gemeente Winterswijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Winterswijk

Nr. 252562

17 oktober

2019

Privacy beleidskader gemeente Winterswijk

Definities

AVG (Algemene Verordening Gegevensbescherming) – Europese wet op de verwerking van persoonsgegevens die rechtstreeks geldt in alle lidstaten.
Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.
FG (Functionaris voor Gegevensbescherming)/ Data Protection Officer (DPO) – wettelijk toezichthouder voor de naleving van privacywetgeving (met name de AVG) en bedrijfsvoorschriften.
Gegevensverwerking – zowel geheel of gedeeltelijk geautomatiseerde operationele informatieverwerking (bijvoorbeeld archiveren, analyseren, doorgeven, raadplegen) als ieder geheel daarvan (bijvoorbeeld de salarisadministratie, gemeentebelastingen of thuiszorg).
Persoonsgegevens – gegevens over personen en waarvan de gegevensverwerking door herleidbaarheid gevolgen heeft in de persoonlijke levenssfeer (privacy impact heeft).
DPIA (data 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).
DPIA-score – getalsmatige classificatie van noodzaak of risico van gegevensverwerking, als uitkomst van een PIA.
PT – het privacy team dat de directie en proceseigenaren ondersteunt.
Portefeuillehouder privacy – het lid van het college dat verantwoordelijk is voor de uitvoering en naleving van privacywetgeving met behulp van het privacybeleidskader.
Privacy programmamanager – degene die namens de portefeuillehouder privacy uitvoering geeft aan het privacybeleid.
Privacyaudit – controles op de naleving van privacybeleid en privacywetgeving.
Privacybeleid – het privacybeleidskader en alle nadere uitwerkingen hiervan.
Privacybeleidskader – het bestuurlijk privacybeleid van een organisatie, dat de kapstok vormt waaraan operationele procesplannen worden opgehangen.
Privacybeleidsvoering – sturing op privacy door het management ('governance').
Privacyincidenten – gebeurtenissen waartegen het privacybeleid en de privacywetgeving bescherming beoogt te bieden.
Privacywetgeving – wetgeving die verwerking van persoonsgegevens regelt, in het bijzonder de AVG.
Procesdoel – een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens.
Proceseigenaren – lijnmanagers die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen of veiligheid.
Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een PIA).
Servicepunt – het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacyrechten.
Uitvoeringsorganisatie – een organisatie waaraan een of meerdere bedrijfsprocessen zijn uitbesteed.

1 Kernpunten

1.1 Voor wie?

Het Privacybeleidskader Gemeente Winterswijk bevat instructies van het college voor proceseigenaren. Deze instructies 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 Winterswijk is om te waarborgen dat gemeente Winterswijk de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie

Visie op privacy gemeente Winterswijk:

'Burgers en maatschappelijke partners kunnen erop rekenen dat bij de gemeente Winterswijk de privacy van persoonsgegevens in goede handen is. In het huidige digitale tijdperk vinden we de vertrouwelijkheid van persoonlijke informatie van groot belang en de gemeente zet zich ervoor in dat de privacy gewaarborgd is en blijft.'

gemeente Winterswijk

1.4 Uitgangspunten

1) Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren sturen op privacy volgens deze uitgangspunten 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 voor het intern melden van 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 Winterswijk beschikt over mechanismes voor privacy-incidentmanagement.
5) Gemeente Winterswijk evalueert driejaarlijks de doeltreffendheid en de doelmatigheid van het gemeentelijk privacybeleid.
6) Het college informeert de raad over de privacybeleidsvoering.
7) Het college handhaaft het privacybeleid. Gemeente Winterswijk heeft een Data Protection Officer / Functionaris voor Gegevensbescherming aangesteld die toeziet op de borging van privacy in de gemeentelijke organisatie.

1.5 Scope

Het Privacybeleidskader gemeente Winterswijk is het algemene deel van het privacybeleid binnen de gemeente. Het algemene beleidskader is de kapstok voor het privacybeleid van gemeente Winterswijk, waaraan aanvullende regelingen zijn opgehangen zoals procesplannen of regelingen voor het uitoefenen van rechten. Het beleidskader gaat over alle verwerkingen van persoonsgegevens, zoals deze voorkomen in de hele organisatie. Het betreft onder meer:

- Alle bedrijfsvoering van gemeente Winterswijk voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.
- Zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil.
- Processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor gemeente Winterswijk informatiediensten verricht.
- Gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders.
- 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.
- De verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.
- De omgang met data gerelateerde incidenten.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van gemeente Winterswijk 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, zoals o.a. beschreven in het tactisch en strategisch informatiebeveiligings beleid.

Kwaliteitsbeleid

Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is een randvoorwaarde voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteit- en risicomanagement
Privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement, omdat privacybeleid afbreuk en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerking een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).

Informatiebeveiliging
Privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens. Informatiebeveiliging wordt uitgevoerd op basis van informatiebeveiligingsbeleid.

Personeel en organisatie
Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie wordt uitgevoerd vanuit het HRM-beleid.

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 waarborgen 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 gemeente Winterswijk is verantwoordelijk voor de naleving van privacywetgeving en voert het 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.
Privacy management 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 laat een register van de gegevensverwerkingen bijhouden die onder hun 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 aanwijst.

Het college heeft uiterlijk 1 mei 2018 een Functionaris voor Gegevensbescherming (FG) aangewezen, zie paragraaf 2.3.

Het college geeft de gemeentesecretaris opdracht om te voorzien in een team van professionals (hierna het Privacy Team, kortweg: PT) die onder de (bestuurlijke) verantwoordelijkheid valt van de portefeuillehouder privacy. Het PT ondersteunt proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleid.

Managers zijn als 'proceseigenaren' (zie onder) op uitvoeringsniveau verantwoordelijk voor privacybestendige bedrijfsvoering en gegevensuitwisseling met derden. Zij leggen hierover via de gemeentesecretaris verantwoording af aan de portefeuillehouder privacy.

2.2 Proceseigenaarschap
De managers 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 manager is **proceseigenaar**.
- 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 (procesplannen zijn procesbeschrijvingen AVG-proof) (zie hierna in hoofdstuk 4.1) die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit privacybeleidskader en is steeds in overeen stemming 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 partij buiten de gemeentelijke organisatie met toestemming van het college (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 kent dwingende bepalingen over wederzijdse verantwoordelijkheden bij ketensamenwerking.

Wanneer gemeentelijke processen zodanig zijn georganiseerd dat de onderliggende gegevensverwerking onder de verantwoordelijkheid van meerdere managers 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 Data Protection Officer (DPO) / Functionaris voor Gegevensbescherming (FG) is de toezichthouder van Gemeente Winterswijk op de naleving van privacywetgeving conform artikel 37-39 AVG.

Het college informeert interne en externe doelgroepen over de DPO/FG en communiceert zijn contactgegevens aan de Autoriteit Persoonsgegevens.

De DPO/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 DPO/FG:
- informeert en adviseert het college, proceseigenaren en het PT over de werking van het privacybeleid van gemeente Winterswijk 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 Winterswijk.
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG.
- controleert de naleving van afspraken door gemeente Winterswijk 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 DPO/FG krijgt de nodige ruimte voor professionele uitvoering van taken.
- Het college en proceseigenaren zorgen ervoor dat de DPO/FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De DPO/FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen Gemeente Winterswijk waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het college en proceseigenaren ondersteunen de DPO/FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De DPO/FG mag niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, of voor de uitvoering van zijn taken als DPO/FG worden gestraft of ontslagen.

De zienswijze van de DPO/FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door de gemeente, onverminderd de opvattingen van landelijke toezichthouders.

De DPO/FG doet jaarlijks verslag van zijn werkzaamheden aan het college. De raad wordt via de (reguliere) planning & controlcyclus geïnformeerd.

3 Privacybeleid gemeente Winterswijk

3.1 Algemeen

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

– voert gemeente Winterswijk proactief privacybeleid op basis van dit privacybeleidskader; faciliteert gemeente Winterswijk de uitoefening van rechten van personen;
– bewaakt gemeente Winterswijk de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

3.2 Noodzakelijke gegevensverwerking

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

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

3.3 Kapstokregeling

Het Privacybeleidskader van gemeente Winterswijk 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 Winterswijk, in samenspraak met het PT en de DPO/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:

– Gemeenteorganisatie
– Cultuur en sport Belastingheffing
– HRM
– Jeugd en onderwijs
– Leefomgeving
– Lokale economie
– Maatschappelijke ondersteuning
– Maatschappelijke opvang
– Milieu en duurzaamheid
– Ruimte en bereikbaarheid
– Services
– Veiligheid en openbare orde
– Werk en inkomen

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat.

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

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

3.4 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader gemeente Winterswijk, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming. Voor zover van toepassing, houden proceseigenaren tevens goed rekening met bijzondere wettelijke voorschriften – met name privacy-relevante bepalingen in de Wet basisregistratie personen, Telecommunicatiewet, Wet gemeentelijke schuldhulpverlening, Participatiewet, de Jeugdwet en 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 PT en de DPO/FG.

Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen Gemeente Winterswijk 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.

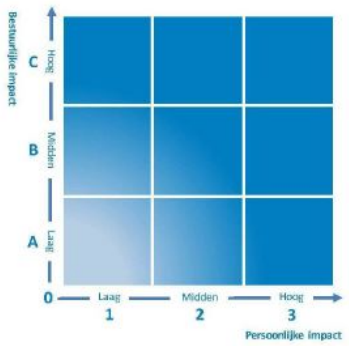
De DPO/FG houd in opdracht van de portefeuillehouder privacy een 'artikel 30-register' (zie §4.4) bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het college vallen. Proceseigenaren helpen om het register volledig en actueel te laten zijn door middel van 'artikel 30-formulieren'.

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

Het college en proceseigenaren dragen het belang uit van privacybeleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt. In de komende paragrafen worden er een aantal voorbeelden beschreven.

4.1 Procesplan-aanpak
Aan procesplannen liggen data privacy impact assessments (DPIA's) ten grondslag. DPIA'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 DPIA, zoals verwoord in het DPIA-rapport.

Voor eenduidig begrip hanteert gemeente Winterswijk een systeem van positieve en negatieve PIA-scores. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen (privacywaarborgen). Proceseigenaren volgen het advies van het PT bij de vaststelling van hun DPIA-score. DPIA-scores worden bepaald aan de hand van de hieronder afgebeelde matrix.



Proceseigenaren zijn goed bekend met hun DPIA-scores en hanteren onderstaande tabel om te bepalen in hoeverre DPIA's tevens deel uitmaken van het procesplan om op die manier de keuzes voor beheersmaatregelen te verantwoorden.

DPIA-Score	Risico Beoordeling	DPIA-rapport	Procesplan	Akkoord DPO/FG
A1	Laag	-	Privacy compliance maakt deel uit van procesplan	-
A2	Midden	Inventarisatie	Privacy compliance maakt deel uit van procesplan	Aanbevolen
A3	Hoog	Volledig	DPIA-rapportmaakt deel uit van procesplan	Verplicht
B1	Midden	Inventarisatie	Privacy compliance maakt deel uit van procesplan	Aanbevolen
B2	Midden	Inventarisatie	Privacy compliance maakt deel uit van procesplan	Aanbevolen

B3	Hoog	Volledig	DPIA-rapportmaakt deel uit van procesplan	Verplicht
C1	Hoog	Volledig	DPIA-rapport maakt deel uit van procesplan	Verplicht
C2	Hoog	Volledig	DPIA-rapport maakt deel uit van procesplan	Verplicht
C3	Hoog	Volledig	DPIA-rapport maakt deel uit van procesplan	Verplicht

DPIA -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 (archiefwet-verplichte vernieting).
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.[1]
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 (risicobeoordeling laag) volstaan algemene oplossingen. Zolang een proces met risicobeoordeling laag gekwalificeerd is, is daarvoor in mindere mate aandacht nodig. De portefeuillehouder privacy laat een lijst van processen met risicobeoordeling laag publiceren.
De werkelijkheid dient in overeenstemming te zijn met het procesplan. Veranderingen in de bedrijfsvoering noodzaken tot aanpassing van procesplannen, waarvoor een nieuwe of geactualiseerde DPIA nodig is.

4.2 Lijst van key controls

Proceseigenaren vatten, in samenspraak met het PT en zo nodig de DPO/FG, hun procesplannen samen in een lijst van kenmerkende beheersmaatregelen ('key controls') voor sturingsdoeleinden en controle (zie paragraaf 0).

DPIA-Score	Risico Beoordeling	Key controls	Samenspraak PT	Samenspraak DPO/ FG
A1	Laag	-	-	-
A2	Midden	Ja	Ja	Aanbevolen
A3	Hoog	Ja	Ja	Verplicht
B1	Midden	Ja	Ja	Aanbevolen
B2	Midden	Ja	Ja	Aanbevolen
B3	Hoog	Ja	Ja	Verplicht
C1	Hoog	Ja	Ja	Verplicht
C2	Hoog	Ja	Ja	Verplicht

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

C3	Hoog	Ja	Ja	Verplicht

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

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

DPIA-Score	Risico Beoordeling	DPIA-rapport maakt deel uit van procesplan	Akkoord DPO/FG
A1	Laag	-	-
A2	Midden	Alleen Inventarisatie	Aanbevolen
A3	Hoog	Ja	Verplicht
B1	Midden	Alleen Inventarisatie	Aanbevolen
B2	Midden	Alleen Inventarisatie	Aanbevolen
B3	Hoog	Ja	Verplicht
C1	Hoog	Ja	Verplicht
C2	Hoog	Ja	Verplicht
C3	Hoog	Ja	Verplicht

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

4.4 Artikel 30-formulieren
Het PT vat het procesplan samen met behulp van 'artikel 30-formulieren' dat de proceseigenaar toevoegt aan het begin van zijn procesplan en waarvan hij via de gemeentesecretaris een kopie verstrekt aan de programmamanager privacy, die zorgdraagt voor opname van het formulier in het Artikel 30-register. Proceseigenaren melden veranderingen voor het artikel 30-register aan de hand van wijzigingsformulieren direct bij de programmamanager privacy.

Artikel 30-formulier bevatten minimaal de volgende informatie:
1. Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking
2. De DPIA-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 DPO/FG-verklaring, indien afgegeven.

4.5 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 DPO/FG om hierbij advies uit te brengen.

DPIA-Score	Risico Beoordeling	Evaluatie	Advies DPO/FG
A1	Laag	4 jaarlijks	-
A2	Midden	3 jaarlijks	Aanbevolen
A3	Hoog	jaarlijks	Verplicht
B1	Midden	3 jaarlijks	Aanbevolen
B2	Midden	3 jaarlijks	Aanbevolen
B3	Hoog	jaarlijks	Verplicht

C1	Hoog	jaarlijks	Verplicht
C2	Hoog	jaarlijks	Verplicht
C3	Hoog	jaarlijks	Verplicht

4.6 Beleidsevaluatie

Proceseigenaren doen via de gemeentesecretaris en de portefeuillehouder privacy jaarlijks verslag aan het college van hun privacybeleidsvoering. Het verslag van de proceseigenaren omvat een stand van zaken-rapportage en verslag van eventuele klachten of andere incidenten die zich binnen hun taakgebied in het afgelopen jaar hebben voorgedaan.

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

De DPO/FG ontvangt van de gemeentesecretaris een kopie van alle verslagen en de visie die hij hier eventueel aan heeft toegevoegd, gelijktijdig met de overlegging hiervan aan het college (portefeuillehouder privacy). Mede aan de hand hiervan brengt hij jaarlijks verslag uit aan het college en adviseert hij het college over verdere optimalisering van de privacybeleidsvoering.

Het college besluit over bijstelling van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de DPO/FG.

5 Privacyservices

5.1 Rechten

Personen hebben er onder meer recht op:

- dat gemeente Winterswijk handelt conform het onderhavige privacybeleidskader;
- dat gemeente Winterswijk de contactgegevens van de DPO/FG bekend maakt;
- dat gemeente Winterswijk 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 gemeente Winterswijk verplicht tot het maken van een afweging;
- dat zij gemeente Winterswijk bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

5.2 Vragen

Bij vragen:

- Hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunten.
- Vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld.
- Een servicepunt kan het PT om advies vragen over de beantwoording vragen.
- Een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot een servicepunt. Het servicepunt behandelt de vraag dan als klacht.

5.3 Klachten

Bij klachten:
Hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunten. Klachten worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld.
Het servicepunt meldt de klacht onmiddellijk bij de klachtencoördinator die de klacht registreert en het PT betrekt voor de feitelijke klachtafhandeling.
Het PT 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 Winterswijk.
Het PT kan de DPO/FG om advies vragen over de afhandeling van de klacht.

5.4 Beroep

Personen hebben het recht om na afhandeling van een klacht conform O hiertegen in beroep gaan bij de DPO/FG voor zover het beroep gericht is op de naleving van privacywetgeving en/of het privacybeleid van gemeente Winterswijk.

6 Privacyprogramma

6.1 Werkprogramma

Het college stelt jaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van de jaarrapportage van de DPO/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 Winterswijk, ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen gemeente Winterswijk, 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 Winterswijk conform de Baseline Informatiebeveiliging Nederlandse Gemeenten wordt georganiseerd. Gemeente Winterswijk beschikt over een gekwalificeerde Chief Information Security Officer (CISO) en nauw contact onderhoudt met de portefeuillehouder privacy. 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 DPIA'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. 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 door het melden van positieve gebeurtenissen en ontwikkelingen over privacy, door voorbeeldgedrag en bespreekbaarheid en door het treffen van disciplinaire maatregelen bij ernstige schending van de integriteitscode/gedragsregels door haar medewerkers. Indien er sprake is van verwerkers draagt het college ervoor zorg dat het gemeentelijk Privacybeleidskader door deze verwerkers via aansprakelijkheids- en boeteregelingen in de verwerkersovereenkomsten wordt nageleefd.

6.8 Beleidsevaluatie
Hoofdproceseigenaren doen halfjaarlijks verslag aan de portefeuillehouder privacy van hun privacybeleid, oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de DPO/FG. De DPO/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 DPO/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 privacyprincipes.

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 DPO/FG en waarbij eventueel een professionele auditor wordt betrokken.

gemeente Winterswijk

Wanneer wordt aangegeven dat de betrokkenheid van de DPO/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.

DPIA-Score	Risico Beoordeling	Type audit	Frequentie	Betrokkenheid DPO/FG	Afschrift DPO/FG
A1	Laag	Quick scan	5 jaarlijks	-	-
A2	Midden	Zelfevaluatie	4 jaarlijks	vrijwillig	ja
A3	Hoog	Externe audit	3 jaarlijks	ja	ja
B1	Midden	Zelfevaluatie	4 jaarlijks	vrijwillig	ja
B2	Midden	Zelfevaluatie	4 jaarlijks	vrijwillig	ja
B3	Hoog	Externe audit	3 jaarlijks	ja	ja
C1	Hoog	Externe audit	3 jaarlijks	ja	ja
C2	Hoog	Externe audit	3 jaarlijks	ja	ja
C3	Hoog	Externe audit	3 jaarlijks	ja	ja