Gemeente Epe

GEMEENTEBLAD

Officiële uitgave van de gemeente Epe

Nr. 178598

20 augustus 2018

Privacybeleidskader Gemeente Epe (algemeen deel - bestuurlijk privacybeleid)

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 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).
KlantContactCentrum – het contactpunt voor personen voor het stellen van eenvoudige vragen en voor het aanvragen van enkelvoudige producten en diensten.
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. Het PIT bestaat uit de privacy-officer (voorzitter), de Informatiebeveiligingsfunctionaris (CISO), de It security officer, de gegevensbeheerder, de procesverantwoordelijke functioneel beheer.
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 dat de kapstok vormt voor het privacybeleid van de gemeente Epe, waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten.
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.
Privacy- officer – medewerker die het privacybeleid vormgeeft en bewaakt en directie en proceseigenaren adviseert in privacy aangelegenheden.
Privacywetgeving – wetgeving die verwerking van persoonsgegevens regelt, in het bijzonder de AVG.
Procesdoel – een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens
Proceseigenaren – afdelingsmanagers die verantwoordelijk zijn voor 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).
Procesverantwoordelijke – medewerker die verantwoordelijk is voor de aansturing van het proces en stuurt op het behalen van de afgesproken kritische prestatie indicatoren (kpi's). Hij/zij ondersteunt en begeleidt procesmedewerkers waar nodig in het proces of faciliteert dat dit gebeurt.
Uitvoeringsorganisatie - een organisatie waaraan een of meerdere bedrijfsprocessen zijn uitbesteed.

Hoofdstuk 1 Kernpunten

Artikel 1.1 Voor wie?

Het Privacybeleidskader Gemeente Epe 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').

Artikel 1.2 Doel

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

Artikel 1.3 Visie en missie

De gemeente Epe 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. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij onenigheid of dilemma's met betrekking tot de verwerking van persoonsgegevens gaan wij de dialoog met betrokkenen aan en zoeken waar mogelijk gezamenlijk naar oplossingen.

De ambitie van de gemeente Epe is om te voldoen aan de bedoeling van de Algemene Verordening Gegevensbescherming (AVG).

Artikel 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. De gemeente Epe beschikt over mechanismes voor privacy-incidentmanagement;
5. Het college evalueert vierjaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader;
6. Het college informeert de raad over de privacybeleidsvoering;
7. Het college handhaaft het privacybeleid en stelt een Functionaris voor Gegevensbescherming aan, die toeziet op de naleving van privacywetgeving.

Artikel 1.5 Scope

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

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

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

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

Het privacybeleid is van ook toepassing op gegevensuitwisseling met derden zoals de Belastingdienst, belastingsamenwerking Tribuut, de Raad voor de Kinderbescherming, de politie, zorgaanbieders etc.

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.

Artikel 1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van de gemeente Epe 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 en de informatiesamenwerking met de Gemeente Apeldoorn.

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.

Hoofdstuk 2 Privacymanagement

Het college van Epe 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 en de organisatie van het bijhouden van het register is belegd bij het PIT, zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming (AVG).

Tabel 1: Rollen en verantwoordelijkheden

Verantwoordelijken	**Vertaald naar privacy**	**ARSCI**
1e lijn - College van B&W (portefeuillehouder)	Eindverantwoordelijk	**A** Accountable
1e lijn - Medewerkers en management (proceseigenaar) Gemeente Epe - Ketenpartners bij inkoop/outsourcing (zoals gemeenschappelijke regelingen)	Feitelijk verantwoordelijk	**R** Responsible
2e lijn PIT (kernteam) bestaande uit: - Informatiebeveiligingsfunctionaris(CISO), - Privacy-officer (voorzitter) - It security officer, - Gegevensbeheerder, - Procesverantwoordelijke functioneel beheer, ad hoc aan te vullen	Ondersteunend	**S** Supportive
3e lijn - Functionaris voor Gegevensbescherming	Toezicht	**C** Consulted (hier: Controlerend)
Belanghebbenden - Burgers - Medewerkers - Gemeenteraad - Autoriteit Persoonsgegevens - Accountant	Geïnformeerd	**I** Informed

Artikel 2.1 Managementstructuur

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

Bestuurlijke verantwoordelijkheid:

Privacy valt onder de verantwoordelijkheid van de portefeuillehouder Privacy.

Ambtelijke verantwoordelijkheid

De directie is ambtelijk verantwoordelijk. De directie mandateert zijn verantwoordelijkheid voor het privacybeleid aan proceseigenaren. Zij zijn als proceseigenaar operationeel eindverantwoordelijk voor de aan hun toegewezen processen.
Proceseigenaren voeren als onderdeel van hun verantwoordelijkheden regie en houden toezicht op hun processen op basis van het privacybeleidskader. De AVG als geheel valt onder een door de directie aangewezen ambtelijk functionaris/proceseigenaar.

PIT
Het college voorziet in een Privacy Informatie Team (PIT) met daarin een aantal professionals (Kernteam) die onder verantwoordelijkheid vallen van de hierboven bepaalde ambtelijk functionaris/proceseigenaar.

Het PIT bestaat uit een aantal vaste leden namelijk:

- De Informatiebeveiligingsfunctionaris (CISO)
- De privacy-officer (voorzitter)
- De Gegevensbeheerder
- ICT/security officer
- Procesverantwoordelijke functioneel beheer (op oproepbasis)

Afhankelijk van welke processen aan de orde zijn, wordt het PIT uitgebreid met een proceseigenaar en/of enkele ad hoc leden.

Taken van het PIT
- Het adviseren van directie en proceseigenaren over de uitvoering van het privacy- en informatie-beveiligingsbeleid;
- het vaststellen van de kaders voor het invullen en muteren van het artikel 30 verwerkingenregister;

- het opstellen van een jaarlijks werkprogramma ter uitvoering van het pbk en het toezien op de uitvoering daarvan;
- het vaststellen van het format voor het houden van Privacy Impact Assessments (PIA's) en het over de uitvoering van de PIA's adviseren van proceseigenaren.

Functionaris gegevensbescherming FG

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen.
Het PIT ondersteunt samen met de FG proceseigenaren bij de uitvoering van het gemeentelijk privacy beleid.

Artikel 2.2 Proceseigenaarschap

Proceseigenaren zorgen ervoor dat de gemeentelijke taakuitoefening, waarvoor zij operationeel verantwoordelijk zijn, binnen de grenzen van het privacybeleidskader plaatsvindt en rapporteren hierover via het PIT aan de Directie en de Portefeuillehouder Privacy.

- De proceseigenaar kan verantwoordelijkheden mandateren aan procesverantwoordelijken;
- 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 § 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 is verantwoordelijk voor en houdt toezicht op de privacybestendige inrichting van zijn proces en documenteert keuzes en oplossingen als bijlagen van de procesplan.

Een proceseigenaar kan proceseigenaarschap mandateren aan een partij buiten de gemeentelijke organisatie met toestemming van de directie (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.

Artikel 2.3 Toezicht

De FG is de toezichthouder van de gemeente Epe 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, 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 taken van de FG:

- informeert en adviseert het college, proceseigenaren en het PIT over de werking van het privacybeleid van de gemeente Epe 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 Epe;
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door Gemeente Epe 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 Epe 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 aan het college van B&W. De raad wordt via de planning & control-cyclus geïnformeerd.

Hoofdstuk 3 Privacybeleid Gemeente Epe

Artikel 3.1 Algemeen
Het college is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:
- voeren wij proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteren wij de uitoefening van rechten van personen;
- bewaken wij de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

Artikel 3.2 Noodzakelijke gegevensverwerking
Proceseigenaren 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 de gemeente Epe of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

Artikel 3.3 Kapstokregeling
Het Privacybeleidskader Gemeente Epe 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 Epe, 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 Tribuut
- Burgerzaken
- 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 Epe bevat ook de aanzet voor het regelen van aspecten van privacy¬beleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

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

Artikel 3.4 Inachtneming bijzondere wettelijke voorschriften

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

Hoofdstuk 4 Gedragsnorm 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 de gemeente 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 directie houdt een ‘artikel 30-register’ (zie §4.6) 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’.

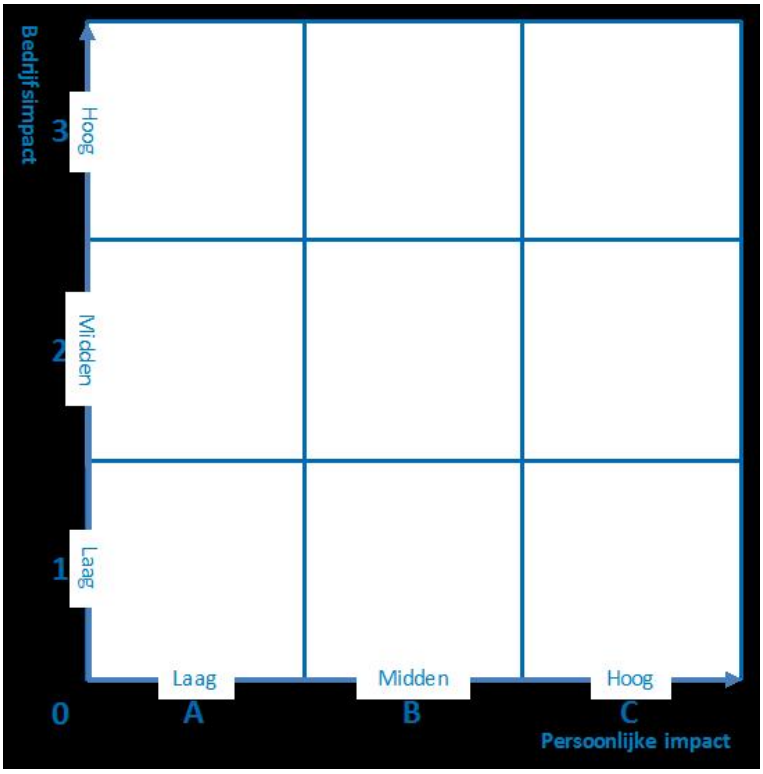
Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking.

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.

Artikel 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 de gemeente 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 het procesplan	Aanbevolen
A3	Volledig	PIA-rapport maakt deel uit van het procesplan	Verplicht
B1	Beknopt	PIA-rapport maakt deel uit van het procesplan	Aanbevolen
B2	Beknopt	PIA-rapport maakt deel uit van het procesplan	Aanbevolen
B3	Volledig	PIA-rapport maakt deel uit van het procesplan	Verplicht
C1	Beknopt	PIA-rapport maakt deel uit van het procesplan	Aanbevolen
C2	Volledig	PIA-rapport maakt deel uit van het procesplan	Aanbevolen
C3	Volledig	PIA-rapport maakt deel uit van het 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 niet beschikbaar te zijn.
6. **Niet-inachtneming van bijzondere wettelijke voorschriften**: bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.(Niet-nakoming: meldplichten, bijzondere regels voor internationaal gegevensverkeer, wettelijke termijnen, verplicht voorafgaand onderzoek AP, toestemmingsverplichtingen)
7. **Onbewaakte gegevensverwerking**: de proceseigenaar verzuimt om te controleren of de privacy waarborgende 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 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.

Artikel 4.2 Inhoud procesplan

Onder verantwoordelijkheid van proceseigenaren worden procesplannen opgesteld die voortbouwen op de uitkomsten uit de risico- en belangenanalyses. De belangrijkste componenten van een procesplan zijn:

1. Risicoanalyse (eventueel in de vorm van PIA) bestaande uit:
   a. Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
   b. Een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden;
   c. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
   d. De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van de persoonsgegevens te garanderen en om aan te tonen dat aan de privacywetgeving is voldaan.
2. Key controls (zie § 4.4);
3. Verwerkersovereenkomsten;
4. Afschrift van artikel 30-register (zie § 4.6);
5. (eventuele) FG-verklaring (zie § 4.5).

Artikel 4.3 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	Aanbevolen
B2	2 jaarlijks	Aanbevolen
B3	Jaarlijks	Verplicht
C1	2 Jaarlijks	Aanbevolen
C2	Jaarlijks	Verplicht
C3	Jaarlijks	Verplicht

Artikel 4.4 Lijst van key controls

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

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

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

Artikel 4.5 FG-verklaring

Een evenwichtig procesplan beschrijft een behoorlijke en zorgvuldige aanpak, in overeen-stemming 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	Aanbevolen
C2	Ja	Verplicht
C3	Ja	Verplicht

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

Artikel 4.6 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 directie 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. Wie is de proceseigenaar;
4. Wie is de procesverantwoordelijke;
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.

Hoofdstuk 5 Privacyservices

Artikel 5.1 Rechten
Personen hebben er onder meer recht op:
- dat de gemeente handelt conform het onderhavige privacybeleidskader;
- dat de gemeente de contactgegevens van de FG bekend maakt;
- dat de gemeente informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;
- dat zij inzage in hun eigen gegevens hebben;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) rectificeren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat de gemeente verplicht tot het maken van een afweging;
- dat zij de gemeente bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

Artikel 5.2 Vragen
Bij vragen:
- kunnen personen zich wenden tot het KlantContactCentrum (KCC);
- het KCC beantwoordt algemene en eenvoudige vragen;
- complexe vragen worden door de privacy-officer beantwoord;
- vragen worden zo snel mogelijk, maar uiterlijk binnen vier weken afgehandeld.

Artikel 5.3 Klachten
Bij klachten:
- een niet tot tevredenheid afgehandelde vraag of een directe klacht geeft personen het recht om zich te wenden tot de klachtencoördinator;
- de klachtenbehandelaar / proceseigenaar is bij een klacht verplicht om de FG om advies te vragen;
- 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.

Artikel 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 privacybeleidskader van de gemeente.

Hoofdstuk 6 Privacy programma

Artikel 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 de gemeente Epe, met gebruikmaking van overige instrumenten die in deze paragraaf worden beschreven.

Artikel 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.

Artikel 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.

Artikel 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.

Artikel 6.5 Informatiebeveiliging

Het college ziet erop toe dat informatieveiligheid van de gemeente Epe in lijn met de geldende normen wordt georganiseerd. De gemeente beschikt over een gekwalificeerde informatiebeveiligingsfunctionaris (CISO) die toeziet op informatieveiligheid binnen de gemeente. De CISO maakt deel uit van het PIT en werkt samen 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.

Artikel 6.6 Regeling privacyincidenten

Het college voorziet in een procedure voor privacyincidenten die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. (zie het document "werkinstructie melden datalekken") Deze procedure voor privacyincidenten bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten. Ook bevordert het college het oefenen op privacyincidenten, incident management en crisiscommunicatie.

Artikel 6.7 Handhaving

Het college hanteert de CAR-UWO bij niet-nakoming van afspraken volgens het Privacybeleidskader Gemeente Epe.

Artikel 6.8 Beleidsevaluatie

Proceseigenaren doen jaarlijks via het PIT 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.

Hoofdstuk 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	vrijwillig	Ja
B3	Externe audit	3 jaarlijks	Ja	Ja
C1	Externe audit	3 jaarlijks	Ja	Ja
C2	Externe audit	3 jaarlijks	Ja	Ja
C3	Externe audit	2 jaarlijks	Ja	Ja

Vastgesteld door het college van burgemeester en wethouders op 22 mei 2018, nr. 2018-04726.