

# Privacybeleidskader Gemeente Bernheze

Algemeen deel (bestuurlijk privacybeleid)

**Vastgesteld door het college:**

24 januari 2017

## Inhoud

<b>1</b>	<b>Kernpunten</b>	<b>3</b>
1.1	Voor wie?	3
1.2	Doel	3
1.3	Missie	3
1.4	Kernpunten	3
1.5	Scope	4
1.6	Raakvlakken en overlap met andere beleidsthema's	4
<b>2</b>	<b>Privacybeleid Gemeente Bernheze</b>	<b>5</b>
2.1	Algemeen	5
2.2	Noodzakelijke gegevensverwerking	5
2.3	Kapstokregeling	5
2.4	Inachtneming bijzondere wettelijke voorschriften	6
<b>3</b>	<b>Privacyservices</b>	<b>7</b>
3.1	Rechten	7
3.2	Vragen	7
3.3	Klachten	7
3.4	Beroep	7
<b>4</b>	<b>Privacy management</b>	<b>8</b>
4.1	Managementstructuur	8
4.2	Proceseigenaarschap	8
4.3	Toezicht	9
<b>5</b>	<b>Gedragshnorm voor proceseigenaren</b>	<b>10</b>
5.1	Procesplan-aanpak	10
5.2	Lijst van key controls	12
5.3	FG-verklaring	12
5.4	Artikel 30-formulieren	12
5.5	Beheer procesplan	13
<b>6</b>	<b>Privacy programma</b>	<b>14</b>
6.1	Werkprogramma	14
6.2	Bewustwording en training	14
6.3	PR & communicatie	14
6.4	Verdere verwerking, archiefbeleid, gegevensvernietiging	14
6.5	Informatiebeveiliging	14
6.6	Regeling privacyincidenten	14
6.7	Handhaving	15
6.8	Beleidsevaluatie	15
<b>7</b>	<b>Auditbeleid</b>	<b>16</b>

# 1 Kernpunten

## 1.1 Voor wie?

Dit Privacybeleidskader Gemeente Bernheze bevat managementafspraken tussen het college en het management. De afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden gebruikt, opgeslagen of uitgewisseld ('verwerking van persoonsgegevens').

Het Privacybeleidskader bestaat naast dit algemene deel ook uit nadere uitwerkingen in bijzondere regelingen en, vooral, de procesplannen. Hierin geeft de gemeente op uitvoeringsniveau aan hoe zij concreet voorziet in passende organisatorische en technische maatregelen voor de bescherming van persoonsgegevens.

Zowel het algemeen deel als de bijzondere regelingen binden iedereen die voor de gemeente werkt of bestuurlijke verantwoordelijkheid draagt.

## 1.2 Doel

Het doel van het privacybeleidskader is om te waarborgen dat de gemeente de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

## 1.3 Missie

- De gemeente Bernheze voert betrouwbaarheid en respect voor inwoners en medewerkers hoog in het vaandel. We staan voor een betrouwbare en gewaardeerde dienstverlening aan onze inwoners met een open en respectvolle benadering. Goede bescherming van persoonsgegevens is cruciaal.
- Onze inwoners mogen er daarom op vertrouwen dat wij persoonsgegevens rechtmatig, behoorlijk en op een transparante wijze verwerken
- Het college stuurt daarom actief op privacy, door te voorzien in praktische waarborgen voor de bescherming van persoonsgegevens conform de Algemene Verordening Gegevensbescherming.
- Bij dilemma's gaan we de dialoog aan.
- Vanaf 2018 kan het college met vertrouwen verantwoording afleggen over de privacybestendigheid van de gemeentelijke bedrijfsvoering.

## 1.4 Kernpunten

*Het college:*

1. draagt verantwoordelijkheden op aan proceseigenaren.  
Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren (domeinmanagers) 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 deze privacybeleidskaders:
  - 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 wordt geen illegale informatie 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 conform de klachtenprocedure binnen vier weken af.
  - i) Bij privacyincidenten hanteert de proceseigenaar de centrale incidentenprocedure.
  - j) Bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen tegen deze privacybeleidskaders en zijn procesplan.
2. voorziet in een team van professionals (het Kernteam) dat het college en de proceseigenaren ondersteunt in de privacybeleidsvoering.
  3. voorziet in faciliteiten voor bewustwording en training.
  4. treft maatregelen voor privacy-incidentmanagement (inclusief datalekken).
  5. evalueert vierjaarlijks de doeltreffendheid en de doelmatigheid van dit beleidskader
  6. informeert de raad over de privacybeleidsvoering.
  7. handhaaft het privacybeleid. De gemeente Bernheze stelt een Functionaris voor Gegevensbescherming (FG) aan die toeziet op de borging van privacy in de gemeentelijke organisatie.

## 1.5 Scope

Het Privacybeleidskader Gemeente Bernheze is van toepassing op alle bedrijfsvoering voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft. Dit beleidskader is het algemene deel van het privacybeleid van Gemeente Bernheze. Het is de kapstok voor het privacybeleid waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten.

Het privacybeleid Gemeente Bernheze omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil. Het beleid is van toepassing op processen die de gemeente uitbesteedt, inkoop of op een andere manier organiseert. Het beleid is ook 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 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. Dit geldt dus voor groepen kleiner dan 8 personen. Het beleid is ook van toepassing op beveiligingsproblemen. ('meldplicht datalekken').

## 1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap, zoals integriteit, kwaliteit, informatiebeveiliging, personeel en organisatie en communicatie. Van belang hierbij is dat de doelen van de privacywetgeving worden behaald

## 2 Privacybeleid Gemeente Bernheze

### 2.1 Algemeen

Wij zijn ons bewust van de maatschappelijke verantwoordelijkheid bij de verwerking van persoonsgegevens. Om deze reden:

- Voeren wij proactief privacybeleid op basis van dit beleidskader;
- Faciliteren wij de uitoefening van rechten van personen;
- Bewaken wij de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

### 2.2 Noodzakelijke gegevensverwerking

Alle medewerkers verwerken persoonsgegevens uitsluitend voor de volgende doelen, voor zover dit valt binnen hun mandaat en noodzakelijk is voor:

1. de uitoefening van publieke taken;
2. de nakoming van wettelijke plichten;
3. de vrijwaring van vitale belangen voor de betrokkene(n);
4. de totstandkoming of uitvoering van een overeenkomst waarbij een betrokkene partij is;
5. de behartiging van een gerechtvaardigd belang van gemeente Bernheze of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

### 2.3 Kapstokregeling

Het Privacybeleidskader Gemeente Bernheze 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 beleidskader. Dit doen zij samen met het Kernteam en de FG (functionaris gegevensbescherming). De procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat.

Op basis van dit privacybeleidskader moet specifiek uitvoeringsbeleid worden gemaakt voor diverse werkerterreinen, bijvoorbeeld:

- Interne organisatie
- Burgerzaken
- Belastingheffing
- Milieu en duurzaamheid
- Leefomgeving (
- Sociaal Domein
- Maatschappelijke ondersteuning
- Maatschappelijke opvang
- Enzovoorts.

Het beleidskader bevat ook de aanzet voor het regelen van aspecten van privacybeleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

Het privacybeleidskader, themabeleid, procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid Gemeente Bernheze. In geval van tegenstrijdigheid heeft het Privacybeleidskader Gemeente Bernheze voorrang.

## **2.4 Inachtneming bijzondere wettelijke voorschriften**

Op basis van het privacybeleidskader, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming (AVG). 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, de Jeugdwet en de Wet maatschappelijke ondersteuning.

## 3 Privacyservices

### 3.1 Rechten

Personen hebben er recht op:

- dat wij handelen volgens het onderhavige privacybeleidskader;
- dat wij informatie verschaffen over doelen van informatieverwerking en privacybeleidsvoering;
- dat zij inzage in hun *eigen* gegevens hebben;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat ons verplicht tot het maken van een afweging;
- dat zij ons bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

Wij respecteren uiteraard ook overige bij wet toegekende privacyrechten.

### 3.2 Vragen

Bij vragen:

- hebben personen het recht om zich te wenden tot het klantencontactcentrum.
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld
- het klantencontactcentrum kan de privacy coördinator om advies over de beantwoording vragen

### 3.3 Klachten

- een niet tot tevredenheid afgehandelde vraag of een directe klacht geeft personen het recht om zich te wenden tot de klachten coördinator.
- de klachten coördinator registreert in dat geval de klacht en stuurt deze door naar de klachtenbehandelaar/proceseigenaar.
- klachten worden door de klachtenbehandelaar/proceseigenaar zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld.
- de klachtenbehandelaar/proceseigenaar is bij een klacht verplicht om de FG om advies te vragen.

### 3.4 Beroep

Na afhandeling van een klacht door de klachtenbehandelaar kan een klager in beroep bij de FG indien de klacht verband houdt met naleving van privacywetgeving en het privacybeleidskader .

## 4 Privacy management

### *Het college*

- 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.
- legt over de privacybeleidsvoering verantwoording af aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting.
- 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.
- houdt een register van de gegevensverwerkingen bij die onder hun verantwoordelijkheid plaatsvinden zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming

Privacy management is SMART-georganiseerd en heeft zelfstandige aandacht binnen de planning & control-cyclus van de gemeentelijke organisatie.

### 4.1 Managementstructuur

Privacy valt onder de verantwoordelijkheid van de portefeuillehouder personeelszaken en organisatie (hierna privacy). De gemeentesecretaris is ambtelijk verantwoordelijk. Proceseigenaren voeren als onderdeel van hun verantwoordelijkheden regie en houden toezicht op hun processen op basis van het privacybeleidskader. Proceseigenaren zijn operationeel eindverantwoordelijk voor de uitvoering van de hun toegewezen processen.

Het college voorziet in een team van professionals (Kernteam) die onder de verantwoordelijkheid vallen van de secretaris. De secretaris kan voor dagelijkse aansturingstaken een privacy coördinator benoemen. De privacy coördinator maakt onderdeel uit van het Kernteam.

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen – zie 4.3. Het Kernteam ondersteunt samen met de FG proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleid.

### 4.2 Proceseigenaarschap

Domeinmanagers zijn ervoor verantwoordelijk dat de gemeentelijke taakuitoefening waarvoor zij operationeel eindverantwoordelijk zijn, binnen de grenzen van dit privacybeleidskader plaatsvindt en rapporteren over dit laatste aan de portefeuillehouder privacy.

- Een domeinmanager is **proceseigenaar**.
- De proceseigenaar kan verantwoordelijkheden mandateren aan medewerkers ('subproceseigenaren')
- De proceseigenaar kan mandateren aan derden buiten de gemeentelijke organisatie.
- 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. De proceseigenaar houdt



pro-actief toezicht op de privacybestendige organisatie van zijn proces en documenteert keuzes en oplossingen op een begrijpelijke manier in zijn procesplan.

Wanneer gemeentelijke processen zodanig zijn georganiseerd dat de onderliggende gegevensverwerking onder de verantwoordelijkheid van meerdere domeinmanagers vallen, is de secretaris de proceseigenaar. De secretaris kan vervolgens een proceseigenaar aanwijzen voor het gezamenlijke deel van de gegevensverwerking.

### 4.3 Toezicht

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van Gemeente Bernheze op de naleving van privacywetgeving conform artikel 37-39 AVG.

Het college informeert indien nodig 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 Kernteam over de werking van het privacybeleid 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 (privacy-ombudsman)
- adviseert bij privacyincidenten over ernst en omvang
- beheert het privacybeleidskader.
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG
- controleert de naleving van afspraken door Gemeente Bernheze 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 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 kan vrij en onafhankelijk advies geven.

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. De raad wordt via de planning en control cyclus geïnformeerd.

## 5 Gedragsnorm voor proceseigenaren

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

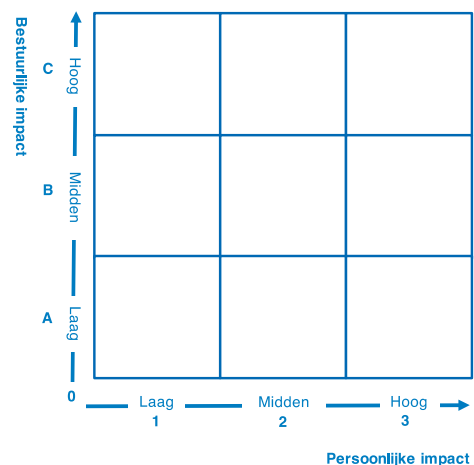
Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking.

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.

### 5.1 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 behoeven, hangen samen met de uitkomsten van de PIA ('PIA-rapport').

Voor eenduidig begrip hanteert Gemeente Bernheze een systeem van positieve en negatieve PIA-scores. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen (privacywaarborgen). Proceseigenaren volgen het advies van het Kernteam 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	-
B2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
B3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C1	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
C2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
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 gegevensverwerking:** gebruik, opslag of uitwisseling van informatie is bij wet verboden.
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.<sup>1</sup>
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 het A1-processen blijven is hiervoor 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 opnieuw een PIA nodig is.

<sup>1</sup> Niet-nakoming van: meldplichten, bijzondere regels voor internationaal gegevensverkeer, wettelijke termijnen, verplicht voorafgaand onderzoek AP, toestemmingsverplichtingen

## 5.2 Lijst van key controls

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

PIA-Score	Key controls	Samenspraak Kernteam	Samenspraak FG
A1	-	-	-
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Verplicht
B1	Ja	Ja	-
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Verplicht
C1	Ja	Ja	Aanbevolen
C2	Ja	Ja	Aanbevolen
C3	Ja	Ja	Verplicht

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

## 5.3 FG-verklaring

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

PIA-Score	PIA-rapport maakt deel uit van procesplan	Akkoord FG
A1	-	-
A2	Ja	Aanbevolen
A3	Ja	Verplicht
B1	Ja	-
B2	Ja	Aanbevolen
B3	Ja	Verplicht
C1	Ja	Aanbevolen
C2	Ja	Aanbevolen
C3	Ja	Verplicht

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

## 5.4 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.

## 5.5 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	2 jaarlijks	Aanbevolen
A3	jaarlijks	Verplicht
B1	4 jaarlijks	-
B2	2 jaarlijks	Aanbevolen
B3	jaarlijks	Verplicht
C1	2 jaarlijks	Aanbevolen
C2	2 jaarlijks	Verplicht
C3	jaarlijks	Verplicht

## **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 is vooral gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen Gemeente Bernheze, met gebruikmaking van overige instrumenten die in deze paragraaf worden beschreven.

### **6.2 Bewustwording en training**

Het college bevordert samen met proceseigenaren 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 Bernheze in lijn met de geldende norm wordt georganiseerd. Gemeente Bernheze beschikt over een gekwalificeerde coördinerende informatiebeveiliging (CISO) die deelneemt in het Kernteam en samenwerkt met de portefeuillehouder privacy en de FG. Geheimhoudingsverklaringen zijn instrumenten binnen de gemeentelijke aanpak voor privacybescherming en informatieveiligheid. Bij processen in de klassen C2-3, B2-3, A2-3 worden aanvullende geheimhoudingsafspraken gehanteerd voor zover uit PIA's blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding functioneel zijn.

### **6.6 Regeling privacyincidenten**

Het college voorziet in een procedure voor privacyincidenten die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. De 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 hanteert de CAR-UWO bij niet-nakoming van afspraken volgens het privacybeleidskader Gemeente Bernheze.

## **6.8 Beleidsevaluatie**

Proceseigenaren doen binnen de planning en controlcyclus verslag aan de portefeuillehouder privacy van hun privacybeleid, 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 van 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
<b>A1</b>	Quick scan	5 jaarlijks	-	-
<b>A2</b>	Zelfevaluatie	5 jaarlijks	vrijwillig	ja
<b>A3</b>	Externe audit	3 jaarlijks	ja	ja
<b>B1</b>	Zelfevaluatie	5 jaarlijks	vrijwillig	ja
<b>B2</b>	Zelfevaluatie	5 jaarlijks	vrijwillig	ja
<b>B3</b>	Externe audit	3 jaarlijks	ja	ja
<b>C1</b>	Externe audit	3 jaarlijks	ja	ja
<b>C2</b>	Externe audit	3 jaarlijks	ja	ja
<b>C3</b>	Externe audit	2 jaarlijks	ja	ja

Wijziging termijnen van de tabellen apart met werkgroep bespreken