Gemeente
Scherpenzeel

Raadsvoorstel

Datum B&W-besluit	: 16 december 2025	Portefeuille	: E. van de Glind
Raadsvergadering	: 12 februari 2026		
Agendapunt	: Vult Griffie in	Zaaknummer	: 150719 / 159798
Bijlage(n)	: 1		

Onderwerp: Strategisch informatiebeveiligings- en privacybeleid

Wettelijke grondslag
De gemeenteraad heeft de verantwoordelijkheid om de kaders vast te stellen voor het informatiebeveiligings- en privacybeleid, dat de richtlijnen, doelstellingen en procedures bevat om de privacy van inwoners te waarborgen (Artikel 169 Gemeentewet). Binnen de overheid is afgesproken om aan de Baseline Informatiebeveiliging Overheid (BIO) te voldoen. Ook moeten gemeenten gaan voldoen aan de Network and Information Security Directive (NIS2- Europese richtlijn). De kaders voor zorgvuldige behandeling van persoonsgegevens zijn uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg).

Deze kaders zijn verder vertaald in het Strategisch informatiebeveiligings- en privacybeleid, vast te stellen door de gemeenteraad.

Beoogd effect
Het Strategisch informatiebeveiligings- en privacybeleid geeft invulling aan onze (wettelijke) verplichting voor een informatiebeveiligings- en privacybeleid.

Beslispunten
1. *Het Strategisch Informatiebeveiligings- en privacybeleid vast te stellen*

Aanleiding
Het Strategisch gemeentebreed Informatiebeveiligingsbeleid 2021 en de Beleidsregels Privacy gemeente Scherpenzeel 2018 zijn gedateerd. Deze documenten worden vervangen door bijgevoegd Strategisch informatiebeveiligings- en privacybeleid. De gemeenteraad dient als kaderstellend en toezichthoudend bestuursorgaan dit beleid vast te stellen voor alle informatiebeveiligingsprocessen en verwerkingen van persoonsgegevens die binnen de gemeente plaatsvinden.

Argumenten

1.1 De gemeenteraad dient als kaderstellend en toezichthoudend bestuursorgaan een informatiebeveiligings- en privacybeleid vast te stellen

De gemeenteraad heeft de verantwoordelijkheid om de kaders vast te stellen voor het informatiebeveiligings- en privacybeleid, dat de richtlijnen, doelstellingen en procedures bevat om de privacy van inwoners te waarborgen. De raad heeft ook een toetsende/controlerende rol om te waarborgen dat de vastgestelde kaders daadwerkelijk worden uitgevoerd volgens het beleid.

1.2 De gemeenteraad dient als verwerkingsverantwoordelijke een IB&P beleid vast te stellen

De gemeenteraad, het college en de burgemeester zijn zelfstandige bestuursorganen met eigen wettelijke taken. Wanneer zij persoonsgegevens verwerken in het kader van hun eigen taken, zijn zij zelf verwerkingsverantwoordelijke volgens de definitie van de Algemene Verordening Gegevensbescherming (artikel 4, lid 7). Elk proces wat vanuit de bevoegdheid van een bestuursorgaan uitgevoerd wordt, kan verwerkingen van persoonsgegevens bevatten en valt daarmee onder het IB&P beleid. Informatiebeveiliging is, naast de verplichting als gemeente om aan de BIO te voldoen, onderdeel van dit beleid gezien o.a. artikel 25 en 32 van de AVG.

1.3 Het IB&P-beleid vormt de basis voor het beheersen van de IB&P-risico's

Met de steeds geavanceerdere technologieën zoals kunstmatige intelligentie en de toename van cyberaanvallen is het passend beheersen van de IB&P-risico’s voor inwoners, ondernemers, de gemeentelijke organisatie en andere belanghebbenden van cruciaal belang. Het IB&P-beleid vormt hiervoor de basis.

<u>De risico's voor betrokkenen zijn:</u>

Het onzorgvuldig omgaan met gegevens en systemen kan enorme gevolgen hebben voor betrokkenen. Denk aan een inbreuk op het grondrecht privacy of slachtoffer worden van digitale criminaliteit. Dit kan de volgende gevolgen hebben:

- Reputatieschade: Het imago van zowel individuen als de gemeente kan worden aangetast.
- Financiële schade: Door bijvoorbeeld afpersing, identiteitsfraude of boetes.
- Emotionele schade: Angst, stress en het gevoel van controleverlies.
- Gevoel van constante surveillance: Bij onrechtmatige tracking of monitoring.
- Uitsluiting en discriminatie: Bijvoorbeeld door algoritmische vooroordelen.
- Onjuiste besluitvorming: Als gevolg van foutieve of onvolledig verwerkte data.

Ook het niet beschikbaar zijn van systemen, dienstverlening en/of bedrijfsvoering kan de gemeentelijke organisatie stil leggen. De gevolgen voor (de veiligheid van) inwoners, gemeentelijke organisatie, ondernemers en andere belanghebbenden kunnen groot zijn en nog veel groter ten tijde van een crisissituatie.

De risico's voor de gemeentelijke organisatie zijn:
Het onvoldoende borgen van informatiebeveiliging en privacy kan leiden tot:

- Uitval van systemen, dienstverlening en bedrijfsvoering.
- Incidenten zoals digitale criminaliteit en datalekken.
- Personen kunnen schadevergoeding eisen als er schade is omdat de gemeentelijke organisatie verwijtbaar in strijd met de privacywetgeving heeft gehandeld.
- Onder verscherpt toezicht worden gesteld door de Autoriteit Persoonsgegevens en sancties opgelegd krijgen. De belangrijkste sancties zijn de boete, de last onder dwangsom, het verwerkingsverbod, de berisping en de waarschuwing.

De gevolgen kunnen hoge (herstel)kosten, impact op de capaciteit, reputatieschade en verlies van vertrouwen in de gemeentelijke organisatie zijn. Het niet beschikbaar zijn van systemen, dienstverlening en/of bedrijfsvoering heeft impact op inwoners, ondernemers, andere belanghebbenden en medewerkers omdat ze hun werk niet of minder goed kunnen doen.

Kanttekeningen
1.1 De implementatie van dit beleid moet nog deels plaatsvinden
De gemeente Scherpenzeel heeft de afgelopen jaren geïnvesteerd in het neerzetten van een stabiele IB&P-organisatie. Diverse maatregelen op gebied van informatiebeveiliging en privacy zijn op basis van de geldende overheidsnormen geïmplementeerd. Een herzien IB&P beleid en bijpassende aanpak zijn nodig om aan te sluiten bij de snelle ontwikkelingen die plaatsvinden op gebied van informatiebeveiliging en privacy alsmede het voortschrijdend inzicht binnen de IB&P-organisatie. Met dit geactualiseerde IB&P-beleid worden daarom kaders gesteld waarvan implementatie deels nog plaats moet vinden.

Financiën
Een principe in het IB&P-beleid is 'Informatiebeveiliging en privacy kosten geld'. Als blijkt dat voor het implementeren van maatregelen ruimere budgetten nodig zijn, dan zal dit bij de gemeenteraad worden aangevraagd.

Proces
De gemeente Scherpenzeel streeft ernaar om in 2027 een volledige Plan-Do-Check-Act-cyclus geïmplementeerd en geborgd te hebben voor de naleving van de IB&P-kaders. We plannen de benodigde maatregelen (Plan), voeren deze zorgvuldig uit (Do), monitoren en evalueren de voortgang op basis van vastgestelde indicatoren (Check), en passen waar nodig het beleid en de uitvoering aan om continue verbetering te waarborgen (Act). Hiermee houden we grip op de IB&P-risico's, zodat onze inwoners, medewerkers, ondernemers en andere belanghebbenden kunnen rekenen op veilige en betrouwbare diensten. De Chief Information Security Officer, de Functionaris Gegevensbescherming en de Privacy Officer coördineren en controleren in opdracht van het college het planmatig inrichten en borgen van de IB&P-maatregelen.

Evaluatie
Het IB&P-beleid wordt jaarlijks geëvalueerd en indien nodig herzien.

Bijlage(n)
1. Strategisch Informatiebeveiligings- en privacybeleid

Burgemeester en wethouders van Scherpenzeel,

A.M. Weststrate	M.C. Teunissen
secretaris	burgemeester