gemeente Capelle aan den IJssel

GEMEENTEBLAD

Officiële uitgave van de gemeente Capelle aan den IJssel

Nr. 124756

18 maart

2026

Privacybeleid gemeente Capelle aan den IJssel 2025 (AVG en Wpg)

1. Het Privacybeleid gemeente Capelle aan den IJssel 2025 (AVG en Wpg) vast te stellen;
2. Het Privacybeleid gemeente Capelle aan den IJssel, vastgesteld d.d. 26 maart 2019, in te trekken;
3. Het Privacyreglement gemeente Capelle aan den IJssel, vastgesteld d.d. 26 maart 2019, in te trekken;
4. Het Organisatiebesluit privacy, vastgesteld d.d. 26 maart 2019, in te trekken.

1. Inleiding

De gemeente Capelle aan den IJssel werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om zijn (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 kunnen uitvoeren, 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 samenleving en overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer. De gemeente Capelle aan den IJssel is zich hiervan bewust en wil met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, in het bijzonder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) (Algemene Verordening Gegevensbescherming (AVG), Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, artikel 9).

Dit privacybeleid bevat ook het Wpg privacybeleid (hierna te noemen: Wpg) (Wet politiegegevens, Wet van 29 maart 2000, houdende regels met betrekking tot de verwerking van politiegegevens, Stb. 2000, 146, artikel 9). De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG, maar ook onder de Wet politiegegevens (hierna te noemen: Wpg); de persoonsgegevens heten dan ook 'politiegegevens'. 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 verwerkingsverantwoordelijke 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 vier jaar een externe audit verplicht en moeten elke jaar interne audits worden gehouden.

Dit beleid geeft aan bestuurders en medewerkers van gemeente Capelle aan den IJssel duidelijke richtlijnen voor het omgaan met privacy en toont aan dat de gemeente zich inzet voor de bescherming, waarborging en handhaving van privacy. Het beleid geldt voor de gehele organisatie en voor alle processen, afdelingen, objecten en gegevensverzamelingen binnen de gemeente waar persoonsgegevens worden verwerkt. Het beleid is zorgvuldig afgestemd binnen de organisatie voordat het ter besluitvorming werd aangeboden aan het college van B&W. Het privacybeleid van de gemeente Capelle aan den IJssel sluit aan bij het algemene gemeentelijke beleid en voldoet aan de geldende lokale, regionale, nationale en Europese wet- en regelgeving.

2. Onze ambitie en privacy

De gemeentelijke organisatie is er voor de burgers en andere betrokkenen. Wij zijn bereikbaar om de burgers zo goed mogelijk te helpen bij het regelen van overheidszaken en het verbeteren van de leefomgeving. Dit is de basis van waaruit we werken. We zijn klaar voor een samenleving die volop initiatief toont. Dankzij onze inwoners, het lokale bedrijfsleven, onze verenigingen en partners kunnen we samen

de juiste keuzes maken. Met lef en daadkracht gaan we met elkaar innovaties en experimenten aan, want onze ambitie is: "*Samen maken we het verschil in Capelle*."

De technologische en maatschappelijke ontwikkelingen gaan snel. Ze zijn van grote invloed in en op het samenleven in onze stad. Zorgen voor een duurzame ontwikkeling van de stad vinden we belangrijk. Net zoals onze maatschappelijke taak zó vormgeven dat iedere Capellenaar mee kan doen. We anticiperen op wat er op ons afkomt.

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De volgende onderdelen uit Onze ambitie staan in het kader van privacy voor ons centraal:
- Transparantie en integriteit
- Bereikbaarheid en toegankelijkheid
- Innovatie
- Samenwerken
- Vertrouwen

Transparantie en integriteit
We luisteren actief en zijn in gesprek met Capellenaren. We schakelen tussen verschillende rollen. In deze netwerksamenleving is onze rol steeds vaker die van bemiddelaar, waarbij we faciliteren en oog houden voor het brede maatschappelijk belang. Indien nodig treden we sturend op of stellen we kaders. Dit vraagt een transparante en integere organisatie die ideeën en initiatieven aanmoedigt.

Openheid binnen privacybescherming betekent transparantie. Wij informeren burgers op een passende manier, via alle relevante kanalen, over de verwerking van hun persoonsgegevens en de mogelijkheden om hun privacyrechten uit te oefenen volgens de geldende wetgeving.

Bereikbaarheid en toegankelijkheid
De wereld wordt steeds digitaler en een groot deel van de Capellenaren doet alles online. Wij waken ervoor om mensen uit te sluiten. Wij zijn bereikbaar voor alle Capellenaren en voor mensen die hier werken, ondernemen of recreëren. Dit doen we door passende en vernieuwende dienstverlening waarbij altijd oog is voor de menselijke maat.

Verantwoordelijkheid nemen voor de privacy van burgers en andere partijen die in contact staan met de gemeente Capelle aan den IJssel, betekent hen serieus nemen en dat ook zichtbaar maken. Dit houdt in dat we zorgvuldig omgaan met hun persoonsgegevens en, indien nodig, anderen aanspreken die niet de vereiste zorgvuldigheid in acht nemen. Bovendien is het belangrijk dat de gemeente altijd goed bereikbaar is voor betrokkenen die hun privacyrechten willen uitoefenen, en dat datalekken direct worden gemeld wanneer er iets misgaat.

Innovatie
Deze uitdagingen en ambities vragen om een wendbare organisatie. Bij ons is de basis op orde en staat innovatie voorop. Onze apparatuur en systemen voldoen aan de eisen van vandaag en morgen. We zijn intern verbonden en hebben een organisatiestructuur die dit ondersteunt.

Innovatie op het gebied van privacybescherming betekent het vergroten van het bewustzijn bij iedere medewerker over het belang van privacy, terwijl we tegelijkertijd zoeken naar nieuwe, efficiënte manieren om deze te waarborgen. Het besef dat het beschermen van privacy hand in hand gaat met het verbeteren van kwaliteit en het ontwikkelen van vernieuwende oplossingen. Dit houdt in dat we niet alleen snel reageren op verzoeken van betrokkenen, maar ook proactief nieuwe methoden en technologieën implementeren om privacy nog beter te beschermen. Daarnaast betekent het verantwoordelijkheid nemen wanneer de bestaande regelgeving niet voldoende is, en innovatieve stappen zetten om zaken effectief en toekomstbestendig op te lossen.

Samenwerken
Samenwerken vinden we vanzelfsprekend. We delen kennis en helpen elkaar. We handelen vanuit een gezamenlijke verantwoordelijkheid, waarbij afspraak afspraak is. Dit vraagt flexibiliteit en professionaliteit.

Het samenwerken binnen onze gemeente en met externe organisaties is cruciaal voor het leveren van de beste dienstverlening. Bij deze samenwerking is het van belang om aandacht te hebben voor privacy en de bescherming van persoonsgegevens. Dit houdt in dat we burgers duidelijk en in begrijpelijke taal informeren over de rechtmatige en gerechtvaardigde doeleinden waarvoor hun persoonsgegevens worden verzameld en, indien van toepassing, met anderen gedeeld.

Vertrouwen
We zijn betrokken, nieuwsgierig en doen ons werk met passie. Lef en daadkracht onderscheiden ons. Vertrouwen staat bij ons centraal en er is alle ruimte om ons werk op een creatieve en experimentele wijze aan te pakken. In Capelle gaan wij samen in vertrouwen op weg!

Betrokkenen moeten te allen tijde vertrouwen kunnen hebben dat hun gegevens veilig worden behandeld. Vertrouwelijkheid en integriteit zijn hierbij van essentieel belang. Dit houdt in dat de gemeente passende organisatorische en technische maatregelen neemt om de privacy van de betrokkenen te waarborgen.

3. Privacybeleid AVG

Dit privacybeleid wordt centraal vastgesteld en geldt voor alle bestuursorganen van de gemeente, voor zover de AVG van toepassing is op de betreffende verwerkingen. Binnen de verschillende afdelingen kan het management, indien nodig, aanvullend beleid opstellen wanneer specifieke processen of procedures dit vereisen. Afwijken van het centraal vastgestelde beleid is enkel mogelijk met voorafgaande toestemming van betreffende afdelingshoofd. De toepassing van het beleid wordt periodiek geëvalueerd en het privacybeleid wordt geïntegreerd in alle relevante beleidsdomeinen.

Begripsbepalingen
De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis. Kernbegrippen uit de AVG zijn:

- Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).
- Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
- Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.
- Verwerkingsverantwoordelijke: Een persoon, bestuursorgaan (raad, college, burgemeester) of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
- Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
- Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffect-beoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (DPIA).

Doel
Vanuit het belang dat wij hechten aan privacy zetten wij blijvend in op het verhogen van de privacybewustwording en 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 van privacy, goed eigenaarschap en risicobewustzijn. Dit betekent dat verantwoord en bewust gedrag van alle medewerkers essentieel is voor het bewaken van privacy binnen de gemeente.

Met dit privacybeleid geven wij 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). Daarnaast bakent dit privacy beleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af.

De verdere uitwerking van dit beleid is / wordt - waar relevant - vastgelegd in operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domein specifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet maatschappelijke ondersteuning (Wmo).

Naast dit privacy beleid 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 privacy beleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacy beleid worden opgevolgd en actief worden uitgedragen.

Reikwijdte
De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en 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.

Principes voor de verwerking van persoonsgegevens
De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. Wij onderschrijven deze principes en verwerken persoonsgegevens dan ook slechts in overeenstemming met deze principes:

1. Rechtmatige grondslag
Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

2. Welbepaalde doeleinden
De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

3. Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

4. Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

5. Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

6. Gegevens worden op tijd vernietigd
De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. De gemeente volgt hierin de VNG selectielijst voor gemeentelijke archiefbescheiden.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente na toestemming van de gemeentearchivaris de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart met toestemming van de gemeentearchivaris gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

7. Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

8. Privacy by Design

De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. De gemeente Capelle aan den IJssel maakt gebruik van privacy by design door privacy te integreren in elk aspect van haar processen, systemen en diensten. Bijvoorbeeld de implementatie van technische maatregelen zoals versleuteling van persoonsgegevens.

9. Privacy by Default

De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk. Gemeente Capelle aan den IJssel zorgt ervoor dat de privacy van betrokkenen wordt gewaarborgd door de standaardinstellingen die de bescherming van persoonsgegevens te maximaliseren, zonder dat betrokkenen hier actief om hoeven te vragen. Dit betekent bijvoorbeeld dat persoonsgegevens standaard niet gedeeld worden, dat er minimaal verzameld wordt en dat de privacy instellingen standaard zo zijn ingesteld dat ze de privacy van de gebruiker optimaal beschermen.

10. Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

11. Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen het protocol beheer beveiligingsincidenten.

12. 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 privacy beleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

13. 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.

14. Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacy beleid.

15. Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

16. Rechten van betrokkenen
Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

17. Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

18. Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Data Protection Impact Assesment (DPIA)
Als een verwerking mogelijk privacy risico's met zich mee brengt voor de betrokkene(n), moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. Allereerst wordt er een pre-DPIA gedaan, hieruit blijkt of een DPIA uitgevoerd dient te worden of niet. De gemeente voert in geval van mogelijke risico's een Data Protection Impact Assessment 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 genoemd, zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging.

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 gemeenteraad en het College van B&W 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 (jaarplan/jaarverslag).

Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar

geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

4. Rollen en verantwoordelijken

Het governancemodel privacy toont hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het model een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam (afdelingshoofden/unithoofden) en medewerkers, Functionaris voor de Gegevensbescherming (FG), Juridisch adviseur Privacy, Privacy Officer en CISO.

Tabel 1: governancemodel privacy

Verantwoordelijk	**Wie**
Eindverantwoordelijk	College van B&W
Integraal verantwoordelijk	Afdelingshoofden
Gemandateerde bevoegdheden	Unithoofden
Adviserend	• Juridisch Adviseur Privacy • CISO • Functionaris Gegevensbescherming
Toezichthoudend	Functionaris Gegevensbescherming
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)
Ondersteunend	Privacy Officer

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 privacy beleid vast;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacy cultuur;
- Geeft sturing aan privacy beleidsvoering

Afdelingshoofden
De afdelingshoofden zijn integraal verantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacy beleid vanuit hun afdeling.
De afdelingshoofden hebben de volgende rollen en verantwoordelijkheden:
- Verantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacy beleid binnen de eigen afdeling;
- Benoemen/ aanwijzen privacycoördinator(en)
- Aansturen van de privacycoördinatoren, voor zover benoemd, 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 verwerkingsregister voor zover dit betrekking heeft op de eigen afdeling;
- Het uitvoeren van DPIA's;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert duurzame privacy cultuur;
- Betrekt Juridisch adviseur Privacy en/of FG en Ciso in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Privacy-coördinatoren
De Privacy-coördinatoren zijn de eerste aanspreekpunten binnen de afdeling waar zij werkzaam zijn en hebben een monitorende en ondersteunde functie rondom het naleven en uitvoeren van het privacy beleid. De Privacy-coördinator is verantwoordelijk voor:

- Beoordeelt of een verwerking een DPIA vereist.
- Voert een verplichte DPIA uit en mitigeert daarbij risico's.
- Behandelt verzoeken van betrokkenen met betrekking tot hun rechten, zoals inzage, correctie, en verwijdering.
- Documenteert verwerkingen en stelt verwerkers- en gezamenlijke verantwoordelijken overeenkomsten op.
- Zorgt ervoor dat externen geheimhoudingsverklaringen ondertekenen, in samenwerking met HR.
- Toetst of verwerkingen voldoen aan de AVG-beginselen (art. 5 en 6).
- Controleert of er sprake is van bijzondere persoonsgegevens en de bevoegdheid om deze te verwerken (art. 9).
- Houdt bij het register van verwerkingen en het algoritmeregister.
- Informeert de FG over relevante privacy-ontwikkelingen, zowel ad hoc als via rapportages.
- Ondersteunt bij het melden van datalekken via Topdesk.
- Zorgt voor correcte informatieverstrekking aan betrokkenen bij het verzamelen van hun gegevens (art. 13 en 14).

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:

- Adviseert aan het bestuurlijke en het hoogst leidinggevende niveau over het voldoen aan de verplichtingen van Europees en nationaal recht met als doel het bevorderen van naleving en het verder ontwikkelen van de organisatie.
- Ontwikkelt visies en strategieën, stimuleert tot normering, en adviseert over het doorvertalen van strategieën naar beleidsdoelen en protocollen in het licht van politiek-maatschappelijke, technologische, organisatorische en juridische ontwikkelingen.
- Verricht diepgaand toezicht en voert audits uit op de effectuering van de ontwikkelde strategieën door toezichtvormen te verbinden, integraal toezicht te realiseren en vanuit de expertrol specialistische adviezen te geven. Hanteert hiertoe PDCA-cycli en ontwikkelt beheersinstrumenten om risico's en verbeterpunten te signaleren.
- Richt cyclische rapportages in vanuit de organisatie aan de FG en analyseert deze rapportages.
- Rapportages gaan over de vertaling van de strategieën op concernniveau naar de doelen en protocollen op afdelingsniveau.
- Functioneert als ombudsfunctionaris voor medewerkers en burgers. Ziet in die hoedanigheid toe op de afhandeling door de organisatie van AVG- en Wpg-klachten en andere knelpunten die burgers en medewerkers signaleren. De FG is tot geheimhouding en vertrouwelijkheid gehouden.
- Treedt op als contactpunt voor de Autoriteit Persoonsgegevens (AP). Werkt samen met de AP ter versterking van haar systeemtoezicht.

Juridisch adviseur privacy
De Juridisch adviseur privacy is voor bestuurders het eerste interne aanspreekpunt voor privacy-gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacy beleid. De Juridisch adviseur privacy heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacy beleid;
- Opstellen privacy beleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- 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 DPIA's 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);
- 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 het protocol beheer informatiebeveiligingsincidenten).

Privacy Officer
De Privacy Officer is verantwoordelijk voor;
- De PO ondersteunt de organisatie bij de uitvoering en implementatie van de privacyregels.
- De PO coördineert de afhandeling van AVG-privacyverzoeken.
- Tevens ondersteunt de PO de organisatie met het uitvoeren van DPIA's en geeft het (on)gevraagd advies op het gebied van privacy.
- Verder draagt de PO namens het management zorg voor de administratieve organisatie op het gebied van privacy (zoals het verwerkingsregister, datalekregister, benodigde procedures e.d.).
- De privacy officer houdt de bewustwording onder collega's op peil om te handelen volgens de AVG- principes.

Ciso
De Ciso is verantwoordelijk voor;
- Implementeert technische en organisatorische maatregelen ter bescherming van persoonsgegevens.
- Adviseert de organisatie bij datalekken volgens de meldprocedure.
- Meldt tijdig informatiebeveiligingsincidenten bij de juridisch adviseur privacy/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.

Betrokkenheid per afdeling
Tabel 2: betrokkenheid per afdeling

Afdeling	Betrokkenheid
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 het protocol Beheer Informatiebeveiligingsincidenten).
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).

Overlegstructuur
In het kader van privacy vinden diverse overleggen plaats binnen de organisatie.

Tabel 3: overlegstructuur

Overleg	Deelnemers	Doel	Frequentie
BreedMT	Management en stuurgroep Privacy & Informatiebeveiliging	Stand van zaken en ontwikkelingen, jaarverslag FG	2x per jaar
Privacy coördinatoren overleg	Alle privacy coördinatoren	Kennisdeling, leren van elkaar, bewustwording vergroten	1 x per kwartaal
FG-JA en PO overleg	Functionaris gegevensbescherming en Juridisch Adviseur Privacy + PO	Voortgang van privacy-ontwikkelingen in de organisatie	Tweewekelijks
Stuurgroep Privacy en Informatiebeveiliging	Capelle (JZ en DIV), Krimpen (PO) en IJsselgemeenten (CISO) FG (optioneel)	Uitwisselen informatie, van elkaar leren, verbinding Informatiebeveiliging en Privacy realiseren.	Maandelijks

FG-CISO	FG-CISO	Bespreken van voortgang van ontwikkelingen in de organisatie	Driewekelijks
FG-Concerncontroller	FG-Concerncontroller	Bespreken van voortgang van ontwikkelingen in de organisatie	Driemaandelijks
FG-GS	FG-GS	Bespreken van voortgang van ontwikkelingen in de organisatie	Driewekelijks

5. Privacybeleid Wpg

Het privacybeleid beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit dit deel van het privacybeleid (specifiek Wpg) bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen (Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de regeling periodieke audit politiegegevens).

Doelstellingen van het privacybeleid
Met het privacybeleid Wpg willen wij bereiken dat de boa's:
- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

Normenkader 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 zijn veelal 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.

Audits
Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacy-audits. 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.

Register van verwerkingen
Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid.
Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

Informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.

Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

FG en bevoegd functionaris
Functionaris Gegevensbescherming (FG):
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Samen met de gemeente Krimpen aan den IJssel en de GR IJsselgemeenten hebben wij een gezamenlijke FG die tevens FG ten aanzien van de Wpg is. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

Bevoegd functionaris:
Er is geen bevoegd functionaris omdat er geen artikel 9-verwerkingen zijn. Artikel 9 Wpg verwerkingen zien op een onderzoek in verband met de handhaving van de rechtsorde.

Rechten van betrokkenen
De rechten van betrokkenen op grond van de Wpg zijn op hoofdlijnen gelijkluidend aan die onder de AVG.

Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar te worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan

aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

Het melden van datalekken
De datalek procedure onder de AVG staan uitgebreid beschreven in het protocol beheer beveiligingsincidenten van de gemeente. Op hoofdlijnen is deze procedure op grond van de Wpg gelijkluidend.

Specifiek voor de Wpg geldt nog het volgende:
Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Bewustwording
Naast het vaststellen van beleid en het treffen van passende beveiligingsmaatregelen is zorgvuldig omgaan met persoonsgegevens ook een kwestie van bewustwording. Het privacy bewustzijn van de boa's wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Medewerkers moeten verplicht trainingen doorlopen op het gebied van privacy en informatiebeveiliging.

Open communicatie
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerken.

Geldigheidsduur
Dit beleid is vastgesteld door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt elk jaar beoordeeld en indien daar aanleiding toe is, bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's, kan het college besluiten tot een herziening.

Afwijken van beleid
Afwijken van het beleid is in beginsel niet toegestaan. Dit privacybeleid treedt in werking na vaststelling door de verantwoordelijke, de burgemeester en het college van burgemeesters en wethouders. Het beleid wordt elk jaar geëvalueerd en indien nodig herzien.

Aldus vastgesteld door burgemeester, college van burgemeester en wethouders van gemeente Capelle aan den IJssel op 15 juli 2025.

Het college van burgemeester en wethouders,

de secretaris,
mr. A.H.P. van Gils

de burgemeester,
drs. J.J. Manusama