gemeente dantumadiel

GEWOAN BYSÛNDER

PRIVACY BELEID

19 mei 2026, versie 1.2

Privacybeleid gemeente Dantumadiel

De gemeente Dantumadiel (hierna: de gemeente) werkt met (persoons)gegevens van onder andere burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna: AVG).

1. Inleiding

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden, naast de bijzondere wetten (zoals de Jeugdwet en de Participatiewet) onder andere de volgende wettelijke kaders:

- De Algemene Verordening Gegevensbescherming (AVG);
- De Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), die de AVG uitwerkt;
- De Wet politiegegevens (Wpg) met onderliggende regelgeving die geldt wanneer boa's persoonsgegevens verwerken in hun opsporingstaak.

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

1. **Rechtmatigheid, behoorlijkheid en transparantie:** De gemeente verwerkt persoonsgegevens op een eerlijke en rechtmatige manier. De gemeente informeert betrokkenen duidelijk over wat er met hun gegevens gebeurt.
2. **Doelbinding:** De gemeente verzamelt gegevens alleen voor specifieke, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De gemeente kan gegevens onder bepaalde voorwaarden gebruiken voor een ander doel.
3. **Dataminimalisatie:** De gemeente verzamelt en verwerkt alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.
4. **Juistheid:** De gemeente zorgt ervoor dat persoonsgegevens correct en actueel zijn. Onjuiste gegevens worden zo snel mogelijk aangepast of verwijderd.
5. **Opslagbeperking:** De gemeente bewaart de gegevens niet langer dan nodig is voor het doel van de verwerking, tenzij er een wettelijke bewaartermijn geldt.

6. **Integriteit en vertrouwelijkheid:** De gemeente neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, misbruik, onbevoegde toegang of openbaarmaking.
7. **Verantwoordingsplicht:** De gemeente kan aantonen dat zij voldoet aan de AVG en legt verantwoording af over de genomen maatregelen en keuzes.
8. **Privacy by Default en Privacy by Design:** De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen en processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens.

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken).

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer en ambtsdrager

Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers, ambtsdragers en andere personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

2. Visie

De gemeente zet zich voortdurend in op het verhogen van het privacy bewustzijn en de verdere professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor de waarborging van privacy binnen de gemeente.

3. Definities

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

4. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers, medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente**;**
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

5. Verwerkingsverantwoordelijke

Ieder bestuursorgaan van de gemeente kan, afhankelijk van zijn taak of bevoegdheid, verwerkingsverantwoordelijke zijn. Hiervan is sprake wanneer zij het doel en de middelen van de verwerking vaststelt. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college en de raad.

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de wet- en regelgeving en de aantoonbaarheid van deze naleving (de verantwoordingsplicht).

6. Verwerkingen (artikel 4, AVG)

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Volgens de AVG valt onder ‘verwerking’ onder andere:

- verzamelen, vastleggen en ordenen;
- bewaren, bijwerken en wijzigen;
- opvragen, raadplegen, 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.

Uit deze niet-uitputtende opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden (artikel 5, AVG)

Volgens de AVG mogen persoonsgegevens alleen verwerkt worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen in beginsel niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (artikel 6, AVG)

De AVG zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- wanneer deze noodzakelijk is om een op de gemeente rustende wettelijke verplichting na te komen;
- wanneer deze noodzakelijk is voor de uitvoering van een overeenkomst waar de betrokkene partij bij is;
- wanneer deze noodzakelijk is om een ernstige bedreiging voor de gezondheid van de betrokkene of van een ander persoon te bestrijden;
- wanneer deze noodzakelijk is voor de goede vervulling van de gemeentelijke taak;
- wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- wanneer deze noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de AVG, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk bij de betrokkene zelf verzameld. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere minder ingrijpende manier kan worden bereikt.

In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende) persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor worden gekozen. Daarnaast betekent het proportionaliteitsvereiste dat de persoonsgegevens niet langer dan noodzakelijk mogen worden bewaard.

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast treft de gemeente nadere beveiligingsmaatregelen om de veiligheid van de persoonsgegevens zo veel mogelijk te waarborgen. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet, staat in het interne informatiebeveiligingsbeleid van de gemeente en in aanvullende beveiligingsplannen specifiek opgesteld voor een proces of registratie.

Doorgifte aan landen buiten de EER

De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie (artikel 44 t/m 50, AVG).

Samenwerking

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

7. Transparantie en communicatie

Informatieplicht (artikel 13, 14, AVG)

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met de persoonsgegevens zal omgaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente deze persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze gegevens voor de eerste keer worden verwerkt.

Verwijdering

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van het doel van de verwerking, of zoals vastgelegd in wetgeving zoals de Archiefwet.[1] Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze, behoudens mogelijke wettelijke bewaringstermijnen, zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

[1] Voor een lijst met termijnen vanuit de Archiefwet zie: https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf.

Rechten van betrokkenen (artikel 12 t/m 22, AVG)

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- **Recht op informatie:** betrokkenen hebben het recht om door de gemeente te worden geïnformeerd wanneer zijn/haar persoonsgegevens worden verwerkt;
- **Inzagerecht:** betrokkenen hebben het recht om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- **Correctierecht:** als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren;
- **Recht op beperking van de verwerking:** betrokkenen hebben onder omstandigheden het recht aan de gemeente te vragen om hun persoonsgegevens tijdelijk niet meer te gebruiken;
- **Recht om vergeten te worden:** betrokkenen hebben onder omstandigheden het recht om verwijdering van de gegevens te verzoeken. Dit is bijvoorbeeld het geval wanneer de gegevens niet langer nodig zijn of wanneer de betrokkene zijn toestemming intrekt.
- **Recht op bezwaar:** betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- **Recht op overdraagbaarheid:** betrokkenen hebben onder omstandigheden het recht om de hem/haar betreffende persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen; en om deze gegevens zonder hinder aan een ander te verstrekken.
- **Recht op menselijke tussenkomst:** betrokkenen hebben het recht om niet aan volledig geautomatiseerde besluitvorming, waaronder profilering, te worden onderworpen. Er moet altijd een mens meekijken die de uiteindelijke beslissing doet.

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek mag op iedere manier worden gedaan, een betrokkene kan bijvoorbeeld een brief sturen maar kan ook persoonlijk langskomen. Wanneer de betrokkene zijn verzoek elektronisch indient moet hier, tenzij de betrokkene om een andere manier van voldoening vraagt, ook elektronisch aan worden voldaan. Dus als een verzoeker per e-mail vraagt om inzage mag de gemeente deze informatie in beginsel niet vervolgens per brief toesturen.

Wanneer de gemeente redenen heeft om te twijfelen aan de identiteit van de verzoeker, mag zij aanvullende informatie opvragen om de identiteit vast te stellen.

Het verstrekken van informatie of het treffen van maatregelen op verzoek van de betrokkene is in beginsel kosteloos. Alleen wanneer verzoeken kennelijk ongegrond of buitensporig zijn, mag de gemeente een redelijke vergoeding in rekening brengen of het verzoek weigeren

De gemeente heeft, vanaf ontvangst van het verzoek, een maand de tijd om hieraan te voldoen of om dit gemotiveerd af te wijzen. Deze termijn van een maand kan onder omstandigheden met

twee maanden worden verlengd, deze verlenging moet binnen een maand aan de betrokkene zijn medegedeeld. Als de gemeente geen gevolg geeft aan het verzoek moet dit zo snel mogelijk, uiterlijk binnen een maand, aan de betrokkenen worden medegedeeld. Hierbij dient de betrokkene ook te worden geïnformeerd over de mogelijkheid om bezwaar te maken bij de gemeente, een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP) en om bij de rechter een beroep in te stellen.

8. Geautomatiseerde verwerkingen

Profilering (artikel 22, AVG)

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn: financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken, gebruiken we het volgende voorbeeld: wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. De gemeente mag wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

Volgens de AVG is het in beginsel niet toegestaan om profilering te gebruiken. In artikel 22.2 worden wel enige uitzonderingen opgesomd: 1. noodzakelijk voor de uitvoering van een overkomst tussen de betrokkene en de verwerkingsverantwoordelijke. 2. toegestaan door Nederlands/EU recht. 3. Na uitdrukkelijke toestemming van de betrokkene.

De gemeente maakt geen gebruik van geautomatiseerde besluitvorming door algoritmes of profilering.

Big data en tracking

Alleen gegevens die niet herleidbaar zijn tot een natuurlijk persoon mogen worden verwerkt door middel van big data-onderzoek of tracking. Dit betekent dat de gegevens worden geanonimiseerd of gepseudonimiseerd. Daarnaast worden deze gegevens uitsluitend verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens mogen alleen worden verwerkt door personen die daartoe gemachtigd zijn.

Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast, dit betekent dat alleen de gegevens die echt nodig zijn voor het behalen van het doel zullen worden gebruikt.

9. Plichten van de gemeenten

Register van verwerkingen (artikel 30, AVG)

De gemeente is verantwoordelijk voor het aanleggen en bijhouden van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Het register bevat per

verwerking een beschrijving van wat er tijdens de verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- de naam van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- de doelen van de verwerking;
- de grondslag voor de verwerking;
- een beschrijving van het soort persoonsgegevens en de daarbij behorende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen;
- de herkomst van de gegevens;
- eventuele verwerkers en subverwerkers.

Register van datalekken (artikel 33 lid 5, AVG)

De gemeente is verantwoordelijk voor het aanleggen en bijhouden van een register van alle datalekken die bij verwerkingen door of voor de gemeente plaatsvinden. Dit register bevat:

- de datum waarop de inbreuk heeft plaatsgevonden;
- een beschrijving van de inbreuk;
- een beschrijving van de mogelijke gevolgen voor betrokkenen;
- een beschrijving van de getroffen maatregelen;
- of er melding is gedaan bij de AP;
- of er melding is gedaan bij de betrokkene.

Data Protection Impact Assessment (DPIA)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevensbeschermingseffectbeoordeling (ook wel Data Protection Impact Assessment of DPIA genoemd) uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[2] genoemd.

[2] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

Wanneer het van tevoren nog niet geheel duidelijk is of een DPIA moet worden uitgevoerd, wordt voordat de verwerking wordt begonnen een pre-DPIA uitgevoerd. Aan de hand van deze pre-DPIA kan worden bepaald of een DPIA al dan niet nodig is.

Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijken van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

10.Datalekken

We spreken van een ‘datalek’ wanneer er sprake is van een inbreuk op de beveiliging die leidt tot de onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking of toegang tot de persoonsgegevens. Wanneer er een datalek heeft plaatsgevonden, meldt de gemeente dit indien wettelijke voorgeschreven zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen, in dat geval meldt de gemeente dit in eenvoudige en duidelijke taal aan de betrokkenen.

Alle datalekken dienen te worden geregistreerd in het datalekkenregister, dus ook de datalekken waarvan geen melding bij de AP hoeft te worden gedaan.

Om toekomstige datalekken te voorkomen, worden bestaande datalekken geëvalueerd.

11.Rollen en verantwoordelijkheden

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Teammanagers en Directeuren • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het college van B&W, de gemeenteraad en/of de burgemeester (de verantwoordelijkheid in een concreet

		geval hangt af van welk bestuursorgaan in dat specifieke geval verwerkingsverantwoordelijke is)
C	Consulted/ Adviserend Aan de verantwoordelijken	• Privacy Officer • CISO/ISO • Functionaris Gegevensbescherming
I	Informerend/ Geïnformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Rollen en verantwoordelijkheden

College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en faciliteert de FG in het uitvoeren van zijn (toezichts)taken;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Teammanagers en directeuren

De teammanagers en directeuren zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.

De teammanagers en directeuren hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;

- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy-ambassadeur, voor zover benoemd binnen de eigen afdeling;
- Bevordert duurzame privacycultuur;
- Betrekt PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Interne toezichthouder op de naleving van de AVG en andere nationale en Europese gegevensbeschermingsbepalingen conform art. 39 lid 1 sub a AVG en 36 Wpg;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan de verwerkingsverantwoordelijken.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van Data Protection Impact Assessment (DPIA) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).
- Beheert het centrale verwerkingenregister;

Andere rollen en verantwoordelijkheden

Afdeling	**Betrokkenheid**
Juridische Zaken	Ondersteunen van Privacy Officer ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
CISO	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van Informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze/ in welk systeem verwerkt kan/ moet worden).
Privacy ambassadeurs	De Privacy ambassadeur is het eerste aanspreekpunt binnen de afdeling waar de Privacy ambassadeur werkzaam is en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

Geldigheidsduur Privacybeleid

Dit beleid is vastgesteld op 19 mei 2026 door het College van de Gemeente Dantumadiel. Het beleid wordt tenminste een keer per 36 maanden beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld in geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's, o.i.d.) kan het college besluiten tot een tussentijdse herziening.