PRIVACYBELEIDSKADER GEMEENTE EDAM-VOLENDAM

Algemeen deel (bestuurlijk privacybeleid)

Versie 1.1
4 mei 2018

Inhoudsopgave

Documentverloop

	d.d.	**versie**	**actie/wijziging**	**aanpassing**
1	8 mei 2018	1.0	DMO	
2	3 mei 2018	1.1	a.g.v. bespreking PH/I-L-GS/ afd.hfd.ID/ Coord. IV/externe/PO	diverse aanpassingen
3	22 mei 2018	1.1	B&W	

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 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 van B&W dat verantwoordelijk is voor de uitvoering en naleving van privacywetgeving met behulp van het privacybeleidskader
Privacybeleidskader – het bestuurlijk privacybeleid van een organisatie, die de kapstok vormt voor
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 – afdelingshoofden, die integraal verantwoordelijk zijn voor (overstijgende) proces en keten processen en uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen en veiligheid.
Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een PIA)
Programmanager Privacy – degene die namens de portefeuillehouder privacy 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 Edam-Volendam bevat managementafspraken tussen het college en proceseigenaren (afdelingshoofden). 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 Edam-Volendam is om te waarborgen dat gemeente Edam-Volendam de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie en missie

Gemeente Edam-Volendam ziet de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Inwoners en medewerkers moeten erop kunnen vertrouwen dat we persoonsgegevens rechtmatig, zorgvuldig en veilig verwerken. Wie voor ons werkt, begrijpt dit 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 adequaat privacybeleid. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij dilemma's met betrekking tot de verwerking van persoonsgegevens gaan wij de dialoog met betrokkenen aan en zoeken waar mogelijk gezamenlijk naar oplossingen.

Privacy gaat iedereen wat aan. Dit gaat niet alleen over elkaar maar vooral met elkaar (verbinden). Dit door zorgvuldig, bewust om te gaan met gegevensverwerking en Privacy. Het wordt vertaald naar het borgen in (primaire) processen, vastleggen in de verwerkingsregistratie en transparantie naar de burgers (vertrouwen). De AVG biedt mogelijkheden (leiderschap) zolang processen goed worden beschreven en/of beargumenteerd (wendbaar). We gaan op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen/burgers en collega's. De gemeente houdt zich hierbij aan de wettelijke uitgangspunten, maar stelt de bedoeling boven de systemen. Het borgen en uitvoeren de wettelijke taken wordt gezien als een uitdaging en niet als belemmering. We kijken naar oplossingen en mogelijkheden.

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 vier weken af;
   i) Bij privacyincidenten hanteert de proceseigenaar de procedure 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 Edam-Volendam beschikt over mechanismes voor privacy-incidentmanagement.
5) Gemeente Edam-Volendam 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. Gemeente Edam-Volendam heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de naleving van privacywetgeving.

1.5 Scope

Het Privacybeleidskader Gemeente Edam-Volendam is van toepassing op alle bedrijfsvoering van gemeente Edam-Volendam voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.

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

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

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

Het privacybeleid Gemeente Edam-Volendam 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 Edam-Volendam 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.

Besluitvorming
Alvorens een besluit door B&W wordt voorgelegd/genomen dient, waar nodig, eerst de privacy adviseur/PO/FG te worden geraadpleegd.

Informatievoorziening
Kwalitatief goede en veilige informatie is voor een organisatie van levensbelang. De juiste informatie op het juiste moment bij de juiste persoon is een uitdaging die vraagt om flexibiliteit en een groot aanpassingsvermogen. Niet alleen flexibiliteit in ICT voorzieningen en toegankelijkheid van gegevens, maar juist van de mensen die er mee werken.
Het goed organiseren van informatiemanagement, waarbij we op basis van goede afspraken over besturen, beheren en uitvoeren voldoen aan wet- en regelgeving en aan (nieuwe) wensen en eisen van de eigen organisatie rondom data en informatie (informatie governance).

2 Privacymanagement

Het college van gemeente Edam-Volendam 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 zijn 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 privacy officer kan benoemen.

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen – zie 2.3.

Het college voorziet in een team van professionals (hierna het P&I-team, kortweg: PIT) die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. Binnen de gemeente Edam-Volendam zal het PIT bestaan uit de Privacy Officer, de CISO (Chief Information Security Officer), medewerker concern control en teamleden van het "Kernteam processen" als vaste kern. Waar nodig wordt het team aangevuld met de FG, proceseigena(a)r(en) en deskundigen. Het PIT ondersteunt proceseigenaren (zie 2.2) 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. Taken kunnen afdelingen overlappen (zie ook defensies!!).
- De proceseigenaar kan verantwoordelijkheden mandateren aan afdelingscoördinatoren ('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 pro-actief 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 verant¬woordelijk 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 verant-woordelijk 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 (loco) gemeentesecretaris de proceseigenaar. De (loco) gemeentesecretaris kan ook een proceseigenaar aanwijzen voor het gezamenlijke deel van de gegevensverwerking.

2.3 Toezicht

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van gemeente Edam-Volendam 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 Edam-Volendam en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving)*[1].
- Houdt toezicht op de nakoming van het privacybeleid en achterliggende wettelijke verplichtingen*.
- Controleert de naleving van afspraken door gemeente Edam-Volendam en ketenpartners, eventueel ook in samenwerking met auditors*.
- Is het contactpunt voor landelijke privacytoezichthouders – met name de Autoriteit Persoonsgegevens*.
- Helpt privacyklachten tot een goed einde te brengen (ombudsfunctie)**[2].
- Adviseert bij privacyincidenten over ernst en omvang**.
- Helpt het privacybeleid en daarmee tevens de visie uit te dragen bij interne en externe doelgroepen.

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 Edam-Volendam 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.

[1] * is wettelijk opgenomen.
[2] ** volgt uit wettelijke beschrijvingen.

- De FG werkt onafhankelijk en mag dus niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen bij normale omstandigheden. Er zijn uitzonderingen waarin deze laatste twee maatregelen wel van toepassing kunnen zijn.

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 Edam-Volendam

3.1 Algemeen

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

- voert gemeente Edam-Volendam proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert gemeente Edam-Volendam de uitoefening van rechten van personen;
- bewaakt gemeente Edam-Volendam 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 doelen (met inbegrip van innovatie) zoals de uitoefening van publieke taken, de nakoming van wettelijke plichten, de vrijwaring van vitale belangen voor de betrokkene(n), de totstandkoming of uitvoering van een overeenkomst waarbij een betrokkene partij is en/of de behartiging van een gerechtvaardigd belang van gemeente Edam-Volendam of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

3.3 Risicogedreven aanpak

De privacybeleidsvoering van Gemeente Edam-Volendam is aantoonbaar en gemeentebreed 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 meebrengen zónder te hebben voorzien in doeltreffende beschermingsmaatregelen.

3.4 Kapstokregeling

Het Privacybeleidskader van gemeente Edam-Volendam 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 Edam-Volendam , 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:

- Interne organisatie
- Gemeentelijke belastingheffing
- 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 Edam-Volendam bevat ook de aanzet voor het regelen van aspecten van privacy¬beleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

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

3.5 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader Gemeente Edam-Volendam, 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 (cookies), de Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning.

4 Verantwoordelijkheden voor proceseigenaren

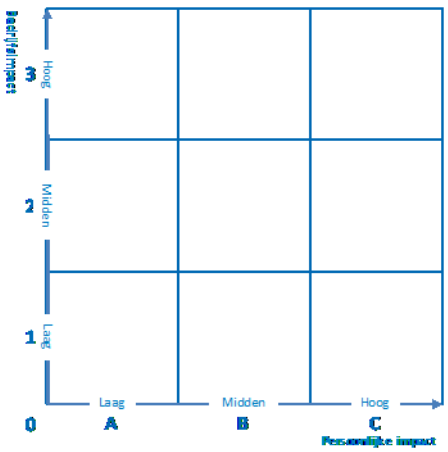
Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het PIT en de FG. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen gemeente Edam-Volendam een privacybestendige 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 Edam-Volendam een systeem van positieve en negatieve PIA-scores. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen (privacy-waarborgen). 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.

PIA-Score	PIA-rapport	Procesplan	Akkoord FG
A1	-	-	-
A2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
A3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
B1	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
B2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
B3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C1	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C2	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C3	Volledig	PIA-rapport maakt deel uit van procesplan	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/meervoudige 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[3].
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.

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

5 Privacyservices

5.1 Rechten

Burgers hebben er onder meer recht op dat:
- gemeente Edam-Volendam handelt conform het onderhavige privacybeleidskader;
- gemeente Edam-Volendam de contactgegevens van de FG bekend maakt;
- gemeente Edam-Volendam informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;
- zij inzage in hun eigen gegevens hebben;
- zij – in geval van fouten – hun gegevens kunnen (laten) rectificeren of verwijderen;
- zij, om tegen het gebruik van hun gegevens verzet aan te tekenen, wat gemeente Edam-Volendam verplicht tot het maken van een afweging;
- zij gemeente Edam-Volendam bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

5.2 Plichten

Burgers hebben de plicht dat zij persoonsgegevens naar waarheid invullen en bij het indienen van de bewijzen en verklaringen, geen valse gegevens te verstrekken.

5.3 Vragen

Bij vragen:
- hebben personen het recht om zich te wenden tot hiervoor aangewezen medewerker;
- dienen personen zich te legitimeren;
- vragen worden zo snel mogelijk, maar uiterlijk binnen vier weken afgehandeld;
- een medewerker kan ook het PIT zijn om advies over de beantwoording vragen.
- een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot een medewerker. De medewerker registreert in dat geval de vraag als een klacht.

5.4 Klachten

Bij klachten:
- hebben personen het recht om zich te wenden tot hiervoor aangewezen medewerker;
- dienen personen zich te legitimeren;
- klachten worden zo snel mogelijk maar uiterlijk binnen twee weken afgehandeld;
- een medewerker 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 Edam-Volendam.
- het PIT kan de FG om advies vragen over de afhandeling van de klacht.

5.5 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 gemeente Edam-Volendam.

6 Privacyprogramma

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 Edam-Volendam, ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen gemeente Edam-Volendam, 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 Edam-Volendam in lijn met de geldende norm wordt georganiseerd en vastgelegd in informatiebeveiligingsbeleid. Gemeente Edam-Volendam beschikt over een informatiebeveiligingsbeleid, daarnaast is er een gekwalificeerde informatiebeveiligingsfunctionaris (CISO) die toeziet op informatieveiligheid binnen de gemeente. De CISO maakt deel uit van het PIT en stemt af met de portefeuillehouder privacy en de FG. Er wordt gebruik gemaakt van geheimhoudingsverklaringen als onderdeel van de gemeentelijke aanpak voor privacybescherming en informatieveiligheid. Bij processen in de klassen C2-3, B2-3, A2-3 worden aanvullende geheimhoudingsafspraken gehanteerd als uit PIA's blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding nodig 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, incident management 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 Edam-Volendam.

6.8 Beleidsevaluatie

Proceseigenaren doen jaarlijks verslag aan de portefeuillehouder privacy van hun privacy-beleid, 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.

	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