Gemeente *Stein*

GEMEENTEBLAD

Officiële uitgave van de gemeente Stein

Nr. 377776

1 september 2025

Strategisch privacy en informatiebeveiligingsbeleid 2025-2027

Uitleg van begrippen

Privacy
Privacy is een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy gaat erover dat mensen regie houden over hun eigen persoonsgegevens.

Informatiebeveiliging
De definitie van informatiebeveiliging is, kort gezegd, de bescherming van alle informatie van een bedrijf, ongeacht de aard of herkomst ervan. Het gaat hierbij om informatie van zowel technische als niet-technische aard.

Algemene Verordening Gegevensbescherming (AVG)
Europese wetgeving over het beschermen van privacy van burgers.

Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
Deze wet geeft in Nederland uitvoering aan de AVG. Deze wet regelt onder andere de taken en bevoegdheden van de toezichthouder de Autoriteit Persoonsgegevens.

Wet Politiegegevens (Wpg)
Wet Politiegegevens. Ziet net als de AVG toe op het beschermen van persoonsgegevens, maar dan specifiek over gegevens die in het kader van opsporingstaken (bij de gemeenten door boa's) worden verzameld.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die zich sterk maakt voor het recht op bescherming van persoonsgegevens.

Baseline Informatiebeveiliging Overheid (BIO)
Normenkader voor alle overheidsinstellingen aangaande informatiebeveiliging. Vanaf medio 2025 geldt de BIO 2.0 ook als normenkader voor de Cyberbeveiligingswet (Cbw).

NIS2-richtlijn
Europese richtlijn over Network & Information Security. In Nederland vertaald in de Cyberbeveiligingswet (Cbw).

Cyberbeveiligingswet (Cbw)
Cyberbeveiligingswet (Cbw) is de Nederlandse vertaling van de hierboven genoemde NIS2-richtlijn. Het doel van deze wet is om de digitale weerbaarheid van organisaties te vergroten en de gevolgen van cyberincidenten te verkleinen. Op deze manier wordt geprobeerd het algemene niveau van cyberbeveiliging te verhogen.

AI Act
Europese wet over het gebruik van algoritmes en Artificial Intelligence (AI). Stelt kaders aan organisaties die dit inzetten met als doel mens en maatschappij te beschermen.

Proceseigenaar
Eindverantwoordelijke voor een proces binnen de gemeente. In het geval van de gemeente Stein betreft dit de teammanager waaronder het proces valt. In het geval van een team overschrijdend proces, neemt het managementteam een besluit welke teammanager proceseigenaar is.

Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)
Binnen informatiebeveiliging wordt er gebruikt gemaakt van de BIV-classificatie om data te classificeren. De afkorting BIV staat voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. Om de risico's in te schatten maak je een belangenafweging. Dat kan met de BIV-classificatie.
Bij een risicoafweging maak je een inschatting van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt.

Informatiebeveiligingsdienst (IBD)
De Informatiebeveiligingsdienst (IBD) is een gezamenlijk initiatief van alle Nederlandse Gemeenten en is onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD is de sectorale CERT/ CSIRT voor alle Nederlandse gemeenten en richt zich op (incident) ondersteuning op het gebied van informa-

tiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

ISMS/ PIMS
Een Information Security Management System (ISMS) is een raamwerk van beleid, procedures, richtlijnen en middelen die worden gebruikt om de informatiebeveiliging te beheren en te verbeteren. Het ISMS helpt organisaties bij het opzetten van een structuur voor operationele planning en de implementatie van passende beveiligingsmaatregelen. Een effectief ISMS maakt gebruik van de Plan-Do-Check-Act (PDCA) cyclus om continue verbetering te stimuleren, waardoor uw organisatie steeds beter wordt in het beveiligen van haar IT systemen (kroonjuwelen) en financiële gegevens. Een Privacy Information Management System zorgt voor het beheren en verbeteren van privacy.

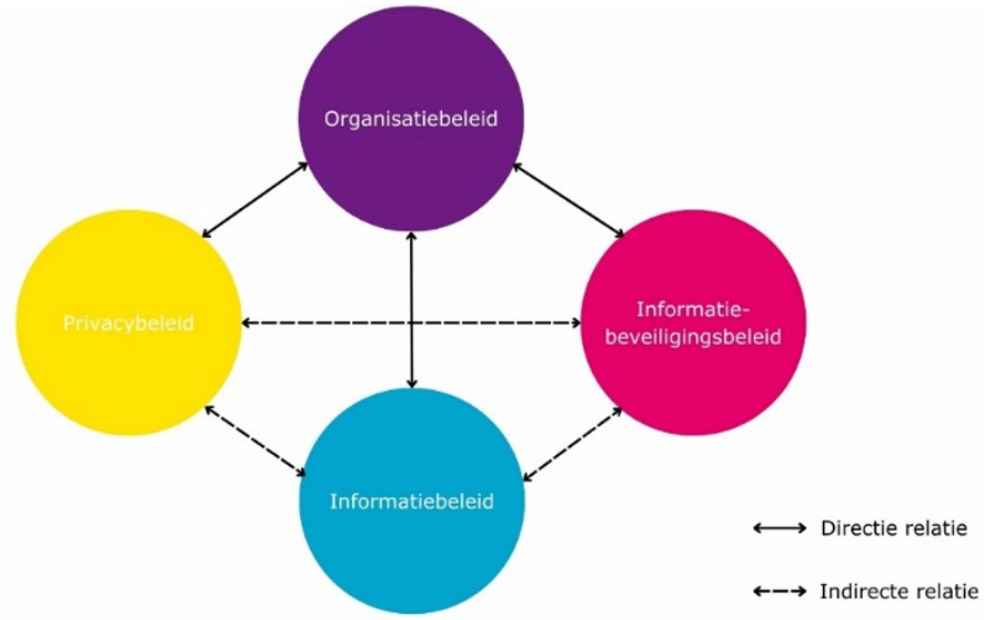
Een ISMS en PIMS vormen de bronsystemen voor compliance, voldoen aan wet- en regelgeving, verantwoordingsplicht, auditplicht en documentatieplicht.

Managementsamenvatting

De gemeente is wettelijk verplicht om een strategisch privacy- en informatiebeveiligingsbeleid door het Bestuur te laten vaststellen. Deze vaststelling dient formeel te gebeuren door het MT en aansluitend door het College van B&W. Hiermee wordt bestuurlijk geborgd dat privacy en informatiebeveiliging als strategische thema's zijn belegd binnen de organisatie en dat er draagvlak is voor de uitvoering van het beleid.

De huidige beleidsstukken op het gebied van privacy en informatiebeveiliging zijn niet meer actueel en voldoen niet langer aan de geldende wet- en regelgeving, noch aan de organisatorische werkelijkheid. Het strategisch beleid schetst de visie, kaders en uitgangspunten voor privacy en informatiebeveiliging binnen de gemeente Stein.

Samenhang tussen gemeentelijke beleid:
Dit beleid heeft een samenhang met het organisatiebeleid en het informatiebeleid. Deze twee beleidsonderdelen zijn nog onderhanden.



Doel van het privacy beleid:
- Waarborgen van privacy bij alle gemeentelijke verwerkingen.
- Integratie van Wpg-verplichtingen in het bredere AVG-beleid.
- Transparantie richting inwoners over gegevensverwerking.

Doel van het informatiebeveiligingsbeleid:
- Richting geven aan het veilig omgaan met informatie, door het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid.
- Voldoen aan wet- en regelgeving zoals de AVG, BIO 2.0 en NIS2, en risico's beheersen.

- Bewustwording en verantwoordelijkheid bevorderen bij medewerkers en bestuur voor veilig en zorgvuldig informatiegebruik.

Kaders en richtlijnen
- AVG, UAVG en Wet Politiegegevens.
- BIO 2.0 als norm voor informatiebeveiliging.
- NIS2/Cbw: met aandacht voor meldplicht, zorgplicht en bestuurlijke Verantwoordelijkheid.
- De AI Act: met regels voor transparant, ethisch en verantwoord AI-gebruik.
- Nieuwe wetgeving zoals PARTA, WGS en WAMS wordt actief gevolgd.

Rollen en verantwoordelijkheden
- Bestuur en directie zijn eindverantwoordelijk.
- Het MT bewaakt borging en voortgang via het uitvoeringsplan.
- De CISO, FG en Privacy Adviseur monitoren en adviseren onafhankelijk.
- Proceseigenaren zijn verantwoordelijk voor naleving binnen hun processen.
- Iedere medewerker draagt bij aan veilig en verantwoord omgaan met informatie.

1. Inleiding

Deze beleidsnota beschrijft het Strategisch privacy- en informatiebeveiligingsbeleid 2025-2027 van de gemeente Stein en vervangt de volgende documenten:
- Het Strategisch Informatiebeveiligingsbeleid 2022-2026
- Het Privacy beleidskader 2017
- Het Privacy reglement 2019

Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor privacy en informatiebeveiliging op tactisch niveau en procedures en werkinstructies op operationeel niveau. Dit beleid is van toepassing op alle medewerkers van de gemeente Stein waaronder alle processen, informatiesystemen en (persoons)gegevens. Bij het opstellen van dit beleid heeft de gemeente gebruik gemaakt van het landelijk sjabloon vanuit de Informatiebeveiligingsdienst (IBD) en verder afgestemd op de gemeente Stein.

Met dit strategisch gemeentelijk beleid zet de gemeente een volgende stap om het niveau van de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te verhogen. De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de Vereniging van Nederlandse Gemeenten (VNG) en de beginselen uit de Algemene Verordening Gegevensbescherming (AVG) voor het verwerken van persoonsgegevens.

Onderdeel van deze beleidsnota is het Addendum Privacy beleid Wet Politiegegevens welke als bijlage is toegevoegd aan dit document. De documenten worden na vaststelling gearchiveerd in het zaaksysteem van de gemeente.

1.1 Scope
De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Dit Strategisch privacy- en informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving en normen af zoals voor:
- De Algemene Verordening Gegevensbescherming (AVG)
  - De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

- De Wet Politiegegevens (Wpg)
- Baseline Informatiebeveiliging Overheid (BIO 2.0)
- Cyberbeveiligingswet (Cbw)
  - NIS2-richtlijn (NIS2)

- De Basisregistratie Personen (BRP)
- Reisdocumenten
- DigiD
- Suwinet

1.2 Buiten scope

De scope van dit beleid heeft enkel betrekking op wetgeving en normen waarin artikelen of regels zijn opgenomen die specifieke kaders geven aan de privacy of informatiebeveiliging. Om het beleid effectief en uitvoerbaar te houden worden specifieke wetgevingen de betreft o.a.:

- **Wet Open Overheid (Woo)**. De Woo heeft als doel openbaarheid van overheidsinformatie te bevorderen. Dit raakt wel informatiebeheer, maar is gericht op openbaarmaking in plaats van beveiliging.
- **Archiefwet**. De Archiefwet richt zich op het bewaren, ordenen en toegankelijk houden van overheidsinformatie voor de lange termijn. Dit gaat vooral over informatiebeheer en duurzaamheid, niet over het voorkomen van incidenten of beschermen van gegevens tegen dreigingen.

Deze wetten zijn niet onbelangrijk en worden behandeld binnen andere beleidskaders die beter passen bij hun specifieke doelstellingen.

1.3 Privacy

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheid of voor publieke zaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk. Bij de omgang met persoonsgegevens hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt niet alleen de toenemende digitalisering, maar ook de fysieke documenten en de fysieke toegangsbeveiliging tot het gemeentehuis, ruimtes en faciliteiten.

Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat. De gemeente houdt zich bij de bescherming van persoonsgegevens aan de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en de Wet Politiegegevens (Wpg).

1.4 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een samenhangend pakket van maatregelen (technische en organisatorische) om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.

Voor de gemeente Stein is het belangrijk dat informatie beschikbaar is wanneer medewerkers of (keten)partners deze nodig hebben om hun taak uit te voeren. Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. De gemeente houdt zich daarbij aan de Cbw, NIS2-richtlijn en het normenkader uit de BIO 2.0.

1.5 AI Act

De gemeente Stein past kunstmatige intelligentie (AI) alleen toe op een verantwoorde transparante en wettelijke manier, in lijn met de Europese AI-verordening (AI Act), de AVG en de BIO 2.0. AI-systemen worden vooraf beoordeeld op risico's met bijzondere aandacht voor toepassingen die invloed hebben op fundamentele rechte of geautomatiseerde besluitvorming. Hoog-risico AI vereist een AI-DPIA, menselijk toezicht en expliciet transparantie naar betrokkenen. De CISO en FG zijn betrokken bij toetsing en borging. AI wordt opgenomen in het reguliere risicobeheer, geëvalueerd op bias en veiligheid. Medewerkers worden opgeleid in het verantwoord gebruik van AI. Zo waarborgt de gemeente ethisch gebruik van AI en behoud van publieke waarden.

1.6 Visie en ambitie

In de 'Visie op privacy en informatiebeveiliging 2022-2026[1]' wordt uitgebreid in gegaan op de visie en ambitie van de gemeente Stein omtrent informatiebeveiliging en privacy. De gemeente Stein ziet informatieveiligheid en privacy als twee belangrijke pijlers van onze democratische rechtstaat. Daarom willen wij een toekomstgerichte, trendbewuste en veilige gemeente zijn. Dit leidt er onder meer toe dat

1) https://www.gemeentestein.nl/privacy

de gemeente steeds meer data gestuurd wil werken en processen wil automatiseren wanneer dat voordelen oplevert voor inwoners, bedrijven en belanghebbenden.

Gemeente Stein heeft de ambitie om in 2026 te voldoen aan volwassenheidsniveau 4 (op een schaal van 5) op het gebied van privacy en informatieveiligheid. Het eerste doel dat de gemeente nu voor ogen heeft is om niveau 3 verder uit te werken en volledig te behalen, het niveau waarop je op alle punten kunt aantonen dat je veilig werkt en dat de beveiligingsmaatregelen werken. De basis is op orde, maar de wet- en regelgeving en de snelheid van alle ontwikkelingen vragen meer.
Op dit niveau heeft de gemeente de informatiebeveiliging en privacy op een professionele wijze geborgd binnen de organisatie en processen. Daarbij zijn de risico's geminimaliseerd tot een acceptabel niveau. Dit niveau is ook noodzakelijk om te kunnen voldoen aan (aankomende) wet- en regelgeving.
Volwassenheidsniveau 5 is het ultieme, maar vraagt een grote betrokkenheid van alle medewerkers voor informatieveiligheid. Dat is voorlopig niet reëel.

De vijf volwassenheidsniveaus

Volwassenheidsniveau		**Omschrijving**
Geoptimali-seerd	5	• Toekomstgericht • Proactieve houding van het college en het bestuur • Privacy en informatiebeveiliging wordt gezien als een vanzelfsprekend-heid • Er wordt continue gezocht naar verbetering • Er wordt verbinding gezocht met andere teams • Kennis en ervaringen worden actief gedeeld met gemeenten en andere relevante organisaties waardoor best practices in gemeenteland ontstaan
Beheerst	4	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd over de realisering van de geconsta-teerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam
Bepaald	3	• Medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoor-delijkheden actief worden opgepakt • Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd • Er wordt aantoonbaar aan verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. • Er is een duidelijke samenhang tussen privacy en informatiebeveiliging • Bewust bekwaam.
Herhaalbaar	2	• Rollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
Ad hoc	1	• Geen of onduidelijke rollen en verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele functionarissen • Onbewust onbekwaam

In deze steeds meer gedigitaliseerde wereld zijn er ook dilemma's, risico's en ethische vraagstukken die spelen, denk bijvoorbeeld aan cybercriminaliteit. Daarom wil de gemeente Stein haar data op een veilige, verantwoorde en ethische manier beschikbaar stellen. De ambitie is dan ook om te blijven werken aan het verhogen van het volwassenheidsniveau op het gebied van privacy en informatieveiligheid.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het Strategisch informatiebeveiliging en privacy beleid voor de jaren 2025 tot 2027. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in de vastlegging van procedures en het jaarlijks bij te stellen 'Uitvoeringsplan privacy en informatiebeveiliging'.

Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van privacy en informatiebeveiliging.

De strategische doelen van het privacy en informatiebeveiligingsbeleid 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 burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en Wpg en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.2 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en procedures en daarmee richting te geven voor de verdere invulling van privacy en informatiebeveiliging op tactisch en operationeel niveau. Deze beleidsnota beschrijft op strategisch niveau het privacy- en informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Uitvoeringsplan privacy en informatiebeveiliging'.

2.3 Ontwikkelingen

De volgende ontwikkelingen zijn van belang bij het actualiseren van dit beleid:

2.3.1 De Baseline Informatiebeveiliging Overheid 2.0 (BIO 2.0)

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De Baseline Informatiebeveiliging Overheid (BIO) is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat medewerkers nu meer dan vroeger moeten werken volgens een aanpak waarbij risicomanagement centraal staat. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen voldoende beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De BIO 2.0 is sinds 2025 het nieuwe kader voor de overheid voor informatiebeveiliging. De nieuwe BIO volgt op de evaluatie van de huidige BIO en valt samen met de ontwikkelingen rondom de Cyberbeveiligingswet. Met de BIO 2.0 wordt er ook invulling gegeven aan eisen uit deze wet die horen bij de beveiliging van overheidsinformatie.

2.3.2 Cyberbeveiligingswet/NIS2

Binnen de Europese Unie geldt sinds 2024 de Network and Information Security 2 (NIS2)-richtlijn. Lidstaten dienen deze om te zetten in nationale wetgeving. In Nederland wordt dit de Cyberbeveiligingswet

2) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

(Cbw) die medio 2025 van kracht moet zijn. Ook overheidsinstellingen vallen onder deze nieuwe wet. Dit betekent dat de gemeente Stein invulling moet geven aan de plichten die hieruit voortvloeien: zorgplicht, meldplicht, registratieplicht en toezicht. Ook worden de verantwoordelijkheden van bestuurders en MT hierin wettelijk verankerd. Uit de NIS2-richtlijn/ Cbw volgt voor overheden een zorgplicht voor informatieveiligheid. De BIO helpt overheden bij het invullen van deze zorgplicht. BZK is van plan om in plaats van de huidige zelfregulering, de BIO als wettelijk verplicht kader voor de hele overheid aan te wijzen.

2.3.3 De AVG en de UAVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Stein is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

2.3.4 De Wet Politiegegevens (Wpg)

Met betrekking tot de Wet politiegegevens (Wpg) moet de gemeente Stein zich via een aparte audit verantwoorden. Deze audit dient elk jaar intern plaats te vinden en een keer in de vier jaar door een externe RE-auditor te worden uitgevoerd. Met dit auditrapport worden het college en gemeenteraad van de gemeente Stein geïnformeerd. Een afschrift van het auditrapport dient te worden gedeeld met de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens.

De gemeente heeft buitengewoon opsporingsambtenaren (boa's) voor taken in het kader van toezicht en handhaving van de openbare orde en de sociale veiligheid. Boa's verwerken bij de uitoefening van hun functie regelmatig persoonsgegevens. Bijvoorbeeld bij het controleren van een identiteitsbewijs, of bij het opleggen van een boete. Soms valt de verwerking van de persoonsgegevens onder het regime van de Wet politiegegevens (Wpg), soms onder de Algemene verordening gegevensbescherming (AVG). De gemeente Stein heeft in het addendum Privacy beleid Wpg de regels vastgelegd die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht. Zie bijlage document: Privacy beleid Wet Politiegegevens Addendum privacy beleid (AVG).

2.3.5 AI Act

Sinds 2024 is de AI Act van kracht binnen de Europese Unie. Doel van de wet is het bevorderen van de ontwikkeling en invoering van veilige en betrouwbare AI-systemen op de interne markt van de Europese Unie (EU). Door zowel private als publieke partijen. Daarnaast is het doel de grondrechten van EU-burgers te beschermen en innovatie op het gebied van AI in Europa te stimuleren. Het stelt verplichtingen voor aanbieders en gebruikers van AI-toepassingen, dus ook voor gemeenten die hier gebruik van maken en stelt hoge boetes in voor overtreders.

Vanaf de inwerkingtreding van deze nieuwe wet, gaat de AI-verordening in fasen van kracht, waarbij de meeste verplichtingen binnen een half en 3 jaar van kracht gaan. Ook geldt dat de verplichtingen over 6 jaar met terugwerkende kracht zullen gelden voor overheidsorganisaties. Hierdoor vinden de veranderingen niet allemaal tegelijk plaats. Dit geeft onze gemeente de tijd om zich op de verplichtingen voor te bereiden. Gemeente Stein gaat als onderdeel van dit beleid aanvullende beleid opstellen met betrekking tot de omgang met algoritmen en het voldoen aan de eisen in de AI act.

2.3.6 De 10 principes voor informatiebeveiliging

Om bestuurders te helpen in het nemen van hun verantwoordelijkheid op het gebied van informatiebeveiliging, heeft de Vereniging voor Nederlandse Gemeenten (VNG) 'De 10 bestuurlijke principes voor informatiebeveiliging' ontwikkeld[3]. De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt.

De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.

3) *https://ib-p.nl/download/de-10-bestuurlijke-principes-voor-informatiebeveiliging/*

7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.3.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

De Informatiebeveiligingsdienst (IBD) is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT/ CSIRT voor alle Nederlandse gemeenten en richt zich op (incident) ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). Elke 2 jaar stelt de IBD een Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten op. De IBD wil met deze publicatie gemeenten ondersteunen bij het in beeld krijgen en managen van de risico's voor inwoners, ondernemers, de ambtelijke organisatie, de politiek en het bestuur.

De gemeente Stein gebruikt dit dreigingsbeeld samen met de incidentmeldingen die door de IBD worden gedeeld met de vertrouwenscontactpersoon (VCIB) binnen de gemeente als onderdeel van de aanpak tegen de risico's op het gebied van informatiebeveiliging en gegevensbescherming.

2.3.8 ISMS/ PIMS

De gemeente maakt gebruik van een Information Security Management Systeem (ISMS) en een Privacy Informatie Management Systeem (PIMS). Een ISMS is in de eerste plaats een managementinstrument om de informatiebeveiliging te waarborgen en te besturen. Het betreft alle zaken die de gemeente gebruikt voor het beveiligen van (vertrouwelijke) informatie binnen de gemeente en geeft waardevolle informatie om van te leren uit incidenten, inbreuken op onze beveiliging en datalekken. PIMS is het managementinstrument om de privacy/gegevensbescherming te waarborgen en te besturen.

Naast de inbedding in de processen maakt de gemeente ook gebruik van een ISMS/PIMS applicatie om overzicht en structuur te behouden en continu te verbeteren. Met behulp van het ISMS/PIMS kan de gemeente anticiperen op (steeds veranderende) bedreigingen en kansen van buitenaf en inspelen op de behoefte binnen de gemeente. Het ISMS/PIMS wordt in Q3 2025 operationeel bij de gemeente.

2.3.9 Eenduidige Normatiek Single Information Audit (ENSIA)

De CISO voert de rol uit van ENSIA-Coördinator. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke medewerkers. De verantwoording over de informatiebeveiliging en privacybescherming komt tot uitdrukking in de collegeverklaring welke wordt opgesteld door de ENSIA Coördinator. Met deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG. Ook worden eventuele verbetermaatregelen vermeld die de gemeente gaat treffen.

Via ENSIA verantwoordt de gemeente zich naast de gemeenteraad ook aan de stelselhouders voor DigiD, BAG, BGT, BRO, BRP en de reisdocumenten. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente Stein informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Voor de beveiligingsmaatregelen voor webapplicaties en/of de infrastructuren voor de netwerksegmenten met webapplicaties in het algemeen waaronder DigiD en andere authenticatie- en identificatiediensten in het bijzonder houdt de gemeente zich aan het normenkader voor ICT beveiligingsassessments DigiD. Het normenkader voor ICT- beveiligingsassessements is bedoeld voor organisaties waaronder de gemeente die DigiD gebruiken en jaarlijks een ICT-beveiligingsassessment moeten doen. Deze norm is vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Audit Dienst Rijk en het NCSC.

2.4 Uitgangspunten en randvoorwaarden

Om dit beleid goed uit te kunnen voeren zijn een aantal uitgangspunten en randvoorwaarden van belang. Deze worden in deze paragraaf verder uitgewerkt.

Het bestuur en het management spelen een cruciale rol bij het uitvoeren van dit strategische beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy)risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor privacy en informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Het bestuur en management zijn verplicht een training te volgen op het gebied van Informatiebeveiliging, dit is een verplichting vanuit de Europese NIS2-richtlijn.

Het gehele gemeentelijk management geeft een duidelijke richting aan privacy en informatiebeveiliging en laat zien dat zij privacybescherming en informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een P&IB beleid van en voor de hele gemeente. Het P&IB beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.4.1 Uitgangspunten

De belangrijkste uitgangspunten van het privacy en informatiebeveiligingsbeleid zijn:

Bewustwording en training
Alle medewerkers, management en bestuur hebben een minimale basiskennis van privacy en informatiebeveiliging en weten deze bewust toe te passen in hun werk. Alle medewerkers worden getraind in het gebruik van beveiligingsprocedures. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.

Proceseigenaar MT Voor
De uitvoering van de privacybescherming en informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle processen, informatiebronnen en -applicaties die gebruikt worden door de gemeente Stein hebben een proceseigenaar. De rol van de proceseigenaar sluit aan op het handboek Procesmatig werken binnen de gemeente Stein. Dit betekent dat de proceseigenaar verantwoordelijk is voor het beheer en de optimalisatie van het proces, bewaakt de resultaten en zorgt voor continue verbetering waar nodig op het gebied van privacy en informatiebeveiliging. De proceseigenaar speelt een cruciale rol bij het waarborgen van risicobeheer en compliance en daarmee ook het uitvoeren van DPIA's.

Periodieke controle
Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Dit beleid vormt samen met het Uitvoeringsplan Privacy & Informatiebeveiliging het fundament voor een betrouwbare informatievoorziening en het beschermen van persoonsgegevens.
Het uitvoeringsplan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor privacy en informatiebeveiliging.

Plan, do, check, act (verbetercyclus)
Privacybescherming en informatiebeveiliging zijn een continu verbeterproces. 'Plan, do, check en act' (PDCA) vormen samen het managementsysteem van privacybescherming en informatiebeveiliging. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid. Regels en verantwoordelijkheden voor het P&IB beleid dienen te worden vastgelegd en vastgesteld. In het jaarlijks op te stellen uitvoeringsplan worden deze zaken opgenomen, waarin specifiek benoemt staat welke capaciteit van wie wordt verwacht en wat het budget is.

Risicomanagement
Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij datalekken of beveiligingsincidenten hiervan melding te maken.

Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting. De proceseigenaren (of degene waaraan dit is gedelegeerd) zijn hier verantwoordelijk voor.

2.4.2 Randvoorwaarden

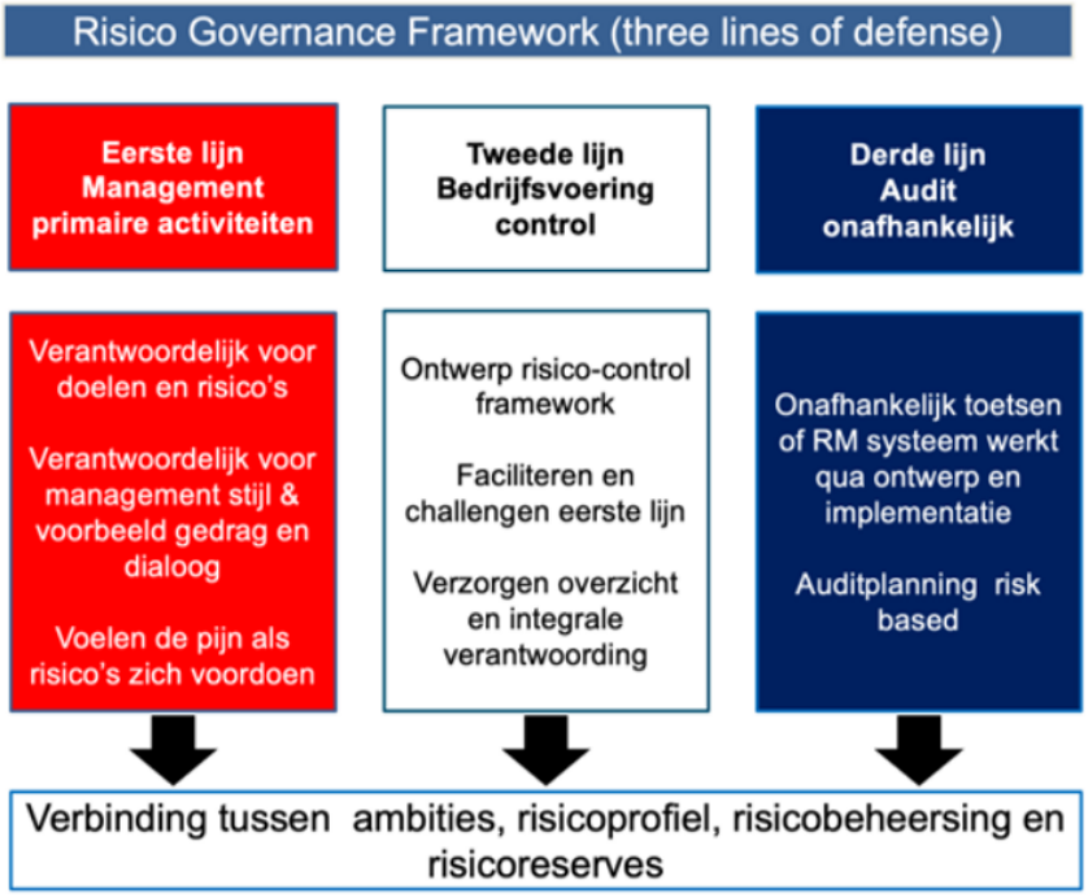
Belangrijke randvoorwaarden zijn:

- De privacy- en informatiebeveiligingseisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden onder andere door middel van een bewustwordingscampagne en het uitvoeringsplan.
- Het uitvoeringsplan Privacy en informatiebeveiliging wordt periodiek geactualiseerd onder leiding van de CISO en Adviseur Privacy, gebaseerd op:
  - Dit strategisch beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - De WPG-audit en andere auditresultaten;
  - Het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risicoanalyses en DPIA's en overige privacy activiteiten;
  - De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld door iets wat voortkomt uit bovengenoemde risicoanalyses of DPIA's.

- Om uitvoering te kunnen geven aan dit strategisch beleid en het uitvoeringsplan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt aangegeven welke taken en verantwoordelijkheden met betrekking tot privacy en informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense').



In dit model is het lijnmanagement verantwoordelijk voor het realiseren van privacy en informatiebeveiliging binnen de eigen processen. De tweede lijn (CISO, Adviseur Privacy) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA coördinator.

Ongeacht het voorgaande is en blijft iedere medewerker, zowel vast als tijdelijk, intern of extern, verplicht (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaarmaking, vernietiging, verlies en/of overdracht en bij mogelijke incidenten/ datalekken hiervan melding te doen.

3.1 Aansturing: managementteam
Het managementteam (MT) zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. Het MT zorgt dat de teammanagers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het MT en de CISO en Adviseur Privacy zorgen ervoor dat de eindverantwoordelijke portefeuillehouder binnen het college gevraagd en ongevraagd geïnformeerd wordt over de mate waarin privacy en informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het MT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het MT draagt zorg voor het uitwerken van tactische privacy- en informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO en Adviseur Privacy van de gemeente. Het MT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp privacybescherming en informatiebeveiliging wordt in de gemeente Stein gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: procesmanager en proceseigenaren
Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Stein hebben een interne eigenaar die de primaire verantwoordelijkheid draagt voor de bescherming van de daarin aanwezige informatie. Om deze verantwoordelijkheid waar te maken moeten zij goed ondersteund worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel (bijvoorbeeld aan een vakspecialist binnen het eigen team). De bedoeling is dat alle processen, systemen, verwerkingen en (persoons)gegevens altijd een eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Enkele belangrijke taken van de procesmanager en proceseigenaren in het kader van informatiebeveiliging en privacybescherming zijn, in samenwerking met de CISO en Adviseur Privacy:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.
- Het (laten) uitvoeren van een risicoanalyse zoals een DPIA.
- Het binnen het eigen team uitdragen van het privacy en informatiebeveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig (laten) betrekken van CISO en Adviseur Privacy bij nieuwe of gewijzigde processen.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen

3.3 Controle en verantwoording
Dit beleid is een verantwoordelijkheid van het bestuur van de gemeente Stein. Bestuur en management werken volgens de 10 principes voor informatiebeveiliging en privacy en de beginselen voor het verwerken van (persoons)gegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.

Tijdens het portefeuillehouder overleg rapporteren de CISO en Adviseur Privacy over informatiebeveiliging en privacy. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. De Functionaris Gegevensbescherming heeft de bevoegdheid om gevraagd en ongevraagd te rapporteren over informatiebeveiliging en privacy aan bestuur en management.

3.4 Governance privacy en informatiebeveiliging
Bestuurlijke verantwoordelijkheid gemeenteraad, college en portefeuillehouder
Dragen bestuurlijke verantwoordelijkheid voor het formuleren en implementeren van beleid op het gebied van informatiebeveiliging en privacy. De gemeenteraad treedt op als toezichthouder.

Organisatie: gemeentesecretaris
Is eindverantwoordelijk voor de borging van informatiebeveiliging en privacy binnen de organisatie.

Managementteam
Verantwoordelijk voor het integreren van informatiebeveiliging en privacy in strategische besluitvorming en processen binnen de organisatie.

Concerncontroller
Adviseert en ondersteunt op het gebied van informatiebeveiliging en privacy in relatie tot risicobeheer en rechtmatigheid.

Teammanagers en proceseigenaren
Verantwoordelijk voor de correcte verwerking van informatie binnen hun processen, inclusief het nemen van maatregelen voor informatiebeveiliging en privacy.

Functionaris Gegevensbescherming
De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W en de gemeenteraad over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin de bevindingen en aanbevelingen zijn vastgelegd.

CISO en Adviseur Privacy
- Zijn beide onafhankelijk gepositioneerd bij Unit Control.
- Rapporteren beide periodiek over de status van informatiebeveiliging en privacy en de afhandeling daarvan aan het bestuur en de directie.
- Adviseren, Coördineren, organiseren en monitoren zodat de juiste acties worden genomen op het gebied van informatiebeveiliging en privacy.
- Formuleren, beheren, evalueren en monitoren beleid en procedures.

Applicatiebeheerders
Verantwoordelijk voor het beheer van informatiesystemen en het implementeren van beveiligings- en privacy maatregelen. Inclusief de bewaking daarvan bij leveranciers. Hierbij hebben zij een signaalfunctie richting de proceseigenaren en het IB&P-team.

Privacy contactpersoon
De privacy contactpersoon is geen functie maar een rol. De persoon die deze rol op zich neemt, vervult deze rol naast zijn/haar andere taken. De privacy contactpersoon is afkomstig uit de eenheid zelf.
De privacy contactpersoon ondersteunt de teammanager/proceseigenaren c.q. organisatieonderdeel met het zorgvuldig omgaan met de privacy/gegevensbescherming van betrokkenen (inwoners en medewerkers) en privacy vragen die er spelen binnen het team. Voor beantwoording van privacy vragen kunnen Privacy adviseur en/of Functionaris Gegevensbescherming om advies gevraagd worden. Voor de Privacy adviseur en/of de FG is de privacy contactpersoon de ingang voor privacy vragen binnen het team.

Iedere medewerker en andere gebruiker van bedrijfsmiddelen
Verantwoordelijk voor het naleven van informatiebeveiligings- en privacyrichtlijnen in hun dagelijkse werkzaamheden en het signaleren van bijzonderheden op dit gebied.

3.5 Nieuwe wet- en regelgeving t.a.v. privacy en informatiebeveiliging

Nieuwe wet- en regelgeving kan ook invloed hebben op privacy en informatiebeveiliging. Aan de hand van de wetgevingskalender[4] van Overheid.nl wordt dit bijgehouden.
Nieuwe landelijke wet- en regelgeving gegevensbescherming 2025:
- Wet gemeenschappelijke samenwerkingsverbanden (WGS) **per 1-3-2025**.
- Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten (PARTA) **per 1-7-2025**.
- Wet aanpak meervoudige problematiek sociaal domein (WAMS) ingangsdatum nog onbekend.

M.b.t. nieuwe EU-wetgeving wordt verwezen naar de “Monitor EU-wetgeving over digitalisering en data”[5].Op onder andere de navolgende digitale thema’s: Gegevensbescherming, Cybersecurity en Artificiële Intelligentie.

4. Formele vaststelling

Managementteam

4) *Home | Overheid.nl | Wetgevingskalender*
5) *Monitor EU-wetgeving over digitalisering en data*

Het managementteam van de gemeente Stein heeft dit document operationeel vastgesteld in de MT-vergadering van 3 juli 2025.

College van burgemeester en wethouders
Het college van burgemeester en wethouders van de gemeente Stein hebben in de collegevergadering van 29 juli 2025 dit document bestuurlijk vastgesteld.

De vaststelling wordt aangetoond aan de hand van het MT- en collegebesluit. Hierdoor heeft er geen ondertekening plaats gevonden.