Strategisch beleid

Informatieveiligheid & Privacy 2019-2021

Versie: 1.0

28 januari 2019

Opstellers:

M. de Bruin (CISO)

P. de Zwart (FG)

gemeente Hilvarenbeek

gemeente Goirle

gemeente Oisterwijk

Inhoud

1. Informatieveiligheid en privacy, randvoorwaarden voor onze ambities en doelen

Het college van B&W geeft middels dit beleid op strategisch niveau duidelijk richting aan informatieveiligheid en privacy. Dit beleid is kaderstellend en beschrijft ook de wijze waarop de verantwoordelijkheden zijn belegd.

De informatiesamenleving en ontwikkelingen

We leven in een informatiesamenleving. We zijn en worden in steeds grotere mate afhankelijk van betrouwbare informatiesystemen en data. Die afhankelijkheid wordt veroorzaakt door diverse ontwikkelingen die kansen bieden om de bedrijfsvoering en dienstverlening effectiever en efficiënter in te richten en te innoveren waardoor voldaan kan worden aan de (veranderende) behoeften en wensen om ons heen, bij onze (samenwerkings)partners, onze inwoners, ondernemers en onszelf.

Zo fungeren wij als gemeente in een keten. Wij ontvangen en delen data met andere organisaties. Voor de keten is het essentieel dat betrouwbare data en informatiesystemen worden gebruikt om inwoners en ondernemers te voorzien van producten en diensten.

Daarnaast zijn belangrijke ontwikkelingen te benoemen als robotisering, blockchain, internet-of-things (waarbij alles aan internet wordt gekoppeld) en de Digitale Agenda 2020 (VNG-realisatie). Zonder deze ontwikkelingen uitgebreid toe te lichten, zijn ook dit ontwikkelingen die zich in razendsnel tempo ontwikkelen en die in de nabije toekomst een effect hebben op de bedrijfsvoering en dienstverlening.

Deze ontwikkelingen bieden onze gemeenten kansen voor het bereiken van haar doelstellingen op een effectievere en efficiëntere wijze. Deze kansen brengen echter ook risico's met zich mee die gemanaged moeten worden. Het maakt de organisatie, en de producten en diensten die zij levert, namelijk kwetsbaarder.

Informatieveiligheid als randvoorwaarde voor een professionele organisatie

Het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) constateren dat overheden steeds vaker het doelwit worden (en gaan worden) van cyberaanvallen. Overheden hebben zogenaamde 'kroonjuwelen' (te beschermen belangen) die bewaakt moeten worden[1]. Denk hierbij aan bevolkingsdata, privacygevoelige informatie, (bovenregionale) beleidsstukken, bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, ICT-beveiliging, medewerkers/kennis en dergelijke.

Digitale spionage, verstoring van de ICT, datalekken en diefstal van informatie nemen toe. Daarom is het belangrijk om informatieveiligheid en privacy te integreren binnen de (bedrijfsvoerings)processen. Voor een professionele gemeentelijke organisatie die hoogwaardige producten en diensten aan haar inwoners moet leveren is informatieveiligheid een randvoorwaarde.

[1] Bron: Cybersecuritybeeld Nederland 2018 (CSBN 2018) van de NCTV

Het belang van privacy

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid voor persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn, waarbij ze vanuit privacy perspectief een van de meest complexe organisaties zijn die we kennen. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt onder andere voor taken op het gebied van basisadministraties, openbare orde en veiligheid en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van openbare veiligheid en nieuwe Europese wetgeving. De gemeente is zich hier van bewust en zorgt ervoor dat de privacy van betrokkenen gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie en gebruikerscontrole.
Tenslotte gaat de gemeente op een transparante wijze om met de gegevens die ze verwerkt. Dit houdt in dat we aan betrokkenen duidelijk maken in welke gevallen we persoonsgegevens verwerken, hoe we dit doen en waarom.

Doel informatieveiligheid en privacy

Met informatieveiligheid wordt gestreefd naar het veilig en geautoriseerd gebruik van gegevens, het voorkomen van schade door verstoring, uitval of misbruik van informatiesystemen en, indien er toch schade is ontstaan, het herstellen hiervan.

Informatieveiligheid waarborgt de betrouwbaarheid van de informatie(systemen). Betrouwbaarheid betekent dat informatie beschikbaar en integer (juist, actueel, tijdig) moet zijn, en dat de vertrouwelijkheid van deze informatie moet zijn geregeld waar dat noodzakelijk is. Dit heeft als doel dat de continuïteit van de bedrijfsvoering en dienstverlening wordt gewaarborgd.

Privacy waarborgt dat de persoonsgegevens die de gemeente verwerkt, niet alleen organisatorisch en passend beveiligd zijn, maar dat de persoonsgegevens ook op de juiste wijze worden gebruikt, met in acht neming van eisen in de AVG zoals noodzakelijkheid, doelbinding, proportionaliteit en subsidiariteit.

Kortom, informatieveiligheid (waaronder privacy) zorgt ervoor dat wij onze missie, visie en (politieke) doelen kunnen realiseren, op een verantwoorde manier, waarbij risico's gemanaged worden.

Risicomanagement

100% informatieveiligheid bestaat niet, want dat maakt de organisatie gesloten; het voldoende weerbaar zijn houdt de gemeentelijke organisatie open en verbonden met de (veranderende) behoeften en wensen van de maatschappij. Het maakt de organisatie flexibel. Risico's moeten voldoende beheerst worden, wat betekent dat een risico-gestuurde aanpak essentieel is. Hiervoor wordt in 2019 een proces ingericht conform de ISO 27001 'Information Security Management System', dat gebaseerd is op de plan-do-check-act-cyclus. Ondanks dat 100% informatieveiligheid niet bestaat, bestaat 100% inzet wel. Door risico's inzichtelijk te hebben, kunnen afgewogen besluiten worden genomen om uitvoering te geven aan onze missie, visie en doelen.

Wettelijke- en normatieve kaders voor de verwerking van en omgang met persoonsgegevens

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van dit beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- de Algemene Verordening Gegevensbescherming (AVG)
- de Uitvoeringswet Algemene Verordening Gegevensbescherming

Naast de algemene wettelijke kaders spelen ook de volgende wetten en normen in het bijzonder een rol:

- De Baseline Informatiebeveiliging Gemeenten (BIG) is een zelfreguleringsinstrument dat alle Nederlandse gemeenten zichzelf hebben opgelegd. Deze is gebaseerd op de NEN ISO 27001 en 27002. De BIG wordt in 2019 vervangen door de Baseline Informatiebeveiliging Overheid (BIO), geldend voor alle overheidsorganen.
- Archiefwet (voor de bewaartermijnen van gegevens)
- Wet openbaarheid van bestuur (WOB)
- Aanvullingen op dit algemene kader in sectorspecifieke wetten, zoals wetten op het terrein van het sociaal domein.

Uitgangspunten verwerking en omgang met persoonsgegevens

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van haar burgers. In de uitoefening van haar publiekrechtelijke taak houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de burger als de doelstellingen van de gemeente naar beste inzicht te behartigen. De gemeente houdt zich hierbij aan de beginselen uit de AVG, die nader zijn omschreven in artikel 3.14 van het strategisch beleid.

Reikwijdte van het beleid

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente en wordt bij voorkeur ook toegepast in samenwerkingsverbanden die de gemeente aangaat. Voor specifieke veel voorkomende processen, zoals bijvoorbeeld het verwerken van gegevens in het kader van het uitvoeren van de Jeugdwet, zullen de betreffende afdelingen een specifiek beleid, reglement, protocol en/of procedure opstellen, zoals omschreven in artikel 3.13 van het hierna volgend strategisch beleid.

Samenwerking gemeenten Goirle, Hilvarenbeek en Oisterwijk

Informatieveiligheid en privacy zijn vakgebieden die zich uitstekend lenen om op samen te werken, zodat krachten, capaciteit en kennis gebundeld worden. Binnen gemeenteland komt dit veel voor, en ook de gemeenten Goirle, Hilvarenbeek en Oisterwijk werken hierop samen. Dit samenwerkingsverband zal in dit document hierna worden aangehaald als ‘GHO’.
Er is gekozen om het strategisch beleid informatieveiligheid en privacy te harmoniseren voor de drie gemeenten.. Op deze wijze wordt het minimale kwaliteitsniveau (de baseline) gelegd die voor alle drie de gemeenten leidend is, en waar gemotiveerd van afgeweken mag worden. De Chief Information Security Officer draagt namens bestuur en management zorg voor het inbedden van het beleid, monitort de voortgang op de implementatie en rapporteert hierover aan de verantwoordelijken.

Opbouw strategisch beleid

Het strategisch beleid bestaat uit de kaders die leidend zijn voor informatieveiligheid en privacy. Deze zijn veelal gebaseerd op bestaande wet- en regelgeving en geven de principes die privacy en de betrouwbaarheid van de informatie(systemen) waarborgen.

Het strategisch beleid vormt samen met een tactisch en operationeel plan één geheel, waarin de gehele set aan eisen en maatregelen ten behoeve van informatieveiligheid en privacy is afgedekt. In het tactische plan worden de kaders uitgewerkt en vertaald in een generieke set van maatregelen die gebaseerd zijn op de

BIG/BIO. Het tactische plan kan daarom ook GHO-breed worden gehanteerd. In operationele plannen (die kunnen voor de gemeente specifiek worden vastgesteld) worden op het laagst mogelijke niveau de maatregelen verder uitgewerkt en vastgesteld door de verantwoordelijke (bijv. teammanager).

Ter illustratie volgt een praktisch voorbeeld van hoe een vraagstuk op basis van het strategisch beleid en tactisch plan wordt vormgegeven en op operationeel niveau divers kan worden ingericht. Voor de uitvoering van een dienst verwerkt de gemeente data in een applicatie. De vraag 'Hoe moeten we de autorisaties inrichten voor de medewerkers' wordt als volgt aangevlogen:

- *Het strategisch beleid geeft aan dat de BIG en de AVG leidend zijn. De BIG en AVG bepalen dat toegang tot informatie passend beveiligd moet zijn. Dit betekent dat de gemeente dient te beschikken over autorisatiebeleid.*
- *Het tactisch plan geeft het autorisatiebeleid en de uitgangspunten weer die gelden. Hierin staat onder andere dat autorisaties rol gebaseerd zijn, worden goedgekeurd door de proceseigenaar van de desbetreffende dienst en dat afhankelijk van de vertrouwelijkheidsclassificatie van de data een wachtwoord met inlognaam voldoende is of dat aansluitend ook nog een tokencode toegepast moet worden.*
- *Op operationeel niveau bepaalt de proceseigenaar (lijnmanager) de specifieke procedure, die voldoet aan het strategisch beleid en de uitgangspunten uit het tactisch plan. Dit kan per proces verschillen, als het maar passend beveiligd is. De proceseigenaar bepaalt namelijk de vertrouwelijkheidsclassificatie van de data, welke rollen worden onderkend, welke autorisaties hierbij horen en welke medewerkers dus welke autorisaties moeten hebben. Ook de wijze waarop de proceseigenaar de autorisaties toekent, mag per proces verschillen.*

2. Strategisch Beleid Informatieveiligheid & Privacy

Het college van B&W besluit het 'Strategisch Beleid Informatieveiligheid & Privacy' vast te stellen.

Artikel 1. Definities

1. **Informatieveiligheid**: is gericht op het waarborgen van de betrouwbaarheid van de informatie(voorziening). Dit betekent dat informatie beschikbaar, tijdig, juist en actueel is, en dat informatie niet beschikbaar is voor onbevoegden.
2. **(Informationele) privacy**[2]: gaat om de informatie die geclassificeerd wordt als persoonsgegeven. Privacy is afhankelijk van adequate informatieveiligheid. Om de privacy te waarborgen geldt onder andere de verplichting om adequate passende technische en organisatorische maatregelen te treffen. Hier gaat het om de effectiviteit van informatieveiligheid. Is de Informatieveiligheid niet op orde, dan kan de privacy niet gewaarborgd worden.
3. **Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)**: dit is het leidende basisbeveiligingsnormenkader voor gemeenten, en wordt in de nabije toekomst vervangen door één basisbeveiligingsnorm voor de gehele overheid (Baseline Informatiebeveiliging Overheid – BIO).
4. **Algemene Verordening Gegevensbescherming (AVG)**: dit is een privacywet die geldt binnen de hele Europese Unie (EU). Hiermee is de bescherming van persoonsgegevens binnen de hele EU op dezelfde manier geregeld.

Artikel 2. Doel

Het waarborgen van een betrouwbare informatievoorziening en daarmee de kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen (informatieveiligheid). Hierbij wordt zorgvuldig, veilig, proportioneel en vertrouwelijk omgegaan met alle (persoons)gegevens die de persoonlijke levenssfeer raken. Mensen mogen erop vertrouwen dat hun privacy is geborgd en hun persoonlijke levenssfeer wordt gerespecteerd. De bescherming van de privacy begint namelijk met het niét verzamelen en verwerken van persoonsgegevens.

Artikel 3. Beleidsregels

1. Informatieveiligheid en informationele privacy dienen bij te dragen aan het realiseren van de organisatiedoelstellingen[3], rekeninghoudend met geldende wet- en regelgeving.
2. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG[4]) en de Algemene Verordening Gegevensbescherming (AVG) zijn leidend ten aanzien van respectievelijk informatieveiligheid en privacy.
3. Deze regelgeving is tevens leidend en bepalend voor de leveranciers en andere partners met wie wordt samengewerkt.
4. Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft afdoende garantie dat informatie betrouwbaar en correct wordt behandeld.

---

2 in het vervolg aangehaald als privacy

3 In de praktijk blijkt soms dat het werken met de privacywetgeving strijdig lijkt of is met andere uitgangspunten van de organisatie zoals dienstverlening / klantvriendelijkheid.

4 2019 is een overgangsjaar waarin de BIG wordt vervangen door de BIO.

5. Het beveiligingsniveau is in lagen uitbreidbaar. Dit betekent dat het basis beveiligingsniveau uitgaat van de BIG en de AVG. Daar waar nodig of vereist kunnen extra maatregelen getroffen worden boven op het basisniveau. Een uitgevoerde risicoanalyse kan hiertoe aanleiding geven.
6. Een baseline informatiebeveiligingstoets en een data protection impact assessment (DPIA) worden in ieder geval uitgevoerd bij de invoering van nieuwe systemen, projecten of processen.
7. Voor het verwerken van persoonsgegevens dient altijd een doel en grondslag te zijn, waarbij adequate passende beveiligingsmaatregelen worden getroffen en de beginselen uit de AVG worden gewaarborgd. Bij de implementatie van beveiligingsmaatregelen uit de BIG geldt het pas-toe-of-leg-uit principe, waarbij rekening wordt gehouden met drie afwegingselementen: de stand van de techniek, kosten van de tenuitvoerlegging en risico's.
8. Het primaire uitgangspunt is risicomanagement. De klassieke aanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig en verantwoord faciliteren.
9. Informatieveiligheid en privacy vereisen een integrale aanpak. De principes 'Security and privacy by design and default' staan daarom centraal. Dit betekent dat maximale privacy en informatieveiligheid wordt betracht en dat dit tevens wordt meegenomen bij de ontwikkeling en inrichting van informatiesystemen, processen en diensten.
10. Verantwoord en bewust gedrag van medewerkers is essentieel. Structureel en planmatig wordt gewerkt aan het bewustzijn.
11. Het systeem van zelfregulering staat centraal voor de gemeentelijke organisatie, waarbij jaarlijks opzet, bestaan en werking van de beleidsregels worden geëvalueerd. Op basis hiervan wordt een verbeterplan opgesteld en wordt via de p&c-cyclus horizontaal verantwoording afgelegd door het college van B&W aan de gemeenteraad. Er wordt gewerkt conform de plan-do-check-act verbetercyclus. De verticale verantwoording aan de verantwoordelijke stelselhouders leunt op de horizontale verantwoording en vindt plaats door middel van ENSIA. Ten behoeve van implementatie en uitwerking van voorliggend strategisch beleid, wordt een doorvertaling gemaakt van dit beleid in een Tactisch Kader voor informatieveiligheid en privacy. Deze wordt waar nodig vertaald in vakspecifieke procedures. Dit geschiedt in ieder geval voor het waarborgen van de eisen die voortvloeien uit de verschillende stelsels, zoals Suwinet, DigiD en de basisregistraties (waaronder BRP, BAG, BGT, Bro).
12. Vakspecifiek(e) procedures, werkinstructies en dergelijke ten aanzien van informatieveiligheid en privacy worden op het laagst mogelijke niveau vastgesteld door de verantwoordelijke. Indien het alleen betrekking heeft op één team, dan kan de lijnmanager dit op het laagste niveau vaststellen. Naar mate dit meer team- en/of afdelingsoverstijgend is, wordt trapsgewijs opgeschaald naar een hoger gremium. Beleid wordt vastgesteld door het college van B&W.
13. De gemeente gaat op een veilige manier om met persoonsgegevens en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende beginselen:
    a) *<u>Rechtmatigheid, behoorlijkheid, transparantie</u>*
    Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
    b) *<u>Juistheid</u>*
    Persoonsgegevens moeten juist en actueel zijn. Het verwerken van onjuiste persoonsgegevens kan tot grote problemen leiden en een inbreuk vormen op de persoonlijke levenssfeer. De gemeente neemt redelijke maatregelen om onjuiste persoonsgegevens te wissen en te rectificeren.
    c) *<u>Grondslag en doelbinding</u>*

Persoonsgegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige, in de wet geregelde, grondslag verwerkt.

d) *Dataminimalisatie*
Persoonsgegevens worden alleen verwerkt die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

e) *Bewaartermijn*
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

f) *Integriteit en vertrouwelijkheid*
Persoonsgegevens worden zorgvuldig en vertrouwelijk behandeld. Persoonsgegevens worden alleen verwerkt voor het doel waarvoor deze gegevens zijn verzameld. Daarbij wordt gezorgd voor passende beveiliging van persoonsgegevens.

g) *Delen met derden*
In het geval van samenwerking met externe partijen (zoals leveranciers en ketenpartners) waarbij sprake is van gegevensverwerking van persoonsgegevens, wordt het thema Informatieveiligheid en Privacy nadrukkelijk opgenomen in de samenwerkingsovereenkomst. In deze overeenkomst worden de doelen speciefiek uitgewerkt, zijn rollen en verantwoordelijkheden duidelijk omschreven en zijn er afspraken gemaakt over de eisen waar gegevensuitwisseling aan moet voldoen. De gemeente houdt toezicht op naleving van deze afspraken.

h) *Subsidiariteit*
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. Indien het doel waarvoor persoonsgegevens worden verwerkt in redelijkheid voor de bij de verwerking betrokkenen op een minder nadelige wijze kunnen worden verwezenlijkt dan kiest de gemeente altijd voor die mogelijkheid.

i) *Proportionaliteit*
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

j) *Rechten van betrokkenen*
De gemeente respecteert alle rechten die een betrokkene toekomen vanuit de AVG, zoals het recht van: inzage, dataportabiliteit, rectificatie, beperking van de gegevensverwerking, wissing van persoonsgegevens, intrekken van de toestemming en bezwaar. De gemeenten faciliteert betrokken bij de uitoefening van hun rechten.

Artikel 4. Verantwoordelijkheden

1. Het college van B&W is bestuurlijk eindverantwoordelijk voor de informatieveiligheid en privacy van haar gemeente en het lijnmanagement is ambtelijk verantwoordelijk voor risicomanagement, implementatie en naleving van deze beleidsregels.
2. De Chief Information Security Officer (CISO) is de hoogste adviseur binnen de organisatie voor informatieveiligheid en de Functionaris Gegevensbescherming (FG) zorgt voor toezicht en ondersteuning m.b.t. de juiste omgang met persoonsgegevens en privacy. Beiden bekleden zij een onafhankelijke positie bij het bewaken en verhogen van informatieveiligheid en privacy. Zij

adviseren (on)gevraagd, doen onderzoek en rapporteren hierover. De CISO en FG stellen organisatiebreed beleid op en coördineren samen de implementatie. Het (virtuele) team informatieveiligheid en privacy bestaat verder uit de ENSIA coördinator en privacy officers. Samen ondersteunen zij bij het uitvoeren van risicoanalyses, verzorgen integrale statusrapportages, monitoren de naleving, en doen voorstellen tot implementatie c.q. verbeteringen. Het team informatieveiligheid en privacy zorgt ervoor dat de verantwoordelijke managers hun verantwoordelijkheid kunnen nemen. Daarnaast kunnen er binnen afdelingen specifieke beveilingsfunctionarissen (security officers) worden aangesteld, met als verantwoordelijkheid de beveiliging voor specifieke systemen zoals BRP of SUWI.

3. Binnen het college van B&W zijn informatieveiligheid en privacy in een portefeuille belegd. De algemeen directeur (gemeentesecretaris) is verantwoordelijk voor integrale sturing binnen de ambtelijke organisatie. De CISO en de FG hebben hiertoe een rechtstreekse rapportagelijn naar de portefeuillehouder én de algemeen directeur (gemeentesecretaris).