Privacybeleidskader 2025 - 2027

Versie 1.0

25 september 2024

Inhoudsopgave

1. Kernpunten

1.1 Voor wie?

Het Privacybeleidskader Gemeente Twenterand 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').

Onder verwerking van persoonsgegevens wordt in de Algemene Verordening Gegevensbescherming verstaan:

- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen en gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikkingstellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

Proceseigenaren hebben kennis van en zicht op de uitvoering van de processen, sturen daarop en betrokken zijn als er iets niet goed gaat in dat proces (welke wijzigingen nodig zijn, en welke veranderingen eraan zitten te komen waar we iets mee moeten). Binnen de gemeente Twenterand zijn het veelal mensen met de functies teamleider, senior-medewerker of coördinator.

1.2 Doel

Het doel van het Privacybeleidskader Gemeente Twenterand is te waarborgen dat gemeente Twenterand aantoonbaar zorgvuldig omgaat met de verwerking van persoonsgegevens van inwoners en medewerkers in overeenstemming met de privacywetgeving.

1.3 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 deze privacybeleidskaders;
    b. Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
    c. Binnen een proces wordt geen illegale informatie verwerkt;
    d. Een proceseigenaar handelt vragen of klachten van inwoners of medewerkers binnen twee waken af;
    e. Bij privacyincidenten hanteert de proceseigenaar de procedure ‘Afhandeling datalekken’;
    f. Bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen tegen deze privacybeleidskaders.
2. Het college voorziet in een werkgroep van professionals dat het college en de proceseigenaren ondersteunt in de privacybeleidsvoering;

3. Het college voorziet in faciliteiten voor bewustwording en training;
4. Gemeente Twenterand beschikt over mechanismes voor privacy-incidentmanagement;
5. Gemeente Twenterand evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader;
6. Het college informeert de raad over de privacybeleidsvoering;
7. Het college handhaaft het privacybeleid. Gemeente Twenterand heeft een Functionaris Gegevensbescherming (hierna: FG) aangesteld die toeziet op de borging van privacy in de gemeentelijke organisatie.

1.4 Scope

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

De scope van het privacybeleid is in de volgende punten omschreven:

- Het privacybeleid is van toepassing op alle bedrijfsvoering van gemeente Twenterand voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.
- 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 gemeente Twenterand informatiediensten verricht.
- Het privacybeleid is van toepassing op gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders.
- Het privacybeleid omvat de gehele 'data life cycle': van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.
- Het privacybeleid is van toepassing op de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

1.5 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Integriteitsbeleid

Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid.

Kwaliteitsbeleid

Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap.

Continuïteit- en risicomanagement

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

Informatiebeveiliging

Privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens. Informatiebeveiliging wordt uitgevoerd vanuit het informatiebeveiligingsbeleid en -plan van de gemeente Twenterand.

Personeel en organisatie

Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie volgt het gemeentelijke personeelsbeleid.

Communicatie

Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatiebeleid.

Aanpak ondermijning

De verwerking van persoonsgegevens komt ook bij de uitvoering van het ‘Protocol aanpak ondermijning gemeente Twenterand’ aan de orde. In het Protocol zijn het Privacybeleidskader en de gemeentelijke Privacyverklaring van toepassing verklaard.

2. Privacy management

Het college van gemeente Twenterand is verantwoordelijk voor de naleving van privacywetgeving en voert pro-actief 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 maakt samen met het informatiebeveiligingsbeleid deel uit van de P&C-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 is verantwoordelijk voor het bijhouden van een ‘Verwerkingsregister’ voor het verwerken van persoonsgegevens die onder hun verantwoordelijkheid plaatsvinden, zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming (AVG) en in artikel 31d Wet politiegegevens (Wpg).

2.1 Managementstructuur en proceseigenaarschap

Het college is eindverantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van gemeentelijke taken (burgerzaken, openbare orde en veiligheid, gemeentebelastingen, sociaal domein, ruimtelijke ordening en milieu, P&O, etc.).

Het college heeft, als de 'verwerkingsverantwoordelijke' in de zin van de AVG, een gemeentelijke toezichthouder voor de privacybescherming aangewezen (de FG, zie paragraaf 2.2).

Er is een werkgroep Security en Privacy (S&P). Hierin zitten de Chief Information Security Officer (CISO), Privacy Officer (PO), Functionaris Gegevensbescherming (FG) en een systeembeheerder. Deze werkgroep maakt deel uit van het team IT en I-Advies (ITIA).

Primair is de directie proces-eindverantwoordelijk voor de vormgeving van privacywaarborgen binnen de teams en de dagelijkse aansturingstaken.

De proceseigenaren verantwoorden zich naar de managers en kunnen, onverlet het proceseigenaarschap, advies en informatie bij de werkgroep S&P aanvragen.

Voor een nadere beschrijving van het proceseigenaarschap wordt verwezen naar het document 'Taken, bevoegdheden en verantwoordelijkheden van de proceseigenaar’ en een aanpak voor implementatie (vastgesteld door het toenmalige CT dd. 03-02-2022).

2.2 Toezicht

De Functionaris voor de Gegevensbescherming (FG) is de interne toezichthouder van de gemeente Twenterand conform artikel 37-39 AVG en tevens conform artikel 36 Wpg. Het college informeert interne en externe doelgroepen over de FG en communiceert zijn contactgegevens aan de Autoriteit Persoonsgegevens.

De FG wordt aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacy management-praktijk; (b) zijn vermogen om de onderstaande taken te vervullen en (c) zijn onafhankelijkheid - met name de afwezigheid van belangenverstrengeling.

De FG:

- informeert en adviseert het college, proceseigenaren en de werkgroep S&P over de werking van het privacybeleid van Gemeente Twenterand 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 Twenterand;
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door Gemeente Twenterand en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacybeleid uit te dragen bij interne en externe doelgroepen;
- is het contactpunt voor de nationale privacytoezichthouder - de Autoriteit Persoonsgegevens (AP).

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 Twenterand 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 mag niet geïnstrueerd worden over invulling van taken, onder druk gezet of gestraft worden. Hij of zij geniet dezelfde ontslagbescherming als leden van de ondernemingsraad, wat betekent dat ontslag pas geoorloofd is na toestemming van de kantonrechter.

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 P&C-cyclus geïnformeerd.

3. Privacybeleid gemeente Twenterand

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

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

3.1 Noodzakelijke gegevensverwerking

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

1. de nakoming van wettelijke plichten;
2. de uitoefening van publieke taken;
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 Twenterand of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert;
6. het kunnen aantonen dat er toestemming door betrokkene(n) is verleend.

Verwerking is alleen toegestaan in overeenstemming met de wet. Persoonsgegevens worden zo veel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit, wat inhoudt dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier bereikt kan worden. Tevens spreekt de wet van proportionaliteit. Persoonsgegevens mogen alleen worden verwerkt als dit in verhouding staat met het doel. De gemeente is verantwoordelijk voor bescherming van persoonsgegevens. Op welke manier dit geregeld wordt, is vastgelegd in het informatie-beveiligingsbeleid.

3.2 Kapstokregeling

Het ‘Privacybeleidskader gemeente Twenterand’ heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Per specifieke activiteit kunnen afspraken gemaakt worden over de waarborging van privacy.

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

Het Privacybeleidskader Gemeente Twenterand en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid. In geval van tegenstrijdigheid heeft het ‘Privacybeleidskader gemeente Twenterand’ voorrang.

3.3 Inachtneming bijzondere wettelijke voorschriften

Op basis van het 'Privacybeleidskader gemeente Twenterand' geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming en de Wet politiegegevens (zie 3.4). Voor zover van toepassing, houden proceseigenaren tevens rekening met bijzondere wettelijke voorschriften - met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Telecommunicatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning (Wmo).

3.4 Verwerking politiegegevens

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.

Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkings-verantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

3.4.1 Kaders Wpg

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zullen worden geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).

- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudit. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

De gemeente Twenterand heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld met daarin de visie op gegevensbescherming en is vastgelegd op welke wijze politiegegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.

a. Omschrijving van de categorieën persoonsgegevens;
b. Beschrijving van de doeleinden van de verwerkingen;
c. Rechten van betrokkenen (zie 4.3)

De gemeente als verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen, genoemd in artikel 4a, lid 1-5 Wpg.

3.4.2 Rol FG en de bevoegd functionaris

Binnen de Wpg worden twee rollen beschreven, n.l. die van FG en de bevoegd functionaris.

De FG is tenminste belast met de volgende taak (36 lid 3a Wpg):

Het toezien op de naleving van het bepaalde bij of krachtens deze wet en op het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van de autorisaties, bedoeld in artikel 6, de bewustmaking en opleiding van de ambtenaren die zijn betrokken bij de verwerking van politiegegevens en de audits, bedoeld in artikel 33.

De teamleider Toezicht Handhaving en Veiligheid (THV) is verantwoordelijk voor het uitvoeren van de taak bevoegd functionaris (BF). Dit is de ‘hoeder’ van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris te hebben. De BF heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevens rechtmatig worden verkregen en verwerkt.

4. Gedragsnorm voor proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support van de FG, PO en CISO. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen Gemeente Twenterand 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 de werkinstructies.

Proceseigenaren zijn verantwoordelijk voor de volledigheid en actualiteit van het 'register van verwerkingen'. Door middel van het formulier "nieuwe/wijziging verwerking persoonsgegevens· geven zij mutaties op het register door aan de PO, die vooralsnog het beheer voert.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeentegegevens verwerkt.

Proceseigenaren verlenen hieraan hun medewerking.

Het college en proceseigenaren dragen het belang uit van privacybeleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

4.1 Privacyrisico’s analyseren

Organisaties kunnen verplicht zijn bij nieuwe verwerkingen van Data Protection Impact Assessments (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna passende maatregelen te kunnen nemen om de risico's te verkleinen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht behoeven, hangen samen met de uitkomsten van de DPIA.

Proceseigenaren volgen het advies van de FG bij de vaststelling van hun DPIA-score.

In de AVG, Wpg en Wet justitiële en strafvorderlijke gegevens (Wjsg) is op hoofdlijnen aangegeven wanneer een DPIA verplicht is. Dat is het geval als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Dit moet de verwerkingsverantwoordelijke en uitdien hoofde de proceseigenaar zelf bepalen. Er mag in dat geval niet worden begonnen met het verwerken van gegevens voordat er een DPIA (en indien nodig een voorafgaande raadpleging) is uitgevoerd. De Autoriteit Persoonsgegevens (AP) heeft op 29 november 2019 een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waarvoor een DPIA verplicht is.

DPIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG, eventueel met ondersteuning van de Privacy Officer (PO) en worden getoetst door de FG.

Proceseigenaren documenteren in werkinstructies 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 niet beschikbaar 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 geeffectueerd of te evalueren in hoeverre zijn proces bijstelling behoeft.

De werkelijkheid dient in overeenstemming te zijn met het proces. Veranderingen in de bedrijfsvoering noodzaken tot aanpassing van processen, waarvoor opnieuw een DPIA nodig is.

4.2 Formulieren voor verwerkingen

Proceseigenaren vatten een verwerking van persoonsgegevens samen in het formulier 'nieuwe/wijziging verwerking persoonsgegevens' dat zij opnemen aan het begin van een proces en waarvan zij een afschrift verstrekken aan de FG voor opname in het ·register van verwerkingen·. Proceseigenaren mailen nieuwe verwerkingen of wijzigingen voor dit register onmiddellijk aan de hand van dit formulier.

Het formulier 'nieuwe/wijziging verwerking persoonsgegevens' bevat de volgende informatie:

1. Een korte omschrijving van het proces, waarop de gegevensverwerking van toepassing is;
2. De naam, team van de contactpersoon en contactgegevens en het mandaat van de proceseigenaar;
3. De bedrijfsdoelen die met het proces zijn gediend;
4. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
5. De categorieën van ontvangers van de persoonsgegevens en, indien van toepassing, informatie over internationaal gegevensverkeer;
6. Informatie op hoofdlijnen over genomen beheersmaatregelen (key controls) - met name termijnen voor gegevensvernietiging en de aanpak op het gebied van informatiebeveiliging;

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

5. Rechten van betrokkenen

Personen hebben er recht op:

- dat gemeente Twenterand binnen dit privacybeleidskader opereert;
- dat gemeente Twenterand 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) verbeteren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat de gemeente Twenterand verplicht tot het maken van een afweging;
- dat zij gemeente Twenterand bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

Deze rechten zijn bekend gemaakt in de privacyverklaring op de gemeentelijke website.

5.1 Vragen

Bij vragen:

- hebben personen het recht om zich te wenden tot de SIB (Service Informatie Balie), welke de betrokken proceseigenaar of teamleider inlicht;
- kan de proceseigenaar of teamleider advies vragen bij de FG/PO.

5.2 Klachten

Een niet tot tevredenheid afgehandelde vraag of een directe klacht geeft personen het recht om een officiële klacht in te dienen; deze klacht wordt afgehandeld volgens de door de raad vastgestelde 'Regeling interne klachtenbehandeling':

1. De klacht dient schriftelijk bij het college van burgemeester en wethouders ingediend te worden.
2. De gemeente zal de klacht intern (binnen 6 weken) beoordelen. Het is mogelijk dat de klacht mondeling toegelicht moet.
3. De gemeente stuurt schriftelijk bericht van de uitspraak over de klacht.
4. Tegen de uitspraak kan een externe beoordeling van de klacht bij de regionale klachtrechtvoorziening (de Nationale Ombudsman) worden aangevraagd.

6. Privacyprogramma

6.1 Evaluatie beleid

Het college laat het privacybeleid jaarlijks evalueren. Dit betreft een zelfevaluatie waarin de FG een leidende rol heeft. Deze zelfevaluatie wordt gekoppeld aan de zelfevaluatie over informatiebeveiliging, waardoor verantwoording afgelegd kan worden aan de raad met een totale evaluatie over informatiebeveiliging en privacy. Het privacybeleid heeft een geldigheid van 3 jaar en zal daarna opnieuw door het college vastgesteld moet worden.

6.2 Rapportage en verantwoording

Met een kwartaalrapportage monitoren CISO en FG in het DirectieOverleg de voortgang van de informatieveiligheid en privacy binnen de organisatie, gebaseerd op het 'Jaarplan Security & Privacy'. De burgemeester en de portefeuillehouder bedrijfsvoering worden ook periodiek ingelicht over de voortgang (minimaal halfjaarlijks). Door middel van het jaarverslag ontvangt ook de raad de jaarstukken inzake informatieveiligheid en privacy (paragraaf bedrijfsvoering).

Het afleggen van verantwoording ('accountability') op basis van deze paragraaf is gebaseerd op de begroting inzake informatieveiligheid en privacy van het betreffende jaar.

6.3 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.

6.4 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.

6.5 Informatiebeveiliging

Het college ziet erop toe dat informatieveiligheid van de gemeente Twenterand in lijn met de geldende norm wordt georganiseerd. Het college beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die samen met de PO, de FG en een systeembeheerder deel uitmaakt van de werkgroep S&P. Geheimhoudingsverklaringen zijn instrumenten binnen de gemeentelijke aanpak voor privacybescherming en informatieveiligheid.

6.6 Privacyincidenten (datalekken)

Datalekken worden veelal veroorzaakt door menselijke fouten. Door het scheppen van een open cultuur waarin medewerkers zich niet gehinderd voelen om een datalek te melden, kunnen zo nodig maatregelen worden getroffen om te voorkomen dat dezelfde datalekken zich herhalen. Zowel richting inwoners, medewerkers, leverancier is de Gemeente verplicht om zorgvuldig met persoonsgegevens om te gaan. Daarnaast wil de gemeente Twenterand richting het college en in voorkomend geval ook de Autoriteit Persoonsgegevens aantoonbaar maken ('accountability') dat het mogelijke is gedaan om datalekken te voorkomen. 'Accountability' wordt georganiseerd door regelmatig te toetsen om de genomen maatregelen hebben geleid tot het gewenste effect. De FG neemt een dergelijke kwaliteitstoets op in een jaarlijks door de directie vast te stellen AVG-jaarplan.

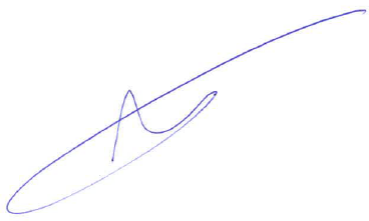
Het college voorziet in een procedure ‘Afhandeling datalekken’, waarbij de privacyincidenten (datalekken) door de FG worden gecoördineerd. De procedure bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten. Indien er sprake is van een datalek heeft iedere medewerker de plicht om na signalering hiervan onmiddellijk een melding te doen in TopDesk (beveiligingsincidenten/datalekken). Zo nodig meldt de FG het datalek binnen 72 uur bij de Autoriteit Persoonsgegevens (AP). Alle datalekken worden in het 'Register van datalekken' opgenomen.

6.7 Handhaving

Het college handhaaft het gemeentelijk privacybeleid door disciplinaire maatregelen in het vooruitzicht te stellen wanneer willens en wetens het privacybeleid omzeild wordt. Disciplinaire maatregelen volgen uit de standaardprocedure die bij P&O bekend is.

Vriezenveen, 28 januari 2025

Burgemeester en wethouders van Twenterand

de secretaris,	de burgemeester,
	
P.F.G. Rossen	mr. J.C.F. Broekhuizen