzicht DPIA's*, datum onbekend
SD	2			Gemeente Putten, *Verwerkingenregister*, datum onbekend
SD	3	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Privacybeleid 2020*, februari 2020
SD	4	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Bijlage 1 bij privacybeleid 2020: Governance Informatieveiligheid en Privacy (IP)*, februari 2020
SD	5	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Bijlage 2 bij privacybeleid 2020: Uitwerking AVG*, februari 2020
SD	6	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Bijlage 3 bij privacybeleid 2020: Incident management en response*, februari 2020
SD	7	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Bijlage 4 bij privacybeleid 2020: Procedure DPIA*, februari 2020

S	Volg-nr.	Jaar	Maand-nr.	Titelbeschrijving
SD	8	2020	2	Gemeenten Bunschoten, Leusden, Nijkerk en **Putten**, *Bijlage 5 bij privacybeleid 2020: Procedure Rechten van Betrokkenen op grond van AVG*, februari 2020
SD	9	2021	11	Gemeente Putten, *Begroting 2022-2025 beleidsdeel,* november 2021
SD	10	2022	5	Gemeente Putten, *Coalitieakkoord 2022-2026 'En nu door'*, mei 2022
SD	11	2022	11	Gemeente Putten, *Begroting 2023-2026 beleidsdeel,* november 2022
SD	12	2022	12	Gemeente Putten, *Memo Actualisatie risicomanagement*, 8 december 2022
SD	13	2023	5	Gemeente Putten, *Jaarstukken 2022*, 23 mei 2023
Gemeente Oldebroek				
SE	1	2017	3	Verwerkersovereenkomst gemeente Oldebroek met Omgevingsdienst Noord-Veluwe, maart 2017.
SE	2	2021	5	Gemeenten Elburg, Hattem, Heerde, Nunspeet en Oldebroek, *rapport onderzoek uitgevoerd door Native: I&A-samenwerking H2ONE*, 4 mei 2021
SE	3	2022	4	Gemeente Oldebroek, *Informerende raadsnota ICT samenwerking H2ONE*, 21 april 2022
SE	4	2022	10	Autoriteit Persoonsgegevens, *Handreiking 'Gemeente en privacy: wat kunt u als raadslid doen?'*, 2 oktober 2022
SE	5	2022	10	Autoriteit Persoonsgegevens, *Handreiking 'Gemeente en privacy: wat kunt u als raadslid doen bij samenwerkingsverbanden?'*, 1 oktober 2022
SE	6	2023		M&I/Partners, *ICT Benchmark gemeenten 2022*, datum onbekend
SE	7	2023	4	Gemeente Oldebroek, *Brief zienswijze begroting 2024-2027 BVO H2O (i-Dienst), 12 april* 2023
SE	8	2023	4	Bedrijfsvoeringsorganisatie H2O, *Begroting i-Dienst 2024-2027*, 3 april 2023
SE	9	2023	4	Bedrijfsvoeringsorganisatie H2O, *Aanbiedingsbrief raadsleden gemeente Hattem, Heerde en Oldebroek bij Begroting 2024-2027*, 12 april 2023
SE	10	2023	7	Gemeente Oldebroek, *Voorstel en besluit gemeenteraad: Kadernota 2024-2027 Bedrijfsvoeringsorganisatie H2O (i-Dienst), 6 juli 2023*