



18.13009



Burgemeester en wethouders van de gemeente Nieuwkoop,

gelezen het voorstel van 19 juni 2018 met kenmerk: 18.11504

gelet op de ter zake geldende bepalingen van de Algemene Verordening Gegevensbescherming;

Besluit:

vast te stellen het navolgende **Privacy beleidskader Gemeente Nieuwkoop**.

Aldus besloten in de vergadering van het college van 19 juni 2018

Burgemeester en wethouders van Nieuwkoop,
de secretaris, de burgemeester,

mr. G.G.G. Sloopers

F. Buijserd

23 mei 2018

Privacybeleidskader Gemeente Nieuwkoop

Algemeen deel (bestuurlijk privacybeleid)

Inhoudsopgave

Definities	3
1 Kernpunten	5
1.1 Voor wie?	5
1.2 Doel	5
1.3 Visie	5
1.4 Kernpunten	5
1.5 Scope	6
1.6 Raakvlakken en overlap met andere beleidsthema's	7
2 Borging privacy	8
2.1 Bestuursstructuur	8
2.2 Proceseigenaarschap	8
2.3 Privacycoördinator	9
2.4 Toezicht	9
3 Privacybeleid Gemeente Nieuwkoop	11
3.1 Algemeen	11
3.2 Noodzakelijke gegevensverwerking	11
3.3 Risicogedreven aanpak	11
3.4 Kapstokregeling	11
3.5 Inachtneming bijzondere wettelijke voorschriften	12
4 Verantwoordelijkheid van proceseigenaren	13
4.1 Procesplan	13
4.2 Artikel 30-formulieren	14
5 Privacyservices	15
5.1 Rechten	15
5.2 Vragen	15
5.3 Klachten	15
5.4 Beroep	15
5.5 Protocol Privacyservices	16
6 Privacyprogramma	17
6.1 Werkprogramma	17
6.2 Bewustwording en training	17
6.3 PR & communicatie	17
6.4 Verdere verwerking, archiefbeleid, gegevensvernietiging	17
6.5 Informatiebeveiliging	17
6.6 Regeling privacyincidenten (!)	17
6.7 Handhaving	18
6.8 Beleidsevaluatie	18
7 Auditbeleid	19

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.

(Gegevens)verwerking – 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 privacy-optiek, 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 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 PIA).

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

1 Kernpunten

1.1 Voor wie?

Het Privacybeleidskader Gemeente Nieuwkoop bevat managementrichtlijnen van het college aan 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 Nieuwkoop is om te waarborgen dat de gemeente Nieuwkoop de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie

Iedereen heeft recht op privacy. Gemeente Nieuwkoop draagt zorg voor de vertrouwelijke behandeling van privacygevoelige gegevens van medewerkers, bezoekers en inwoners. Mensen mogen erop vertrouwen dat Gemeente Nieuwkoop persoonsgegevens volgens de wet, behoorlijk, correct, terughoudend, veilig en op een transparante wijze verwerkt. Binnen de drie kernwaarden van Nieuwkoop (dichtbij, doelgericht en lef) levert gemeente Nieuwkoop dienstverlening met een persoonlijke benadering. Het college van B&W stuurt actief op privacy en ziet erop toe dat de privacywetgeving door alle medewerkers wordt nageleefd. Bij dilemma's of kwesties gaat Gemeente Nieuwkoop de dialoog aan en zoekt samen met betrokkenen naar oplossingen.

1.4 Kernpunten

In deze alinea wordt de kern van het beleidskader uiteengezet. Deze kernpunten zullen in het beleidskader verder toegelicht worden.

- 1) Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren sturen op privacy volgens deze kernpunten van privacymanagement:
 - a) Het belang van personen is leidend. De bescherming van persoonsgegevens vindt op evenwichtige wijze plaats, waarbij alle relevante aspecten zijn gewogen op een manier dat daarover verantwoording kan worden afgelegd;
 - b) Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toezicht op zijn proces(sen) op basis van dit privacybeleidskader;
 - c) Bij processen waaraan privacyrisico's zijn verbonden, hanteert de proceseigenaar een procesplan;
 - d) Een procesplan is duidelijk, actueel, stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd;
 - e) Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
 - f) Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt;
 - g) Een procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering;
 - h) Een procesplan omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden;

- i) Een proceseigenaar handelt privacyrechten van inwoners of medewerkers binnen vier weken af.
 - j) Bij privacyincidenten hanteert een proceseigenaar de procedure Melding datalekken;
 - k) 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. (algemeen directeur/gemeentesecretaris)
 - 3) Het college voorziet in faciliteiten voor bewustwording en training.
 - 4) De gemeente Nieuwkoop beschikt over mechanismes voor privacy-incidentmanagement.
 - 5) De gemeente Nieuwkoop evalueert vierjaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader. Dit valt binnen de gebruikelijke evaluatiecyclus van de gemeente Nieuwkoop.
 - 6) Het college informeert de raad over de privacybeleidsvoering.
 - 7) Het college handhaaft het privacybeleid.
 - 8) De gemeente Nieuwkoop heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de naleving van privacywetgeving.

1.5 Scope

- Het Privacybeleidskader Gemeente Nieuwkoop is van toepassing op alle bedrijfsvoering van Gemeente Nieuwkoop voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.
- Het Privacybeleidskader Gemeente Nieuwkoop is het algemene deel van het privacybeleid binnen de gemeente. Het algemene beleidskader is de kapstok voor het privacybeleid van de gemeente Nieuwkoop, waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten.
- Het privacybeleid van de gemeente Nieuwkoop omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil.
- Het privacybeleid van de gemeente Nieuwkoop is van toepassing op processen die de gemeente uitbesteedt, inkoop of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor de gemeente Nieuwkoop informatiediensten verricht. (verifiëren van verwerkersovereenkomsten enz.)
- Het privacybeleid van de gemeente Nieuwkoop is van toepassing op gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders.
- Het privacybeleid van de gemeente Nieuwkoop 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 van de gemeente Nieuwkoop 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 van de gemeente Nieuwkoop is van toepassing op informatieveiligheidsproblemen.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van de gemeente Nieuwkoop 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 een randvoorwaarde 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.

Communicatie

Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatiebeleid.

2 Borging privacy

Het college van de gemeente Nieuwkoop 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 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 Bestuursstructuur

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

Privacy valt onder de verantwoordelijkheid van het college. Binnen het college is een portefeuillehouder privacy aangewezen.

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen (zie §2.4).

Het college geeft de gemeentesecretaris opdracht om te voorzien in een team van professionals (hierna het Privacy & Informatie-team, kortweg: PIT). Het PIT ondersteunt proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleid. Het PIT wordt samengesteld met 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.

De bestuurlijk opdrachtgever is het college. Het ambtelijk opdrachtgeverschap is belegd bij de gemeentesecretaris. Het PIT ondersteunt proceseigenaren (zie §2.2) bij de uitvoering van het gemeentelijk privacybeleid.

Afdelingsmanagers zijn operationeel eindverantwoordelijk voor de uitvoering van gemeentelijke taken.

2.2 Proceseigenaarschap

Afdelingsmanager 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 gemeentesecretaris.

- Een afdelingsmanager is **proceseigenaar**.
- De proceseigenaar kan verantwoordelijkheden mandateren aan een teamleider ('sub-proces-eigenaren')

Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen (zie §4) 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 verantwoordelijkheden opdragen aan teamleiders binnen de gemeente. Bij mandatering blijft de opdrachtgevende proceseigenaar verantwoordelijk voor de privacybestendigheid van de aanpak door de proceseigenaar.

Een proceseigenaar kan procesverantwoordelijkheid ook 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 teamleiders vallen, is de proceseigenaar verantwoordelijk. De gemeentesecretaris kan ook een proceseigenaar aanwijzen voor het gezamenlijke deel van de gegevensverwerking.

2.3 Privacycoördinator

De privacycoördinator ontwikkelt en bewaakt het privacybeleid. Daarnaast geeft hij samen met het PIT advies aan de proceseigenaren over een privacybestendige uitvoering van de processen. In hoofdlijnen voert hij de volgende taken uit:

- 1) Ondersteunen bij privacy-analyses waaronder het aanwijzen van passende beheersmaatregelen;
- 2) Ontwikkelen van toegepast privacybeleid en -procedures;
- 3) Inschakelen van deskundigen (intern/extern);
- 4) Stimuleren van bewustwording en training van medewerkers van de gemeente Nieuwkoop ;
- 5) Voeren van incidentmanagement met betrekking tot datagerelateerde incidenten;
- 6) Opstellen van een werkprogramma/ jaarplan met betrekking tot privacy;
- 7) Monitoren en rapporteren over de uitvoering van het beleid en het werkprogramma;
- 8) 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 de gemeente Nieuwkoop op de naleving van privacywetgeving conform artikel 37-39 AVG.

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

De FG wordt aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van ethiek, 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 de gemeente Nieuwkoop 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 (conform het protocol) tot een goed einde te brengen (ombudsfunctie): waarborgen het recht om toegang.
- adviseert bij privacyincidenten over ernst en omvang
- ziet toe op het register van verwerkingen conform artikel 30 AVG
- controleert de naleving van afspraken door de gemeente Nieuwkoop en haar ketenpartners, eventueel ook in samenwerking met auditors
- helpt zo nodig 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 geïnformeerd over aspecten van de bedrijfsvoering binnen de gemeente Nieuwkoop 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 onder druk worden gezet of geïnstrueerd worden over de invulling van zijn taken. Daarnaast mag de FG niet gestraft of ontslagen worden voor het uitvoeren 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 de gemeente Nieuwkoop. 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 of anders de rechter om een beslissing te vragen.

Een stap naar de rechter doet de FG op eigen titel. De gemeente Nieuwkoop is geen partij in de procedure. De gemeente Nieuwkoop valt de FG niet af maar wacht op rechterlijke beslissing.

De FG levert binnen de planning & control-cyclus input voor het privacyonderdeel. De input betreft een overzicht van de stand van zaken.

3 Privacybeleid Gemeente Nieuwkoop

3.1 Algemeen

De gemeente Nieuwkoop is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:

- voert de gemeente Nieuwkoop proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert de gemeente Nieuwkoop de uitoefening van rechten van personen;
- bewaakt de gemeente Nieuwkoop de evenwichtige nakoming van wet- en regelgeving op het gebied van privacybescherming.
- optimaliseert de gemeente Nieuwkoop het privacybeleid op basis van voortdurende monitoring en evaluaties.

3.2 Noodzakelijke gegevensverwerking

Proceseigenaren verwerken persoonsgegevens voor zover dit noodzakelijk is voor het realiseren van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen (met inbegrip van innovatie), de nakoming van wettelijke of contractuele verplichtingen of ter bescherming van de veiligheid, gezondheid en/of het welzijn van personen.

3.3 Risicogedreven aanpak

De privacybeleidsvoering van de gemeente Nieuwkoop is erop gericht dat binnen de gemeente Nieuwkoop aantoonbaar is voorzien in passende organisatorische en technische maatregelen voor doeltreffende bescherming van persoonsgegevens en de rechten van personen. Wat 'passend' is, hangt af van de concrete risico's die de verwerking van persoonsgegevens voor mens en gemeente met zich meebrengen zónder te hebben voorzien in doeltreffende beschermingsmaatregelen.

3.4 Kapstokregeling

Het Privacybeleidskader Gemeente Nieuwkoop 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 Nieuwkoop, 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 zes programma's worden binnen de gemeente Nieuwkoop onderscheiden:

- Ruimtelijke ontwikkeling
- Ruimtelijk beheer
- Sociaal domein
- Bestuur en dienstverlening
- Bedrijfsvoering
- Algemene dekkingsmiddelen

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacy-waarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat (zie §4.1)

Het Privacybeleidskader Gemeente Nieuwkoop, de procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid van de gemeente Nieuwkoop. Het Privacybeleidskader Gemeente Nieuwkoop is daarbij leidend.

3.5 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader Gemeente Nieuwkoop geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming. Voor zover van toepassing houden proceseigenaren tevens rekening met bijzondere wettelijke voorschriften – met name privacyrelevante bepalingen in de Wet basisregistratie personen, Telecommunicatiewet, Participatiewet, Jeugdwet en Wet maatschappelijke ondersteuning. Dit alles gericht op een evenwichtige toepassing van de AVG in relatie met de specifieke wetgeving.

4 Verantwoordelijkheid van proceseigenaren

Van proceseigenaren wordt verwacht dat 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 de gemeente Nieuwkoop 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 §4.1).

De algemeen directeur houdt een 'artikel 30-register' (zie §4.2) bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het college vallen. Proceseigenaren hebben de opdracht om het register volledig en actueel te laten en gebruiken daar de 'artikel 30-formulieren' voor.

De algemeen directeur 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.

De algemeen directeur 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

Proceseigenaren stellen procesplannen op die voortbouwen op de uitkomsten uit de risico- en belangenanalyses. De belangrijkste componenten van een procesplan zijn:

1. Risicoanalyse (eventueel in de vorm van PIA) bestaande uit:
 - a) Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden
 - b) Een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden
 - c) Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
 - d) De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van de persoonsgegevens te garanderen en om aan te tonen dat aan de privacywetgeving is voldaan.
2. Key controls (zie §4.2)
3. Verwerkersovereenkomsten
4. Afschrift van artikel 30-register (zie §4.2)
5. (eventuele) FG-verklaring

4.1.1 Beheer

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.

4.2 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 via de gemeentesecretaris een kopie verstrekt aan de privacycoördinator, 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 privacycoördinator.

Artikel 30-formulieren 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.

De gemeentesecretaris heeft de ruimte om aan de verslagen zijn eigen visie toe te voegen op de uitvoering van taken door proceseigenaren binnen het privacybeleidskader Gemeente Nieuwkoop.

De FG ontvangt van de gemeentesecretaris een kopie van alle verslagen en de visie die hij hier eventueel aan heeft toegevoegd. Mede aan de hand hiervan brengt hij 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.

5 Privacyservices

5.1 Rechten

Personen hebben er onder meer recht op:

- dat de gemeente Nieuwkoop conform het onderhavige privacybeleidskader handelt;
- dat de gemeente Nieuwkoop de contactgegevens van de FG bekend maakt;
- dat de gemeente Nieuwkoop 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) rectificeren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat de gemeente Nieuwkoop verplicht tot het maken van een afweging;
- dat zij de gemeente Nieuwkoop 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 hiervoor aangewezen contactpersonen en/of servicepunten;
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- het PIT adviseert desgevraagd over de beantwoording;
- bij een niet tot tevredenheid afgehandelde vraag kunnen personen een beroep doen op de gemeentelijke klachtenprocedure.

5.3 Klachten

Bij klachten:

- hebben/heeft de betrokkene(n) het recht om zich te wenden tot hiervoor aangewezen servicepunten;
- klachten worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- het servicepunt meldt de klacht bij het PIT. Het PIT betreft voor de feitelijke klachtafhandeling een incidentenprocedure of -voorschrift;
- 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 de gemeente Nieuwkoop;
- 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 5.3, hiertegen in beroep gaan bij de FG voor zover het beroep gericht is op de naleving van privacywetgeving en/of het privacybeleid van de gemeente Nieuwkoop.

5.5 Protocol Privacyservices

De punten uit §5.1 t/m 5.4 zijn nader uitgewerkt in het Protocol Privacyservices. Daar waar sprake is van een uitoefening van rechten volgens hoofdstuk III AVG, dient bovendien rekening te worden gehouden met de **wettelijke behandelingstermijn van één maand**. Het protocol beschrijft de stappen voor soepele afhandeling van vragen, verzoeken of klachten. Er wordt daarbij uitgegaan van een 'escalatieladder' op vier niveau's dat er op gericht is dat escalaties juist worden voorkomen.

1. Algemene informatievoorziening;
2. Afhandeling van specifieke vragen en verzoeken in eerste instantie (verzoekprocedure);
3. Afhandeling van specifieke vragen en verzoeken in tweede instantie (klachtenprocedure);
4. Afhandeling van specifieke vragen en verzoeken in derde instantie (beroepprocedure).

6 Privacyprogramma

6.1 Werkprogramma

De algemeen directeur stelt jaarlijks het werkprogramma privacy vast, mede op basis van de jaar-rapportage van de FG en de aanbevelingen die hij hierin doet. Het werkprogramma bevordert op-zet, bestaan en werking van passende waarborgen voor de bescherming van persoonsgegevens binnen de kaders van het privacybeleid van de gemeente Nieuwkoop, ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een evenwich-tige en privacybestendige bedrijfscultuur binnen de gemeente Nieuwkoop, met gebruikmaking van overige instrumenten die in deze paragraaf worden beschreven.

6.2 Bewustwording en training

De algemeen directeur bevordert samen met proceseigenaren een privacybewuste organisatiecul-tuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden.

6.3 PR & communicatie

De algemeen directeur is transparant over de privacybeleidsvoering en voert op dit thema even-wichtig communicatiebeleid waarbij proceseigenaren zo nodig voorzien in bijzondere voorlichting aan specifieke doelgroepen.

6.4 Verdere verwerking, archiefbeleid, gegevensvernietiging

De algemeen directeur voorziet samen met proceseigenaren in met passende waarborgen om-klade verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van manage-mentinformatie. Ook wordt voorzien in met passende waarborgen omklade oplossingen voor ar-chivering en adequate oplossingen voor gegevensvernietiging.

6.5 Informatiebeveiliging

De algemeen directeur ziet erop toe dat informatieveiligheid van de gemeente Nieuwkoop in lijn met de geldende norm wordt georganiseerd (Baseline Informatieveiligheid Gemeenten). De ge-meente Nieuwkoop beschikt over een gekwalificeerde coördinerende informatiebeveiliging (CISO) die deelneemt in het PIT en samenwerkt met de gemeentesecretaris en de FG.

6.6 Regeling privacyincidenten

De algemeen directeur voorziet in een procedure voor privacyincidenten¹. 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 privacyincidenten, incidentmanagement en crisiscom-municatie.

6.7 Handhaving

De algemeen directeur handhaaft het gemeentelijk privacybeleid conform de Regeling Integriteit bij niet-nakoming van afspraken volgens het Privacybeleidskader Gemeente Nieuwkoop.

6.8 Beleidsevaluatie

Proceseigenaren doen jaarlijks verslag van de uitvoering van het privacybeleid, oplossingen en incidenten die zich onder hun verantwoordelijkheid hebben voorgedaan aan de algemeen directeur met afschrift aan de FG. Dit proces wordt gecoördineerd door de privacycoördinator. 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 incidentmanagement zijn in wezen steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaagd, 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