



Gemeente Velsen 2018

Burgemeester en wethouders van Velsen hebben op 4 december 2018 het Privacybeleidskader gemeente Velsen vastgesteld.

1 Kernpunten

1.1 Voor wie?

Het Privacybeleidskader Gemeente Velsen bevat managementafspraken tussen het college en 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 Velsen is om te waarborgen dat Gemeente Velsen 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 Velsen ziet de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Inwoners en medewerkers moeten erop kunnen vertrouwen dat we persoons-gegevens 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 scheidt 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.

1.4 Kernpunten

1) Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren sturen op privacy volgens deze kernpunten van privacymanagement:

- a) Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toezicht op zijn proces(sen) op basis van dit privacybeleidskader;
 - b) Bij processen waaraan privacyrisico's zijn verbonden, hanteert de proceseigenaar een procesplan;
 - c) Een procesplan is duidelijk, actueel, stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd;
 - d) Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
 - e) Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt;
 - f) Een procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering;
 - g) Een procesplan omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden;
 - h) Een proceseigenaar handelt vragen of klachten van inwoners of medewerkers binnen twee weken af.;
 - i) Bij privacyincidenten hanteert de proceseigenaar de procedure beveiligingsincidenten en 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 Velsen beschikt over mechanismes voor privacy-incidentmanagement.
- 5) Gemeente Velsen evalueert jaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader.
- 6) Het college informeert de raad over de privacybeleidsvoering.
- 7) Het college handhaaft het privacybeleid. Gemeente Velsen heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de naleving van privacywetgeving.

1.5 Scope

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

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

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

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



Het privacybeleid Gemeente Velsen 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 Velsen 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.

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 HR-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 inkoop, of waarbij wordt samengewerkt met derden. Hierbij worden eisen gesteld aan de privacywaarborgen die de betreffende derde partij kan bieden. Deze dienen in lijn te zijn met de eisen aan privacywaarborgen die vanuit de gemeente gesteld worden.

2 Privacymanagement

Het college van de Gemeente Velsen 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 programmamanager privacy kan benoemen.

Het college heeft een Functionaris Gegevensbescherming (FG) aangewezen.

Het college voorziet in een team van professionals (hierna het Team Informatiebeveiliging en Privacy, kortweg: TIP) die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. Binnen Gemeente Velsen zal het TIP bestaan uit de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en een Controller. Het TIP ondersteunt proceseigenaren (zie 2.2) bij de uitvoering van het gemeentelijk privacybeleid.



Afdelingsmanagers 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

Afdelingsmanagers 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 afdelingsmanager is proceseigenaar.
- De proceseigenaar kan verantwoordelijkheden mandateren aan afdelingsmedewerkers ('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 hoofdstuk 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 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 afdelingsmanagers vallen, is de portefeuillehouder privacy de proceseigenaar. De portefeuillehouder privacy 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 Velsen 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 TIP over de werking van het privacybeleid van Gemeente Velsen en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving).
- houdt toezicht op de nakoming van het privacybeleid en achterliggende wettelijke verplichtingen
- helpt privacyklachten tot een goed einde te brengen (ombudsfunctie)
- adviseert bij privacyincidenten over ernst en omvang
- beheert het Privacybeleidskader Gemeente Velsen
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG
- controleert de naleving van afspraken door Gemeente Velsen 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 Velsen 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.



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 Velsen. 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. Gemeente Velsen is geen partij in de procedure. Gemeente Velsen valt de FG niet af maar wacht op rechterlijke beslissing.

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 Velsen

3.1 Algemeen

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

- voert Gemeente Velsen proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert Gemeente Velsen de uitoefening van rechten van personen;
- bewaakt Gemeente Velsen 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), 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 Gemeente Velsen is erop gericht dat binnen de gemeente 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 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 van Gemeente Velsen heeft een algemeen karakter en een raamwerk-functie (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 Velsen, in samenspraak met het TIP 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
- belastingheffing
- burgerzaken
- ruimte en bereikbaarheid
- milieu en duurzaamheid
- leefomgeving
- veiligheid en openbare orde
- jeugd en onderwijs
- maatschappelijke ondersteuning
- werk en inkomen
- lokale economie
- maatschappelijke opvang
- cultuur en sport

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacy-waarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat. Het Privacybeleidskader Gemeente Velsen bevat ook de aanzet voor het regelen van aspecten van privacy-beleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

Het Privacybeleidskader Gemeente Velsen, de procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacy-beleid Gemeente Velsen. Het Privacybeleidskader Gemeente Velsen is daarbij leidend.

3.5 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader Gemeente Velsen 2018, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming. Voor zover van toepassing, houden proces-eigenaren tevens goed rekening met bijzondere wettelijke voorschriften – met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Telecommunicatiewet, de Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning.



4 Gedragsnorm voor proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het TIP en de FG. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen Gemeente Velsen 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.

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, geven zelf het goede voorbeeld en 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 Velsen 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 TIP 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 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 onbeschikbaar 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 PIA nodig is.

4.2 Procesplan

Procesverantwoordelijken 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 privacywetgeving is voldaan.

2. Key controls (zie §4.3)

3. Verwerkersovereenkomsten

4. Afschrift van artikel 30-register (zie §4.5)

5. (eventuele) FG-verklaring (zie §4.4)

4.3 Lijst van key controls

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

PIA-Score Key controls Samenspraak TIP 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

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

4.4 FG-verklaring

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

PIA-Score PIA-rapport maakt deel uit van procesplan Akkoord FG

A1 - -

A2 Ja Aanbevolen

A3 Ja Verplicht

B1 Ja Aanbevolen

B2 Ja Aanbevolen

B3 Ja Verplicht

C1 Ja Verplicht

C2 Ja Verplicht

C3 Ja Verplicht

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

4.5 Artikel 30-formulieren

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

Artikel 30-formulier bevatten de volgende informatie:

1. Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking
2. De PIA-scoring van het proces
3. De naam, contactgegevens en het mandaat van de proceseigenaar
4. Indien van toepassing: de contactgegevens van degene die die proceseigenaar assisteert in privacyaangelegenheden.



5. De bedrijfsdoelen die met het proces zijn gediend
6. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens
7. De categorieën van ontvangers van de persoonsgegevens en, indien van toepassing, informatie over internationaal gegevensverkeer.
8. Informatie op hoofdlijnen over genomen beheersmaatregelen (key controls) – met name termijnen voor gegevensvernietiging en de aanpak op het gebied van informatiebeveiliging.
9. De FG-verklaring, indien afgegeven.

4.6 Beheer procesplan

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

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

PIA-Score Evaluatie Advies FG

A1 4 jaarlijks -

A2 3 jaarlijks Aanbevolen

A3 jaarlijks Verplicht

B1 3 jaarlijks Aanbevolen

B2 2 jaarlijks Aanbevolen

B3 jaarlijks Verplicht

C1 jaarlijks Verplicht

C2 jaarlijks Verplicht

C3 jaarlijks Verplicht

5 Privacyservices

5.1 Rechten

Personen hebben er onder meer recht op:

- dat Gemeente Velsen handelt conform het onderhavige privacybeleidskader;
- dat Gemeente Velsen de contactgegevens van de FG bekend maakt;
- dat Gemeente Velsen informatie verschaft over doelen van informatieverwerking en privacy-beleidsvoering;
- 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 Gemeente Velsen verplicht tot het maken van een afweging;
- dat zij Gemeente Velsen 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 een hiervoor aangewezen servicepunt;
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- een servicepunt kan het TIP om advies over de beantwoording vragen.
- een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot een servicepunt. Het servicepunt registreert in dat geval de vraag als een klacht

5.3 Klachten

Bij klachten:

- hebben personen het recht om zich te wenden tot het hiervoor aangewezen servicepunt;
- klachten worden zo snel mogelijk maar uiterlijk binnen twee weken afgehandeld;
- het servicepunt meldt de klacht onmiddellijk bij de incidentenregeling volgens paragraaf 6.6, die het TIP betreft voor de feitelijke klachtafhandeling.
- Het TIP 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 Velsen.
- Het TIP 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 Gemeente Velsen.

6 Privacy programma

6.1 Werkprogramma

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



binnen Gemeente Velsen, 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 Velsen in lijn met de geldende norm wordt georganiseerd en vastgelegd in informatiebeveiligingsbeleid. De gemeente Velsen beschikt over een informatiebeveiligingsbeleid ('Zo sterk als de zwakste schakel, 2016'), daarnaast is er een gekwalificeerde informatiebeveiligingsfunctionaris (CISO) die toeziet op informatie-veiligheid binnen de gemeente. De CISO maakt deel uit van het TIP 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 PIAs 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, 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 Velsen.

6.8 Beleidsevaluatie

Hoofdproceseigenaren 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 incidentmanagement zijn in wezen steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaagd, is het zaak dat proces-eigenaren 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

