Steenwijkerland

GEMEENTEBLAD

Officiële uitgave van de gemeente Steenwijkerland

Nr. 453506

15 december 2021

Beleid privacy, informatiebeveiliging en informatiebeheer gemeente Steenwijkerland 2021-2024

1 Organisatievisie en -doelstellingen

De gemeente staat midden in de informatiesamenleving en draagt daar actief aan bij. Inwoners en ondernemers van de gemeente moeten kunnen rekenen op een betrouwbare overheid die luistert naar hun wensen en zorgen en vervolgens daarop inspeelt in haar dienstverlening. Zij moeten er op kunnen vertrouwen dat de gemeente voor een veilige leefomgeving zorgt, hun gegevens als ook die van de medewerkers, veilig zijn, compliant verwerkt en dat de gemeente gegevens uitwisselt met betrouwbare partners.

Anders gezegd: we stellen de samenleving centraal. Onze inwoners hebben er recht op dat wij zorgen voor betrouwbare informatie en professioneel werken met persoonsgegevens (ons hogere doel).

We zetten de inwoner op één: bij 90% van wat de gemeente doet, komen persoonsgegevens te pas. Wij zorgen ervoor dat deze zorgvuldig worden toegepast, beschermd en bewaard, niet meer dan nodig en niet langer dan nodig. Betrokkenen mogen weten wat wij doen. Transparant zijn is een bewuste keuze. Wij communiceren vanuit vertrouwen, dragen ons hogere doel intern en extern uit en handelen hiernaar.

In dat verband hanteert de gemeente voor de periode 2021–2024 de volgende organisatievisie en -doelstellingen.

Wij waarborgen een veilige omgeving voor alle gegevens die wij verwerken.

Dat geldt voor alle informatie in het archief, beleidsinformatie, bedrijfsinformatie en ook persoonsgegevens, (vertrouwelijke) gegevens van en over onze inwoners, ondernemers, andere belanghebbenden, onze bestuurders en onze medewerkers.

Die informatie kunnen wij zelf hebben vergaard, via de betrokkenen, maar ook van overheids- en ketenpartners. Alle informatie, die niet voor anderen (onbevoegden) toegankelijk mag zijn, beschermen wij en hebben wij op orde. Dat betekent dat informatie actueel en beschikbaar is voor degenen die dit in het kader van hun taken en werkzaamheden moeten hebben en dat de integriteit en vertrouwelijkheid van die informatie geborgd is.

2 Uitgangspunten

Bij het realiseren van de organisatievisie en -doelstellingen worden de navolgende zeven uitgangspunten gehanteerd.

Uitgangspunt 1: betrouwbaarheid

Betrouwbare informatie en een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en is de basis voor het beschermen van inwoners en ondernemers. De beveiliging van informatie en informatiebeheer, waarbij het gaat om overzicht en inzicht hebben in de informatiehuishouding, worden daarbij als kritische randvoorwaarden door de organisatie onderschreven.

Het recht op gegevensbescherming als grondrecht is hierbij een kader dat gewaarborgd wordt omdat de wettelijke regels gekoppeld aan het verzamelen en verwerken van persoonsgegevens door de organisatie in acht worden genomen.

Uitgangspunt 2: verantwoordelijkheid

Informatiebeveiliging en gegevensbescherming is een zaak van iedereen. Daarbij bevorderen bestuurders een veilige cultuur, controleren en evalueren en zijn de direct leidinggevenden niet alleen PIOFACH verantwoordelijk maar ook inhoudelijk voor de werkprocessen. Zowel het directieteam als de teamleiders geven duidelijk richting aan informatiebeveiliging en gegevensbescherming en laten zichtbaar zien dat zij dit ondersteunen en zich hierbij betrokken voelen. Zij zijn verantwoordelijk voor de toerusting van medewerkers t.a.v. het hanteren van de spelregels, en m.b.t. informatieveiligheid en gegevensbescherming zijn zij ook (gemandateerd) verantwoordelijk voor de verwerkingsactiviteiten, informatiebeheer, informatiebeveiliging en incidentmanagement.

Uitgangspunt 3: risk- based aanpak

Bij informatiebeveiliging gaat het om organisatierisico's. Bij privacy gaat het om risico's voor personen van wie persoonsgegevens worden verwerkt. Voor beide is inzicht in de eigen informatiehuishouding vanuit informatiebeheer essentieel.

De nauwe samenhang van informatiebeheer, informatiebeveiliging en gegevensbescherming volgt ook uit de privacywetgeving. Daarin is bepaald dat de organisatie passende technische en organisatorische maatregelen dient te treffen en te onderhouden om een op het risico afgestemd beveiligingsniveau te waarborgen. Daarbij dient onzekerheid te worden ingecalculeerd. Risicomanagement is een onderdeel van de besluitvorming, is een proces en kost uren en geld. De hierin gekozen aanpak is risk-based dat wil zeggen dat besluiten nemen (waaronder risico acceptatie) en monitoring op teamniveau door de teamleider gebeurt en bij teamoverschrijdende of organisatiebrede besluiten, dit door het directieteam gebeurt.

Uitgangspunt 4: integrale aanpak
Informatiebeheer, informatiebeveiliging en gegevensbescherming treffen elkaar op drie punten: de onderlinge verbondenheid, 'de omgang met gegevens' en een op risico's gebaseerde aanpak. Tegelijk zijn ze op dezelfde leidinggevenden en medewerkers gericht en kennen dezelfde organisatorische vraagstukken, zoals prioriteren en keuzes maken. Dit vraagt om een integrale aanpak in beleid en uitvoering. Niet alleen intern maar ook in de (keten)samenwerking.

Uitgangspunt 5: leren en ervaren
De aanpak en realisatie van informatiebeveiliging en gegevensbescherming i.c.m. informatiebeheer wordt niet eenmalig verbeterd en geoptimaliseerd maar gebeurt vanuit een continu proces van leren, ervaren en equiperen, ruimte die vanuit goed werkgeverschap aan alle medewerkers wordt geboden. Daartoe worden interne bronnen ingezet (zoals inzicht in de eigen informatiehuis-houding, de analyse van incidenten, datalekken, klachten en vragen, interne audits en (zelf)valuaties), maar ook externe bronnen (zoals het dreigingsbeeld informatiebeveiliging Nederlandse gemeenten en de focusgebieden Autoriteit Persoonsgegevens 2020 – 2023) en worden relevante ontwikkelingen gevolgd.

Uitgangspunt 6: maatwerk per domein
Zowel de aanpak en realisatie van privacy, informatiebeveiliging en gegevensbescherming i.c.m. informatiebeheer verschilt per domein. Ter illustratie: daar waar gemeente breed geldt dat zorgvuldig en veilig moet worden omgegaan met persoonsgegevens is de context waarbinnen dat dient te gebeuren binnen het sociaal domein veel complexer dan binnen het fysiek domein, terwijl soms ook 'spontaan' ideeën, initiatieven en projecten ontstaan waar persoonsgegevens in verwerkt moeten gaan worden, terwijl niet direct aan de spelregels wordt gedacht. In dat verband zullen onderwerpen als noodzakelijke kennis en kunde en te hanteren uitvoeringskaders in het werk, per domein verschillen en een andere aanpak vragen.

Uitgangspunt 7: één loket gedachte
De invulling van de verantwoordelijkheid voor informatiebeveiliging, gegevensbescherming en informatiebeheer van de team- en programmaleiders is, gezien de overige uitgangspunten, geen sinecure. Leidinggevenden moeten in het kader van uitgangspunt 2 weten waar ze verantwoordelijk voor zijn om aan de uitgangspunten 3 en 4, risk-based respectievelijk integrale aanpak invulling te kunnen geven. Daar hoort wellicht een aanpak bij vanuit een hulpstructuur die indachtig uitgangspunt 4 en 6 werkt vanuit een integrale aanpak respectievelijk op basis van maatwerk. Om te voorkomen dat hierdoor een leidinggevende met verschillende experts aan tafel komt te zitten is het uitgangspunt dat daarbij de één-loket-gedachte nagestreefd wordt. Dus 1 expert/adviseur op 1 team-/programmaleider. Hierdoor ontstaat er een brede borging binnen de organisatie en dit biedt de mogelijkheid voor het inrichten van eerste en tweedelijns hulp. Erg belangrijk is dat team- & programmaleiders bevraagd worden op hun specifieke behoeftestelling en de hulpstructuur in nauw overleg wordt gevormd en samengesteld, eveneens in overleg en afstemming met het directieteam.

3 Beleidsthema's

De realisatie van organisatievisie en -doelstellingen vindt tussen 2021-2024 plaats o.b.v. de geformuleerde uitgangspunten en a.d.h.v. de volgende strategische beleidsthema's:

1. verantwoordelijkheden en eigenaarschap (w.o. governance);
2. hulpstructuur en relevante ontwikkelingen;
3. informatiehuishouding, processen kennen en transparantie;
4. awareness en kennis;
5. rechten van betrokkenen;
6. toegang tot gegevens en tot de informatievoorziening;
7. betrouwbare informatievoorziening en continuïteit van de bedrijfsvoering;
8. incidenten en datalekken (w.o. aandachtspunten, preventie en repressie);
9. nieuwe verwerkingen;
10. verantwoording en naleving (zowel t.a.v. privacy, informatiebeveiliging en informatiebeheer: dit laatste punt waar het om het voldoen aan de regels m.b.t. de duurzame toegankelijkheid van overheidsinformatie gaat).

De beleidsthema's zijn hierna op hoofdlijnen gegeven en zullen in de vorm van tactische jaarplannen nader uitgewerkt worden zodat ze door de leidinggevenden geoperationaliseerd kunnen worden aan de hand van concrete actiepunten.

1. Verantwoordelijkheden en eigenaarschap
Leidinggevenden kennen hun verantwoordelijk waar het gaat om gegevensbescherming, informatieveiligheid en informatiebeheer, gekoppeld aan hun taak- en werkveld. Daarbij is de directie eindverantwoordelijk en hebben de medewerkers in het werk t.a.v. de genoemde punten hun eigen verantwoordelijkheid. Zowel het directieteam als de team- en programmaleiders geven duidelijk richting aan informatiebeveiliging en gegevensbescherming en laten zichtbaar zien dat zij dit ondersteunen en zich hierbij betrokken voelen. Zij zijn verantwoordelijk voor de toerusting van medewerkers t.a.v. het hanteren van de spelregels, en m.b.t. informatieveiligheid en gegevensbescherming zijn zij ook (gemandateerd) verantwoordelijk voor de verwerkingsactiviteiten, informatiebeheer, informatiebeveiliging en incidentmanagement.

Beschreven is wie welke rol, taak en bevoegdheid heeft t.a.v. de genoemde onderwerpen (governance) alsmede de besturings- en rapportagecyclus die daarbij wordt gehanteerd. Risk-based besturen en inbedding van comply or explain is daarbij de basis.

2. Hulpstructuur en relevante ontwikkelingen
Ter ondersteuning van de directie en de team- en programmaleiders waar het gaat om de invulling en uitvoering van hun verantwoordelijkheden, is een hulpstructuur ingericht met expertise op het gebied van privacy, informatiebeveiliging en informatiebeheer. Deze hulpstructuur biedt eerste- en tweedelijns ondersteuning en houdt zicht op relevante wijzigingen en ontwikkelingen t.a.v. privacy en gegevensbescherming zoals die voort kunnen komen uit jurisprudentie, sectorale aanwijzingen en verkregen inzichten.

De bedoelde ontwikkelingen en wijzigingen worden wanneer dat van belang is, doorgevoerd in het beleid en de uitvoeringskaders maar kunnen ook een onderdeel zijn van (initiële) opleidingen en instructies.

3. Informatiehuishouding, processen kennen en transparantie
De gemeente beschikt over een register van verwerkingsactiviteiten aan de hand waarvan proceseigenaren vanuit hun verantwoordelijkheid op dit punt, invulling en inhoud kunnen geven aan het vereiste dat de verwerkingen die plaatsvinden, inzichtelijk en gedocumenteerd zijn. Het register is dusdanig ingericht en onderhouden dat het een belangrijk instrument en een belangrijke bron is waar het om informatiemanagement gaat.

In uitingen is de gemeente transparant waar het bijvoorbeeld gaat om de verwerkingsdoelen, welke persoonsgegevens daarbij gehanteerd worden, op basis van welke wettelijke grondslag de organisatie dat doet, met wie persoonsgegevens worden gedeeld en welke bewaartermijnen worden gehanteerd.

4. Awareness en kennis
In het kader van het nemen en onderhouden van passende technische en organisatorische maatregelen m.b.t. de gegevensbescherming en privacy, hanteert en onderhoudt elke leidinggevende de bewustwording en de kennis van hun medewerkers, specifiek waar het gaat om informatieveiligheid en hun verantwoordelijkheid in de omgang met persoonsgegevens. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

5. Rechten van betrokkenen
De gemeente heeft haar processen ingericht op het in ontvangst nemen en compliant afhandelen van verzoeken i.v.m. de rechten die betrokkenen hebben. De resultaten van de processen zijn input voor de besturings- en daar waar van toepassing, beleidscyclus.

6. Toegang tot gegevens en tot de informatievoorziening
In het kader van het nemen en onderhouden van passende technische en organisatorische maatregelen m.b.t. gegevensbeheer, privacy en informatiebeveiliging, hanteert en onderhoudt de gemeente specifieke oplossingen en toepassingen om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en daar waar nodig, aan te pakken.

7. Betrouwbare informatievoorziening en continuïteit van de bedrijfsvoering
In het kader van het nemen en onderhouden van passende technische en organisatorische maatregelen m.b.t. privacy, informatiebeveiliging en informatiebeheer, hanteert en onderhoudt de gemeente specifieke oplossingen en toepassingen voor de borging van de beschikbaarheid van gegevens, de informatievoorziening en daarmee de dienstverlening eveneens in geval van incidenten en calamiteiten.

Waar in de verwerkingsketens van de organisatie sprake is van het inzetten van derde partijen of samenwerking met ketenpartners, wordt vooraf zoveel mogelijk ingeschat welke risico's dat met zich

meebrengt t.a.v. privacy, informatiebeveiliging en informatiebeheer. O.b.v. de uitkomsten worden mitigerende maatregelen overeengekomen. Met derden die specifiek en in opdracht van de gemeente persoonsgegevens verwerken worden verwerkersovereenkomsten gesloten en met ketenpartners worden afspraken gemaakt welke partij waarvoor verantwoordelijk is.

8. Incidenten en datalekken
De gemeente onderhoudt een procedure resp. protocol en bijbehorende processen ter identificatie van, melding en opvolging bij incidenten en bij inbreuken m.b.t. privacy en de bescherming van gegevens. Daar waar van toepassing zijn proces(onderdelen) via communicatie, awareness sessies, trainingen/opleidingen bekend gemaakt bij de leidinggevenden en de medewerkers. Waar zij verwerkingsverantwoordelijke is meldt de gemeente in de gevallen waar dat wettelijk is voorgeschreven en conform de daartoe vastgestelde procedure, een inbreuk bij de Autoriteit Persoonsgegevens (AP) en/of andere relevante toezichthouders of stakeholders. De organisatie documenteert de inbreuken. Waar dat is voorgeschreven doet zij de betrokkene van de inbreuk een mededeling conform de daartoe vastgestelde procedure. Op inbreuken wordt adequaat gereageerd door de gemeente: ze worden geanalyseerd, beoordeeld, opgevolgd en afgehandeld. Tevens worden ze (achteraf) geanalyseerd op leer- en verbeterpunten die vervolgens geïmplementeerd worden in de werkwijze van de organisatie.

9. Nieuwe verwerkingen
De gemeente heeft haar processen zodanig ingericht dat bij het ontwikkelen en wijzigen van werkprocessen en procedures alsmede bij de aanschaf of wijziging van systemen en toepassingen een compliance check wordt gedaan en de principes van privacy by design/default worden toegepast. Gestart wordt met de vraag of sprake is van nieuwe verwerkingen voor nieuwe doeleinden of van verwerkingen van persoonsgegevens die verenigbaar zijn met al bestaande, gedefinieerde doeleinden (verenigbaar gebruik). Daarbij wordt altijd nagegaan of mogelijk sprake is van een voor betrokkene en vanuit privacy oogpunt gezien, risicovolle verwerking waarvoor een DPIA moet worden uitgevoerd. De genoemde processen zijn vaste onderdelen van het project-, programmamanagement, inkoop-, verwerkings- of voortbrengingsproces.

10. Verantwoording en naleving
Op regelmatige basis voert de Functionaris Gegevensbescherming (FG) een AVG compliance check uit op basis van verschillende bestaande informatiebronnen en doet tussentijdse beoordelingen van de wijze waarop de verwerking van persoonsgegevens binnen de organisatie plaatsvindt. De Chief Information Security Officer (CISO) doet dat t.a.v. informatiebeveiligingsaspecten. Hierover vindt integrale rapportage plaats naar leidinggevende, de directie en het bestuur. Over de frequentie van de uit te voeren checks door de FG en de CISO zijn afspraken gemaakt om zo de uitkomsten op een effectieve wijze input te laten zijn voor de besturings- en beleidscyclus.

Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van Steenwijkerland van 7 december 2021.

Burgemeester en wethouders van Steenwijkerland,
de secretaris,
Judith de Groot

de burgemeester,
Rob Bats