Gemeente Gouda

memo aan de gemeenteraad

aan	de gemeenteraad
dossiernummer	8123
onderwerp	Raadsmemo collegeverklaring ENSIA 2023
van	het college van burgemeester en wethouders
datum	9 april 2024

Memo

Inleiding
Jaarlijks moet het college zich verantwoorden over de kwaliteit van de informatieveiligheid van DigiD en Suwinet aan de hand van de Eenduidige Normatiek Single Information Audit (ENSIA). Het doel van deze audit systematiek is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad en aan de nationale toezichthouders.

Toelichting
Naar aanleiding van een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG, heeft de VNG samen met het rijk een efficiënte verantwoordingssystematiek ontwikkeld: de Eenduidige Normatiek Single Information (ENSIA).Hiervoor zijn de verantwoordingssystematieken voor de Basisregistratie Personen (BRP), Reisdocumenten (PUN en PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en Inkomen (Suwinet) samengevoegd en gestroomlijnd. Dit betekent dat er niet voor alle onderdelen afzonderlijke audits (die elkaar deels overlappen) moeten worden uitgevoerd. Ook hoeven er geen afzonderlijke rapportages opgesteld worden

Per 2018/2019 zijn gemeenten eveneens wettelijk verplicht om een jaarlijkse zelfevaluatie in te vullen voor de BAG, BGT en BRO, waarmee het college van burgemeester en wethouders horizontaal verantwoording aflegt aan de gemeenteraad voor het gevoerde beleid. Tevens wordt met deze zelfevaluatie verticaal verantwoording afgelegd aan het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, als formeel toezichthouder.

Zelfevaluatie en resultaten

Collegeverklaring ENSIA 2023
Met de voorliggende ENSIA-collegeverklaring 2023 geeft het college aan in hoeverre de beheersingsmaatregelen voldoen aan de normen die gelden voor DigiD en Suwinet en op welke onderdelen de gemeente niet voldoet aan deze normen. De collegeverklaring is opgesteld aan de hand van de uitkomsten van de zelfevaluaties die door de lijnverantwoordelijken zijn uitgevoerd, onder coördinatie van de ENSIA coördinator / CISO.

In de collegeverklaring verklaart het college dat de gemeente Gouda op 31 december 2023 niet geheel voldoet aan alle geselecteerde normen inzake DigiD en Suwinet die nodig zijn voor de informatieveiligheid. Zowel voor DigiD als voor Suwinet is een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

Rapportage BAG, BGT en BRO
De kwaliteit en actualiteit van de BAG en BGT zijn hoog. Bij de BAG komt dit door de goede samenwerking met de ODMH en de BSGR (Belastingen). Voor het bijhouden van de BGT geldt dat voor de samenwerking met de collega's van Projecten openbare ruimte en Beheer openbare ruimte.

De bekendheid met de basisregistratie ondergrond (BRO) wordt steeds groter hoewel sommige bedrijven het lastig blijven vinden. Positieve ontwikkeling is dat er steeds meer bodem- en grondonderzoeken worden aangeleverd. Ook is een 2e BRO beheerder aangesteld om de organisatie robuuster te maken. BRO wordt ook steeds meer gevuld. We scoren goed. Het beheer hiervan is complexer omdat de aanleverplicht bij opdracht nemende partijen ligt. Deze zijn nog niet allemaal even ervaren met deze relatief nieuwe basisregistratie.

Status implementatie Baseline Informatiebeveiliging Overheid (BIO)
Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht geworden en vormt de BIO het normenkader voor informatiebeveiliging. In 2022 heeft de gemeente Gouda een organisatiebrede risico- en GAP-analyse uitgevoerd op vlak van informatiebeveiliging. In 2023 is de GAP-analyse geactualiseerd. Met een GAP-analyse vindt er een toetsing plaats van de verschillen tussen het vastgestelde informatieveiligheidsbeleid (BIO) en de situatie in praktijk. De BIO vormt het normenkader voor informatiebeveiliging en bestaat uit ruim 251 maatregelen waarvan op dit moment ongeveer 86% geheel of gedeeltelijk door de gemeente Gouda zijn geïmplementeerd. Dit is landelijk gezien een bovengemiddelde score. Als dit percentage wordt vertaald naar concrete verbeteracties, dan blijkt dat in totaal 39 maatregelen (van de ruim 251 maatregelen) nog geheel of gedeeltelijk moeten worden uitgevoerd om aan alle normen van de BIO te voldoen.

Het voldoen aan de eisen en normen van de BIO is natuurlijk geen doel op zich, maar wel een belangrijke graadmeter van onze volwassenheid als organisatie en kwetsbaarheden op het gebied van informatiebeveiliging. Vanuit de bevindingen van de organisatiebrede risicoanalyse, de ENSIA-audit 2023 en het Dreigingsbeeld 2023-2024[1] van de Informatiebeveiligingsdienst (IBD) wordt hier proactief op ingespeeld. Onderstaand de status van de acties m.b.t. de implementatie van de BIO zoals deze in 2023 door de gemeente Gouda zijn gestart:

- Strategisch informatieveiligheidsbeleid (BIO-maatregel 5.1.1)
  Door het college is op 13 maart 2024 het strategisch informatiebeveiligingsbeleid Gouda 2024 vastgesteld. Met het nieuwe strategisch informatiebeveiligingsbeleid gaat de gemeente Gouda verder op de ingeslagen weg van verbetering van de beveiliging van (vertrouwelijke) informatie en persoonsgegevens binnen de gemeente. Het strategisch informatiebeveiligingsbeleid is richtinggevend en kader stellend en onverkort van toepassing op de hele gemeentelijke organisatie. De komende jaren zetten we in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfuncties, zodat we blijven aansluiten op de veranderende wetgeving (o.a. NIS2) en dat informatiebeveiliging bij alle ontwikkelingen vanaf het begin als belangrijk thema wordt meegenomen.

- Bewustwording (BIO-maatregel 7.2)
  Uit de risico-inventarisatie is naar voren gekomen dat vooral bewustwording/menselijk gedrag, een aandachtspunt is binnen de gemeente Gouda. Aangezien dit ook een aandachtspunt is uit het Dreigingsbeeld 2023-2024 is dit een belangrijk onderdeel om de weerbaarheid van Gouda te verhogen. Op basis van de resultaten van de nulmeting wordt in 2024 een bewustwordingsprogramma opgesteld. Het streven is om het bewustwordingsprogramma in 2025 te implementeren.

- Bedrijfscontinuïteit (BIO- maatregel 17.1)
  Gemeente Gouda wil graag het continuïteitsmanagement beter inrichten. Dit om zich beter voor te bereiden in het geval van een continuïteitsprobleem. Inmiddels zijn op basis van een dataclassificatie de volgende 6 kritieke processen bepaald:
  - Burgerzaken
  - IT-infrastructuur (essentiële componenten)
  - Betaling van uitkeringen
  - Rioolbeheer
  - Verkeersregeling
  - Brugbediening

[1] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2022/10/IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf

Vervolgens is er een bedrijfscontinuïteitsplan opgesteld inclusief een crisisstructuur voor specifieke calamiteiten met gevolgen voor de bedrijfsvoering van de gemeentelijke organisatie. Hierbij is zoveel mogelijk aangehaakt bij de bestaande veiligheid crisisorganisatie. Voor deze kritieke processen is een Business Impact Analyse (BIA) uitgevoerd en in de loop van 2024 wordt per proces een draaiboek opgesteld met als doel de basistaken van de gemeente te waarborgen bij calamiteiten/crisis zoals een hack, ransomware aanval, brand, extreem weer, lekkage, pandemie, explosies of uitval van (nuts)voorzieningen.

- Logging en Monitoring (BIO-maatregel 12.4)
  Een van de eisen die de BIO stelt (onder het hoofdstuk 'verslaglegging en monitoren') aan overheden, is het gebruik van SIEM en SOC. SIEM staat voor Security Information & Event Management, SOC voor Security Operations Center. Een dergelijke SIEM/SOC oplossing draagt er toe bij dat computerdreigingen, zoals hackpogingen of malware, beter worden gemonitord en vooral sneller worden gedetecteerd. Het helpt overheden om digitaal weerbaarder te worden. Gemeente Gouda heeft hierin ook een verantwoordelijkheid t.a.v. de deelnemende gemeenten aan de samenwerking ICT Gouwe-IJssel (Zuidplas, Waddinxveen, Montfoort en IJsselstein). In 2022 is gestart met een SIEM/SOC leverancier voor een kort lopend contract om ervaring op te doen en tijd te krijgen voor een Europese aanbesteding. Deze aanbesteding is gestart en naar verwachting vindt gunning medio 2024 plaats.

- Chief Information Security Officer, CISO (BIO-maatregel 6.1)
  Gemeente Gouda werkte vanaf 2022 met een interim CISO. Inmiddels is per augustus 2023 een CISO in vaste dienst benoemd waarmee de continuïteit in de informatieveiligheidsorganisatie is geborgd.

Ontwikkelingen
De Europese NIS2-richtlijn wordt omgezet in nationale wetgeving (Wbni, Wet beveiliging netwerk- en informatiesystemen) en wordt per 17 oktober 2024 van kracht[2]. Het doel van de richtlijn is de cyberbeveiliging van essentiële diensten in EU-lidstaten te verbeteren. Gemeenten zijn door de Rijksoverheid aangemerkt als essentiële dienst.

Enkele belangrijke aspecten van de impact van de NIS2 zijn:

- Verhoogde Veiligheidseisen: NIS2 stelt strengere beveiligingseisen aan gemeenten die als aanbieder van essentiële diensten worden aangemerkt. Gemeenten vallen onder deze categorie, gezien hun rol in het aanbieden van kritieke openbare diensten.
- Meldplicht en Samenwerking: NIS2 introduceert meldplichten voor ernstige incidenten en vereist samenwerking met nationale cybersecurity instanties. Gemeenten moeten in staat zijn om snel en effectief te reageren op cyberincidenten en deze te melden aan relevante autoriteiten.
- Kritieke Infrastructuur Bescherming: NIS2 benadrukt de bescherming van kritieke infrastructuren. Dit omvat vitale diensten zoals brugbediening en digitale diensten die van cruciaal belang zijn voor het functioneren van de gemeenschap.
- Continuïteit en herstelplannen: Gemeenten moeten robuuste bedrijfscontinuïteitsplannen opstellen, inclusief herstelplannen voor kritieke processen, om de impact van incidenten te minimaliseren en de normale dienstverlening zo snel mogelijk te hervatten.
- Bewustwording: NIS2 benadrukt het belang van bewustwording van medewerkers op het gebied van informatiebeveiliging. Gemeenten dienen structureel programma's te implementeren om cybersecuritybewustzijn te vergroten en het personeel op te leiden om mogelijke dreigingen te herkennen en te voorkomen.

[2] De minister van justitie en veiligheid heeft op 31 januari de kamer geïnformeerd dat zij meer tijd nodig heeft om de richtlijn om te zetten in nationale wetgeving. Zij streeft ernaar om de wetsvoorstellen in het najaar van 2024 aan de kamer aan te bieden. Zij benadrukt het belang dat bedrijven en organisaties niet afwachten totdat de nieuwe wet- en regelgeving volledig duidelijk is, maar nu al maatregelen nemen ter bescherming van de continuïteit van hun bedrijfsprocessen.

- Risicomanagement: Gemeenten moeten een actief risicomanagementbeleid voeren, waarbij regelmatige risico analyses van potentiele risico's worden uitgevoerd en passende maatregelen worden genomen om deze te mitigeren.
- Verantwoording, toezicht en boetes: Gemeenten moeten zich aantoonbaar kunnen verantwoorden dat ze voldoen aan de eisen van de NIS2 zowel in opzet, bestaan als werking van maatregelen (de zogenaamde audit driehoek). Dit is een duidelijke verzwaring t.o.v. de BIO waarbij het aantonen van de werking niet werd vereist. De toezichthouder heeft de mogelijkheid om bij nalatigheid hoge boetes op te leggen.

Deze aspecten vormen een belangrijk onderdeel van de brede inspanningen die we zullen ondernemen om te voldoen aan de eisen van NIS2 en om de algehele informatiebeveiliging van onze organisatie te versterken.

Consequenties
Met het opstellen van een collegeverklaring toont de gemeente Gouda aan in control te zijn ten aanzien van geldende eisen en normen inzake DigiD en Suwinet. Hiermee wordt voldaan aan de eisen die de toezichthouders stellen aan informatiebeveiliging op deze onderdelen. Hiermee wordt het gebruik van de DigiD-aansluiting en Suwinet ook in de toekomst geborgd; het blijvend niet voldoen aan de verantwoordingseisen kan immers leiden tot afsluiting van Suwinet en DigiD.

Opleggen geheimhouding door college i.v.m. beveiligingsinformatie
De geheimhouding op de bij dit raadsmemo opgenomen bijlagen met de aanduiding GEHEIM is opgelegd o.g.v. art. 25 lid 2 Gemeentewet, in verband met de belangen genoemd in artikel 5.1 lid 2 sub h en sub i van de Wet open overheid (Woo). De geheimhouding is opgelegd omdat de genoemde stukken informatie bevatten over beveiligingsmaatregelen die de gemeente treft om de systemen en de gegevens te beveiligen. De informatie kan kwaadwillenden helpen bij het doorbreken van de beveiliging van personen en bedrijven en kan leiden tot sabotage (artikel 5.1, pagina 3 tweede lid, sub h van de Woo) en deze informatie kan leiden tot het disfunctioneren van de gemeente (artikel 5.1, tweede lid, sub i van de Woo). De geheimhouding is niet van toepassing op toezending van de bijlagen aan de landelijke toezichthouders voor de DigiD- en Suwinet aansluitingen, die de bijlagen moeten ontvangen in het kader van het verticale toezicht.

Geheimhouding raad
De gemeenteraad heeft de mogelijkheid om middels een besluit de door het college opgelegde verplichting tot geheimhouding op onderstaande documenten op te heffen.

Vervolg
De collegeverklaring en bijlagen zijn toegezonden aan de toezichthouders.

Bijlagen

Collegeverklaring DigiD en Suwinet ENSIA 2023:	Intern 8123 (GEHEIM)
Bijlage 1 DigiD 2023 eDiensten Burgerzaken:	Intern 8123 (GEHEIM)
Bijlage 1 DigiD 2023 eZaken:	Intern 8123 (GEHEIM)
Bijlage 1 DigiD 2023 MijnInkomen:	Intern 8123 (GEHEIM)
Bijlage 2 Suwinet 2023:	Intern 8123 (GEHEIM)
Verantwoordingsrapportage BAG, BGT en BRO 2023:	Intern 8123