CVDR

Officiële uitgave van Heiloo.

Nr. CVDR467459_1

10 oktober 2017

Beleidsregels Informatieveiligheid & Privacy

Het college van burgemeester en wethouders van de gemeente Heiloo;
gelet op de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
besluit vast te stellen de volgende beleidsregels: Beleidsregels Informatieveiligheid & Privacy

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**: gaat om de informatie die geclassificeerd wordt als persoonsgegeven. Privacy is afhankelijk van adequate informatieveiligheid. Om de privacy te waarborgen geldt 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 basisnormenkader voor gemeenten ten aanzien van informatieveiligheid.
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. Vanaf 25 mei 2018 verdwijnt de Wet bescherming persoonsgegevens (Wbp) en is de AVG van toepassing.

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.

Artikel 3. Beleidsregels

1. Informatieveiligheid en informationele privacy[1] dienen bij te dragen aan het realiseren van de bestuurlijke- en organisatiedoelstellingen, rekeninghoudend met geldende wet- en regelgeving.
2. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Algemene Verordening Gegevensbescherming (AVG) zijn leidend ten aanzien van respectievelijk informatieveiligheid en privacy.
3. De BIG en de AVG zijn tevens leidend en bepalend voor de partijen met wie de gemeente en de Werkorganisatie BUCH samenwerken.
4. Het inrichten van de informatievoorziening volgens deze beleidsregels in opzet, bestaan en werking, geeft afdoende garantie dat informatie betrouwbaar en correct wordt behandeld.
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.
6. 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 der techniek, kosten van de tenuitvoerlegging en risico's.
7. Het primaire uitgangspunt is risicomanagement. De klassieke aanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig en verantwoord faciliteren.
8. 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.
9. Verantwoord en bewust gedrag van medewerkers is essentieel. Structureel en planmatig wordt gewerkt aan het bewustzijn.
10. Het systeem van zelfregulering staat centraal, waarbij jaarlijks opzet, bestaan en werking van de beleidsregels wordt geëvalueerd. Op basis hiervan wordt een verbeterplan opgesteld en wordt via de p&c-cyclus horizontaal verantwoording aflegd door het college aan de gemeenteraad. Er wordt gewerkt conform de plan-do-check-act verbetercyclus.

1) in het vervolg aangehaald als privacy

11. Ten behoeve van implementatie en uitwerking van deze beleidsregels, wordt een doorvertaling gemaakt van deze beleidsregels in een concernarchitectuur voor informatieveiligheid en privacy. Deze wordt waar nodig vertaald in vakspecifieke procedures. Dit geschiedt in ieder geval voor het waarborgen van de kwaliteit, beveiliging en privacy rondom de processen van de Basisregistratie Personen, paspoorten en identiteitskaarten, DigiD en SUWInet.
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 teammanager dit op het laagste niveau vaststellen. Naar mate dit meer team- en/of domeinoverstijgend is, wordt trapsgewijs opgeschaald naar een hoger gremium. Beleid wordt vastgesteld door het college.
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) *Rechtmatigheid, behoorlijkheid, transparantie*
    Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
    b) *Grondslag en doelbinding*
    De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.
    c) *Dataminimalisatie*
    De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
    d) *Bewaartermijn*
    Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.
    e) *Integriteit en vertrouwelijkheid*
    De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Persoonsgegevens worden alleen verwerkt voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens.
    f) *Delen met derden*
    In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente houdt toezicht op naleving van deze afspraken.
    g) *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.
    h) *Proportionaliteit*
    De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.
    i) *Rechten van betrokkenen*
    De gemeente respecteert de rechten van de betrokkene die betrokkene toekomt vanuit de AVG, zoals het recht van: inzage, dataportabiliteit, rectificatie, beperking van de gegevensverwerking, wissing van persoonsgegevens, intrekken van de toestemming en bezwaar.

Artikel 4. Verantwoordelijkheden

1. Het college van B&W is bestuurlijk integraal eindverantwoordelijk voor de informatieveiligheid en privacy van haar gemeente; het bestuur van de Werkorganisatie BUCH is dit voor zijn werkorganisatie; en het lijnmanagement is ambtelijk verantwoordelijk voor risicomanagement, implementatie en naleving van deze beleidsregels.
2. De Chief Information Security Officer (CISO) voor informatieveiligheid en de Functionaris Gegevensbescherming (FG) voor privacy ondersteunen vanuit een onafhankelijke positie bij het bewaken en verhogen van informatieveiligheid en privacy. Zij adviseren (on)gevraagd, stellen organisatiebreed beleid op en coördineren de implementatie, ondersteunen bij het uitvoeren van risicoanalyses, verzorgen integrale statusrapportages, monitoren naleving, doen voorstellen tot implementatie c.q. verbeteringen. Zij zorgen ervoor dat de verantwoordelijken hun verantwoordelijkheid kunnen nemen. Hiervoor hebben zij een rechtstreekse rapportagelijn naar de desbetreffende verantwoordelijken.
3. Binnen het college van B&W, het bestuur van de Werkorganisatie BUCH en de directie zijn informatieveiligheid en privacy in een portefeuille belegd voor integrale sturing; waarbij de portefeuillehouders de eerste aanspreekpunten zijn voor de CISO en FG op dit niveau.

Artikel 5 Inwerkingtreding

1. De Beleidsregels Informatieveiligheid & Privacy treden in werking met ingang van de dag na bekendmaking.

Artikel 6. Citeertitel

De beleidsregels worden aangehaald als: Beleidsregels Informatieveiligheid & Privacy

Aldus besloten door het college van burgemeester en wethouders in zijn vergadering van 19 september 2017.

de secretaris,

GuyHeemskerk

de burgemeester,

HansRomeyn

Toelichting op Beleidsregels Informatieveiligheid & Privacy

Door en namens de gemeente wordt veel gewerkt met informatie, waaronder persoonsgegevens. Persoonsgegevens worden voornamelijk verzameld voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente ervoor zorgt dat zorgvuldig en veilig met deze persoonsgegevens wordt omgegaan.
In deze tijd gaat de gemeente ook mee met nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitale overheid. Dit stelt andere eisen aan de bescherming van de informatie en persoonsgegevens. Hier is de gemeente zich bewust van en zorgt dat de privacy gewaarborgd blijft door het treffen van maatregelen op het gebied van informatieveiligheid, dataminimalisatie, transparantie en gebruikerscontrole.
De gemeente geeft middels dit beleid een duidelijke richting aan informatieveiligheid en privacy, en is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van of namens de gemeente.

Waarom

De waarde van informatie neemt toe, steeds meer (persoons)gegevens worden met andere partijen gedeeld en informatie(systemen) worden op afstand benaderbaar door digitalisering en internet. Dit bevordert de dienstverlening, maar maakt de informatievoorziening ook kwetsbaarder.

Ontwikkelingen

Binnen de overheid is een aantal bewegingen gaande, passend bij onze informatiesamenleving, waardoor de waarde van informatie toeneemt en (persoons)gegevens onderling steeds meer gedeeld worden. Dit onderschrijft het belang van een betrouwbare informatievoorziening om goed te kunnen (blijven) besturen:

- Digitalisering en informatisering
  Steeds meer processen en diensten worden geautomatiseerd en gedigitaliseerd. Het internet groeit en zorgt ervoor dat informatie breder toegankelijk wordt en dat diensten op afstand kunnen worden aangeboden; met alle bijbehorende dynamiek van dien.
- Flexibel organiseren
  Steeds meer overheden, en ook de Werkorganisatie BUCH, kiezen voor een gedeeltelijke programmatische- of netwerkorganisatie. Diensten worden anders georganiseerd met als doel om de kwaliteit van de dienstverlening te verhogen, kosten te besparen en of de kwetsbaarheid te verminderen.
- Keten van verantwoordelijkheden
  Steeds vaker komt het voor dat de overheid niet meer de enige producent is van een specifiek resultaat, maar deel uitmaakt van een keten of samenwerkt met andere publieke partijen, private organisaties, sociale verbanden en inwoners om resultaten te realiseren. Dit betekent dat de gehele keten dient bij te dragen aan een betrouwbare informatievoorziening.
- Verknoping van steeds grotere vraagstukken
  Vraagstukken hebben vaak een meerdimensionaal karakter: economisch, sociaal, openbare orde en veiligheid, cultureel, moreel en dergelijke. Denk onder andere aan de sociale transitie en de aankomende omgevingswet. De informatievoorziening wordt hierin steeds belangrijker om deze complexe vraagstukken integraal te kunnen besturen.
- Nieuwe wet- en regelgeving

Op (inter)nationaal niveau is of wordt gewerkt aan nieuwe wet- en regelgeving om informatieveiligheid en privacy te waarborgen. Hierbij kan onder andere gedacht worden aan de Baseline Informatiebeveiliging Gemeenten (BIG) en de Algemene Verordening Gegevensbescherming (AVG).

Uitdagingen
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. Gemeenten hebben zogenaamde 'kroonjuwelen' (te beschermen belangen) die bewaakt moeten worden. Denk hierbij aan bevolkingsdata, privacygevoelige informatie, (bovenregionale) beleidsstukken, bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, ICT-beveiliging, medewerkers/kennis en dergelijke.
De grootste dreigingen voor de overheid zijn: digitale spionage, verstoring van de ICT, diefstal van informatie en datalekken. Informatieveiligheid en privacy zorgen ervoor dat de gemeentelijke belangen adequaat beveiligd zijn en de organisatie voldoende weerbaar is tegen deze dreigingen. Het basisbeveiligingsniveau van de BIG en de AVG zorgen voor deze weerbaarheid. Hierin is het gedrag van medewerkers cruciaal, en daarom wordt structureel gewerkt aan het bewustzijn.
Het streven is het voorkomen van schade door verstoring, uitval of misbruik van informatiesystemen en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit: aantasting van de betrouwbaarheid van informatie(systemen), beperking van de beschikbaarheid en de schending van de vertrouwelijkheid en/of integriteit van de in informatiesystemen opgeslagen informatie en de herkomst hiervan.
100% informatieveiligheid bestaat niet, want dat maakt de organisatie gesloten; het voldoende weerbaar zijn houdt de organisatie open en verbonden. Risico's moeten voldoende beheerst worden, wat betekent dat een risicogestuurde aanpak essentieel is – en daarom staat risicomanagement ook centraal binnen informatieveiligheid en privacy.
Door (technologische) ontwikkelingen ontstaan dagelijks nieuwe kwetsbaarheden in de informatievoorziening, die misbruikt kunnen worden. Daarbij ontwikkelen kwaadwillenden hun vaardigheden en tools om misbruik te maken van deze kwetsbaarheden. Daarom wordt gewerkt met een plan-do-check-act-cyclus en zelfregulering waarin continu (nieuwe) dreigingen, kwetsbaarheden en risico's in beeld worden gebracht en voorstellen worden gedaan om voldoende weerbaar te blijven.

Aanpak gemeente
De ambtelijke organisatie van de gemeente is per 1 januari 2017 gefuseerd en opgegaan in de werkorganisatie BUCH (Bergen, Uitgeest, Castricum en Heiloo). Deze werkorganisatie heeft informatieveiligheid en privacy als prioriteit bestempeld in de samenwerking.
Op bestuurlijk en directie niveau is een portefeuillehouder aangewezen om te sturen op informatieveiligheid en privacy. Tevens zijn de functies van Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en privacy-officer belegd. Zij vormen de *drivers* in de realisatie en naleving van deze beleidsregels.
Jaarlijks wordt via een zelfevaluatie de stand van zaken in beeld gebracht en via de jaarstukken van de gemeente verantwoording afgelegd aan de gemeenteraad. Ingezet wordt op mens, organisatie en techniek. Bij mens gaat het erom dat medewerkers zich bewust zijn van hetgeen dat van hen wordt verwacht qua kennis, houding en gedrag. Op organisatorisch niveau gaat het om governance (verantwoordelijkheden en bevoegdheden), beleid en procedures. En bij de techniek gaat het om het treffen van passende technische maatregelen om weerbaar te zijn tegen (cyber)dreigingen.