Algemeen privacybeleid Gemeente Katwijk

Versie: 1.0
Januari 2023
Vastgesteld door B&W op 31-01-2023

Inhoudsopgave

1. Inleiding

De gemeente Katwijk gebruikt bij het uitvoeren van haar (wettelijke) taken persoonsgegevens. Zonder deze gegevens is het bijvoorbeeld onmogelijk om een uitkering aan een burger te verstrekken of een vergunning te verlenen. Het gaat onder andere om persoonsgegevens van inwoners, medewerkers en ondernemers. Al deze betrokkenen moeten er op kunnen vertrouwen dat de gemeente zorgvuldig met hun persoonsgegevens omgaat en dat de gemeente passende bescherming in acht neemt bij het verwerken van persoonsgegevens.

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

Dit privacybeleid is vastgesteld door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking, en is een vervanging van het privacybeleid van 11 juli 2017 en van het document ‘Governance van privacy voor de gemeente Katwijk’ van januari 2018. Het beleid wordt periodiek beoordeeld en zo nodig herzien, en indien daar aanleiding toe is kan het college besluiten tot een tussentijdse herziening.

Voor dit privacybeleid is het product ‘Privacybeleid’ van de Infomatiebeveiligingsdienst (IBD) als bron gebruikt[1].

1.1 Doel

Dit privacybeleid legt uit hoe de gemeente Katwijk zorgvuldig met persoonsgegevens omgaat en hoe de gemeente Katwijk passende bescherming in acht neemt of dient te nemen bij het verwerken van persoonsgegevens. Daarnaast geeft dit privacybeleid een afbakening van taken en verantwoordelijkheden op het gebied van bescherming van persoonsgegevens. Het is van toepassing op de gehele organisatie (dus ook bestuur, gemeenteraad en griffie) en is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken. Het privacybeleid is een overkoepelend kader waarin de maatregelen op hoofdlijnen zijn uitgewerkt. In operationele documenten zoals handreikingen, protocollen, procedures en werkinstructies is een verdere uitwerking van dit beleid vastgelegd[2].

[1] Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten, Producten - Informatiebeveiligingsdienst

[2] Dit zijn onder andere procedures rondom datalekken en inzageverzoeken. In bijlage 1 is een overzicht opgenomen met de bedoelde operationele documenten.

1.2 Verhouding tot informatiebeveiliging

Naast dit privacybeleid is er een informatiebeveiligingsbeleid vastgesteld. Bescherming van persoonsgegevens kan niet zonder informatiebeveiliging, informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Informatiebeveiliging is gericht op de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van alle gegevens van een organisatie, waaronder ook persoonsgegevens. In het informatiebeveiligingsbeleid van de gemeente Katwijk is opgenomen hoe de gemeente Katwijk met informatiebeveiliging omgaat.

1.3 Leeswijzer

Dit privacybeleid is opgedeeld in 4 delen en sluit af met een bijlage.

- Het eerste deel betreft de inleiding, met daarin o.a. het doel van het privacybeleid en een leeswijzer.
- Het tweede deel geeft een toelichting op bepalingen van de AVG, zodat voor de lezer vóóraf veel termen duidelijk zijn.
- Het derde deel beschrijft de uitgangspunten bij het werken met persoonsgegevens aan de hand van verschillende artikelen vanuit de AVG.
- Het vierde deel beschrijft de verantwoordelijkheden voor de uitvoering van dit beleid en hoe de ondersteuning plaatsvindt.
- Ten slotte gaat het vijfde deel over toezicht en controle.

De vijf delen worden opgevolgd door een bijlage (bijlage 1). In dit privacybeleid wordt geregeld aangegeven dat er procedures zijn voor wat betreft bepaalde onderwerpen. In de bijlage is een lijst opgenomen waarin wordt aangegeven welke onderliggende / ondersteunende documentatie er is, en de vindplaats daarvan.

2. Bepalingen AVG

Betrokkene: een natuurlijk persoon op wie de persoonsgegevens betrekking hebben. Meestal een inwoner of een medewerker van de gemeente. Ook een bezoeker kan een betrokkene zijn. Overleden personen of organisaties zijn geen betrokkenen volgens de AVG.

Data Protection Impact Assessment (DPIA): door middel van een DPIA worden de effecten en risico's van een nieuwe of bestaande gegevensverwerking op de bescherming van de persoonsgegevens beoordeeld.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar een persoon te herleiden is. In sommige gevallen kan het zijn dat een enkel gegeven geen persoonsgegeven is, maar door deze te combineren met andere gegevens dat dan wel weer is. Bijvoorbeeld een postcode in combinatie met een huisnummer.

Persoonsgegevens zijn bijvoorbeeld:

- Naam, adres, woonplaats (NAW)
- Geboortedatum en plaats
- Geslacht
- Contactgegevens; emailadres, telefoonnummer
- BSN
- Rekeningnummers

Bijzondere persoonsgegevens: Bijzondere persoonsgegevens persoonsgegevens die door hun aard bijzonder gevoelig zijn, en worden door de AVG extra beschermd. Het verwerken van bijzondere persoonsgegevens is in beginsel verboden. Bijzondere persoonsgegevens gaan bijvoorbeeld over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, de gezondheid, iemands seksueel gedrag of seksuele gerichtheid, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon.

Voor strafrechtelijke persoonsgegevens gelden onder de AVG specifieke eisen.

Datalek: Een beveiligingsincident waarbij het gaat om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens, zonder dat dit de bedoeling is van de organisatie.

Doeleinden van een verwerking: elke verwerking is gebonden aan een specifiek doel. Dit doel moet ook rechtmatig zijn. Dat wil zeggen: vastgelegd per wet.

Grondslag: Elke verwerking moet een rechtmatige grondslag hebben. De grondslagen zijn in de AVG geregeld en vallen uiteen in de volgende categorieën: algemeen belang/openbaar gezag; wettelijke verplichting; vitaal belang; overeenkomst; ander gerechtvaardigd belang; toestemming (enkel vereist als geen andere grondslag van toepassing is).

Ketensamenwerking: Wanneer de verwerkingsverantwoordelijke samen met anderen doel en middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van gezamenlijke verantwoordelijkheid.

Privacyverklaring: een verklaring om betrokkenen te informeren over wat er met persoonsgegevens wordt gedaan en waarom.

***Privacy by design*:** tijdens de ontwikkelingen van producten /diensten wordt aandacht besteed aan privacy verhogende maatregelen.

***Privacy by default*:** onderdeel van privacy by design, helpt privacy van betrokkenen te beschermen door instellingen en functies van bijvoorbeeld diensten standaard op de meest privacyvriendelijke stand te zetten.

Proceseigenaar: clustermanager verantwoordelijk voor de uitvoering van de taken, processen en levering van producten binnen zijn cluster.

Register van verwerkingen: Register waarin alle verwerkingsactiviteiten worden bijgehouden.

Verwerking: alles wat je met een persoonsgegeven doet, zoals verzamelen, vastleggen, bewaren, vernietigen, verstrekken aan een ander, bij elkaar voegen, etc.

Verwerker: een externe organisatie die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de gemeente. De verwerker staat nooit onder het rechtstreekse gezag van één van de bestuursorganen, heeft nooit zeggenschap over de gegevens (hij mag bijvoorbeeld niet de bewaartermijnen bepalen) en mag alleen handelen onder de schriftelijke instructies van de gemeente, bijvoorbeeld als dat in een verwerkersovereenkomst is bepaald.

Verwerkersovereenkomst: Overeenkomst waarin schriftelijke afspraken worden gemaakt tussen verwerkingsverantwoordelijke en verwerker. Deze afspraken gaan over hoe om wordt gegaan met persoonsgegevens en informatieveiligheid. Door VNG Realisatie is een Standaard model Verwerkersovereenkomst voor Gemeenten opgesteld, die vanaf 2020 (verplicht) door alle gemeenten wordt gebruikt. Deze overeenkomst is afgestemd op de, eveneens door de VNG opgestelde, Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).

Indien één van de bestuursorganen, als verwerker optreedt, dan dient de gemeente zelf deze verplichtingen op te volgen.

Verwerkingsverantwoordelijke: een persoon of instantie die alleen of samen met een ander het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is in de gemeentelijke organisatie een bestuursorgaan, zoals het College van B&W, de Burgemeester, de gemeenteraad of de Commissie Bezwaar en Beroep. Zie verder ook onder het eerste deel van dit beleid.

3. Hoe gaan we met persoonsgegevens om?

In dit deel worden de uitgangspunten bij het verwerken van persoonsgegevens beschreven, aan de hand van de verschillende artikelen vanuit de AVG.

3.1 Wettelijk kader

Voor de bescherming van persoonsgegevens gelden de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Daarnaast is de verwerking van persoonsgegevens geregeld in diverse andere wet- en regelgeving. Bijvoorbeeld de Gemeentewet, Wet maatschappelijke ondersteuning 2015, Jeugdwet, Participatiewet, Wet Suwi, Wet Basisregistraties personen, Wet en besluit justitiële en strafvorderlijke gegevens, Telecommunicatiewet, Wet tijdelijk huisverbod, Algemene wet bestuursrecht, Wet open overheid, Wet hergebruik overheidsinformatie, Archiefwet 1995 en het ministerieel besluit Informatiebeveiliging Overheid.

3.2 Verwerken persoonsgegevens

De gemeente verwerkt ter uitvoering van de aan haar opgedragen publieke taken persoonsgegevens in de volgende domeinen:

- Dienstverlening;
- Inclusieve samenleving;
- Leefbaarheid

In het domein Dienstverlening gaat het bijvoorbeeld om gegevens uit de basisregistratie personen (naam, adres, woonplaats, Burgerservicenummer). In het domein Inclusieve samenleving gaat het onder andere om gegevens bij het casusoverleg jeugd en alle eventueel gevoelige persoonsgegevens die daarbij koen kijken. In het domein Leefbaarheid gaat het tenslotte om onder meer naam, adres, woonplaats gegevens bij verstrekte vergunningen en meldingen openbare ruimte, maar ook om opsporingsgegevens.

Naast de domeinen zijn er units. De meeste aangelegenheden die organisatie-breed moeten worden opgepakt, zijn belegd bij de units. Te denken valt aan personeelszaken, met de daarbij behorende gegevens zoals sollicitatiegegevens en gegevens over ziekte en arbeidsongeschiktheid.

Welke persoonsgegevens precies worden verwerkt per verwerking, is vastgelegd in ons verwerkingsregister. Deze is zowel intern als extern raadpleegbaar, waarbij de interne versie meer categorieën toont dan de externe versie.

3.3 Uitgangspunten bij het verwerken van persoonsgegevens (artikel 5 AVG)

Iedereen die binnen de gemeente werkzaam is, dient verantwoord om te gaan met de bescherming van persoonsgegevens. In artikel 5 AVG worden een aantal principes voor de verwerking van persoonsgegevens genoemd. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes:

a) Rechtmatigheid, behoorlijkheid en transparantie

De gemeente verwerkt alleen persoonsgegevens als er een grondslag uit de AVG is aan te wijzen en op een behoorlijke en zorgvuldige wijze. De verwerking moet in verhouding staan tot het doel en als het doel met een vergelijkbare inspanning bereikt kan worden met een minder zwaar middel, wordt er voor dat minder zware middel gekozen.

Er zijn zes grondslagen in artikel 6 AVG opgenomen:

- Toestemming
- Overeenkomst;
- Wettelijke verplichting
- Vitaal belang;
- Algemeen belang / openbaar gezag;
- Ander gerechtvaardigd belang.

De verwerking van bijzondere persoonsgegevens, zoals gegevens over gezondheid, is in principe verboden, tenzij er een uitzondering vanuit artikel 9 AVG van toepassing is, en er daarnaast een beroep kan worden gedaan op één van de uitzonderingsgronden die genoemd zijn in de Uitvoeringswet AVG.

In het register van verwerkingen heeft de gemeente voor elke verwerking vastgelegd welke grondslag van toepassing is.

b) Doelbinding

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De gemeente verwerkt persoonsgegevens alleen volgens vooraf bepaalde en precies omschreven doeleinden. Soms is een doel vastgelegd bij wet, zo staan er doelen en bijbehorende verwerkingen van persoonsgegevens beschreven in onder andere de Jeugdwet en de Participatiewet.

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 hier extra waarborgen voor zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt.

c) 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.

d) Juistheid

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn. Gegevens die dat niet (meer) zijn worden gewist of gecorrigeerd.

e) Opslagbeperking

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.

Als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid, waarbij persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk.

f) Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking, en handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid.

3.4 Informeren van betrokkenen (artikel 13 en 14 AVG)

De gemeente is open en transparant over hoe zij met persoonsgegevens omgaat. Dit betekent dat personen waarvan persoonsgegevens worden verwerkt worden geïnformeerd. Dit doet de gemeente via de algemene en specifieke privacy pagina op de website.

3.5 Rechten van de betrokkene (artikel 12 en 15-22 AVG)

Personen van wie persoonsgegevens worden verwerkt, ook wel betrokkenen genoemd, hebben diverse rechten om controle te houden over hun persoonsgegevens. Deze rechten zijn vastgelegd in de AVG. Het gaat om de volgende rechten:

- recht op inzage (artikel 15 AVG) (iedere betrokkene heeft het recht om de persoonsgegevens die van hem verzameld zijn in te zien);

- recht op rectificeren en aanvullen van persoonsgegevens (artikel 16 AVG) (iedere betrokkene heeft het recht om persoonsgegevens die van hem verwerkt worden aan te vullen of te rectificeren);

- recht op vergetelheid (gegevenswissing) (artikel 17 AVG) (onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten verwijderen);

- recht op beperking van de verwerking (artikel 18 AVG) (betrokkenen hebben in bepaalde situaties de mogelijkheid om de verwerking van hun persoonsgegevens tijdelijk 'stil te laten zetten');

- recht op dataportabiliteit (overdraagbaarheid van de gegevens) (artikel 20 AVG) (geeft de betrokkene het recht om een kopie te krijgen van de persoonsgegevens, zodat deze meegenomen kunnen worden naar bijvoorbeeld een andere aanbieder);

- recht op bezwaar tegen de verwerking (artikel 21 AVG) (een betrokkene kan onder omstandigheden bezwaar maken tegen de (verdere) verwerking van zijn gegevens);

- recht niet te worden onderworpen aan geautomatiseerde besluitvorming / profilering (artikel 22 AVG) (betrokkenen hebben in bepaalde situaties het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking -waaronder profilering- gebaseerd besluit).

Om een beroep te kunnen doen op een van deze rechten kunnen betrokkenen een verzoek indienen, dit kan onder meer via de website. Het afhandelen van dergelijke verzoeken vindt plaats volgens de daartoe aangewezen procedures, en is doorgaans gratis.

Daarnaast heeft de betrokkene recht op contact met de Functionaris Gegevensbescherming (FG) (artikel 37 AVG) en recht om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens (AP) (artikel 77 AVG).

3.6 Data Protection Impact Assessment (artikel 35 AVG)

Voorafgaande aan verwerkingen die waarschijnlijk een hoog privacyrisico opleveren, moet een Data protection impact assessment (hierna: DPIA) worden uitgevoerd. De DPIA is een instrument om inzicht te geven in de risico's die verwerkingen van persoonsgegevens met zich meebrengen voor betrokkenen, zodat maatregelen getroffen kunnen worden om de risico's te mitigeren. In de AVG is vastgesteld in welke gevallen er in ieder geval sprake is van een hoog privacyrisico. Daarnaast is er door de AP een lijst met hoog risico verwerkingen opgesteld én is er door de Europese privacytoezichthouders een lijst met criteria voor hoog risico verwerkingen opgesteld.

Een aantal voorbeelden waarbij sprake is of kan zijn van een hoog risico verwerking:

- er is sprake van beoordeling vanuit persoonskenmerken -zoals profilering- waarop besluiten worden gebaseerd;
- er is sprake van stelselmatige en grootschalige monitoring;
- er worden gegevens van kwetsbare personen verwerkt;
- er wordt gebruik gemaakt van nieuwe technologieën;
- er worden op grote schaal bijzondere persoonsgegevens verwerkt;
- er is sprake van heimelijk onderzoek;

- er is sprake van verwerkingen over strafrechtelijke veroordelingen en strafbare feiten, bijvoorbeeld zwarte lijsten.

De hoog risico verwerkingen en de criteria voor hoog risico verwerkingen zijn onderdeel van de zogenaamde Checklist privacy. De Checklist privacy moet worden uitgevoerd in een vroegtijdig stadium, en afhankelijk van de uitkomst moet vervolgens al dan niet een DPIA worden uitgevoerd door of namens de proceseigenaar van de verwerking.

De resultaten van de DPIA worden afgestemd met de Privacy Officer, en aan de FG/CISO en TISO voorgelegd. Indien de proceseigenaar niet of onvoldoende maatregelen treft om (hoge) risico's te mitigeren, kan de FG nadrukkelijk adviseren om hiervan melding te maken bij de AP, en bij niet-opvolging van dit advies kan de FG besluiten om zelfstandig een signaal af te geven aan de AP.

Het uitvoeren van een DPIA vindt plaats volgens de DPIA-procedure.

3.7 Ketensamenwerking (artikel 26 AVG)

Van een ketensamenwerking is sprake wanneer de verwerkingsverantwoordelijke samen met andere verwerkingsverantwoordelijken een verwerking uitvoert, waarbij de verwerkingsverantwoordelijken samen het doel en middelen van een verwerking bepalen. Bijvoorbeeld in een samenwerkingsverband. Er kan dan sprake zijn van een gezamenlijke verantwoordelijkheid. Vanwege de juridische complexiteit dienen in geval van ketensamenwerking onderling duidelijke afspraken te worden gemaakt over de wijze waarop wordt voldaan aan de AVG. Bij het starten van een nieuwe samenwerking wordt de Privacy Officer betrokken voor advies.

3.8 Doorgifte (artikel 44-49 AVG)

Gegevens worden in beginsel alleen binnen de EER verwerkt. Indien een (sub)verwerker buiten de EER gevestigd is, moet er voldaan worden aan alle eisen van doorgifte vanuit de AVG. Doorgifte buiten de EER is alleen mogelijk wanneer de Europese Commissie heeft besloten dat het gegevensbeschermingsniveau in dat andere land adequaat is. Wanneer daar geen sprake van is, dan is verstrekking mogelijk op grond van bijvoorbeeld standaard contractbepalingen of kan het gelegitimeerd worden door bindende bedrijfsvoorschriften.

3.9 Register van verwerkingen (artikel 30 AVG)

De gemeente houdt een register van verwerkingen bij. In het register wordt onder andere de volgende informatie opgenomen:

- omschrijving van de verwerking;
- welke persoonsgegevens er worden verwerkt;
- de wettelijke grondslag van de verwerking;
- wie de verwerkingsverantwoordelijke is;
- betrokken verwerkers en subverwerkers.

- welke beheersmaatregelen er zijn genomen om persoonsgegevens te beschermen.

Wijzigingen en gestaakte verwerkingen worden met het oog op de bewijslast gearchiveerd.

Het register van verwerkingen wordt bijgehouden volgens een daartoe aangewezen procedure.

3.10 Verwerkersovereenkomsten (artikel 28 AVG)

Daar waar persoonsgegevens worden verwerkt door derden sluiten wij te allen tijde een verwerkersovereenkomst af. Bijvoorbeeld met Cloudleveranciers, of partijen aan wie de gemeente werkzaamheden uitbesteed.

In een verwerkersovereenkomst wordt vastgelegd hoe de verwerker met persoonsgegevens moet omgaan. Bijvoorbeeld welke persoonsgegevens worden er verwerkt, voor welk doel, voor welke duur, onder welke beveiligingsmaatregelen en wat er ná de verwerking met de persoonsgegevens moet gebeuren. Zo wordt gewaarborgd dat persoonsgegevens op de juiste wijze verwerkt en beveiligd worden.

De gemeente gebruikt uitsluitend de standaard verwerkersovereenkomst van die door de Vereniging van Nederlandse Gemeenten (VNG) beschikbaar is gesteld. De Privacy Officer wordt betrokken bij het aangaan van verwerkersovereenkomsten.

3.11 Datalekken (artikel 4, 33 en 34 AVG)

Bij een datalek, in de zin van de AVG, is sprake van een inbreuk op de beveiliging, waarbij persoonsgegevens betrokken zijn. Hieronder valt onder andere een dergelijke inbreuk welke leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens.

Er kan ook sprake zijn van een inbreuk op de beveiliging waarbij geen persoonsgegevens betrokken zijn. Er is dan niet sprake van een datalek in de zin van de AVG, en dergelijke beveiligingsincidenten vallen buiten de kaders van dit privacybeleid.

Voorbeelden van datalekken:

- een brief of mail met persoonsgegevens wordt aan een verkeerde ontvangere gestuurd, bijvoorbeeld door verkeerde adressering of door het stoppen van 2 brieven in 1 envelop;
- het verlies van een map met daarin een papieren klantdossier
- het verlies van een usb stick met niet-versleutelde persoonsgegevens
- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt of onbeschikbaar gemaakt.

Afhankelijk van de ernst van het datalek, wordt deze al dan niet aan de AP en aan de betrokkene gemeld. Bij de beoordeling van de ernst van het datalek zijn de FG, CISO en / of PO betrokken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen deze direct te melden. Het melden en het afhandelen van datalekken vindt plaats volgens de procedure datalekken en er wordt een registratie van alle incidenten en datalekken bijgehouden in een register.

3.12 Awareness

Om het onderwerp ‘privacy’ goed levend te houden binnen de gemeente is het noodzakelijk om het bewustzijn van privacy binnen de gemeentelijke organisatie voortdurend aan te scherpen. In dit kader zijn er verschillende activiteiten, zo worden medewerkers aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via Nano learnings, en er zijn binnen de clusters en units privacy contactpersonen.

4. Gemeentelijke organisatie

Dit deel van het privacybeleid beschrijft de rollen, taken en verantwoordelijkheden met betrekking tot het beschermen van persoonsgegevens.

4.1 Controlerend: Gemeenteraad

De gemeenteraad ziet er op toe (controleert) dat het college overkoepelend beleid ten aanzien van bescherming van persoonsgegevens voor de organisatie vaststelt en uitvoert. Dit is onder meer het jaarlijkse verslag van de Functionaris Gegevensbescherming (FG), dat door het college wordt verstrekt.

4.2 Eindverantwoordelijk: College van B&W

Het college is eindverantwoordelijk voor zorgvuldigheid van verwerking van persoonsgegevens, en stelt het privacybeleid vast. Het college:

- is verantwoordelijk voor een duidelijk privacybeleid;
- doet aan de gemeenteraad voorstellen over in te zetten middelen;
- stelt specifieke regelingen en procedures vast;
- controleert het management van de organisatieonderdelen op de maatregelen die verband houden met de bescherming van persoonsgegevens.

Het college heeft een portefeuillehouder aangewezen die namens het college de beleidsvoering waarborgt. Daarnaast legt deze (politieke) verantwoording af over de privacy beleidsvoering aan de gemeenteraad.

4.3 Aansturing: Gemeentesecretaris /directie

De uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De gemeentesecretaris is de Algemeen directeur, de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur aan het college. Hij of zij vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk.

De Algemeen directeur is samen met de directie verantwoordelijk voor de uitvoering van het privacybeleid en stuurt op (concern) risico’s. Daarnaast zorgen zij voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

4.4 Uitvoering: Clustermanagers / units

De zorgvuldige omgang van verwerkingen vallen onder de clustermanagers/Units (proceseigenaar) binnen de verschillende clusters en Units. Dat betekent dat zij zelf moeten zorgdragen over het nakomen van de naleving van het privacybeleid binnen hun cluster/Unit, en dit dienen te waarborgen in de werkprocessen. In dat kader zijn zij verantwoordelijk voor voldoende bewustwording van privacy, en kennis van het privacybeleid. Periodiek worden centraal bewustzijnscampagnes georganiseerd.

De clustermanager/vertegenwoordiger van de Unit stuurt onder meer aan op:

- risico-gestuurd werken. Hiervoor wordt gebruik gemaakt van de vastgestelde modellen van de Data Protection Impact Assessments (DPIA's);
- naleving van principes van *privacy by design* en *privacy by default*;
- het hanteren van daartoe vastgestelde procesplannen en formats, zoals de DPIA en de (door de VNG vastgestelde) verwerkersovereenkomst;
- het melden van datalekken volgens de daartoe beschikbare procedure;
- het opnemen van nieuwe verwerkingen en gewijzigde verwerkingen in het register van verwerkingsactiviteiten;
- het meewerken en/of faciliteren van meewerken aan het afhandelen van de rechten van betrokkene;
- het maken van schriftelijke afspraken bij risicovolle verwerkingen en verwerkingen bij ketensamenwerking (verwerkingen in een samenwerkingsverband);
- het bijstaan van de uitvoering door professionals op het gebied van privacy en informatieveiligheid waar nodig;
- het bekend maken van dit beleid bij de medewerkers.

4.5 Uitvoering: Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn ervoor verantwoordelijk dat zorgvuldig wordt omgegaan met persoonsgegevens. Dat betekent dat iedereen, binnen de kaders van zijn taak, zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Indien er twijfel bestaat of aan deze beginselen uitvoering wordt gegeven kan er met een aantal personen worden geschakeld: de clustermanager, een van de privacy contacpersonen, de Privacy Officer, de FG en de CISO.

4.6 Ondersteuning en advies

Om de clusters/Units te ondersteunen bij vraagstukken omtrent de bescherming van persoonsgegevens en de directie te ondersteunen bij de uitvoering van het privacybeleid, zijn de volgende professionals belast:

4.6.1 Privacy Officer (PO)

Operationeel: de Privacy Officer (PO) is als specialist op het gebied van de AVG eerste aanspreekpunt van de gemeente rondom privacygerelateerde vraagstukken, en adviseert en ondersteunt vanuit de tweede-lijn bij vraagstukken omtrent de bescherming van persoonsgegevens. Gevraagd en ongevraagd adviseert de PO over activiteiten ter bescherming van persoonsgegevens, onder andere bij DPIA's, datalekken, het register van verwerkingen, verwerkersovereenkomsten en bij vragen vanuit de vakafdelingen. Verder is de PO betrokken bij het creëren van awareness met betrekking tot privacy onder de medewerkers.

Tactisch / strategisch: de PO is op tactisch en strategisch niveau betrokken bij privacy-gerelateerde zaken, zoals privacygovernance, procedures / werkinstructies, het privacybeleid, beleidsnotities, jaarplannen en roadmap.

Verder is de PO de verbindende schakel tussen de organisatie en de FG.

4.6.2 Technical Information Security Officer (TISO) en Changemanager

De TISO is verantwoordelijk voor het inrichten, uitvoeren en testen van het technische informatiebeveiligingsbeleid en vormt de verbinding tussen de CISO en de beheerorganisatie. De rol als Changemanager is verantwoordelijk voor het changemanagementproces en de juiste besluitvorming aangaande het doorvoeren van wijzigingen in de informatievoorziening en infrastructuur.

4.6.3 Chief Information Security Officer (CISO)

De CISO heeft ondersteunende en adviserende rol met betrekking tot privacy in de organisatie. Op het gebied van informatiebeveiliging heeft hij een controlerende en toezichthoudende taak. Informatiebeveiliging maakt een wezenlijk onderdeel uit van de bescherming van persoonsgegevens. Hij adviseert voornamelijk bij nieuwe applicaties en het beheersen van risico’s.

4.6.4 Juridische Zaken

Bij de meeste (complexe) privacyvraagstukken is ook juridische ondersteuning noodzakelijk, vanwege kennis van de AVG, ook in relatie tot overige wetgeving. Daarnaast kan juridische ondersteuning noodzakelijk zijn bij de afhandeling van inzageverzoeken of bij datalekken waar schade is ontstaan en waar juridische vertegenwoordiging in gerechtelijke procedures nodig is. Waar nodig zoekt de PO samenwerking met Juridische Zaken op.

4.6.5 Privacy Contactpersonen

Onder meer om de zelfredzaamheid en de awareness van de units en clusters op het gebied van privacy en informatiebeveiliging te verhogen zijn er, per cluster en unit, privacy contactpersonen worden aangesteld. De privacy contactpersoon functioneert als eerste aanspreekpunt binnen de verschillende clusters / units waar de contactpersoon werkzaam is, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. Ook kan de privacy contactpersoon verwijzen naar de juiste medewerker (zoals de PO, de FG of de CISO) voor verder advies.

5. Toezicht, controle en evaluatie

Om het privacybeleid binnen de gemeentelijke organisatie te borgen, is het van belang dat hier toezicht en controle op plaatsvindt. Bij niet naleving kunnen er gevolgen (zoals sancties) volgen. Daarnaast moet het privacybeleid periodiek geëvalueerd worden. Hoe toezicht, controle en evaluatie plaatsvindt, is in dit deel van het privacybeleid beschreven.

5.1 Privacy en security administratie

Er is een privacy en security administratie op basis waarvan de gemeente de naleving van wetgeving kan aantonen (artikel 5.2 AVG, de verantwoordingsplicht/accountability). De gemeente verantwoordt zich over hoe zij omgaat met Privacy, wat haar beleid is en verantwoordt zich achteraf over de uitvoering van dit beleid.

5.2 Functionaris Gegevensbescherming

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.

Dit houdt onder meer in dat de FG:

- de organisatie informeert en adviseert over de werking van de AVG, overige wetgeving en het beleid;
- toezicht houdt op de naleving van het privacybeleid en achterliggende wettelijke verplichtingen;
- privacy-klachten tot een goed einde helpt te brengen (ombudsfunctie);
- bij privacy-incidenten adviseert over ernst en omvang;
- toeziet op het beheer van het register van verwerkingen conform artikel 30 AVG;
- de naleving van afspraken door de gemeente en ketenpartners controleert, eventueel ook in samenwerking met auditors;
- helpt het privacybeleid uit te dragen en bewustzijn te creëren bij interne en externe doelgroepen;
- de contactpersoon is voor landelijke toezichthouders – zoals de AP.

De FG krijgt de ruimte voor professionele uitvoering van taken. Dat betekent dat de FG:

- naar behoren en tijdig wordt betrokken bij aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens.
- volledig wordt geïnformeerd over aspecten van de bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.

Het college, directie 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.

Minimaal één keer per jaar brengt de FG verslag uit over zijn werkzaamheden, bevindingen en aanbevelingen aan de directie en het college.

5.3 Planning en Control

Het privacybeleid en de naleving daarvan volgt het patroon van de gebruikelijke P&C-cyclus binnen de gemeente. Dit betekent het volgende: het start met het opstellen en vaststellen van privacybeleid, de belangrijke voornemens worden eventueel in de begroting meegenomen en uiteindelijk is het dan onderdeel van het jaarverslag en jaarrekening in het kader van de verantwoordingsfunctie (maatschappelijke verantwoording). In de loop van het jaar en na afloop van het jaar vindt een periodieke evaluatie van het beleid plaats. De uitkomsten van die evaluatie leiden zo nodig tot aanpassing van het beleid.

5.4 Controller

Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie, zo ook op het gebied van privacy. De controller rapporteert -in het geval van bijzonderheden- aan de directie over de naleving van wet- en regelgeving en het privacybeleid, richtlijnen en processen. Daarnaast heeft de controller een belangrijke signaalfunctie om te kijken wat er speelt op het gebied van gegevensbescherming op de werkvloer, en schakelt indien nodig met de CISO, de FG en / of de Privacy Officer. Dit om de uitvoeringsverantwoordelijkheid binnen de gemeentelijke organisatie op diverse plekken te waarborgen.

5.5 Naleving en sancties

Het niet-naleven van hetgeen opgenomen is in dit privacybeleid of in de onderliggende documentatie zoals opgenomen in bijlage 2, kan negatieve gevolgen hebben voor betrokkenen (o.a. inwoners en medewerkers van de gemeente Katwijk) én voor de gemeente Katwijk als organisatie. Iedere medewerker heeft daarom waar het gaat om gegevensbescherming een belangrijke verantwoordelijkheid, afgestemd op de eigen functie. Bij ernstige tekortkoming op dit gebied kan, binnen de wettelijke kaders en de kaders van de CAO, een sanctie worden opgelegd.

5.6 Verhouding tot en verantwoording aan de gemeenteraad

Jaarlijks legt het college verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot informatiebeveiligingsbeleid, via de paragraaf bedrijfsvoering in de jaarstukken. De gemeenteraad controleert vervolgens het college door middel van de verantwoordingsrapportages.

In de verantwoording in de jaarstukken komen in elk geval de volgende onderwerpen aan de orde:

- realisatie en uitvoering privacybeleid en integratie wettelijke eisen AVG in de werkprocessen;
- inventarisatie en implementatie per afdeling van de risico-inventarisatie (afgenomen DPIA’s),

- stand van zaken met betrekking tot het verwerkingsregister, conform artikel 30 AVG;
- activiteiten die hebben plaatsgevonden op bewustwording en training;
- aard, omvang en afhandeling van eventuele klachten van de betrokkene;
- aard, omvang en afhandeling van (vermoedelijke) datalekken.

5.7 Evaluatie privacybeleid

Dit privacybeleid wordt na vier jaar indien nodig herzien. Dat zal zijn eind 2026. Indien nodig wordt het privacybeleid tussentijds herzien.

Proceseigenaren doen periodiek verslag binnen de gemeentelijke vastgestelde P&C-cyclus over de naleving van dit beleid
, waaronder oplossingen en incidenten die zich hebben voorgedaan.

Het college van B&W (college) legt over de privacy beleidsvoering (politieke) verantwoording af aan de gemeenteraad en is transparant over de verwerkingen van persoonsgegevens naar betrokkenen.

De gemeente draagt zorg voor de documentatie van beleid en maatregelen, zodat het op ieder moment voor een ieder inzichtelijk en transparant is, en het maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak (aantoonbaarheid).

De Functionaris Gegevensbescherming (FG) doet jaarlijks rechtstreeks verslag aan het college en geeft aanbevelingen die strekken tot verdere optimalisering van de privacy beleidsvoering. Het college besluit over bijsturen van dit beleid met inachtneming van de aanbevelingen van de FG.

Bijlage 1[3]: overzicht met onderliggende / ondersteunende documentatie

Er zijn diverse procedures, richtlijnen, beleidsstukken, werkafspraakdocumenten etc. die een meer gedetailleerde invulling geven op verschillende onderwerpen. Deze bijlage geeft een overzicht van deze onderliggende danwel ondersteunende documentatie (deze bijlage gaat niet over de inhoud van de documentatie)

Onderwerp + hoofdstuk in privacybeleid	**documentnaam**	**vindplaats**	**Eventuele toelichting**
Anonimiseren	Anonimiseringsrichtlijn	Intranet	
Burgerparticipatie	Beleid Burgerparticipatie en privacy	Intranet	
Camerabeelden	Privacyreglement cameratoezicht	Intranet	
Datalek	Datalekprocedure	ntb	Nog maken
Datalek	Datalekregistratie	ntb	Nog maken
Datalekmelding	datalekmeldingsformulier	Intranet	
DPIA	DPIA format	Intranet	
DPIA	DPIA overzicht	MS Teams, groep Privacy	
DPIA	DPIA procedure	ntb	
DPIA	Privacy checklist	Intranet	
Gedragscode medewerkers	Gedragscode ambtenaren Gedragscode raadsleden Gedragscode college	Intranet	
MS Teams	Veilig samenwerken in MS Teams	Intranet	
Privacybeleid	privacybeleid	Website gemeente Katwijk Intranet	
Privacy contactpersonen	Memo privacy contactpersonen	O-schijf privacy	
Privacy reglement	Privacyreglement	Website gemeente Katwijk	
Privacyverklaring medewerkers	Privacyverklaring medewerkers	Intranet	
Rechten van betrokkenen	Procedure rechten van betrokkenen	O-schijf privacy	
Social media	Reglement gebruik social media	ntb	Nog maken
Training / awareness (nieuwe) medewerkers	Awarenessprogramma	ntb	Nog maken
Toestemming gebruik beeldmateriaal	Procedure toestemming gebruik beeldmateriaal	ntb	Nog maken
Uitwisselen gegevens	Procedure uitwisselen gegevens	ntb	Nog maken
Uitwisselen gegevens: doorgifte buiten EU/EER	Stroomschema doorgifte buiten EU/EER	ntb	Nog maken
Uitwisselen gegevens: veilig mailen (intern én extern)	Stroomschema of reglement veilig mailen	ntb	Er zal ook een functionaliteit in outlook hiervoor komen, maar stroomschema/toelichting is alsnog nuttig
Verwerkersovereenkomsten	Overzicht verwerkersovereenkomsten	ntb	Navragen Inkoop
Verwerkersovereenkomsten	Rol privacy-organisatie	ntb	Nog maken / afstemmen met inkoop
Verwerkingsregister	Procedure aanpassen verwerkingsregister	ntb	Nog maken

[3] Verwacht wordt dat bijlage 1 geregeld aanpassing zal behoeven, eventuele aanpassingen zullen daarom in mandaat door de Privacy Officer gedaan worden, en niet door het college.

Verwerkingsregister	Verwerkingsregister	Website gemeente Katwijk Intranet	
Wachtwoord	Wachtwoordbeleid	ntb	Ntb of dat onder privacy valt, of misschien meer onder IB