Strategisch beleid
Privacy en Informatieveiligheid
2025-2028

Gemeenteraad Teylingen

Datum: 08-04-2025

Opgesteld door:

Functionaris Gegevensbescherming
Chief Information Security Officer

Inhoudsopgave

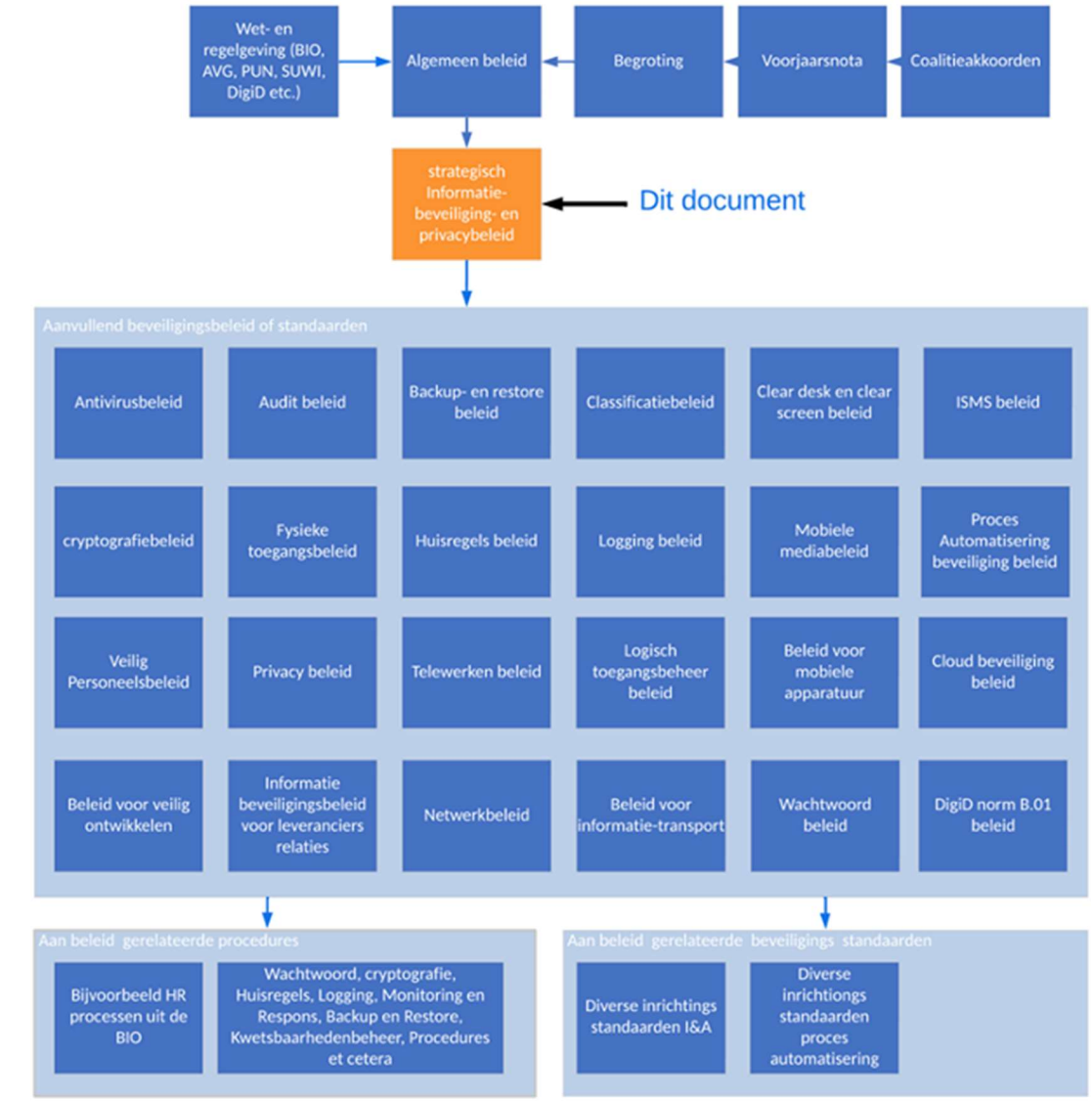
Inhoudsopgave 2
1. Inleiding 3
1.1 Waarom dit beleid 4
1.2 Visie en ambitie 4
1.3 Privacy & Gegevensbescherming (AVG) 4
1.4 Informatieveiligheid 5
1.5 Toepassingsgebied 5
2. Strategisch beleid 6
2.1 Doel 6
2.2 Kaders en Risico's 6
2.3 Doelen en Uitgangspunten 8
3. Controle en verantwoording 9
3.1 Controlerende functie van de Gemeenteraad 9
3.2 Rapportages 9
3.3 Toezicht 9
Afkortingen 10

1. Inleiding

In deze beleidsnota wordt het strategisch beleid op het gebied van privacy en informatieveiligheid voor de Gemeenteraad Teylingen beschreven. Met dit beleid, geldig van 2025 – 2028, zet de gemeenteraad een volgende stap om de beveiliging van persoonsgegevens en andere informatie op peil te houden en te verbeteren.

De gemeenteraad verwerkt binnen de uitvoering van haar taken (persoons)gegevens en draagt verantwoordelijkheid om deze verwerkingen binnen de wettelijke kaders te laten plaatsvinden. In haar ondersteunende rol aan de gemeenteraad draagt de griffie voor haar verwerkingen dezelfde verantwoordelijkheid.

Dit beleid omschrijft de kaders waarbinnen de verwerkingen plaats dienen te vinden, en biedt een basis voor verdere tactische uitwerking van informatieveiligheid- en privacy beleid. Dit beleid sluit aan op de bestaande *Gedragscode van de gemeenteraad van de gemeente Teylingen aangaande de persoonsgegevensverwerking in het kader van de AVG.*



Bovenstaande figuur geeft een indicatie van een breed beleidslandschap Privacy en Informatieveiligheid.

1.1 Waarom dit beleid

De snelle digitalisering en de groei in het gebruik van data zorgen ervoor dat informatieveiligheid en privacy steeds nauwer met elkaar verweven raken. Binnen de gemeenteraad worden met regelmaat gevoelige persoonsgegevens en vertrouwelijke informatie verwerkt. Dit kan complexe dataverwerkingen met zich meebrengen, waarbij zowel de bescherming van persoonsgegevens (privacy) als de beveiliging van systemen en informatie (informatieveiligheid) essentieel zijn. Door deze disciplines in één beleid te bundelen, kan er efficiënt ingespeeld worden op de uitdagingen en kansen binnen een snel ontwikkelende digitale wereld.

Met dit beleid geeft de gemeenteraad zowel interne als externe partijen en de samenleving duidelijkheid over de kaders waarbinnen de verwerkingen van (persoons)gegevens plaatsvinden.

Dit strategisch beleid is gericht op de lange termijn en heeft als doel een baken te zijn voor verdere tactische en operationele uitwerking van privacy en informatieveiligheid. Met de reeds vastgestelde *Gedragscode van de gemeenteraad van de gemeente Teylingen aangaande de persoonsgegevensverwerking in het kader van de AVG* is een start gemaakt om beleid gerelateerde procedures vorm te geven. Verdere tactische en operationele uitwerking moet op basis van een inventarisatie van processen en risicoafweging wel of niet worden uitgevoerd.

1.2 Visie en ambitie

De gemeenteraad van Teylingen is een betrouwbare partij voor alle gegevens die zij verwerkt van inwoners, ondernemers, medewerkers en partners. Als gemeente staan wij voor een digitaal veilige gemeente waarin alle betrokkenen samen kunnen leven, werken en genieten.

Om deze visie te bereiken hanteert de gemeenteraad de volgende ambitie. Wij zetten ons in voor een digitale veilige omgeving waarin inwoners, ondernemers, medewerkers en partners met vertrouwen kunnen leven, werken en genieten. We blijven ons voortdurend inzetten voor de verbetering van onze privacy- en informatieveiligheidsmaatregelen, waarbij we onze processen en technologieën cyclisch versterken om de benodigde normen van gegevensbescherming te waarborgen. Dit sluit aan bij het standpunt in het raadsprogramma 2022-2026 van een betrouwbare overheid en de aanpak van digitale criminaliteit door het eigen huis op orde te brengen en houden.

1.3 Privacy & Gegevensbescherming (AVG)

Het privacy beleid biedt de kaders voor een zorgvuldige verwerking van persoonsgegevens. Inwoners, ondernemers, medewerkers en partners moeten erop kunnen vertrouwen dat persoonsgegevens die worden verwerkt door de gemeenteraad passend worden beschermd.

Een rechtmatige verwerking van persoonsgegevens draagt bij aan een transparante overheid en zorgt ervoor dat inwoners vrij en veilig kunnen participeren in het democratisch proces, zonder zorgen over schending van hun privacy of misbruik van hun persoonsgegevens.

1.4 Informatieveiligheid

Informatieveiligheid gaat om het beschermen van informatie, inclusief persoonsgegevens, en is nodig om de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie te borgen. **Beschikbaarheid** is van belang, omdat we zonder gegevens en systemen de raadstaken niet uit kunnen voeren. De **integriteit** van gegevens is van belang, omdat we ervan uit moeten kunnen gaan dat de gebruikte gegevens correct zijn en rechtmatig worden gebruikt. De **vertrouwelijkheid** is van belang, omdat iedereen recht heeft op een overheid die op een correcte, veilige en betrouwbare manier met haar informatie omgaat.

1.5 Toepassingsgebied

Dit beleid is van toepassing op alle gegevensverwerkingen van de gemeenteraad en griffie, inclusief de ondersteunende informatiesystemen en processen.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het strategisch beleid Privacy en Informatieveiligheid voor 2025 - 2028. Dit beleid dient ter ondersteuning aan de gemeenteraad en griffie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Kaders en Risico's

2.2.1 Technologisch kader

Onze snel digitaliserende wereld maakt ons leven makkelijker, maar leidt ook tot nieuwe uitdagingen op het gebied van privacy en informatieveiligheid. Recente technologische ontwikkelingen zoals online opslag, slimme apparaten, kunstmatige intelligentie en andere innovaties hebben en zullen onze manier van leven, werken en communiceren ingrijpend veranderen.

Deze enorme vooruitgang brengt naast de nieuwe kansen en mogelijkheden ook grote risico's met zich mee op het gebied van gegevensbescherming. De toenemende afhankelijkheid van digitale systemen, de groeiende complexiteit ervan en de grote hoeveelheden gegevens die worden verwerkt hebben geleid tot een grote toename van cyberaanvallen en datalekken. Daarnaast worden er veel gegevens gedeeld met externe instanties en applicaties die een verhoogd risico tot oneigenlijk gebruik meebrengen.

Kwaadwillende actoren, zoals hackers en cybercriminelen, maken gebruik van de nieuwste technieken om deze gevoelige en vertrouwelijke informatie te bemachtigen. systemen te verstoren en schade toe te brengen aan zowel individuen als (overheids)organisaties. Daarbij is menselijke onachtzaamheid vaak de oorzaak. Naast het inrichten van een adequaat afgeschermde informatiehuishouding is continue aandacht en bewustwording bij medewerkers over informatieveiligheid en privacy randvoorwaardelijk bij het voorkomen van veiligheidsincidenten en datalekken.

2.2.2 Wettelijk kader

Dit beleid geeft in algemene zin invulling aan nationale en Europese wet- en regelgeving op het gebied van privacy en informatieveiligheid, voornamelijk zijn dit de drie onderstaande kaders:

- De Algemene Verordening Gegevensbescherming (AVG)[1]
- De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)[2]
- De Baseline Informatiebeveiliging Overheid (BIO)[3]

Deze kaders verplichten een gemeenteraad om strategisch beleid te ontwikkelen dat de beveiliging en privacy van informatie waarborgt. Dit beleid moet zorgen voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens, en moet risicomanagement integreren in de processen. Daarnaast moet de organisatie een veilige cultuur bevorderen en continu aandacht besteden aan de bescherming van persoonsgegevens.

[1] Verordening - 2016/679 - EN - avg - EUR-Lex
[2] wetten.nl - Regeling - Uitvoeringswet Algemene verordening gegevensbescherming - BWBR0040940
[3] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/10/BIO-versie-1.04zv.docx

2.2.3 De risico's

Er zijn verschillende risico's relevant voor de gemeenteraad welke met dit beleid worden geadresseerd. Deze risico's zijn onderverdeeld in drie hoofdcategorieën:

- **Beschikbaarheid**
  Niet-beschikbare systemen hinderen een groot deel van de raadsprocessen. De afwezigheid van het Raadsinformatiesysteem maakt vergaderen een grote uitdaging. Indien een raadsvergadering niet uitgezonden kan worden wegens een fout in de apparatuur kan transparantie richting de inwoner niet worden gegarandeerd. Risico's op het gebied van beschikbaarheid hebben een grote impact op de dagelijkse bedrijfsvoering van de gemeenteraad.

- **Integriteit**
  Foutieve of verouderde informatie in de systemen van de gemeenteraad hebben een grote invloed op het besluitvormingsproces. Hiermee loopt de gemeenteraad het risico op het nemen van foutieve of zelfs onwettige besluiten. Systemen dienen voldoende beveiligd en ingericht te zijn om dit te voorkomen. Risico's op het gebied van de integriteit hebben een grote impact op het imago van en het vertrouwen in de gemeenteraad.

- **Vertrouwelijkheid**
  Onzorgvuldig omgaan met informatie, waaronder persoonsgegevens, heeft op verschillende plekken een grote impact. Door menselijke fouten, onvoldoende beveiliging of cyberaanvallen kunnen gevoelige of persoonlijke gegevens van inwoners, ondernemers, raadsleden of ambtenaren, maar ook andere vertrouwelijke informatie zoals strategische plannen, openbaar worden gemaakt of bij (kwaadwillende) derden terechtkomen (datalek). Dergelijke datalekken kunnen leiden tot imago schade en persoonlijke (im)materiële schade. Bovendien kan het onzorgvuldig omgaan met persoonsgegevens leiden tot onwettige verwerkingen en daarmee een overtreding van de AVG met risico op sancties van de Autoriteit Persoonsgegevens.

2.2.4 Privacy versus Tranparantie

De openbaarheid van bestuur, versterkt door de Wet open overheid (Woo), is cruciaal voor een democratische gemeenschap. De Woo verplicht tot actieve openbaarmaking van informatie en sluit aan bij het recht van raadsleden om vragen te stellen, wat de controlerende taak van de raad en de transparantie ten goede komt. Echter, deze openbaarheid botst soms met het recht op privacy, beschermd door de AVG. Het is daarom essentieel om bij elke openbaarmaking een zorgvuldige afweging te maken. Persoonsgegevens moeten worden geminimaliseerd, en openbaarmaking moet proportioneel zijn en subsidiair aan andere oplossingen. In de praktijk betekent dit anonimisering of afscherming van persoonsgegevens, tenzij er een wettelijke basis is voor verwerking. De gemeente dient duidelijke richtlijnen te hanteren en raadsleden en medewerkers hierover te informeren, om zo transparantie te waarborgen met respect voor de privacy van inwoners.

2.3 Doelen en Uitgangspunten

2.3.1 Strategische doelen

De strategische doelen van dit beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en BIO en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.3.2 Belangrijkste uitgangspunten

De volgende uitgangspunten dienen leidend te zijn:

1. Er zijn heldere afspraken over de eigenaar of eigenaren van de processen om bovengenoemde risico's te voorkomen en mitigeren.
2. De taken en bijbehorende verantwoordelijkheden van de eigenaar of eigenaren dienen duidelijk en transparant te worden vastgelegd en vastgesteld.
3. De hierboven genoemde eigenaren zijn bekend en gekend binnen de gemeenteraad en griffie, schriftelijk vastgelegd en naar gelang de potentiële (veiligheids- en privacy-) risico´s ter zake kundig en adequaat uitgerust.
4. De gemeenteraad en griffie bevordert actief goed gedrag in het kader van privacy en informatieveiligheid en stimuleert deelname aan bewustwordingsinitiatieven op dit gebied.
5. Privacy en Informatieveiligheid is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatieveiligheid en privacybescherming.
6. Het managementsysteem maakt zoveel als mogelijk gebruik van meetinstrumenten zoals het AVG-borgingsproduct[4] en de Microsoft Secure Score[5].
7. Iedere griffiemedewerker of raads- en commissielid, zowel vast als tijdelijk, intern of extern, is verplicht (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan direct melding te maken conform afgesproken proces.
8. Het borgen van privacy en informatieveiligheid in de uitvoering van raadsprocessen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen op basis van een risico-inschatting.
9. Nieuwe ontwikkelingen, toepassingen, verwerkingen of wijzigingen van verwerkingen worden voorafgaand aan het in dienst nemen door middel van een risicoanalyse getoetst aan het beleid en geldende wet- en regelgeving.
10. Om uitvoering te kunnen geven aan dit strategisch beleid, en tactische invulling daarvan, zijn voldoende financiële middelen en uitvoeringscapaciteit nodig.

[4] AVG Borgingsproduct 3.0 - Informatiebeveiligingsdienst
[5] Microsoft Secure Score - Microsoft Defender XDR | Microsoft Learn

3. Controle en verantwoording

3.1 Controlerende functie van de Gemeenteraad

De gemeenteraad heeft naast haar eigen verantwoordelijkheid voor een zorgvuldige gegevensverwerking ook een toezichthoudende rol op de verwerking van persoonsgegevens binnen de gemeente en Werkorganisatie HLTsamen. Dit houdt in dat de raad erop toeziet dat de verschillende verwerkingen plaatsvinden volgens wet- en regelgeving en intern beleid, en dat privacy risico's zorgvuldig worden beheerst.

De raad houdt toezicht, stelt vragen en beoordeelt beleidsvoorstellen om de rechtmatigheid, transparantie en proportionaliteit van gegevensverwerking te waarborgen. Dit draagt bij aan de bescherming van de privacy van inwoners en zorgt ervoor dat de gemeente verantwoording aflegt over haar handelen met betrekking tot privacy en informatieveiligheid.

3.2 Rapportages

3.2.1 Rapportages Informatieveiligheid

De CISO rapporteert in het jaarrapport over de mate waarin de BIO maatregelen zijn geïmplementeerd of aangepast, een overzicht van de bijzondere gebeurtenissen en incidenten die hebben plaatsgevonden en de daarop toegepaste maatregelen, alsmede de bijzondere gebeurtenissen binnen de van toepassing zijnde verticale verantwoording (zoals BRP, Reisdocumenten, Suwinet en de DigiD aansluitingen). De gemeente verantwoordt zich al jaarlijks over informatieveiligheid met de ENSIA[6]-systematiek.

3.2.2 Rapportages Privacy

De Functionaris Gegevensbescherming rapporteert de bevindingen over de mate waarin de organisatie voldoet aan de wettelijk gestelde AVG-eisen, welke veranderingen zijn opgetreden ten opzichte van het voorgaande jaar, in hoeverre de voor dat jaar opgestelde verbeter- en/of jaarplannen zijn uitgevoerd, een overzicht van de in dat jaar opgetreden calamiteiten en geeft ten slotte een advies over welke structurele maatregelen genomen kunnen worden om geconstateerde hiaten te mitigeren of benodigde verbeteringen aan te brengen.

3.3 Toezicht

De Autoriteit Persoonsgegevens is de externe toezichthouder voor de AVG. De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van de gemeenteraad over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG is binnen de gemeentelijke organisatie onafhankelijk gepositioneerd en brengt jaarlijks een verslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.

[6] ENSIA - Eenduidige Normatiek Single Information Audit (het verantwoordingsproces over informatieveiligheid en datakwaliteit bij overheidsorganisaties)

Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatieveiligheid Overheid
BRP	Basis Registratie Personen
CISO	Chief Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
IBD	Informatiebeveiligingsdienst
PIV	Privacy en Informatieveiligheid
VNG	Vereniging Nederlandse Gemeenten
Woo	Wet open overheid