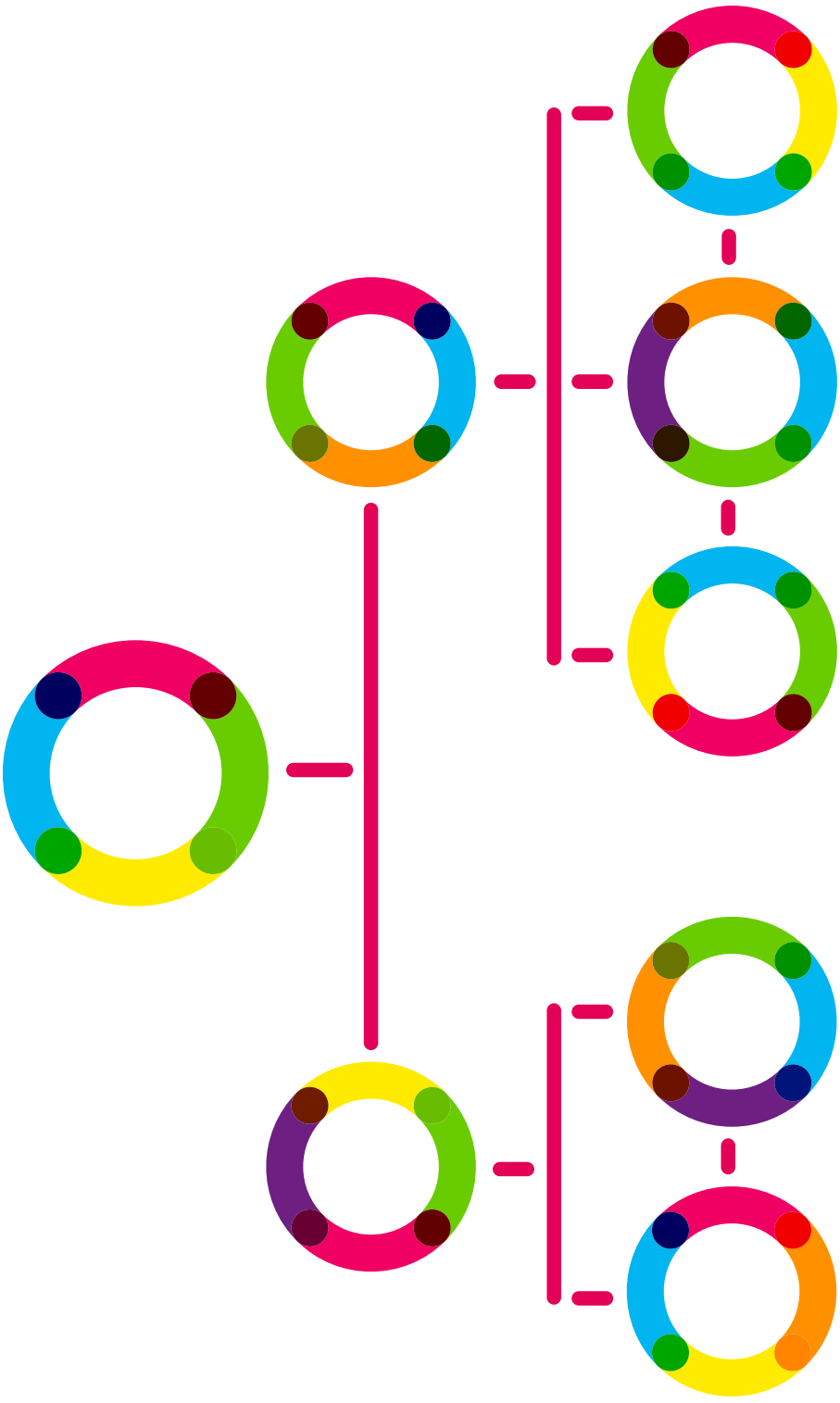

Visie op privacy en informatiebeveiliging 2022-2026

Gemeente *Stein*

Inhoudsopgave

Inleiding

Informatieprocessen binnen de gemeente Stein nemen een steeds belangrijkere plaats in. Door een veelheid aan factoren ontstaat de noodzaak om meer gegevens vast te leggen, te verwerken en zelfs aan elkaar te koppelen. De prominente plaats die informatieprocessen hebben gekregen binnen de gemeente heeft ook tot gevolg dat de afhankelijkheid van deze informatie sterk is toegenomen. Deze grote afhankelijkheid blijkt overigens pas indien informatie niet voorhanden is of indien de kwaliteit van informatie niet aan de normen voldoet. Waar in het verleden wellicht in een dergelijke situatie gesproken kon worden in termen van ‘ongemak’ of ‘vervelend’, komen nu complete processen stil te liggen als informatie niet voorhanden is of indien informatie niet aan de kwaliteitseisen voldoet dan wel niet betrouwbaar is.

Naast de steeds belangrijkere plaats die informatie in neemt is ook de vorm waarin informatie wordt vastgelegd, verwerkt en gekoppeld aan sterke ontwikkelingen onderhevig. Deze ontwikkelingen leiden niet alleen tot een grote afhankelijkheid van informatie in algemene zin, maar tevens van het beveiligen van informatie in het bijzonder.

Deze ontwikkelingen vragen om bijzondere aandacht voor de aandachtsgebieden privacy en informatiebeveiliging. Voor privacy betekent dit onder andere dat aan de voorkant van een proces al nagedacht moet worden over het veilig en rechtmatig verwerken van persoonsgegevens en het maken en vastleggen van privacy afspraken. Voor informatiebeveiliging betekent dit het bepalen van de **B**eschikbaarheid, **I**ntegriteit (=betrouwbaarheid) en **V**ertrouwelijkheid (BIV) van informatie(systeem). Dit helpt bij het bepalen van het gewenste niveau van informatiebeveiliging.

In dit document is de visie vastgelegd die de gemeente Stein volgt ten aanzien van een veilige omgang van persoonsgegevens en informatie en hoe daar in de toekomst mee om te gaan. Omdat privacy en informatiebeveiliging hand in hand gaan en het ene feitelijk niet zonder het andere kan, is er specifiek voor gekozen privacy en informatiebeveiliging te verwerken in een gezamenlijk visiedocument.

De wijze waarop er toegewerkt wordt aan de uitgangspunten in dit document is verwerkt in het uitvoeringsplan privacy & informatiebeveiliging. Ieder jaar wordt er door de CISO/ Adviseur privacy verantwoording afgelegd aan het managementteam en het college over de actiepunten in dit uitvoeringsplan.

Aanpak en uitgangspunten

Aanpak en uitgangspunten

Het privacy- en informatiebeveiligingsbeleid en de activiteiten die van daaruit worden ontplooid, staan nooit op zich maar zijn afgeleid van de doelstellingen van de organisatie. Gegevensbescherming is in deze een kwaliteitsaspect wat de gemeente helpt om haar doelen te bereiken. Hierbij staat centraal dat de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), de Baseline Informatiebeveiliging Overheid (BIO) en de Wet Politiegegevens (Wpg) als uitgangspunt worden gebruikt. Samenwerking is een strategisch middel om de doelen van de gemeente efficiënter en effectiever te bereiken. Er wordt kritisch gekeken naar de meerwaarde van samenwerking, maar zodra deze tot stand komt zal een structureel veilige gegevensuitwisseling noodzakelijk zijn.

Deze visie is opgesteld vanuit een integrale benadering. Uitgangspunt voor deze visie zijn de volgende documenten:

- Bestuursakkoord
- Strategische toekomstvisie
- Visie op dienstverlening
- Concernplan

De gemeente Stein heeft vanuit bovenstaande documenten een aantal strategische keuzes gemaakt. Hieronder volgen de beleidskeuzes en relevante privacy en informatiebeveiligingsaspecten. ***Let wel: deze keuzes en aspecten zijn nog redelijk abstract. In het privacy- en informatiebeveiligingsbeleid en in het (meerjarig) uitvoeringsplan privacy en informatiebeveiliging worden onderstaande punten concreet uitgewerkt.***

De coalitiepartijen spreken zich uit om bestaande samenwerkingen (sub)-regionaal en grensoverschrijdend te verstreken en daar waar mogelijk te intensiveren. De ambtelijke organisatie moet in staat worden gesteld een kwalitatief goede dienstverlening aan inwoners, instellingen en bedrijven te leveren. Wij als coalitiepartijen moeten dus waarborgen dat de organisatie over voldoende capaciteiten en faciliteiten beschikt om zodoende het huidige kwaliteitsniveau te waarborgen en waar nodig aan te passen en te verbeteren [1].

Dit heeft de volgende consequenties:

- De gemeente levert betrouwbare informatie;
- De gemeente heeft integere en verantwoordelijke medewerkers die goed weten om te gaan met privacy gevoelige informatie;
- De gemeente voert proactief beleid op de doorontwikkeling van kennis en bewustwording op het gebied van privacy en informatiebeveiliging;
- De gemeente heeft een goede informatievoorziening;
- De gemeente heeft de informatiesystemen zodanig op orde dat gevraagde informatie juist en volledig wordt opgeleverd;

[1] Bron: bestuursakkoord 2022-2026, bestuur pag. 11

- In het geval van calamiteiten heeft de gemeente maatregelen getroffen om de beschikbaarheid van informatie zo snel mogelijk te herstellen;
- Indien informatie uitlekt dan wordt dit gemeld aan de betreffende personen;
- De gemeente voldoet aantoonbaar aan de wettelijke eisen op het gebied van privacy en informatiebeveiliging;
- Voor aanvang van een mogelijke samenwerking worden heldere afspraken gemaakt over gegevensbescherming en informatiebeveiliging;
- De gemeente controleert op de naleving van de gemaakte afspraken;
- De gemeente maakt een risicoafweging bij de inzet van middelen voor informatiebeveiliging (proportionaliteitsbeginsel);
- De gemeente heeft de informatiebeveiliging goed georganiseerd;
- De gemeente integreert privacy en informatiebeveiliging binnen haar werkprocessen;

De genoemde uitgangspunten leiden tot een grotere afhankelijkheid en complexiteit van de informatievoorziening. De vraag is: "*Hoe kunnen we als gemeente het kwaliteitsaspect van gegevensbescherming en informatiebeveiliging toevoegen aan de producten en diensten die we leveren?*". Het is van belang te bepalen waar de grenzen liggen en wat het ambitieniveau van de gemeente is. De uitdaging is met name binnen de wettelijke kaders te zoeken naar werkbare toepassingen. De gemeente kiest ervoor een goede invulling te geven aan de kwaliteitsaspecten op het gebied van privacy en informatiebeveiliging.

Dit met in achtneming van de volgende kaders:
1. De verwachtingen van de klanten van de organisatie (burgers en ondernemers);
2. De eisen die de gemeente er zelf aan stelt (ambitieniveau);
3. De wettelijke kaders.

Ambitie

Onze ambitie

Privacy en informatieveiligheid zijn twee belangrijke pijlers van onze democratische rechtstaat. Privacy is een grondrecht en een fundamentele vrijheid, maar het gaat ook om de bescherming van (persoons)gegevens en vertrouwelijke informatie. Dat gevoel van veiligheid, dat rust op deze twee pijlers is een vereiste voor het uitoefenen van andere fundamentele vrijheden zoals de vrijheid om voor je mening uit te komen in spreken en schrijven.

Wij willen als gemeente Stein bijdragen aan de democratische rechtstaat door een toekomstgerichte, trendbewuste en veilige gemeente te zijn. Daarom blijven wij investeren in kennis en kunde. Zo kunnen wij actuele vraagstukken rondom privacy en informatieveiligheid goed aanpakken. De bescherming van de privacy van onze inwoners richten wij in volgens de meest passende normen van informatiebeveiliging. Wij volgen daarom trends en ontwikkelingen op de voet.

In de gemeente Stein werken we steeds meer datagestuurd en gebruiken we onze data om ons te ondersteunen in onze (maatschappelijke) vraagstukken. Onze digitale ambities liggen hoog en onze processen worden daar waar dit voordeel brengt geautomatiseerd. Dit biedt voordelen voor onze inwoners, voor bedrijven en belanghebbenden. Digitaliseren kan procedures vergemakkelijken. Omdat niet alle inwoners mee kunnen komen in de digitale ontwikkelingen, houden we de papieren processen daar waar nodig in stand.

Niet alleen onze administratieve processen digitaliseren, ook de openbare ruimte digitaliseert. Gemeenten, bedrijven en kennisinstanties verzamelen en gebruiken steeds meer data. Aan deze ontwikkelingen zitten ook dilemma’s, risico’s en ethische vraagstukken. Daarnaast is er de dreiging van cybercriminaliteit. Wij willen onze data op een veilige, verantwoorde en ethische manier beschikbaar stellen. Het versterken van het volwassenheidsniveau van de gemeente is hierdoor continue onder de aandacht. De wijze waarop er zo goed mogelijk gebruik wordt gemaakt van nieuwe ontwikkelingen en tegelijkertijd de risico’s worden beperkt is uitgewerkt in het privacy- en informatiebeveiligingsbeleid.

Volwassenheidsniveau

Het is een wettelijke verplichting en een maatschappelijke plicht om de juiste maatregelen te nemen binnen de organisatie en de techniek. Dit wordt uitgedrukt in volwassenheidsniveaus. De volwassenheid geeft aan hoe volwassen de gemeente Stein is in het borgen van gegevensbescherming en informatiebeveiliging.

De 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.

Afgelopen jaren laten een stijgende lijn zien in de mate waarop gemeente Stein voldoet aan de AVG en de BIO. Nu komt privacy en informatieveiligheid vaak nog vanuit de CISO/ Adviseur Privacy, de Functionaris Gegevensbescherming of de ICT afdeling. Beide thema's moeten onderdeel gaan vormen van ieders werk. Nu is het nog te vaak iets wat erbij moet, wat lastig is. Het zou ingebakken moeten zijn bij iedereen, bij alles wat je doet. Welke gevolgen heeft het voor betrokkenen als je een applicatie aanschaft? Welke afspraken moeten er met de leverancier gemaakt worden over beschikbaarheid, integriteit en vertrouwelijkheid? Welke maatregelen tref ik om te zorgen dat een hacker geen toegang heeft tot de gegevens? Dat vraag wel om specifieke kennis. Om dit te bereiken staat tone at the top en samenwerking centraal.

De vijf volwassenheidsniveaus

Geoptimaliseerd	5	• Toekomstgericht • Proactieve houding van het college en het bestuur • Privacy en informatiebeveiliging wordt gezien als een vanzelfsprekendheid • Er wordt continue gezocht naar verbetering • Er wordt verbinding gezocht met andere afdelingen • Kennis en ervaringen worden actief gedeeld met gemeenten en andere relevante organisaties waardoor best practices in gemeentenland ontstaan
Beheerst	4	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd over de realisering van de geconstateerde 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 verantwoordelijkheden 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

Leidende principes

Leidende principes

De volgende principes zijn leidend bij onze visie op privacy en informatiebeveiliging.

Inwoners kunnen vertrouwen op onze zorgvuldigheid.
Inwoners, bedrijven en belanghebbenden moeten erop kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan. Wij zijn een betrouwbare overheid, zeker omdat mensen niet altijd de keuze hebben om hun (soms zeer privacygevoelige) gegevens aan ons te geven. Wij informeren de inwoners actief over welke gegevens wij voor welke doeleinden verzamelen en verwerken, tenzij wet- en regelgeving ons dit niet toestaat.

Wij beschermen onze informatie.
We beschermen onze systemen en de informatie die we daarin verwerken en hebben opgeslagen. Medewerkers die toegang hebben tot informatie worden zorgvuldig gescreend en zijn aan geheimhouding gebonden.

Wij geven toegang tot informatie volgens een ‘need-to-know’ principe.
We besluiten op basis van het need-to-know en need-to-use principe op verzoeken tot informatie. Onze medewerkers mogen en kunnen alleen die informatie zien die zij voor hun werkprocessen nodig hebben. We beschermen onze (persoons)gegevens tegen ongeoorloofde toegang. Waar nodig passen we anonimisering en pseudonimisering toe, zodat gegevens niet direct herleidbaar zijn tot een persoon.

Wij passen privacy-by-design en security-by-design toe.
We nemen privacy afwegingen en informatieveiligheidsmaatregelen vanaf het begin mee bij aanpassingen van processen en systemen. We zoeken daarbij actief naar oplossingen. We gebruiken daarvoor instrumenten zoals zij uit de Algemene Verordening Gegevensbescherming en de Baseline Informatiebeveiliging Overheid worden aangereikt.

Wij nemen maatregelen gebaseerd op risico acceptatie.
Wij beschermen de privacy en informatie door een mix van maatregelen op het gebied van Mensen, Processen en Techniek. Onze maatregelen zijn risico gebaseerd. Wij kiezen bij het nemen van informatieveiligheidsmaatregelen voor de juiste balans tussen informatieveiligheid en gebruiksgemak. Zo wordt voorkomen dat die de werkprocessen belemmeren.

Wij innoveren en investeren in maatregelen.
Hackers worden slimmer en de druk op privacy neemt toe. Wij moeten onze beveiliging up-to-date houden. Wij innoveren en investeren aantoonbaar en blijvend in privacy en informatieveiligheid. Daarmee vergroten wij het vertrouwen bij onze inwoners, bedrijven en belanghebbenden. Hierbij zoeken we de balans tussen de te nemen maatregelen en de betaalbaarheid van de kosten.

Bij dataverzamelingen en gebruik zetten wij het maatschappelijk belang voorop.
Dataverzameling en gebruik moet noodzakelijk zijn voor het maatschappelijk belang en bijdragen aan de leefbaarheid van de kernen in de gemeente. Daarbij mag de data alleen worden verzameld voor een gerechtvaardigd doel en niet verder worden verwerkt voor andere doeleinden.

Wij blijven verantwoordelijk voor gegevens “in huis” en bij “derden”.
We zijn ook verantwoordelijk voor de verwerkingen en de informatie die we door “derden” laten uitvoeren. Daar maken we goede afspraken over met de ketenpartners en leveranciers die we in (verwerkers)overeenkomsten vastleggen.

Wij informeren medewerkers periodiek (bewustwording)
Wij stimuleren medewerkers in onze organisatie in het nemen en voelen van verantwoordelijkheid voor de zorg rond privacy en informatieveiligheid. Medewerkers worden bijgestaan door specialisten uit de organisatie in vraagstukken rondom de Algemene Verordening Gegevensbescherming, de Uitvoeringswet Algemene Verordening Gegevensbescherming, de Baseline Informatiebeveiliging Overheid en de Wet Politiegegevens.

Dat maakt Stein voor mij...

Gemeente *Stein*