GEMEENTE ZUNDERT

# GEMEENTEBLAD

Officiële uitgave van de gemeente Zundert

Nr. 62807

14 februari 2023

## Privacyreglement gemeente Zundert 2023-2026

Het college van burgemeester en wethouders van de gemeente Zundert;

gelezen het bepaalde in art. 24 lid 2 van Algemene verordening gegevensbescherming

overwegende dat artikel 24 lid 1 van de Algemene verordening gegevensbescherming een periodieke beleidsevaluatie en -actualisering veronderstelt

**besluit:**

1. Vast te stellen de beleidsregel "Privacyreglement gemeente Zundert 2023-2026"

### Hoofdstuk 1 Inhoudelijke bepalingen

### Artikel 1 Inleiding

Privacy speelt een belangrijke rol in de relatie tussen de gemeente Zundert en haar inwoners en medewerkers en verdient daarom bijzondere aandacht. De Nederlandse gemeenten beschikken over veel persoonsgegevens en zijn verplicht daar zorgvuldig, veilig, vertrouwelijk en proportioneel mee om te gaan. Het is een dagelijks terugkerende verantwoordelijkheid voor alle gemeentelijke medewerkers. Dat is geen eenvoudige taak want het beschermen van persoonsgegevens wordt steeds complexer door bijvoorbeeld technologische ontwikkelingen, samenwerkingsverbanden, cybercriminaliteit en nieuwe wetgeving.

De gemeente Zundert vindt het belangrijk om een open en betrouwbare overheid te zijn die in direct contact staat met haar inwoners. Bescherming van persoonsgegevens is een belangrijk onderwerp dat voldoende aandacht krijgt binnen alle lagen van de gemeentelijke organisatie, gemeenteraad, college van B&W, directie en medewerkers.

In het “Privacybeleid Gemeente Zundert 2023-2026” wordt generiek en op hoofdlijnen beschreven hoe de gemeente Zundert aantoonbaar op een goede manier omgaat met persoonsgegevens. De verdere uitwerking daarvan vindt plaats in dit Privacyreglement. In het privacybeleid is beschreven welke uitgangspunten, kernwaarden en ambities wij hanteren en welke belangenafwegingen wij maken. In het privacyreglement staat dat specifieker uitgewerkt.

Er is bewust gekozen voor een kort en bondig privacybeleid met een operationele uitwerking in het privacyreglement. Het privacyreglement kan daardoor eenvoudiger een leidraad zijn voor de medewerkers van de gemeente Zundert. Het voorkomt bovendien dat het privacybeleid té dynamisch wordt en een te korte houdbaarheid heeft.

De Algemene verordening gegevensbescherming (hierna Avg) is het centrale wettelijke kader. Alle inhoudelijke keuzes passen binnen de verplichtingen uit de Avg.

Naast het privacybeleid en het privacyreglement wordt de privacyorganisatie afzonderlijk beschreven in de privacygovernance en is de privacyverklaring (of -belofte) de laagdrempelige vertaling naar de inwoners toe. Deze vier documenten vormen tezamen het gemeentelijk privacybeleid.

Zowel het geformuleerde privacybeleid als -reglement zijn van toepassing op de verwerking van persoons- én politiegegevens door de gemeente Zundert.

### Artikel 2 Leeswijzer

Dit privacyreglement is een uitwerking van het privacybeleid. In het privacybeleid wordt beschreven hoe de gemeente op hoofdlijnen invulling geeft aan de privacy-uitgangspunten en de verplichtingen die de Algemene verordening gegevensbescherming (hierna: Avg) met zich meebrengt. In het privacyreglement worden de hoofdlijnen verder uitgewerkt in hanteerbare richtlijnen.

Het privacybeleid en -reglement vormen tezamen met de privacygovernance en de privacyverklaring één kader voor de omgang met persoonsgegevens in de organisatie.

Dit reglement begint met een beschrijving van de achtergrond van het document, het wettelijk kader, en met een verklaring en definiëring van gebruikte privacytermen, gevolgd door de scope van het reglement en een beschrijving van de verwerkingsverantwoordelijken.

In het privacybeleid worden de drie uitgangspunten benoemd waarop het beleid is gefundeerd: rechtmatigheid, behoorlijkheid en transparantie. In artikel 7 van dit privacyreglement worden de uitgangspunten verder uitgewerkt.

De Avg kent vele verplichtingen toe aan verwerkingsverantwoordelijken. Hoe in de gemeente Zundert invulling wordt gegeven aan deze verplichtingen staat in de artikel 8 tot en met 22. Behalve de verplichte nummers bevat dit reglement ook de ambities van de gemeentelijke organisatie. Hoe bij het waarmaken van de ambities de Avg gehanteerd wordt staat beschreven in de artikelen 23 tot en met 33.

Zoals in de inleiding reeds benoemd, zijn het gemeentelijk privacybeleid en -reglement niet alleen van toepassing op persoonsgegevens maar ook op politiegegevens. Aan politiegegevens is artikel 34 gewijd. Hiermee wordt tevens voldaan aan dwingende aanbevelingen die een gevolg zijn van de externe Wpg-audit.

Dit privacyreglement beschrijft hoe de gemeente Zundert invulling geeft aan de wettelijke verplichtingen en het waarmaken van de ambities. Het is primair bestemd voor de interne organisatie. Iedere medewerker hoort het privacybeleid en -reglement toe te passen bij de dagelijkse routine. Het privacyreglement is geschreven vanuit het perspectief van de gemeente Zundert. Als gesproken wordt over ‘de gemeente’, ‘ons’ of ‘wij’ dan heeft dat altijd betrekking op de gemeente Zundert.

## Artikel 3 Wettelijk kader

Het wettelijk kader voor de bescherming van persoonsgegevens bestaat voornamelijk uit de Europese algemene verordening gegevensbescherming en de Nederlandse uitvoeringswet, de Uavg. Het wettelijk kader voor de verwerking van politiegegevens is de Wet politiegegevens, de Wpg.

Daarnaast is er veel materiele wetgeving dat van belang is bij de bescherming van persoonsgegevens. Daarbij kan bijvoorbeeld gedacht worden aan de Wet basisregistratie personen, de Wet maatschappelijke ondersteuning, de Jeugdwet, de Archiefwet en de Wet algemene bepalingen burgerservicenummer.

Alle relevante wettelijke regelgeving en normen betrekken wij bij de belangenafwegingen en het hanteren van de privacy-uitgangspunten uit het privacybeleid.

## Artikel 4 Definities

In dit privacyreglement worden de volgende definities gehanteerd:

***Algemene verordening gegevensbescherming ( Avg )***
Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens). In het Engels de General Data Protection Regulation (GDPR).

***Betrokkene***
De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt, bijvoorbeeld een inwoner, ondernemer, medewerker of contactpersoon van een (keten)partner.

***Datalek***
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (Avg artikel 4 lid 12).

***Functionaris Gegevensbescherming (FG)***
Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Avg en de Wpg.

***Persoonsgegevens***
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (Avg artikel 4 lid 1). Gegevens die herleidbaar zijn tot een individueel persoon. De identiteit moet redelijkerwijs, zonder onevenredige inspanning kunnen worden vastgesteld. Denk hierbij aan naam, adres, geboortedatum. Naast deze “gewone” persoonsgegevens kent de Avg ook bijzondere persoonsgegevens. Deze gegevens gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeur of gezondheid.

***Politiegegevens***

Persoonsgegevens die in het kader van een politietaak worden verwerkt. Een gemeentelijke BOA kan beëdigd zijn om politietaken te verrichten en politiegegevens te verwerken. Daar waar in dit document persoonsgegevens staat worden ook politiegegevens bedoeld.

***Risicoanalyse informatiebeveiliging en privacy (IB&P)***
Dit wordt ook wel een data protection impact assessment (DPIA) of een gegevensbeschermings-effectbeoordeling (GEB) genoemd maar deze termen worden in Zundert zo min mogelijk gebruikt. Het is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te nemen om de risico's te verkleinen of weg te halen. Een risicoanalyse IB&P is verplicht als een gegevensverwerking een waarschijnlijk hoog privacyrisico oplevert voor de betrokkenen.

***Verwerken***
Alles wat je met persoonsgegevens kan doen: "het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van persoonsgegevens."

***Verwerker***
De organisatie of persoon die, in opdracht en ten behoeve van de verwerkingsverantwoordelijke, bepaalde onderdelen van of de gehele verwerking van persoonsgegevens voor zijn rekening neemt.

***Verwerkersovereenkomst***
Een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke.

***Verwerkingsverantwoordelijke***
De organisatie, bestuursorgaan of persoon die bepaalt waarom de verwerking van persoonsgegevens plaatsvindt en die vaststelt met welke middelen dat gebeurt.

***Wet politiegegevens***
De Wet politiegegevens (2020) regelt de rechten en de plichten van de politie, maar ook die van de burger, voor wat betreft het verwerken van politiegegevens. De rechten van betrokkenen zijn onder de Wpg anders dan onder de Avg.

## Artikel 5 Reikwijdte
Dit privacyreglement is van toepassing op alle verwerkingen van persoons- en politiegegevens door alle bestuursorganen van de gemeente, medewerkers van de gemeente, of ingehuurd personeel werkend in opdracht van de gemeente Zundert. Met andere woorden: voor alle verwerkingen van persoons- en politiegegevens die binnen de gemeente of in opdracht van de gemeente plaatsvinden.

## Artikel 6 Verwerkingsverantwoordelijken
De verschillende bestuursorganen van de gemeente Zundert zijn verwerkingsverantwoordelijk voor de verwerkingen die door of namens de gemeente uitgevoerd worden. De belangrijkste bestuursorganen zijn:
- De gemeenteraad
- Het college van burgemeester en wethouders
- De burgemeester

Voor de verwerking van politiegegevens is uitsluitend het college, als werkgever van de BOA's, het verwerkingsverantwoordelijke bestuursorgaan.

Verwerkingsverantwoordelijken bepalen het doel en de middelen van de verwerking van persoonsgegevens. Het doel: waarom worden persoonsgegevens verwerkt? De middelen: op welke wijze gebeurt dat?

## Artikel 7 Uitgangspunten uit het privacybeleid
### Rechtmatigheid
Wij gaan uit van de geldende wet- en regelgeving voor de verwerking van persoonsgegevens en hanteren de Avg en de Uavg als basis. Voor een verwerking van persoonsgegevens hebben wij altijd een geldige grondslag. Deze grondslag stellen wij vast voorafgaand aan de eerste verwerking van persoonsgegevens. De rechtmatigheid van de grondslag wordt getoetst.

Als wij persoonsgegevens vaker gebruiken, intern of extern verstrekken, delen of uitwisselen dan is het doel daarvan verenigbaar met de oorspronkelijke verzameldoeleinden (doelbinding). Het belang van doelbinding wordt zeker zo belangrijk als het om politiegegevens gaat. Als blijkt dat het niet vere-

nigbaar is dan wordt gekeken naar een rechtmatige grondslag. De privacy officer ondersteunt de organisatie daarbij. De FG adviseert en toetst.

Wij leggen alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking (het noodzakelijkheidsvereiste). Het kan zijn dat de wet het ons verplicht of om de belangen van betrokkenen te beschermen. Diverse gemeentelijke taken (algemeen belang/openbaar gezag) vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. In het verwerkingsregister wordt per verwerking concreet gemaakt op basis van welke grondslag en met welk doel verwerking van persoonsgegevens gerechtvaardigd is.

Bij de verwerking van persoonsgegevens wordt rekening gehouden met de beginselen van 'proportionaliteit' en 'subsidiariteit'. Wij vragen slechts díe persoonsgegevens die noodzakelijk zijn om het beoogde doel te bereiken (proportionaliteit). Daarbij gebruiken wij altijd de methode die de minste inbreuk maakt op de persoonlijke levenssfeer van de betrokkenen (subsidiariteit).

**Behoorlijkheid**
Wij hanteren het principe van 'minimale gegevensverwerking', ofwel 'dataminimalisatie'. Dat betekent dat er geen overbodige persoonsgegevens worden gevraagd voor het vastgestelde doel. Wij richten onze systemen en processen zodanig in dat niet te veel persoonsgegevens worden gevraagd. Het toepassen van 'dataminimalisatie' maakt deel uit van een continu proces van bewustwordingsacties.

Wij hanteren het beginsel van 'éénmalige vastlegging, meervoudig gebruik': persoonsgegevens die bekend zijn worden in principe niet opnieuw gevraagd. Wij maken zo veel mogelijk gebruik van brongegevens zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is slechts mogelijk als er een wettelijke grondslag en een verenigbaar doel is.

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is de gemeente gebonden aan archiefwettelijke bewaartermijnen. Wanneer de Archiefwet hier niet in voorziet staan de bewaartermijnen beschreven in het verwerkingsregister.
De gemeente Zundert bewaart persoonsgegevens in overeenstemming met de "Selectielijst gemeenten en intergemeentelijke organen 2020".

Persoonsgegevens worden vertrouwelijk behandeld. Het gemeentelijk autorisatiebeleid borgt dat functionarissen alleen toegang krijgen tot persoonsgegevens als zij hier een functioneel doel voor hebben en dit voor de directe taakuitvoering noodzakelijk is.
Met externen, samenwerkingspartners, verwerkers en leveranciers maken wij schriftelijke privacyafspraken, vastgelegd in overeenkomsten en convenanten.
Persoonsgegevens worden goed beveiligd opgeslagen zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. De Baseline informatiebeveiliging overheid (BIO) is daarvoor het gehanteerde normenkader. Door gebruik te maken van 'privacy door ontwerp' (privacy by design) wordt al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht geschonken aan privacyverhogende maatregelen.

Het is voor zowel de gemeente Zundert en haar (keten)partners als voor de burgers van belang dat persoonsgegevens actueel en correct zijn.

**Transparantie**
Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente Zundert over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website. Verder wordt per nieuwe verwerking van persoonsgegevens bekeken hoe de betrokkenen op een passende wijze geïnformeerd kunnen worden. Wij voldoen aan de informatieplicht onder de Avg.

Burgers hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens wij van hen verwerken, het recht van inzage. Wij verstrekken de gevraagde informatie binnen de gestelde termijn, tenzij de wet anders aangeeft. Verder kunnen burgers om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken, zie ook artikel 19. Deze verzoeken worden gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald.

Om recht te doen aan verzoeken van betrokkenen hebben wij een 'interne procedure rechten van betrokkenen' vastgesteld. Hierin is beschreven hoe verzoeken van betrokkenen door ons worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft.

Wij zijn transparant over het type persoonsgegevens dat wij voor een specifiek doel met anderen delen. Daarbij kan het zijn dat er een uitzondering is wanneer er belangen zijn, genoemd in wet- of regelgeving,

die zich daartegen verzetten. Het type persoonsgegeven wordt bijgehouden in het verwerkingsregister en is opvraagbaar.

Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan.

**Artikel 8 Het verwerkingsregister**
De gemeente Zundert heeft een verwerkingsregister, een overzicht van alle verwerkingen van persoonsgegevens die binnen de organisatie plaatsvinden en waarvoor de gemeente verwerkingsverantwoordelijk is. Het register is vormvrij. Zundert maakt voor het verwerkingsregister gebruik van een privacy managementsysteem (PMS). Het register is een middel om aantoonbaar te maken hoe de gemeente omgaat met persoonsgegevens. In het verwerkingsregister worden onder meer de volgende beschrijvende gegevens opgenomen:

a) Naam en contactgegevens van de FG en eventuele andere organisaties waarmee de gemeente Zundert gezamenlijk verwerkingsverantwoordelijk is (verplicht);
b) Het verwerkingsverantwoordelijke bestuursorgaan (verplicht);
c) Doelstelling van de verwerking van persoonsgegevens (verplicht);
d) Wettelijke grondslag voor de verwerking (verplicht);
e) De categorieën betrokkenen;
f) De categorieën persoonsgegevens die verwerkt worden (verplicht);
g) De ontvangers, met wie persoonsgegevens uitgewisseld worden (verplicht);
h) Of een verwerking ook in derde landen plaatsvindt (verplicht);
i) De getroffen technische en organisatorische beveiligingsmaatregelen (verplicht);
j) De ingeschakelde verwerkers en afgesloten verwerkersovereenkomsten;
k) De applicaties en informatiesystemen die bij de verwerking ingezet worden;
l) De herkomst van de persoonsgegevens die verwerkt worden;
m) Hoe aan de informatieplicht is voldaan;
n) De uitgevoerde risicoanalyses informatiebeveiliging en privacy.

De privacy officer beheert en onderhoudt het verwerkingsregister en de interne procedure. De FG controleert of het register juist volledig en actueel is. Uit oogpunt van transparantie wordt er toegewerkt naar het publiceren van een openbare samenvatting van het verwerkingsregister op de website met een periodieke update.

**Artikel 9 Data Protection Impact Assessment (DPIA)**
Zundert spreekt liever van een "risicoanalyse informatiebeveiliging en privacy" in plaats van de wettelijke Engelstalige afkorting uit de Avg. In feite geeft dát ook precies aan wat er gebeurt voorafgaande aan de start van een nieuwe verwerking van persoonsgegevens of bij de wijziging van een bestaande verwerking. Als bij de verwerking van persoonsgegevens een mogelijk hoog risico bestaat voor de privacy van de betrokkenen, dan inventariseren wij voorafgaande aan de eerste verwerking de risico's en voorzien ze van maatregelen om de risico's weg te nemen of te verkleinen.
Om de mogelijkheid van een hoog risico te bepalen voeren wij eerst een verkennend onderzoekje uit (een pré-DPIA of een DPIA-scan). De gemeente analyseert altijd vooraf de risico's als de verwerking voorkomt op de lijst van verplichte 'DPIA's' en de criteria van de AP. Er is een interne procedure opgesteld voor risicoanalyses informatiebeveiliging en privacy.

De risicoanalyse informatiebeveiliging en privacy wordt uitgevoerd door de medewerker die de nieuwe verwerking van persoonsgegevens gaat starten of de bestaande verwerking gaat wijzigen. Daarbij wordt de medewerker procedureel ondersteund en geadviseerd door de privacy officer. De privacy officer kan ook zelf het initiatief nemen voor een risicoanalyse. De risicoanalyse wordt getoetst door de FG die een advies over de maatregelen uitbrengt aan de verwerkingsverantwoordelijke.
Als blijkt dat er ondanks de maatregelen een hoog restrisico overblijft, dan leggen wij de voorgenomen verwerking voor aan de AP voor de zogenaamde "voorafgaande raadpleging". De gemeente start niet met een verwerking van persoonsgegevens voordat alle risico's zijn weggenomen of zijn teruggebracht tot een acceptabel niveau.

De privacy officer documenteert de risicoanalyses, plant en programmeert de analysecyclus (in het Programma risicoanalyses informatiebeveiliging en privacy) en onderhoudt de interne procedure.

**Artikel 10 Privacy by design & Privacy by default**
Vertaald: 'privacy door ontwerp' en 'privacy door standaardinstellingen'. Privacy door ontwerp en standaardinstellingen zijn randvoorwaardelijk voor alle informatiesystemen, al dan niet in eigen beheer. De gemeente hanteert actief deze twee principes op haar verwerkingen van persoons- én politiegegevens. Als passende maatregelen nog niet worden afgedwongen in systemen zorgen wij voor aanvullende organisatorische en/of technische maatregelen om dit alsnog te borgen.

Privacy door ontwerp houdt in dat wij er bij het ontwerpen van producten en diensten voor zorgen dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of de bouw van een systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische beveiligingsmaatregelen. Privacy wordt aan het begin van projecten en inkoopprocessen meegenomen. De privacy officer is betrokken in de voorfase van een project. De FG ziet er op toe dat dit ook gebeurt.

Privacy door standaardinstellingen houdt in dat wij werkprocessen inrichten en de standaardinstellingen van een programma instellen op de meest privacyvriendelijke manier. Zonder daarbij de functionaliteit, gebruiksvriendelijkheid, werkbaarheid, effectiviteit en efficiency uit het oog te verliezen. In de risicoanalyse (zoals beschreven in artikel 9) worden de voor privacy door ontwerp/standaardinstellingen noodzakelijke aspecten meegenomen in de voorgenomen verwerking. Op deze manier borgen wij dat nieuwe verwerkingen volgens de normen van privacy door ontwerp/standaardinstellingen worden ingericht.

De gemeente Zundert heeft daarnaast op het inkoopstartformulier waarborgen opgenomen om privacy door ontwerp/standaardinstellingen mee te nemen bij de inkoop en aanbesteding van producten en diensten. Bij de aanschaf van nieuwe, persoonsgegevens verwerkende informatiesystemen en applicaties wordt de systeemeisenset van de VNG/IBD actief door ons gebruikt.

**Artikel 11 Datalekken**

Een datalek is een inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens. Een datalek heeft potentieel een (grote) impact op de rechten en vrijheden van natuurlijke personen en op ons als organisatie. Volledig voorkómen van datalekken is een utopie. Wij creëren een laagdrempelige en veilige cultuur waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Desgewenst kan anoniem gemeld worden en veroorzakers van datalekken worden daarop niet afgerekend (no naming and shaming). De gemeente stelt alles in het werk om het datalek zo snel mogelijk te dichten en het zo nodig binnen 72 uur te melden bij de AP en/of de betrokkenen. Als dit niet haalbaar is in de tijd doet de gemeente een voorlopige melding bij de AP die later wordt aangevuld of ingetrokken. Het informeren van de betrokkenen doen wij op een eenvoudig en begrijpelijk taalniveau. Het voorkomen en melden van datalekken is met grote regelmaat onderwerp van onze bewustwordingsprogramma's.

De gemeente hanteert een 'Protocol Meldplicht Datalekken' dat door de directie is vastgesteld. Hierin staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij taken en verantwoordelijkheden hebben.

In dit protocol, dat in gelijke mate van toepassing is op politiegegevens, staat ook beschreven hoe en wanneer een datalek door ons wordt gemeld bij de AP en/of de betrokkenen. De gemeente heeft een datalekteam dat na de melding direct met de afhandeling van het datalek aan de slag gaat.

De gemeente houdt een register bij waarin alle datalekken en beveiligingsincidenten worden vastgelegd, inclusief de afhandeling en de evaluatie. Trends in incidenten worden gedetecteerd en kunnen leiden tot specifieke bewustwordingsacties en interne verbetering van werkprocessen en systemen. Dringende aanpassingen voeren wij direct door.

**Artikel 12 Bijzondere en strafrechtelijke persoonsgegevens**

Persoonsgegevens die door hun aard bijzonder gevoelig zijn, krijgen extra bescherming in de Avg. Verwerking van bijzondere persoonsgegevens is niet toegestaan, tenzij voldaan is aan in de Avg genoemde voorwaarden (Avg artikel 9) én er een rechtmatige verwerkingsgrondslag is.

Onder bijzondere persoonsgegevens vallen genetische en biometrische gegevens als deze herleidbaar zijn tot een persoon. Genetische persoonsgegevens geven unieke informatie over iemands fysiologie of gezondheid en/of over de gezondheid van familieleden, bijvoorbeeld een DNA-analyse. Biometrische persoonsgegevens geven unieke informatie over iemands fysieke, fysiologische of gedragsgerelateerde kenmerken, bijvoorbeeld vingerafdrukken.

De Avg ziet daarnaast de volgende gegevens als bijzondere persoonsgegevens:
- persoons- of politiegegevens waaruit ras of etnische afkomst blijkt;
- persoons- of politiegegevens waaruit politieke opvattingen blijken;
- persoons- of politiegegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- persoons- of politiegegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- gegevens over iemands gezondheid;
- gegevens over iemands seksueel gedrag of seksuele gerichtheid;

Strafrechtelijke gegevens zijn geen bijzondere persoonsgegevens maar voor de verwerking daarvan gelden wel specifieke eisen. Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken

hebben met strafrechtelijke veroordelingen en strafbare feiten of met veiligheidsmaatregelen die daarmee verband houden, zoals een door de rechter opgelegd verbod. Ook de verwerking van strafrechtelijke persoonsgegevens is niet toegestaan, tenzij één van de wettelijke uitzonderingen van toepassing is en er daarnaast een rechtmatige verwerkingsgrond is.

De eerste wettelijke uitzondering voor het verwerken van strafrechtelijke persoonsgegevens is dat de verwerking onder toezicht van de overheid staat. De tweede uitzondering is dat de verwerking is toegestaan bij nationaal recht (zie ook Uavg artikelen 32 en 33).

Een wettelijk identificatienummer zoals het burgerservicenummer (BSN) is een gevoelig maar geen bijzonder persoonsgegevens. Het BSN mag door overheidsorganen gebruikt worden om hun taak uit te voeren maar alleen als het daarvoor noodzakelijk is.

De gemeente Zundert respecteert het verbod op de verwerking van bijzondere en strafrechtelijke persoonsgegevens of kan aantoonbaar maken welke wettelijke voorwaarden, uitzonderingsgronden en grondslagen van toepassing zijn.

**Artikel 13 Functionaris Gegevensbescherming (FG)**
De gemeente Zundert is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Het is in dit geval een wettelijke verplichting om een FG aan te stellen. De gemeente Zundert heeft FG's aangewezen voor zowel de Avg als de Wpg.

De FG is een interne en onafhankelijke toezichthouder die actief door ons betrokken wordt bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG brengt gevraagd en ongevraagd advies uit op het gebied van de Avg. De FG voert jaarlijks een interne audit uit op grond van het normenkader uit het 'Avg Borgingsproduct' van de IBD en maakt een toezichtsplan. De FG rapporteert jaarlijks over de naleving van privacy wet- en regelgeving aan het college van B&W. De FG heeft de volgende wettelijke taken: informeren, adviseren, toezicht houden, bewustwording creëren en optreden als contactpersoon van de AP.

**Artikel 14 Beveiliging**
Gemiddeld zit iemand met zijn persoonsgegevens in honderden tot duizenden bestanden, zowel van het bedrijfsleven als van de overheid. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van gegevens.

Op grond van de Avg artikel 32 dienen organisaties passende technische en organisatorische maatregelen te nemen om de persoonsgegevens die zij verwerkt, te beveiligen.

De gemeente Zundert heeft strategisch en tactisch informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling wordt gegeven aan de passende maatregelen ter beveiliging van persoonsgegevens. De gemeente Zundert conformeert zich aan de Baseline Informatiebeveiliging Overheid. Dit normenkader wordt door ons actief toegepast op alle verwerkingen van persoonsgegevens. Wij hebben een Chief Information Security Officer (CISO) aangesteld die de passende maatregelen implementeert en een veilig gebruik van persoonsgegevens bevordert.

De gemeente Zundert gebruikt zoveel mogelijk moderne technieken om persoonsgegevens te beveiligen. Daar waar het mogelijk is, zorgen wij voor anonimisering, pseudonimisering of versleuteling van persoonsgegevens. Wij bouwen controlemechanismen in om de betrouwbaarheid van persoonsgegevens te garanderen en uitwijkmogelijkheden om de beschikbaarheid van persoonsgegevens bij een incident zo snel mogelijk te herstellen. Behalve technische maatregelen nemen wij ook organisatorische maatregelen om persoonsgegevens te beveiligen.
Zo hanteren wij het principe van 'roll based access' waarbij medewerkers slechts toegang krijgen tot die informatie die benodigd is voor het uitvoeren van de eigen taken. We hebben niet alleen logisch toegangsbeleid vastgesteld, maar ook testbeleid, logbeleid en back-up en recoverybeleid.

Om in een vroegtijdig stadium de verwerkingen van persoonsgegevens te voorzien van passende maatregelen wordt de CISO actief betrokken bij de risicoanalyses informatiebeveiliging en privacy (zie artikel 9).

Het passende technische en organisatorische beveiligingsniveau voor persoonsgegevens, dat wij onszelf opleggen, leggen wij ook op aan door ons ingeschakelde verwerkers. Daartoe maken wij schriftelijke afspraken in de verwerkersovereenkomst.

### Artikel 15 Gegevens delen met derden

Wanneer er sprake is van een eenmalige, structurele of gevoelige gegevensuitwisseling met derde partijen, maken wij afspraken over de gegevensuitwisseling.
Deze afspraken voldoen tenminste aan de Avg en andere relevante wetgeving en worden vastgelegd in een onderlinge regeling, een samenwerkingsovereenkomst (convenant), een gegevensuitwisselingsovereenkomst of een verwerkersovereenkomst.

Bij het intern en extern delen en uitwisselen van persoonsgegevens zorgen wij dat er een aantoonbare binding is met het oorspronkelijke doel. Politiegegevens worden slechts verwerkt en gedeeld voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn (Wpg artikel 3 lid 2).

De gemeente Zundert gebruikt landelijke standaarden en richtlijnen om de contractuele verplichtingen te regelen met derden. Wij hanteren het landelijk toegepaste en bindende model van de verwerkersovereenkomst van de VNG/IBD in een Zundertse lay-out, en de landelijke modellen van overeenkomsten tussen gezamenlijk en zelfstandig verwerkingsverantwoordelijken. Verwerkers en verwerkersovereenkomsten worden bijgehouden in het verwerkingsregister. De ondertekende versies van de verwerkersovereenkomsten worden door de medewerkers zelf gearchiveerd in het betreffende zaakdossier.

De gemeente Zundert geeft geen persoonsgegevens door aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is. In de volgende vier gevallen mogen persoonsgegevens doorgegeven worden aan een derde land buiten de EER:
- Met een adequaatheidsbesluit;
- Met passende waarborgen met een modelcontract (ook wel: Standard Contractual Clauses);
- Met binding corporate rules (BCR);
- Met specifieke uitzonderingen overeenkomstig Avg artikel 49.

### Artikel 16 Grondslag en doelstelling

Wij realiseren ons dat het gebruik van persoonsgegevens invloed kan hebben op de persoonlijke levenssfeer van betrokkenen. Daarom verwerken wij alleen persoonsgegevens als het echt niet anders kan, als wij zonder deze gegevens ons doel niet kunt bereiken.

Voorafgaand aan iedere verwerking van persoonsgegevens heeft de gemeente Zundert een rechtmatige grondslag en een doelstelling. Wij maken dit aantoonbaar in het verwerkingsregister.

De verwerking van persoonsgegevens is altijd gebaseerd op één van de zes grondslagen uit de Avg artikel 6. De motivatie voor het toepassen van de grondslag beschrijven wij in het verwerkingsregister. Bij een hoog risico verwerking beschrijven wij de grondslag ook in de risicoanalyse informatiebeveiliging en privacy (zie artikel 9). Als er geen rechtmatige grondslag is vindt de verwerking van persoonsgegevens geen doorgang.

Wij beschrijven het doel wat wij met de verwerking van persoonsgegevens voor ogen hebben voorafgaand aan de eerste verwerking en leggen dit vast in het verwerkingsregister. De doelstelling kan in een wet benoemd zijn. Iedere afzonderlijke verwerking van persoonsgegevens (bijvoorbeeld registreren, bewaren, uitwisselen) moet onder de doelbeschrijving vallen. De gemeente beschrijft de doelstelling to-the-point en niet te ruim; de vlag dekt de lading (Avg artikel 5). De doelstelling bepaalt eveneens de bewaartermijn van de persoonsgegevens en iedere uitwisseling van persoonsgegevens, zowel intern als extern, heeft een binding of is verenigbaar met dit doel.

Tezamen met de Avg-grondslag vormt de doelbeschrijving de rechtsgrond voor het mogen verwerken van persoonsgegevens. Wij informeren tijdig de betrokkenen over op grond van welke wettelijke grondslag en doelstelling wij hun persoonsgegevens verwerken (zie ook artikel 20).

### Artikel 17 Toestemming als grondslag

Toestemming van de betrokkene is één van de zes grondslagen uit de Avg waarop een verwerking van persoonsgegevens gebaseerd mag worden. Aan het gebruik van deze grondslag zijn vier vereisten verbonden:
- Vrijelijk gegeven, betrokkenen voelen zich vrij om al dan niet toestemming te geven;
- Ondubbelzinnig, er moet sprake zijn van een duidelijke actieve handeling;
- Geïnformeerd, betrokkenen moeten vooraf geïnformeerd worden in voor hen begrijpelijke taal;
- Specifiek, toestemming wordt gegeven voor een specifiek doel dat niet kan veranderen.

Burgers en medewerkers staan als betrokkenen vaak in een afhankelijkheidsrelatie met de gemeente als overheid of werkgever. Toestemming kan dan niet vrijelijk gegeven worden. Daarom is de gemeente Zundert zeer terughoudend in het gebruik van toestemming als grondslag.

Als de grondslag toestemming gebruikt wordt dan kunnen wij aantoonbaar maken dat aan de vier vereisten is voldaan. Daartoe leggen wij de gemaakte afwegingen vast in het register van verwerkingen. Betrokkenen kunnen te allen tijde hun toestemming intrekken. Wij zorgen er voor dat de toestemming op een laagdrempelige manier ingetrokken kan worden en geven aan het verzoek direct gehoor. De intrekking van toestemming geldt niet met terugwerkende kracht.

Aan kinderen onder de 16 jaar vragen wij toestemming aan hun wettelijk vertegenwoordigers.

**Artikel 18 Subsidiariteit, proportionaliteit en dataminimalisatie**
Voorafgaand aan de start beoordelen wij iedere verwerking van persoonsgegevens op de principes subsidiariteit en proportionaliteit. De uitwerking daarvan nemen wij op in de risicoanalyse informatiebeveiliging en privacy en/of in het verwerkingsregister.

Het subsidiariteitsprincipe komt neer op de vraag of wij het doel ook op een andere wijze kunnen bereiken waarbij de impact op de privacy van de betrokkenen minder groot is. Zo ja, dan zullen wij altijd voor die andere wijze kiezen.
Dat is passend bij ons uitgangspunt ‘rechtmatigheid’ uit het privacybeleid en zoals beschreven in artikel 7. Wij streven naar het zo min mogelijk schaden van de privacy van de betrokkenen.

Het proportionaliteitsbeginsel komt neer op de vraag of het doel van de verwerking in verhouding staat tot de inbreuk op de privacy van de betrokkenen. Dit betekent bijvoorbeeld dat wij persoonsgegevens niet langer bewaren dan noodzakelijk is voor het beschreven doel en dat persoonsgegevens alleen toegankelijk zijn voor de medewerkers die dat nodig hebben voor de uitvoering van hun eigen taken. Als met de verwerking van persoonsgegevens het doel niet bereikt wordt, is de verwerking disproportioneel. Dit houden wij in de gaten.

Daarnaast passen wij het beginsel van minimale gegevensverwerking toe. Persoonsgegevens die wij verwerken zijn voor het doel toereikend en ter zake dienend. Er worden niet meer en niet minder persoonsgegevens verwerkt dan noodzakelijk is.

**Artikel 19 Rechten van betrokkenen**
De Avg bepaalt niet alleen de plichten van verwerkingsverantwoordelijke bestuursorganen die persoonsgegevens verwerken maar ook de rechten van personen van wie persoonsgegevens verwerkt worden. Deze rechten worden “rechten van betrokkenen” genoemd en zijn bedoeld om controle te kunnen houden op de eigen persoonsgegevens. De gemeente Zundert geeft betrokkenen alle ruimte om van hun rechten gebruik te maken. Het gaat om de volgende rechten:

- Recht op informatie. Het recht om geïnformeerd te worden als de gemeente persoonsgegevens gaat verwerken, zie ook artikel 20.
- Recht op inzage. Het recht om in te zien welke persoonsgegevens de gemeente verwerkt, met welk doel en of de gegevens correct zijn.
- Recht op rectificatie. Het recht om onjuiste gegevens te laten wijzigen.
- Recht op vergetelheid. Het recht om persoonsgegevens te laten verwijderen of vernietigen.
- Recht op intrekking toestemming. Het recht om eens gegeven toestemming voor het verwerken van persoonsgegevens op elk moment in te trekken, zonder opgaaf van redenen.
- Recht op bezwaar. Het recht om bezwaar te maken tegen de verwerking van persoonsgegevens.
- Recht op beperking van de verwerking. Het recht om minder gegevens te laten verwerken.
- Recht op dataportabiliteit. Het recht op het overdragen van persoonsgegevens aan een andere partij.
- Het recht op menselijke interventie. Het recht op een menselijke blik bij besluiten in het kader van geautomatiseerde besluitvorming en profilering, zie ook artikel 22.

De Wpg heeft een eigen regime met betrekking tot de rechten van betrokkenen uitgewerkt in paragraaf 4. Betrokkenen hebben op basis van de Wpg recht op informatie, verstrekking van informatie, inzage, rectificatie en wissing. De gemeente Zundert beantwoordt ontvangen verzoeken binnen de door de Wpg gestelde termijnen en richtlijnen en draagt zorg voor een deugdelijke identificatie van de verzoeker. Een ontvangen verzoek wordt getoetst aan de voorwaarden van de Wpg.

Wij zorgen er door middel van bewustwording voor dat de rechten van betrokkenen genoegzaam bekend zijn bij alle medewerkers en wij hebben een interne procedure om op ontvangen verzoeken binnen 1 maand te kunnen beschikken. Wij zorgen voor laagdrempelige manieren om verzoeken schriftelijk en

mondeling te kunnen indienen. Op onze website en in onze privacyverklaring informeren wij betrokkenen over hun rechten en hoe zij eenvoudig een verzoek kunnen doen. Wij brengen in principe geen kosten in rekening. Wij stellen op een deugdelijke manier de identiteit van de verzoeker vast zodat wij geen informatie aan de verkeerde personen verstrekken. Als identificatie nodig is doen wij dat aan de hand van DigiD, een gewaarmerkte kopie ID, of persoonlijke identificatie. Betrokkenen kunnen alleen een beroep doen op hun rechten voor zover het de eigen persoonsgegevens betreft of die van hun minderjarige kinderen over wie zij het ouderlijk gezag uitoefenen, of via een geïdentificeerde vertegenwoordiger. Een beschikking op een verzoek is een beschikking in de zin van de Algemene wet bestuursrecht waartegen bezwaarmogelijkheden open staan.

Wij beseffen dat gehoor geven aan betrokkenen die een beroep doen op hun privacyrechten een belangrijk onderdeel is van een gezond privacybeleid en dat het bijdraagt aan het vertrouwen in de gemeente.

**Artikel 20 Informatieplicht**
De betrokkenen hebben van tevoren recht op heldere en voor hen begrijpelijke informatie over wat wij als gemeente met hun persoonsgegevens gaan doen zodat zij zelf kunnen beslissen of zij dat willen. Ook als betrokkenen verplicht zijn om persoonsgegevens af te staan, hebben zij recht op informatie.

Wij verstrekken voorafgaand aan het verwerken van persoonsgegevens minimaal informatie aan betrokkenen over welke persoonsgegevens wij verwerken, voor welk specifiek doel, aan wie wij eventueel de persoonsgegevens doorgeven en waarom en contactgegevens voor het stellen van vragen en het indienen van klachten of bezwaren.

Om aan de informatieplicht te voldoen publiceren wij een privacyverklaring online op onze website. Deze privacyverklaring is kort, duidelijk en voor iedereen begrijpelijk. Per verwerking bekijken wij hoe wij de informatieplicht het beste kunnen invullen. Dat kan bijvoorbeeld ook door het toevoegen van teksten aan folders of formulieren.

**Artikel 21 Bewaartermijnen**
De Avg geeft geen bewaartermijnen voor persoonsgegevens. De gemeente bepaalt zelf hoe lang persoonsgegevens bewaard worden. Daarbij hanteren wij het uitgangspunt dat persoonsgegevens niet langer bewaard worden dan dat zij noodzakelijk zijn voor het bereiken van de doelstelling waarvoor zij verzameld of ontvangen zijn.

Wij houden ons aan wetgeving die wel richtlijnen geeft voor het bewaren van persoonsgegevens zoals fiscale wetgeving en de Archiefwet.

Op grond van artikel 3 van de Archiefwet is de gemeente verplicht “de onder haar berustende archiefbescheiden in goede, geordende en toegankelijk staat te brengen en te bewaren, alsmede zorg te dragen voor een tijdige vernietiging van daarvoor in aanmerking komende archiefbescheiden (met of zonder persoonsgegevens)”. De gemeente houdt zich aan de termijnen van de zogenaamde ‘selectielijst’ voor de gemeentelijke overheid. Als archiefbescheiden met persoonsgegevens blijvend bewaard worden, treffen wij zo nodig maatregelen voor beperking van de openbaarheid.
Wij borgen zoveel mogelijk een tijdige vernietiging of verwijdering van persoonsgegevens na het verstrijken van de bepaalde bewaartermijn. Gedurende de bewaring van persoonsgegevens zorgen wij voor een passend niveau van beveiliging en treffen wij daarvoor technische en organisatorische maatregelen.

Een van de doelen van archivering is om de gemeente in staat te stellen zich over een bepaalde periode te verantwoorden over haar handelen en besluitvorming. Archivering wordt in de Avg beschouwd als een verdere verwerking van persoonsgegevens die doelgebonden (artikel 5 lid 1b) is.

De van toepassing zijnde bewaartermijn leggen wij voorafgaand aan de eerste verwerking van persoonsgegevens vast bij de risicoanalyse informatiebeveiliging en privacy en in het verwerkingsregister. In het kader van de informatieplicht zullen wij zoveel mogelijk transparant zijn over de gehanteerde bewaartermijn.

**Artikel 22 Profilering en geautomatiseerde besluitvorming**
Betrokkenen hebben het recht op menselijke interventie, zie ook artikel 19, het recht op een menselijke blik bij de geautomatiseerde individuele besluitvorming (Avg artikel 22).
Van geautomatiseerde besluitvorming is sprake als er uitsluitend met technologische middelen een besluit wordt genomen zonder menselijke inmenging met rechtsgevolgen voor de betrokkenen, zoals het geautomatiseerd beoordelen van sollicitaties. Profilering is een geautomatiseerde verwerking van persoonsgegevens voor het evalueren van persoonlijke aspecten (profiel), met name om zaken over

natuurlijke personen te categoriseren, evalueren of te voorspellen, zoals iemands gedrag, prestatie, gezondheid of financiële situatie.

De gemeente Zundert is uiterst terughoudend in de toepassing van geautomatiseerde besluitvorming en profilering. Ten aanzien van politiegegevens zijn besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerkingen verboden; er is altijd menselijke besluitvorming nodig. Wij zijn ons bewust van de technologische mogelijkheden van data-analyse en kunstmatige intelligentie, zie artikelen 24 en 25, maar ook van de privacyrisico's die daaraan verbonden zijn. Wij nemen geen geautomatiseerde besluiten op basis van profielen als daaraan rechtsgevolgen voor de betrokkenen verbonden zijn of als het besluit de betrokkenen in aanmerkelijke mate treft, tenzij:
- Het noodzakelijk is voor de uitvoering van een overeenkomst met de betrokkene;
- Het is toegestaan op basis van Europees of Nederlands recht;
- Het berust op uitdrukkelijke toestemming van de betrokkene en specifiek voor de geautomatiseerde besluitvorming/profilering.

Wij waken voor omzeiling van het recht op menselijke interventie. Menselijke inmenging betekent een daadwerkelijke invloed op het resultaat.
Bij de afwegingen voorafgaande aan geautomatiseerde besluitvorming en profilering worden de richtsnoeren van de 'Groep gegevensbescherming artikel 29' en de jurisprudentie toegepast.

Wij betrekken geautomatiseerde besluitvorming en profilering bij de risicoanalyse informatiebeveiliging en privacy. We leggen de soort verwerking van persoonsgegevens vast in het verwerkingsregister en leggen de afwegingen aantoonbaar vast.

### Artikel 23 Ambitie en bewegingsvrijheid
De wereld staat niet stil. Technologische ontwikkelingen hebben ongekende mogelijkheden. De gemeente beschikt over veel data waaronder veel persoonsgegevens. Binnen de kaders van de wetgeving en de benoemde uitgangspunten bestaat er voor de gemeente ruimte om te bewegen. Bijvoorbeeld om gebruik te maken van nieuwe technologieën en ontwikkelingen. Hierna worden er een aantal beschreven die binnen de kaders van de geldende wet- en regelgeving en de ethiek toegepast kunnen worden.

### Artikel 24 Datagedreven werken en big data
De gemeente Zundert beschikt over veel gegevens van haar inwoners en haar medewerkers waaronder ook persoonsgegevens. Veel data die slim gebruikt kan worden om (strategische) doelstellingen en resultaten te behalen. De gemeente Zundert zal de privacy van de betrokkenen en ethische afwegingen altijd betrekken bij het datagedreven werken met persoonsgegevens en het verzamelen van big data. Met big data wordt het verzamelen van grote gestructureerde en ongestructureerde gegevens uit meerdere bronnen bedoeld.

Wij zorgen er voor dat datagedreven werken voldoet aan het noodzakelijkheidsvereiste uit de Avg. Hoewel dat lastig en complex kan zijn, onderwerpen wij iedere verzameling van persoonsgegevens aan de toets op doelbinding, het verenigbaar zijn met het oorspronkelijke doel.
Voor datagedreven werken voeren wij standaard een risicoanalyse informatiebeveiliging en privacy uit als er bijzondere persoonsgegevens bij betrokken zijn. Verder voldoen wij aan de criteria die gelden voor een verplichte risicoanalyse, zie ook artikel 9, en hanteren wij randvoorwaarden voor datagedreven werken. Bij het verwerken van grote hoeveelheden persoonsgegevens passen wij het concept van privacy door ontwerp (privacy by design) toe, zie ook artikel 10, en schenken wij naast doelbinding voldoende aandacht aan dataminimalisatie en transparantie.

Vanuit de ethiek zien wij datagedreven werken als middel, niet als doel op zich. Datagedreven werken staat altijd ten dienste van de mens, onze inwoner of medewerker. Ook als de privacywet- en regelgeving geen belemmering vormt voor datagedreven werken, stellen wij ons altijd de vraag: "moeten wij dit wel willen?". Wij experimenteren niet met persoonsgegevens, voelen de morele verplichting om daar zorgvuldig mee om te gaan en realiseren ons dat wij het vertrouwen van de inwoner in de gemeente niet mogen schaden. De ethische afweging maken wij onderbouwd en aantoonbaar.

### Artikel 25 Artificial intelligence en algoritmen
Artificial intelligence (AI of kunstmatige intelligentie) is het vermogen van computers om taken uit te voeren waarvoor mensen hun intelligentie inzetten, bijvoorbeeld: redeneren, analyseren, voorspellen en problemen oplossen. AI bestaat uit twee delen: algoritmen en gegevens. Een algoritme is het recept of het stappenplan voor AI, een reeks instructies die leidt tot een bepaald resultaat. Het zijn technische termen die zich het beste laten uitleggen aan de hand van praktische voorbeelden van AI:
- Het analyseren van ons kijk- en luistergedrag op basis waarvan Netflix of Spotify ons aanbevelingen doen;

- Het gebruik van Siri en beeldherkenning op de mobiele telefoon;
- Schaakcomputers.

Binnen de context van dit privacyreglement gaat het hier uitsluitend om het gebruik van persoonsgegevens bij artificial intelligence en algoritmen. De gemeenten Zundert zal bij de inzet van AI en algoritmen de gevaren ervan bewaken zoals het gevaar op oneerlijke, bevoordeelde of discriminatoire uitkomsten, het onnodig verwerken van te veel persoonsgegevens en het ontstaan van een zogenaamde 'black box' bij het verlies van de menselijke autonomie, waarbij betrokkenen geen zicht meer hebben op wat er met hun persoonsgegevens gebeurt. Ook ten aanzien van de inzet van AI en algoritmen hanteren wij de uitgangspunten rechtmatigheid, behoorlijkheid en transparantie, zie artikel 7, en zijn de rechten van betrokkenen van toepassing, zie artikel 19.

Op het gebruik van persoonsgegevens bij AI en algoritmen passen wij privacy door ontwerp (privacy by design) toe en testen wij vooraf de werking van de algoritmen ter voorkoming van de hiervoor vermelde gevaren. Als de verwerking van persoonsgegevens bij AI en algoritmen een mogelijk hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voeren wij daarnaast eerst een risicoanalyse informatiebeveiliging en privacy uit. Indien nodig vragen wij een 'voorafgaande raadpleging' aan bij de AP. Belangrijke besluiten laten wij in principe niet zonder menselijke tussenkomst door algoritmen nemen.

### Artikel 26 WiFi-tracking en monitoring van de openbare ruimte

Met WiFi-tracking wordt de techniek bedoeld om WiFi- of Bluetooth-signalen van mobiele devices in de openbare ruimte te lokaliseren, op te slaan en te verwerken. Hier worden geen vaste camera's bedoeld. Op deze manier zijn grote groepen mensen in kaart te brengen en te tellen, bijvoorbeeld bij grote evenementen. Zo kan achterhaald worden waar het op een bepaald moment te druk wordt, omleidingen ingesteld moeten worden of waar extra hulpdiensten of personeel ingezet moet worden, crowdcontrol. Als naast anonieme locatiegegevens ook persoonsgegevens verwerkt worden, is de Avg van toepassing. Ook als persoonsgegevens versleuteld (gepseudonimiseerd) worden verwerkt of bewaard. Een IP-adres is in combinatie met andere persoonsgegevens herleidbaar naar een natuurlijke persoon.

WiFi-tracking, sensoren en andere technische middelen ter monitoring van de openbare ruimte voldoen maar zelden aan de strikte voorwaarden die er voor gelden. Vaak is er geen goede rechtsgrond en zijn er minder ingrijpende methoden voorhanden. Het is een grote vrijheid om je in de openbare ruimte onbespied te weten. De gemeente Zundert gaat daarom uiterst terughoudend om met monitoring van de openbare ruimte.

Wij zijn ons terdege bewust van de grote risico's en eventuele sancties bij onzorgvuldigheid. Als de gemeente over gaat tot monitoring van de openbare ruimte (of een pilot), dan geschiedt dat zeer zorgvuldig en worden tenminste de volgende stappen doorlopen:

1. Bepaal of er persoonsgegevens verwerkt worden en of de verwerking rechtmatig (doelstelling en grondslag) is;
2. Stel vast wat de vervolgstappen zijn als de toepassing niet slaagt of als ongewenste neveneffecten optreden;
3. Voer een voorafgaande risicoanalyse informatiebeveiliging en privacy (DPIA) uit, zie artikel 9;
4. Stel beleid en principes vast voor de inzet van sensoren en monitoring van de openbare ruimte die voldoen aan de Avg en betrek daar ethische afwegingen en burgerbelangen bij. Werk deze uit in concrete werkinstructies.;
5. Informeer de gemeenteraad of neem de raad mee in de besluitvorming;
6. Mobility as a Service (MaaS). Neem bij het opstellen van het programma van eisen bij de aanbesteding, of de voorwaarden die gelden bij een vergunning, expliciet eisen op ten aanzien van de verwerking van persoonsgegevens. Stel periodiek vast of er aan de overeengekomen eisen wordt voldaan, en of de eisen zelf nog in lijn zijn met de Avg. Maak schriftelijke privacyafspraken bijvoorbeeld in de vorm van een verwerkersovereenkomst.

### Artikel 27 Cookies

Cookies zijn kleine bestanden die bij internetgebruik in de browser op de computer van een websitebezoeker worden geplaatst. Cookies worden lokaal opgeslagen en kunnen gemakkelijk bekeken en verwijderd worden. Als cookies gebruikers kunnen identificeren dan zijn het persoonsgegevens en is de Avg van toepassing. Op het plaatsen van cookies is ook de Telecommunicatiewet van toepassing, artikel 11.7A. Zogenaamde tracking cookies volgen internetgebruikers en houden bij welke internetpagina's bezocht worden. Op deze wijze kan een interesse- en voorkeurenprofiel opgebouwd worden, zie artikel 22.

De gemeente Zundert gebruikt slechts functionele en analytische (statistische) cookies om haar website goed en veilig te laten functioneren en om het gebruik van de website te meten. Daarbij worden geen persoonsgegevens vastgelegd.
Wij verzamelen de gebruiksgegevens van de website zelf en delen de gegevens niet met derden. Wij vragen eerst toestemming en plaatsen daarna pas de cookies. De toestemming kan geweigerd worden. De gemeente gebruikt de 'opt-in-functie' en geen 'cookiewall' (een cookiewall voorkomt vrijelijke toestemming doordat internetgebruikers geen toegang krijgen tot een website als zij toestemming weigeren voor het plaatsen van cookies). De meetgegevens worden gebruikt om de dienstverlening te verbeteren. Wij slaan de IP-adressen automatisch geanonimiseerd op. Bekeken webpagina's zijn niet te koppelen aan bepaalde IP-adressen. Wij bewaren cookies niet langer dan strikt noodzakelijk is.
Wij respecteren de "do-not-track-functie" van browsers. Als deze functie is ingeschakeld worden geen gebruiksgegevens opgeslagen.
Wij gebruiken geen tracking cookies, ook niet van andere partijen en waken er voor dat tracking cookies 'embedded' op de website worden geplaatst, bijvoorbeeld met een YouTube-link. Op onze website informeren wij bezoekers in begrijpelijke taal over het cookiegebruik.

De gemeente Zundert plaatst op haar website links naar haar social mediakanalen maar heeft geen invloed op het gebruik van cookies door de social mediaproviders.

**Artikel 28 Samenwerkingsverbanden en ketensamenwerking**
De gemeente Zundert werkt veel samen in de regio West-Brabant. Er zijn verschillende samenwerkingsverbanden met andere overheden, organisaties en marktpartijen waarbij gemeentelijke taken en verwerkingen van persoonsgegevens buiten de deur worden gezet en worden uitbesteed. Bij het aangaan van samenwerkingsverbanden, gemeenschappelijke regelingen en ketensamenwerking besteden wij aandacht aan het maken van goede privacyafspraken met onze partners en leggen deze schriftelijk vast in convenanten en servicelevel agreements.

Onze bestuurders nemen daarbij de juiste grondhouding aan en nemen het onderwerp privacy mee in de besluitvorming. Wij zijn ons ervan bewust dat het mandateren of delegeren van bevoegdheden en verantwoordelijkheden niet automatisch betekent dat er geen verwerkingsverantwoordelijkheid bestaat. Onze bestuurders zetten zich in om de verwerking van (persoons)gegevens goed te organiseren zonder daarbij de focus op het doel van de samenwerking te verliezen. Wij toetsen de samenwerking eveneens aan onze uitgangspunten rechtmatigheid, behoorlijkheid en transparantie.

**Artikel 29 Social media en chatdiensten**
De gemeente Zundert onderhoudt verschillende social media-accounts zoals Facebook, Twitter, Instagram en LinkedIn. Daarnaast maken medewerkers van de gemeente Zundert gebruik van verschillende chatdiensten zoals SMS, WhatsApp, Signal en iMessenger. Tevens staan medewerkers hulpmiddelen ten dienste zoals WeTransfer en Dropbox. Wij zijn ons er terdege van bewust dat veel van deze media en hulpmiddelen privacyrisico's inhouden.

Om die reden zullen medewerkers van de gemeente Zundert zich weerhouden van het gebruik van persoonsgegevens bij de inzet van social media, chatdiensten en internettools, met inbegrip van naar individuen herleidbaar beeld- en geluidmateriaal.

**Artikel 30 Nieuwe technologieën**
Ook de gemeente Zundert omarmt de vooruitgang waarbij de mens centraal staat. De technologie moet de mens immers blijven dienen. Als de technologische ontwikkelingen snel gaan is het belangrijk dat het wel verantwoord blijft. Met alleen maar goede bedoelingen komen we in een tijdperk van cybercriminaliteit niet meer weg.
Om innovatieve technologische oplossingen compliant aan de Avg te ontwikkelen dient in een vroegtijdig stadium over privacyvraagstukken nagedacht te worden. Dat is uiteraard geen taak voor de gemeente, de gemeente past alleen nieuwe technologieën toe.

Bij nieuwe technologieën moet, naast AI zie artikel 25, bijvoorbeeld gedacht worden aan blockchaintechnologie (veilige transacties tussen partijen), automatische nummerplaatherkenning, quantum computing, biometrie (vingerafdruk, gezichtsherkenning), nieuwe tools voor tijd- plaats- en apparaatonafhankelijk werken enzovoorts.
Niet alle nieuwe technologieën zijn al in ontwikkeling. En wat de toekomst brengt is onvoorspelbaar. Een totaal nieuwe oplossing kan zich plotseling aandienen.

Als de gemeente Zundert overweegt nieuwe technologieën toe te passen bij de verwerking van persoonsgegevens dan geschiedt dat op een verantwoorde wijze. Wij passen de uitgangspunten toe, zie artikel 7, en zorgen voorafgaand voor een risicoanalyse bij een verwacht hoog privacyrisico voor de betrokken.

**Artikel 31 Discriminatie en etnisch profileren**
Bij de verwerking van persoonsgegevens waakt de gemeente Zundert voor vooroordelen, discriminatie en etnische profileren, zie ook artikel 22. Er wordt geen onderscheid gemaakt tussen mensen op basis van ras en etniciteit, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gezondheid, seksueel gedrag of seksuele gerichtheid of andere kenmerken. Wij gaan op een integere wijze om met de vele (bijzondere) persoonsgegevens waarover wij beschikken zoals nationaliteit en geboorteplaats. Met name bij verwerkingen van persoonsgegevens waarbij discriminatie en etnisch profileren op de loer ligt zoals bij de opsporing van fraude, datagedreven werken en gebruik van algoritmes. Wij houden ons aan de principes van dataminimalisatie, het noodzakelijkheidsvereiste en de beperkingen ten aanzien van het verwerken van bijzondere persoonsgegevens. Wij misbruiken onze wettelijke bevoegdheden niet en maken ethische afwegingen. Door te voldoen aan onze verantwoordingsplicht kunnen wij aantoonbaar maken in hoeverre onderscheidende kenmerken zoals etniciteit een rol hebben gespeeld bij de besluitvorming.

**Artikel 32 Volgen en controleren personeel**
De gemeente Zundert mag onder voorwaarden als werkgever haar werknemers volgen en controleren. Daarbij zal de gemeente Zundert zoveel mogelijk rekening houden met de privacy van haar werknemers en de eisen die de Avg stelt. Voor heimelijke controle gelden strengere voorwaarden. In dat geval is er altijd sprake van een redelijke verdenking van strafbare feiten, is de controle incidenteel en worden werknemers achteraf geïnformeerd.

Bij het volgen en controleren van personeel moet gedacht worden aan bijvoorbeeld: GPS-trackers in bedrijfswagens, het opnemen van telefoongesprekken, camera's op de werkvloer, computervolgsoftware, Corona- en ADM-testen (alcohol, drugs en medicijnen), screening enzovoorts.

De gemeente maakt een afweging tussen het bedrijfsbelang en het persoonlijk belang van de werknemer. Dat gerechtvaardigd belang van de werkgever moet zwaarder wegen. De werkgever kan dat beargumenteren. Voorafgaand aan de eerste inzet van volg- en controlemiddelen heeft een risicoanalyse plaatsgevonden. Het inzetten van middelen voor het volgen en controleren van personeel heeft de instemming van de ondernemingsraad.

De gemeente als werkgever zal haar werknemers alleen volgen en controleren als dat noodzakelijk is en er geen andere minder ingrijpende manieren voorhanden zijn om hetzelfde doel te bereiken. Werknemers worden over het volgen en controleren door de werkgever geïnformeerd.

**Artikel 33 Cameratoezicht**
In het kader van de openbare orde en veiligheid mogen de gemeente Zundert en de politie, structureel of incidenteel, toezicht houden met camera's. De camerabeelden zijn politiegegevens, zie artikel 34. De gemeente beslist over de inzet van regulier cameratoezicht; de politie (korpschef) is verantwoordelijk voor de verwerking van de camerabeelden. De gemeente en de politie kunnen kiezen tussen het inzetten van vaste en/of mobiele camera's.

De burgemeester van de gemeente Zundert zal alleen besluiten cameratoezicht in te zetten als blijkt dat er in een bepaald gebied sprake is van een onveilige situatie of van regelmatige wanordelijkheden. Andere middelen, die minder inbreuk maken op de privacy, leiden dan aantoonbaar niet tot het bereiken van het gewenste doel. De inzet van cameratoezicht moet noodzakelijk zijn en voldoet altijd aan de eisen uit Gemeentewet artikel 151c. De verwerking van camerabeelden door de politie, voldoet aan alle eisen uit de Wet politiegegevens (Wpg).

Voorafgaand aan de inzet van cameratoezicht in de openbare ruimte wordt een risicoanalyse informatiebeveiliging en privacy uitgevoerd. Voor deze risicoanalyse is de korpschef van de politie verantwoordelijk. De korpschef is eveneens verantwoordelijk voor het informeren van het publiek over het cameratoezicht en het duidelijk kenbaar maken dat men een gebied betreedt waar cameratoezicht plaatsvindt. Zowel bij het uitvoeren van de risicoanalyse als bij de informatieplicht werkt de politie samen met de gemeente. Tenslotte zorgt de korpschef van de politie als verwerkingsverantwoordelijke ook voor de tijdige vernietiging van camerabeelden, het treffen van technische en organisatorische informatiebeveiligingsmaatregelen, de rechten van betrokkenen en het maken van schriftelijke afspraken met eventuele verwerkers.

De gemeente kan ook besluiten om camera's te plaatsen in de publiek toegankelijke delen van de gemeentelijke kantoren. Het doel is dan bescherming van eigendommen, bezoekers en personeel. In dat geval zullen wij een risicoanalyse informatiebeveiliging en privacy uitvoeren voorafgaand aan het besluit tot stelselmatige monitoring van openbaar toegankelijke ruimten. Dat geldt ook wanneer de gemeente

besluit cameratoezicht te houden op niet openbaar toegankelijke ruimten zoals de werkplekken van ambtenaren.

**Artikel 34 Politiegegevens**
Zoals in artikel 1 al staat vermeld is dit Privacyreglement onverkort van toepassing op de verwerking van politiegegevens. Politiegegevens zijn persoonsgegevens die verwerkt worden in het kader van de uitvoering van politietaken op grond van de Politiewet. De gemeente Zundert is werkgever van BOA's (buitengewone opsporingsambtenaren) op domein I en III, respectievelijk openbare ruimte en onderwijs. Bij de opsporing en vervolging van strafbare feiten op deze domeinen verwerkt de gemeente politiegegevens.

De gemeente Zundert verwerkt politiegegevens overeenkomstig de Wet politiegegevens en slechts als dat nodig is voor in de wet genoemde doeleinden.
Daartoe treffen wij regelingen en maatregelen die getoetst worden op opzet, bestaan en werking. Jaarlijks voeren wij een interne audit uit, eens in de vier jaar een externe audit.
Ofschoon de uitvoering van de Wpg anders is dan de Avg, gelden voor de verwerkingen van politiegegevens de regels analoog aan de Avg. Zo houden wij een register bij, hebben wij een datalekprotocol, voeren wij risicoanalyses informatiebeveiliging en privacy uit, beantwoorden verzoeken in het kader van de rechten van betrokkenen en voldoen wij aan de informatieplicht. Bij het verwerken letten wij op de doelbinding en de rechtmatigheid. De informatiesystemen of applicaties die wij inzetten bij het verwerken van politiegegevens zijn onderworpen aan de principes van privacy door ontwerp en standaardinstellingen.

**Artikel 35 Klachten**
Betrokkenen, diegenen waarvan persoonsgegevens verwerkt worden, kunnen over de verwerking van persoonsgegevens door de gemeente een schriftelijke klacht indienen.

Voor het beantwoorden van vragen en het behandelen van klachten is de gemeente Zundert bereikbaar op een specifiek e-mailadres: privacy@zundert.nl. Betrokkenen kunnen hier gebruik van maken. Dit adres is zowel voor vragen en klachten gericht aan de verwerkingsverantwoordelijke bestuursorganen als aan de interne toezichthouder, de functionaris voor de gegevensbescherming (FG). Vragen en klachten worden binnen 4 weken afgehandeld en vertrouwelijk behandeld.
Tegen gemeentelijke besluiten staan bezwaar- en beroepsmogelijkheden open.

Als betrokkenen er met de gemeente niet uitkomen kunnen zij een klacht indienen bij de externe toezichthouder op de privacy, de Autoriteit Persoonsgegevens (Avg artikel 77), bij de Nationale Ombudsman of naar de rechter gaan. Een klacht bij de AP kan louter ingediend worden voor zover het de eigen persoonsgegevens betreft of op basis van een machtiging.

**Artikel 36 Bewustwording**
De gemeente Zundert beseft dat een juiste veiligheidscultuur van groot belang is. Cultuur vertaalt zich naar houding, gedrag en kennis van medewerkers die maken dat technische en organisatorische maatregelen het juiste effect hebben. De mens is een beïnvloedbare en belangrijke schakel in het grotere geheel van informatiebeveiliging en bescherming van persoonsgegevens. De mate waarin medewerkers zich bewust zijn van de risico's die samenhangen met het verwerken van persoonsgegevens (en digitaal werken), bepaalt de sterkte en de zwakte van deze schakel. Bij bewustwording worden informatiebeveiliging en privacy als één geheel gezien.

De gemeente Zundert heeft een Bewustwordingsplan informatiebeveiliging en privacyHoofdstuk 2 ~Slotbepalingen dat zich vertaalt naar concrete bewustwordingsacties. De directie draagt bewustwording actief uit in de organisatie. BOA's trainen wij op het omgaan met politiegegevens, zoals het verbod op geautomatiseerde besluitvorming en profilering met politiegegevens en discriminatie op grond van bijzondere categorieën van politiegegevens. Nieuwe medewerkers krijgen een introductiecursus, van bestaande medewerkers wordt de kennis regelmatig opgefrist. Daarbij bereiken wij de gehele organisatie. Wij zetten daar onder andere de volgende middelen in: bewustwordingssessies, het Leermanagementsysteem, publicaties op intranet, workshops en trainingen. Lokaal en regionaal initiëren wij acties die bijdragen aan de vergroting van het collectieve bewustzijn. Deze acties zijn informatief, zoveel mogelijk informeel en repetitief van karakter. Geregeld steken wij de thermometer in de organisatie om het collectieve bewustzijnsniveau te meten waarna wij weer een volgend bewustwordingsprogramma uitzetten. Bewustwording is een continu proces van plan-do-check-act.

## Hoofdstuk 2 Slotbepalingen

### Artikel 37 Intrekking oude regeling
Met het vaststellen van de beleidsregel “Privacyreglement gemeente Zundert 2023-2026” wordt gelijktijdig ingetrokken de beleidsregel “Privacyreglement gemeente Zundert d.d. 22-5-2018”.

### Artikel 38 Inwerkingtreding
Deze beleidsregels treden in werking één dag na bekendmaking op www.officielebekendmakingen.nl

### Artikel 39 Citeertitel
Deze beleidsregels worden aangehaald als “Privacyreglement gemeente Zundert 2023-2026”.

*Aldus besloten in de vergadering van 10-01-2023*

*Burgemeester en wethouders van Zundert,*

*de secretaris,*
*drs. J.W.F. Compagne*

*de burgemeester,*
*J.G.P. Vermue*