GEMEENTE Nunspeet

GEMEENTEBLAD

Officiële uitgave van de gemeente Nunspeet

Nr. 101255

1 april 2021

Privacybeleidskader Gemeente Nunspeet 2020-2024

Burgemeester en wethouders van Nunspeet;
gelezen het voorstel van 21 december 2020, kenmerk 0302102101;
besluiten vast te stellen de volgende beleidsregels:

Strategisch Gemeentelijk Informatiebeveiligingsbeleid Nunspeet 2021 tot 2024

Inhoud

1. Kernpunten
1.1. Voor wie?
1.2. Doel
1.3. Visie
1.4. Kernpunten
1.5. Scope
1.6. Raakvlakken en overlap met andere beleidsthema's
1.6.1. Integriteitsbeleid
1.6.2. Kwaliteitsbeleid
1.6.3. Continuïteit- en risicomanagement
1.6.4. Informatiebeveiliging
1.6.5. Personeel en organisatie
1.6.6. Communicatie
2. Privacymanagement
2.1. Managementstructuur
2.2. Proceseigenaarschap
2.3. Privacy officer
2.4. Toezicht
3. Privacybeleid Gemeente Nunspeet
3.1. Algemeen
3.2. Noodzakelijke gegevensverwerking
3.3. Risicogedreven aanpak
3.4. Uitwerking per thema's
3.5. Inachtneming bijzondere wettelijke voorschriften
4. Gedragsnorm voor proceseigenaren
4.1. Procesplan-aanpak
4.2. Lijst van key controls
4.3. FG-verklaring
4.4. Artikel 30-formulieren
4.5. Beheer procesplan
5. Privacyservices
5.1. Rechten
5.2. Vragen
5.3. Klachten
5.4. Beroep
6. Privacyprogramma
6.1. Werkprogramma
6.2. Bewustwording en training
6.3. PR & communicatie
6.4. Verdere verwerking, archiefbeleid, gegevensvernietiging
6.5. Informatiebeveiliging
6.6. Regeling privacyincidenten
6.7. Handhaving
6.8. Beleidsevaluatie
7. Auditbeleid

Definities

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

Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.
FG (Functionaris voor Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften.
(Gegevens)verwerking – zowel geheel als 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).
DPIA (data protection impact assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacy-optiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen).
DPIA-score – getalsmatige classificatie van noodzaak of risico van gegevensverwerking, als uitkomst van een DPIA.
PIT – het privacy- en informatiebeveiligingsteam dat de directie en proceseigenaren ondersteunt.
Portefeuillehouder privacy – het lid van het college van B&W die het onderwerp in portefeuille heeft.
Privacybeleidskader – het bestuurlijk privacybeleid van een organisatie, die de kapstok vormt.
Privacyaudit – controles op de naleving van privacybeleid en privacywetgeving.
Privacybeleid – het privacybeleidskader en alle nadere uitwerkingen hiervan.
Privacybeleidsvoering– sturing op privacy door het management ('governance').
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 en veiligheid.
Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen per proces voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een DPIA).
Privacycoördinator – degene die namens de algemeen directeur uitvoering geeft aan het privacybeleid.
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.
Verwerking – elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.'

1. Kernpunten

1.1. Voor wie?
Het Privacybeleidskader van Gemeente Nunspeet bevat managementafspraken tussen het college en de afdelingshoofden/teamleiders (hierna: "Proceseigenaar" of in geval van meervoud: "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 van Gemeente Nunspeet is om te waarborgen dat Gemeente Nunspeet de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3. Visie
Gemeente Nunspeet ziet het belang van juiste, tijdige en zorgvuldige gegevensverwerking om te kunnen voldoen aan de aan haar opgedragen taken. Bij de uitvoering van die taken houdt zij rekening met de belangen van de inwoners, de medewerkers en van ieder ander persoon waarvan zij gegevens verwerkt en voert de werkzaamheden binnen de kaders van de wet uit. De wijze waarop de gemeente daar invulling aan geeft is verder uitgewerkt in dit beleid.

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 persoonsgegevens 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 de goede uitvoering van werkzaamheden;
h. Een proceseigenaar handelt in samenspraak met de privacy officer vragen of klachten van inwoners of medewerkers binnen een maand af;
i. Bij privacyincidenten hanteert de proceseigenaar met advies van de privacy officer het protocol behandelen 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 Nunspeet beschikt over mechanismes voor (privacy)-incidentmanagement.
5. Gemeente Nunspeet evalueert driejaarlijks 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 Nunspeet heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de borging van privacy in de gemeenteorganisatie.

1.5. Scope

Het Privacybeleidskader van Gemeente Nunspeet is van toepassing op alle bedrijfsvoering van Gemeente Nunspeet voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft. Dit beleid treedt in de plaats van het Privacybeleid gemeente Nunspeet dat in 2018 is vastgesteld.
Het Privacybeleidskader van Gemeente Nunspeet is het algemene deel van het privacybeleid binnen de gemeente. Het algemene beleidskader is de kapstok voor het privacybeleid van Gemeente Nunspeet, waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten.
Het privacybeleid Gemeente Nunspeet omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil.
Het privacybeleid van Gemeente Nunspeet is van toepassing op processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor Gemeente Nunspeet informatiediensten verricht.
Het privacybeleid van Gemeente Nunspeet 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 Nunspeet heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

1.6.1. Integriteitsbeleid

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

1.6.2. 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').

1.6.3. 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).

1.6.4. 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.

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

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

2. Privacymanagement

Het college van Gemeente Nunspeet 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.
Privacymanagement is SMART-georganiseerd en heeft zelfstandige aandacht binnen de voortgangscyclus 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.
De directie houdt in opdracht van het college 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.
Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen (zie paragraaf 2.4)
Het college geeft de directie opdracht om te voorzien in een team van professionals (hierna het P&I-team, kortweg: PIT) die onder de verantwoordelijkheid valt van de directie. Het PIT ondersteunt proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleid. Het PIT wordt samengesteld uit professionals op het gebied van bijvoorbeeld (privacy-)juridische zaken, informatiebeveiliging, informatiemanagement, audit en communicatie. Het doel van het team is om het vliegwiel van de verbetercycli die horen bij informatiebeveiliging en privacy op gang te krijgen en te houden.
Proceseigenaren zijn op uitvoeringsniveau verantwoordelijk voor privacybestendige bedrijfsvoering en gegevensuitwisseling met derden. Zij leggen hierover middels de voortgangsrapportage verantwoording af aan de directie, het college en de raad.

2.2. Proceseigenaarschap
De afdelingshoofden en teamleiders zijn ervoor verantwoordelijk dat de gemeentelijke taakuitoefening waarvoor zij verantwoordelijk gesteld zijn, binnen de grenzen van dit privacybeleidskader plaatsvindt en rapporteren via de voortgangsrapportages aan de directie, het college en de raad.
- Een afdelingshoofd/teamleider is proceseigenaar (hierna: "proceseigenaar" of in geval van meervoud: "proceseigenaren").
- 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 paragraaf 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 pro-actief toezicht op de privacybestendige organisatie van zijn proces en documenteert keuzes, bijbehorende afwegingen 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/teamleiders vallen, is de gemeentesecretaris de proceseigenaar.

2.3. Privacy officer

1. De privacy officer ontwikkelt en bewaakt het privacybeleid. Daarnaast geeft hij advies aan de proceseigenaren over een privacybestendige uitvoering van de processen. In hoofdlijnen voert hij de volgende taken uit:
2. Ondersteunen bij privacy-analyses waaronder het aanwijzen van passende beheersmaatregelen;
3. Ontwikkelen van toegepast privacybeleid en -procedures;
4. Inschakelen van deskundigen (intern/extern);
5. Stimuleren van bewustwording en training van medewerkers van de Gemeente Nunspeet;
6. Voeren van incidentmanagement met betrekking tot datagerelateerde incidenten;
7. Opstellen van een werkprogramma/ jaarplan met betrekking tot privacy;
8. Monitoren en rapporteren over de uitvoering van het beleid en het werkprogramma;
9. Evalueren van het privacybeleidskader en doen van aanbevelingen over wijzigingen ten aanzien daarvan aan het college.

2.4. Toezicht

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van Gemeente Nunspeet 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 Nunspeet 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;
- ziet toe op het beheer door de directie van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door Gemeente Nunspeet en ketenpartners, eventueel ook in samenwerking met auditors;
- 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 Nunspeet 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 op basis van de uitoefening van zijn taken.

Vanwege zijn expertise van wetgeving en de praktijk, geldt een advies van de FG als zwaarwegend en de geëigende wijze voor naleving van privacywetgeving door Gemeente Nunspeet. Voor zover het voorkomt dat het advies van de FG afwijkt van de zienswijze van een landelijke toezichthouder en de FG beroepshalve aan zijn advies moet vasthouden, krijgt de FG de ruimte en de vrijheid om samen met de AP tot een vergelijk te komen.
De FG doet jaarlijks verslag van zijn werkzaamheden aan het college. De raad wordt via de begrotingscyclus geïnformeerd.

3. Privacybeleid Gemeente Nunspeet

3.1. Algemeen
Gemeente Nunspeet is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:
- voert Gemeente Nunspeet proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert Gemeente Nunspeet de uitoefening van rechten van personen;
- bewaakt Gemeente Nunspeet de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

3.2. Noodzakelijke gegevensverwerking
Proceseigenaren verwerken persoonsgegevens voor zover dit noodzakelijk is voor het realiseren van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde publieke taken, de nakoming van wettelijke of contractuele verplichtingen, vrijwaring van vitale belangen voor de betrokkene(n), totstandkoming of uitvoering van een overeenkomst waarbij een burger partij is of de behartiging van een gerechtvaardigd belang van Gemeente Nunspeet of een derde aan wie gegevens worden verstrekt, tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert en voor zover het gerechtvaardigd belang geen grondslag voor de uitoefening van een publieke taak vormt.

3.3. Risicogedreven aanpak
De privacybeleidsvoering van Gemeente Nunspeet is erop gericht dat aantoonbaar is voorzien in passende organisatorische en technische maatregelen voor doeltreffende bescherming van persoonsgegevens en de bescherming van rechten van personen. Wat ‘passend’ is, hangt af van de concrete risico’s die de verwerking van persoonsgegevens voor mens en bedrijf met zich meebrengt zónder te hebben voorzien in doeltreffende beschermingsmaatregelen.

3.4. Uitwerking per thema’s
Het Privacybeleidskader van Gemeente Nunspeet 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 Nunspeet.
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 Nunspeet onderscheiden:
- Burgerzaken
- Gemeentelijke belastingheffing
- Gemeentelijke organisatie
- Economische zaken
- Jeugd
- Maatschappelijke opvang
- Onderwijs
- Sport, cultuur, recreatie en openbaar groen
- Veiligheid en openbare orde
- Verkeer, vervoer en waterstaat
- Volksgezondheid en milieu
- Volkshuisvesting, Ruimtelijke ordening en stedelijke vernieuwing
- Werk en inkomen
- WMO

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat. (zie paragraaf 4.1)
Het Privacybeleidskader Gemeente Nunspeet bevat ook de aanzet voor het regelen van aspecten van privacybeleidsvoering die onder de directe verantwoordelijkheid van de verschillende bestuursorganen van de gemeente vallen.
Het Privacybeleidskader Gemeente Nunspeet , themabeleid, procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid Gemeente Nunspeet . In geval van tegenstrijdigheid heeft het Privacybeleidskader Gemeente Nunspeet voorrang.

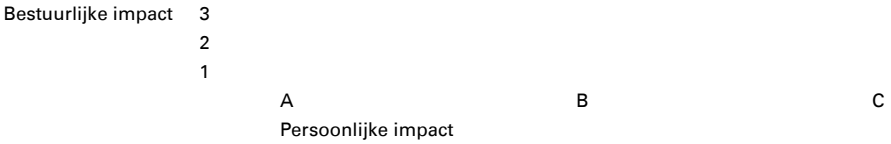
3.5. Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader Gemeente Nunspeet, 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, Telecommunicatiewet, Participatiewet, Jeugdwet en Wet maatschappelijke ondersteuning enzovoort. Dit alles gericht op een evenwichtige toepassing van de AVG in relatie met de specifieke wetgeving.

4. Gedragsnorm voor proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor, indien daarom verzocht, rekenen op support door het PIT en advies van de FG. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen Gemeente Nunspeet 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 (zie paragraaf 4.1).
De directie houdt een register van gegevensverwerkingen conform artikel 30 AVG (zie paragraaf 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, de directie 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 data protection impact assessments (DPIA's) ten grondslag. DPIA'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 DPIA, zoals verwoord in het DPIA-rapport.
Voor eenduidig begrip hanteert Gemeente Nunspeet een systeem van positieve en negatieve DPIA-scores. Hoe hoger de DPIA-score, hoe robuuster de beheersmaatregelen (privacywaarborgen). Proceseigenaren volgen het advies van het PIT bij de vaststelling van hun DPIA-score. DPIA-scores worden bepaald aan de hand van de hiernaast afgebeelde matrix.
Proceseigenaren zijn goed bekend met hun DPIA-scores en hanteren onderstaande tabel om te bepalen in hoeverre DPIA's tevens deel uitmaken van het procesplan om op die manier de keuzes voor beheersmaatregelen te verantwoorden.

DPIA-score	DPIA-rapport	Procesplan	Akkoord FG
A1	-	-	-
A2	Beknopt	DPIA-rapport maat deel uit van procesplan	Aanbevolen

A3	Volledig	DPIA-rapport maat deel uit van procesplan	Verplicht
B1	Beknopt	DPIA-rapport maat deel uit van procesplan	Aanbevolen
B2	Beknopt	DPIA-rapport maat deel uit van procesplan	Aanbevolen
B3	Volledig	DPIA-rapport maat deel uit van procesplan	Verplicht
C1	Volledig	DPIA-rapport maat deel uit van procesplan	Verplicht
C2	Volledig	DPIA-rapport maat deel uit van procesplan	Verplicht
C3	Volledig	DPIA-rapport maat deel uit van procesplan	Verplicht

Het DPIA-rapporten worden opgesteld conform het bepaalde in 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, opslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd.
4. Onnauwkeurige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid.
5. Onveilige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie dreigt te gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of niet beschikbaar te zijn.
6. Niet-inachtneming van bijzondere wettelijke voorschriften: bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.
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 DPIA 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 hoofdstuk 7).

DPIA-score	Key controles	Samenspraak PIT	Samenspraak FG
A1	-	-	-
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Verplicht
B1	Ja	Ja	Aanbevolen
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Verplicht
C1	Ja	Ja	Verplicht
C2	Ja	Ja	Verplicht
C3	Ja	Ja	Verplicht

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.

DPIA-score	DPIA 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

Het PIT vat het procesplan samen met behulp van 'artikel 30-formulieren' dat de proceseigenaar toevoegt aan het begin van zijn procesplan en waarvan hij een kopie verstrekt aan de Privacy Officer, die zorgdraagt voor opname van het formulier in het Artikel 30-register. Proceseigenaren melden veranderingen voor het artikel 30-register aan de hand van wijzigingsformulieren direct bij de Privacy Officer.
Artikel 30-formulier bevatten de volgende informatie:

1. Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking;
2. De DPIA-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 organisatiedoelen 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 rapporteert via de voortgangsrapportage aan de directie, het college en de raad over de privacybeleidsvoering. Het verslag omvat een stand van zaken-rapportage en verslag van eventuele klachten of andere incidenten die zich binnen hun taakgebied in het afgelopen jaar hebben voorgedaan.
De directie heeft de ruimte om aan het verslag zijn eigen visie toe te voegen op de uitvoering van taken door proceseigenaren binnen het privacybeleidskader Gemeente Nunspeet
De FG ontvangt van de directie een kopie van het verslag en andere relevante stukken gelijktijdig met de overlegging hiervan aan het college (portefeuillehouder privacy). Mede aan de hand hiervan brengt de FG jaarlijks verslag uit aan het college en adviseert hij het college over verdere optimalisering van de privacybeleidsvoering.
Het college besluit over bijstelling van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.
Hoe dan ook evalueert de proceseigenaar een procesplan periodiek en vraagt zo nodig de FG om hierbij advies uit te brengen.

DPIA-score	Evaluatie	Advies FG
A1	3 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 hebben er recht op:

- dat Gemeente Nunspeet handelt conform het onderhavige privacybeleidskader;
- dat Gemeente Nunspeet informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;

- dat zij inzage in hun eigen gegevens hebben;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat Gemeente Nunspeet verplicht tot het maken van een afweging;
- dat zij Gemeente Nunspeet bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

5.2. Vragen
Bij vragen:
- hebben personen het recht om zich te wenden tot de (digitale/telefonische) gemeentebalie;
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- op vragen die via e-mail binnenkomen wordt binnen vijf werkdagen gereageerd;
- de Privacy Officer of het PIT kan om advies over de beantwoording vragen.

5.3. Klachten
- een niet tot tevredenheid afgehandelde vraag of een directe klacht geeft personen het recht om zich opnieuw te wenden tot de gemeentebalie;
- de gemeentebalie registreert in dat geval een klacht en legt hem voor aan de klachtencommissie;
- klachten worden zo snel mogelijk maar uiterlijk binnen zes weken afgehandeld;
- bij privacygerelateerde klachten wordt de Privacy Officer om advies gevraagd;

5.4. Beroep
Na afhandeling van een klacht door de klachtencommissie kan een klager in beroep gaan. Dit beroep wordt voorgelegd aan de FG indien de klacht verband houdt met naleving van privacywetgeving en/of het Privacybeleidskader Gemeente Nunspeet.

6. Privacyprogramma

6.1. Werkprogramma
De directie 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 Nunspeet , ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen Gemeente Nunspeet , 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 Nunspeet in lijn met de geldende norm wordt georganiseerd. Gemeente Nunspeet beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die deelneemt in het PIT en samenwerkt met de portefeuillehouder privacy 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 DPIA'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 . 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, incidentmanagement en crisiscommunicatie.

6.7. Handhaving

Het college handhaaft het gemeentelijk privacybeleid op basis van een regeling voor beloning van voorbeeldig gedrag en disciplinaire maatregelen bij niet-nakoming van afspraken volgens het Privacybeleidskader Gemeente Nunspeet.

6.8. Beleidsevaluatie

Hoofdproceseigenaren doen via de voortgangsrapportage verslag aan de directie, het college en de raad over de uitvoering van het privacybeleid, de geïmplementeerde 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.

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.

DPIA-score	Type audit	Frequentie	Betrokkenheid FG	Afschrift FG
A1	Quick scan	3 jaarlijks	-	-
A2	Zelfevaluatie	3 jaarlijks	Vrijwillig	Vrijwillig
A3	Externe audit	3 jaarlijks	Ja	Ja
B1	Zelfevaluatie	3 jaarlijks	Vrijwillig	Ja
B2	Zelfevaluatie	3 jaarlijks	Ja	Ja
B3	Externe audit	3 jaarlijks	Ja	Ja
C1	Externe audit	3 jaarlijks	Ja	Ja
C2	Externe audit	3 jaarlijks	Ja	Ja
C3	Externe audit	2 jaarlijks	Ja	Ja

Aldus vastgesteld in de collegevergadering van 21 december 2020.
Burgemeester en wethouders van Nunspeet,
de secretaris, de burgemeester,
mr. A. Heijkamp B. van de Weerd