Gemeente Stein

Gemeente Stein

Privacy beleidskader 2017-2019

Documentcode:	0971136621
Versie:	1.0
Versiedatum	10 oktober 2017
Gemaakt door:	Adviseur privacy
Goedgekeurd door:	Managementteam / College van B&W

Inhoudsopgave

Definities

AVG (Algemene Verordening Gegevensbescherming) – Europese wet op de verwerking van persoonsgegevens, die rechtstreeks geldt in alle lidstaten.

Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.

FG (Functionaris voor Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften.

Gegevensverwerking – zowel geheel of gedeeltelijk geautomatiseerde operationele informatieverwerking (bijvoorbeeld archiveren, analyseren, doorgeven, raadplegen) als ieder geheel daarvan (bijvoorbeeld de salarisadministratie, gemeentebelastingen of thuiszorg).

Persoonsgegevens – gegevens over personen en waarvan de gegevensverwerking door herleidbaarheid gevolgen heeft in de persoonlijke levenssfeer (privacy impact heeft).

PIA (privacy impact assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacyoptiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen).

PIA-score – getalsmatige classificatie van noodzaak of risico van gegevensverwerking, als uitkomst van een PIA.

PIT – het privacy- en informatiebeveiligingsteam dat de directie en proceseigenaren ondersteunt.

Portefeuillehouder privacy – het lid van het college dat verantwoordelijk is voor de uitvoering en naleving van privacywetgeving met behulp van het privacybeleidskader.

Privacyaudit – controles op de naleving van privacybeleid en privacywetgeving.

Privacybeleid – het privacybeleidskader en alle nadere uitwerkingen hiervan.

Privacybeleidskader – het bestuurlijk privacybeleid van een organisatie, dat de kapstok vormt waaraan operationele procesplannen worden opgehangen.

Privacybeleidsvoering – sturing op privacy door het management ('governance') .

Privacycoördinator – degene die namens de portefeuillehouder privacy uitvoering geeft aan het privacybeleid.

Privacyincidenten – gebeurtenissen waartegen het privacybeleid en de privacywetgeving bescherming beoogt te bieden.

Privacywetgeving – wetgeving die verwerking van persoonsgegevens regelt, in het bijzonder de AVG.

Procesdoel – een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens.

Proceseigenaren – lijnmanagers die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen of veiligheid.

Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een PIA).

Servicepunt – het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacyrechten.

Uitvoeringsorganisatie - een organisatie waaraan een of meerdere bedrijfsprocessen zijn uitbesteed.

1 Kernpunten

1.1 Voor wie?

Het privacybeleidskader Gemeente Stein bevat managementafspraken tussen het college en het management (proceseigenaren). De afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden gebruikt, opgeslagen of uitgewisseld ('verwerking van persoonsgegevens').

1.2 Doel

Het doel van het privacybeleidskader Gemeente Stein is om te waarborgen dat gemeente Stein de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie

In aansluiting op de toekomstvisie 'Het Stein van Morgen', beschouwt Gemeente Stein de bescherming van persoonsgegevens als vanzelfsprekend en een kwestie van behoorlijk bestuur. Wij stellen de burger centraal en willen goed werkgever zijn. Inwoners en medewerkers kunnen er dan ook op vertrouwen dat de gemeente persoonsgegevens rechtmatig, zorgvuldig en veilig verwerkt. Wie voor Gemeente Stein werkt, begrijpt dat en laat zich hierdoor leiden in zijn of haar dagelijks werk. Het college van B&W schept de voorwaarden voor een privacybewuste organisatiecultuur en voert in dat kader niet aflatend privacybeleid. Wij zijn transparant over onze gegevensverwerking en privacybeleidsvoering. Bij dilemma's gaan wij de dialoog aan met betrokkenen en zoeken gezamenlijk naar oplossingen.

1.4 Kernpunten

1) Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren sturen op privacy volgens deze kernpunten van privacymanagement:
   a) Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toezicht op zijn proces(sen) op basis van dit privacybeleidskader;
   b) Bij processen waaraan privacyrisico's zijn verbonden, hanteert de proceseigenaar een procesplan;
   c) Een procesplan is duidelijk, actueel, stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd;
   d) Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
   e) Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt;
   f) Een procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering;
   g) Een procesplan omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden;
   h) Een proceseigenaar handelt vragen of klachten van inwoners of medewerkers binnen twee weken af.;
   i) Bij privacyincidenten hanteert de proceseigenaar de Werkinstructie melden datalekken;
   j) Bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen op grond van dit privacybeleidskader en het betreffende procesplan.

2) Het college voorziet in een team van professionals dat het college en de proceseigenaren ondersteunt in de privacybeleidsvoering.
3) Het college voorziet in faciliteiten voor bewustwording en training.
4) Gemeente Stein beschikt over mechanismes voor privacy-incidentmanagement.
5) Gemeente Stein evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader.
6) Het college informeert de raad over de privacybeleidsvoering.
7) Het college handhaaft het privacybeleid.
8) Gemeente Stein heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de borging van privacy in de gemeenteorganisatie.

1.5 Scope

Het privacybeleidskader Gemeente Stein is van toepassing op alle bedrijfsvoering van gemeente Stein voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.

Het privacybeleidskader Gemeente Stein is het algemene deel van het privacybeleid binnen de gemeente. Het algemene beleidskader is de kapstok voor het privacybeleid van Gemeente Stein, waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten.

Het privacybeleid Gemeente Stein omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil.

Het privacybeleid Gemeente Stein is van toepassing op processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor Gemeente Stein informatiediensten verricht.

Het privacybeleid Gemeente Stein is van toepassing op gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders.

Het privacybeleid omvat de gehele 'data life cycle': van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

Het privacybeleid is van toepassing op de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

Het privacybeleid is van toepassing op informatieveiligheidsproblemen.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van Gemeente Stein heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Integriteitsbeleid
Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid.

Kwaliteitsbeleid
Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteit- en risicomanagement
Privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerking een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).

Informatiebeveiliging
Privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens. Informatiebeveiliging wordt uitgevoerd op basis van informatiebeveiligingsbeleid.

Personeel en organisatie
Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie wordt uitgevoerd vanuit het P&O beleid.

Communicatie
Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatiebeleid.

Inkoopbeleid
Het inkoopbeleid betreft alle diensten en processen die de gemeente uitbesteed of inkoopt, of waarbij wordt samengewerkt met derden. Hierbij worden eisen gesteld aan de privacywaarborgen die de betreffende derde partij kan bieden. Deze dienen in lijn te zijn met de eisen aan privacywaarborgen die vanuit de gemeente gesteld worden.

2 Privacy management

Het college van gemeente Stein is verantwoordelijk voor de naleving van privacywetgeving en voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat dit evenwichtig plaatsvindt. Dat wil zeggen; behoorlijk, zorgvuldig en in overeenstemming met de wet.

Privacy management is SMART-georganiseerd en heeft zelfstandige aandacht binnen de planning & control-cyclus van de gemeentelijke organisatie.

Het college legt over de privacybeleidsvoering verantwoording af aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting.

Het college draagt zorg voor de documentatie van beleid en maatregelen zodat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.

Het college houdt een register van de gegevensverwerkingen bij die onder hun verantwoordelijkheid plaatsvinden zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming (AVG).

2.1 Managementstructuur

Het college is verantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van gemeentelijke taken.

Privacy valt onder de verantwoordelijkheid van de portefeuillehouder privacy in het college, die voor dagelijkse aansturingstaken een privacycoördinator aanwijst.

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen.

Het college geeft de gemeentesecretaris opdracht om te voorzien in een team van professionals (hierna het Privacy & Informatiebeveiligings-team, kortweg: PIT) die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. Het PIT ondersteunt proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleid.

Afdelingshoofden zijn operationeel eindverantwoordelijk voor de uitvoering van gemeentelijke taken (burgerzaken, openbare orde en veiligheid, gemeentebelastingen, sociaal domein, ruimtelijke ordening en milieu, e.a.).

2.2 Proceseigenaarschap

Afdelingshoofden zijn ervoor verantwoordelijk dat de gemeentelijke taakuitoefening waarvoor zij verantwoordelijk zijn, binnen de grenzen van dit privacybeleidskader plaatsvindt en rapporteren over dit laatste aan de portefeuillehouder privacy.

- Een afdelingshoofd is **proceseigenaar**.
- De proceseigenaar kan verantwoordelijkheden mandateren aan teamleiders ('subproceseigenaren')
- Het college blijft eindverantwoordelijk voor de privacybestendigheid van gemeentelijke processen als de **'verwerkingsverantwoordelijke'** in de zin van de AVG.

Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen (zie hierna in hoofdstuk 4.1) die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit privacybeleidskader en is steeds in overeenstemming met de feitelijke situatie.

Een proceseigenaar houdt proactief toezicht op de privacybestendige organisatie van zijn proces en documenteert keuzes en oplossingen als bijlagen van het procesplan.

Een proceseigenaar kan proceseigenaarschap mandateren aan een subproceseigenaar binnen de gemeente. Bij mandatering blijft de opdrachtgevende proceseigenaar verantwoordelijk voor de privacybestendigheid van de aanpak door de subproceseigenaar.

Een proceseigenaar kan proceseigenaarschap mandateren aan een partij buiten de gemeentelijke organisatie met toestemming van de hoofdproceseigenaar (samenwerking met externe ketenpartners). Het mandaat blijkt uit, bijvoorbeeld, een inkoopcontract, de deelname in een gemeenschappelijke regeling of gebruikmaking van een landelijke voorziening. Bij externe ketensamenwerking blijft de opdrachtgevende proceseigenaar namens het college verantwoordelijk voor de privacybestendigheid van de aanpak door hem ingeschakelde ketenpartner(s) en houdt hierop toezicht. De wet kan dwingende bepalingen bevatten over wederzijdse verantwoordelijkheden bij ketensamenwerking.

Wanneer gemeentelijke processen zodanig zijn georganiseerd dat de onderliggende gegevensverwerking onder de verantwoordelijkheid van meerdere afdelingshoofden vallen, is de gemeentesecretaris de proceseigenaar. De gemeentesecretaris kan vervolgens eventueel een bijzondere proceseigenaar aanwijzen voor het gezamenlijke deel van de gegevensverwerking.

2.3 Toezicht

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van Gemeente Stein op de naleving van privacywetgeving conform artikel 37-39 AVG.

Het college informeert interne en externe doelgroepen over de FG en communiceert zijn contactgegevens aan de Autoriteit Persoonsgegevens.

De FG wordt aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacy management-praktijk; (b) zijn vermogen om de onderstaande taken te vervullen en (c) zijn onafhankelijkheid – met name de afwezigheid van belangenconflict.

De FG:

- informeert en adviseert het college, proceseigenaren en het PIT over de werking van het privacybeleid van Gemeente Stein en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving);
- houdt toezicht op de nakoming van het privacybeleid en achterliggende wettelijke verplichtingen;
- helpt privacyklachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacyincidenten over ernst en omvang;
- beheert het Privacybeleidskader Gemeente Stein;
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG;

- controleert de naleving van afspraken door Gemeente Stein en ketenpartners op privacygebied en coördineert in dit verband de uitvoering van privacyaudits, waarbij hij streeft naar minimale belasting van de gemeentelijke organisatie door controle-activiteiten;
- helpt het privacybeleid uit te dragen bij interne en externe doelgroepen;
- is het contactpunt voor landelijke privacytoezichthouders – met name de Autoriteit Persoonsgegevens.

De FG krijgt de nodige ruimte voor professionele uitvoering van taken.

- Het college en proceseigenaren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen Gemeente Stein waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het college en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De FG mag niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen.

De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door de gemeente, onverminderd de opvattingen van landelijke toezichthouders.

De FG doet jaarlijks verslag van zijn werkzaamheden aan het college van B&W. De raad wordt via de Planning & Control cyclus geïnformeerd.

3 Privacybeleid Gemeente Stein

3.1 Algemeen

Gemeente Stein is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:

- voert Gemeente Stein proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert Gemeente Stein de uitoefening van rechten van personen;
- bewaakt Gemeente Stein de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

3.2 Noodzakelijke gegevensverwerking

Proceseigenaren verwerken persoonsgegevens uitsluitend voor de volgende doelen, voor zover dit valt binnen hun mandaat en noodzakelijk is voor:

1. de uitoefening van publieke taken;
2. de nakoming van wettelijke plichten;
3. de vrijwaring van vitale belangen voor de betrokkene(n);
4. de totstandkoming of uitvoering van een overeenkomst waarbij een betrokkene partij is;
5. de behartiging van een gerechtvaardigd belang van Gemeente Stein of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

3.3 Kapstokregeling

Het privacybeleidskader van Gemeente Stein heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Voor zover dit speelt, geven proceseigenaren via themabeleid en procesplannen nadere invulling aan het privacybeleidskader Gemeente Stein, in samenspraak met het PIT en de FG.

Privacybeleid per domein beschrijft de aanpak op specifieke domeinen en thema's waarop de gemeente een taak heeft. De volgende domeinen en thema's worden binnen de gemeente onderscheiden:

- Gemeentelijke organisatie;
- Gemeentelijke belastingheffing;
- Burgerzaken;
- Ruimte en bereikbaarheid;
- Milieu en duurzaamheid;
- Leefomgeving;
- Veiligheid en openbare orde;
- Jeugd en onderwijs;
- Maatschappelijke ondersteuning;
- Maatschappelijke opvang;
- Werk en inkomen;
- Lokale economie;
- Cultuur en sport.

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat.

Het privacybeleidskader Gemeente Stein bevat ook de aanzet voor het regelen van aspecten van privacybeleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

Het privacybeleidskader Gemeente Stein, themabeleid, procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid Gemeente Stein. In geval van tegenstrijdigheid heeft het privacybeleidskader Gemeente Stein voorrang.

3.4 Inachtneming bijzondere wettelijke voorschriften

Op basis van het privacybeleidskader Gemeente Stein, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming. Voor zover van toepassing, houden proceseigenaren tevens goed rekening met bijzondere wettelijke voorschriften – met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Telecommunicatiewet, de Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning.

4 Gedragsnorm voor proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het PIT en de FG. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen Gemeente Stein een privacybestendige cultuur te realiseren.

Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen ('privacywaarborgen') en documenteren die maatregelen in procesplannen.

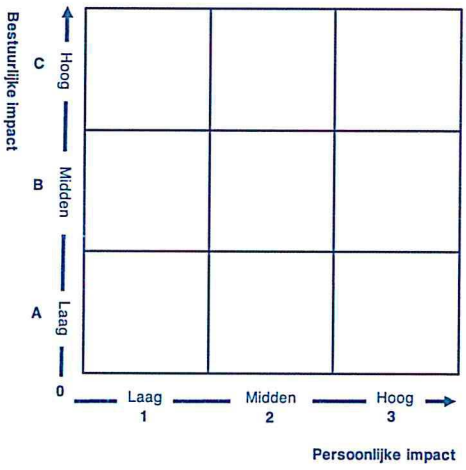
De portefeuillehouder privacy houdt een 'artikel 30-register' (zie §4.4) bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het college vallen. Proceseigenaren helpen om het register volledig en actueel te laten zijn door middel van 'artikel 30-formulieren'.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking.

Het college en proceseigenaren dragen het belang uit van privacybeleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

4.1 Procesplan-aanpak

Aan procesplannen liggen privacy impact assessments (PIA's) ten grondslag. PIA's zijn instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de PIA, zoals verwoord in het PIA-rapport. Voor eenduidig begrip hanteert Gemeente Stein een systeem van positieve en negatieve PIA-scores. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen (privacywaarborgen). Proceseigenaren volgen het advies van het PIT bij de vaststelling van hun PIA-score. PIA-scores worden bepaald aan de hand van de hiernaast afgebeelde matrix.



Proceseigenaren zijn goed bekend met hun PIA-scores en hanteren onderstaande tabel om te bepalen in hoeverre PIA's tevens deel uitmaken van het procesplan om op die manier de keuzes voor beheersmaatregelen te verantwoorden. Het artikel 30 formulier levert de input voor het verwerkingsregister.

PIA-Score	PIA-rapport	Procesplan	Artikel 30 formulier	Akkoord FG
A1	Summier	Nee (wordt gedekt door informatiebeveiliging)	Ja	-
A2	Beknopt	PIA-rapport maakt deel uit van procesplan	Ja	Aanbevolen
A3	Volledig	PIA-rapport maakt deel uit van procesplan	Ja	Verplicht
B1	Beknopt	PIA-rapport maakt deel uit van procesplan	Ja	Aanbevolen

B2	Beknopt	PIA-rapport maakt deel uit van procesplan	Ja	Aanbevolen
B3	Volledig	PIA-rapport maakt deel uit van procesplan	Ja	Verplicht
C1	Volledig	PIA-rapport maakt deel uit van procesplan	Ja	Verplicht
C2	Volledig	PIA-rapport maakt deel uit van procesplan	Ja	Verplicht
C3	Volledig	PIA-rapport maakt deel uit van procesplan	Ja	Verplicht

PIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG.

Proceseigenaren documenteren met behulp van hun procesplannen hoe zij op een praktische manier in passende organisatorische en technische privacybeschermende maatregelen voorzien – met name om de volgende fouten te voorkomen:

1. **Illegale/onrechtmatige gegevensverwerking:** gebruik, opslag of uitwisseling van informatie is bij wet verboden (middels een rechtstreeks verbod of een beperking van het toegestane gebruik).
2. **Disproportionele gegevensverwerking:** gebruik, opslag of uitwisseling van informatie is (a) ontoereikend of juist overmatig of (b) het organisatiebelang bij de gegevensverwerking is onevenredig klein terwijl de impact op personen onevenredig nadelig kan zijn.
3. **Irrelevante gegevensverwerking:** de gebruikte, opgeslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd.
4. **Onnauwkeurige gegevensverwerking:** de gebruikte, opgeslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid.
5. **Onveilige gegevensverwerking:** de gebruikte, opgeslagen of uitgewisselde informatie dreigt te gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of onbeschikbaar te zijn.
6. **Niet-inachtneming van bijzondere wettelijke voorschriften:** bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.[1]
7. **Onbewaakte gegevensverwerking:** de proceseigenaar verzuimt om te controleren of de privacywaarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn procesplan bijstelling behoeft.

Voor A1-processen volstaan algemene oplossingen. Zolang een proces als A1 gekwalificeerd is, is daarvoor in mindere mate aandacht nodig. De portefeuillehouder privacy publiceert een lijst van A1-processen.

De werkelijkheid dient in overeenstemming te zijn met het procesplan. Veranderingen in de bedrijfsvoering noodzaken tot aanpassing van procesplannen, waarvoor een nieuwe of geactualiseerde PIA nodig is.

4.2 Lijst van key-controls

Proceseigenaren vatten, in samenspraak met het PIT en zo nodig de FG, hun procesplannen samen in een lijst van kenmerkende beheersmaatregelen ('key-controls') voor sturingsdoeleinden en controle (zie paragraaf 7).

PIA-Score	Key-controls	Samenspraak PIT	Samenspraak FG
A1	-	-	-
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Verplicht

[1] Niet-nakoming van: meldplichten, bijzondere regels voor internationaal gegevensverkeer, wettelijke termijnen, verplicht voorafgaand onderzoek AP, toestemmingsverplichtingen

B1	Ja	Ja	Aanbevolen
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Verplicht
C1	Ja	Ja	Verplicht
C2	Ja	Ja	Verplicht
C3	Ja	Ja	Verplicht

Proceseigenaren nemen de lijst van key-controls op aan het einde van het procesplan.

4.3 FG-verklaring

Een evenwichtig procesplan beschrijft een behoorlijke en zorgvuldige aanpak, in overeenstemming met de wet. De FG bevestigt dit aan de hand van een verklaring waarbij hij eventueel ook aanbevelingen doet voor verdere optimalisering van de bedrijfsvoering.

PIA-Score	PIA-rapport maakt deel uit van procesplan	Akkoord FG
A1	-	-
A2	Ja	Aanbevolen
A3	Ja	Verplicht
B1	Ja	Aanbevolen
B2	Ja	Aanbevolen
B3	Ja	Verplicht
C1	Ja	Verplicht
C2	Ja	Verplicht
C3	Ja	Verplicht

Proceseigenaren nemen FG-verklaringen op aan het einde van het procesplan.

4.4 Artikel 30-formulieren

Proceseigenaren vatten hun procesplan samen in een 'artikel 30-formulier' dat zij opnemen aan het begin van het procesplan en waarvan zij een afschrift verstrekken aan de portefeuillehouder privacy voor opname in het artikel 30-register. Proceseigenaren melden veranderingen voor het artikel 30-register onmiddellijk aan de hand van wijzigingsformulieren.

Artikel 30-formulier bevatten de volgende informatie:

1. Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking.
2. De PIA-scoring van het proces.
3. De naam, contactgegevens en het mandaat van de proceseigenaar.
4. Indien van toepassing: de contactgegevens van degene die die proceseigenaar assisteert in privacyaangelegenheden.
5. De bedrijfsdoelen die met het proces zijn gediend.
6. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens.
7. De categorieën van ontvangers van de persoonsgegevens en, indien van toepassing, informatie over internationaal gegevensverkeer.
8. Informatie op hoofdlijnen over genomen beheersmaatregelen (key-controls) – met name termijnen voor gegevensvernietiging en de aanpak op het gebied van informatiebeveiliging.
9. De FG-verklaring, indien afgegeven.

4.5 Beheer procesplan

De proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Een procesplan wordt bijgesteld wanneer in de praktijk blijkt dat de maatregelen onvoldoende passend blijken naar aanleiding van terechte klachten of andere onacceptabele incidenten.

Hoe dan ook evalueert de proceseigenaar een procesplan periodiek en vraagt zo nodig de FG om hierbij advies uit te brengen.

PIA-Score	Evaluatie	Advies FG
A1	4 jaarlijks	-
A2	3 jaarlijks	Aanbevolen
A3	jaarlijks	Verplicht
B1	3 jaarlijks	Aanbevolen
B2	2 jaarlijks	Aanbevolen
B3	jaarlijks	Verplicht
C1	jaarlijks	Verplicht
C2	jaarlijks	Verplicht
C3	jaarlijks	Verplicht

5 Privacyservices

5.1 Rechten

Personen mogen de Gemeente Stein houden aan het navolgende:

- dat Gemeente Stein handelt conform het onderhavige privacybeleidskader;
- dat Gemeente Stein de contactgegevens van de FG bekend maakt;
- dat Gemeente Stein informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;
- dat zij van hun inzagerecht gebruik kunnen maken;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) rectificeren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat Gemeente Stein verplicht tot het maken van een afweging;
- dat zij Gemeente Stein bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

5.2 Vragen

Bij vragen over privacy:

- hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunten;
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- een servicepunt kan het PIT om advies over de beantwoording vragen;
- een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot een servicepunt;
- Het servicepunt registreert in dat geval de vraag als een klacht.

5.3 Klachten

Bij klachten:

- hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunten;
- klachten worden zo snel mogelijk maar uiterlijk binnen twee weken afgehandeld;
- het servicepunt meldt de klacht onmiddellijk bij de incidentenregeling volgens paragraaf 6.6, die het PIT betrekt voor de feitelijke klachtafhandeling;
- Het PIT onderzoekt de gegrondheid van de klacht, waarbij zij name nagaat of de klacht betrekking heeft op de naleving van privacywetgeving en/of het privacybeleid van Gemeente Stein;
- Het PIT kan de FG om advies vragen over de afhandeling van de klacht.

5.4 Beroep

Personen hebben het recht om na afhandeling van een klacht conform paragraaf 5.3, hiertegen in beroep te gaan bij de FG voor zover het beroep gericht is op de naleving van privacywetgeving en/of het privacybeleid van Gemeente Stein.

6 Privacy programma

6.1 Werkprogramma

Het college stelt jaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van de jaarrapportage van de FG en de aanbevelingen die hij hierin doet. Het werkprogramma bevordert opzet, bestaan en werking van passende waarborgen voor de bescherming van persoonsgegevens binnen de kaders van het privacybeleid Gemeente Stein, ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen Gemeente Stein, met gebruikmaking van overige instrumenten die in deze paragraaf worden beschreven.

6.2 Bewustwording en training

Het college bevordert samen met hoofdproceseigenaren een privacybewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden.

6.3 PR & communicatie

Het college is transparant over de privacybeleidsvoering en voert op dit thema evenwichtig communicatiebeleid waarbij proceseigenaren zo nodig voorzien in bijzondere voorlichting aan specifieke doelgroepen.

6.4 Verdere verwerking, archiefbeleid, gegevensvernietiging

Het college voorziet samen met proceseigenaren in met passende waarborgen omklede verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt voorzien in met passende waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

6.5 Informatiebeveiliging

Het college ziet erop toe dat informatieveiligheid van Gemeente Stein in lijn met de geldende norm wordt georganiseerd. Gemeente Stein beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die deelneemt in het PIT en samenwerkt met de portefeuillehouder privacy, de privacycoördinator en de FG. Geheimhoudingsverklaringen zijn instrumenten binnen de gemeentelijke aanpak voor privacybescherming en informatieveiligheid. Bij processen in de klassen C2-3, B2-3, A2-3 worden aanvullende geheimhoudingsafspraken gehanteerd voor zover uit PIA's blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding functioneel zijn.

6.6 Regeling privacyincidenten

Het college voorziet in een procedure voor privacyincidenten die onder de verantwoordelijkheid valt van de portefeuillehouder privacy[2]. Deze procedure voor privacyincidenten bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten. Ook bevordert het college het oefenen op privacy-incidenten, incident management en crisiscommunicatie.

6.7 Handhaving

Het college handhaaft het gemeentelijk privacybeleid op basis van een regeling voor disciplinaire maatregelen bij niet-nakoming van afspraken volgens het privacybeleidskader Gemeente Stein.

6.8 Beleidsevaluatie

Hoofdproceseigenaren doen halfjaarlijks verslag aan de portefeuillehouder privacy van hun privacybeleid, oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de FG. De FG doet jaarlijks verslag aan het college en geeft aanbevelingen die strekken tot verdere optimalisering de privacybeleidsvoering. Het college besluit over bijsturing van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.

[2] Zie het document 'Werkinstructie melden datalekken'

7 Auditbeleid

Vragen, klachten en het incident management zijn in wezen steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaatst, is het zaak dat proceseigenaren ook zelf periodiek (laten) controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand van privacyaudits op de gehanteerde ijkpunten.

Zie het onderstaande schema voor de benodigde zwaarte en frequentie van privacyaudits.

- Quick scan is een beknopte toets onder de verantwoordelijkheid van de proceseigenaar
- Zelfevaluatie is een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar
- Externe audit is een audit die de proceseigenaar organiseert in samenwerking met de FG en waarbij eventueel een professionele auditor wordt betrokken.

Wanneer wordt aangegeven dat de betrokkenheid van de FG aanbevolen of verplicht is, is het raadzaam om hem van begin af aan te betrekken in het audittraject. Maar bij verplichte betrokkenheid dient hij in ieder geval medeontvanger te zijn van het auditrapport.

	Type audit	Frequentie	Betrokkenheid FG	Afschrift FG
A1	Quick scan	5 jaarlijks	-	-
A2	Zelfevaluatie	4 jaarlijks	vrijwillig	vrijwillig
A3	Externe audit	3 jaarlijks	ja	ja
B1	Zelfevaluatie	5 jaarlijks	vrijwillig	ja
B2	Zelfevaluatie	4 jaarlijks	ja	ja
B3	Externe audit	3 jaarlijks	ja	ja
C1	Externe audit	4 jaarlijks	ja	ja
C2	Externe audit	3 jaarlijks	ja	ja
C3	Externe audit	2 jaarlijks	ja	ja

8 Formele vaststelling

Het college van burgemeester en wethouders van de gemeente Stein heeft dit document formeel vastgesteld op 7 november 2017.