Privacybeleid
2024-2026

Gemeente De Wolden

Auteurs : Jasmijn de Pruis, Jan Lemstra

Versie : 2.0
Status : Definitief
Datum : 18 oktober 2024

Inhoudsopgave

Documenthistorie

Versie	Datum	Auteur(s)	Status / omschrijving wijziging
0.1	30-06-2022	Jan Lemstra	Concept obv handreiking iBD
1.0c	21-04-2023	Jan Lemstra	Definitieve conceptversie
1.0	10-11-2023	Jasmijn de Pruis	Review CISO, akkoord directie SWO
1.0def	04-03-2024	Jasmijn de Pruis	Voorstel aan B&W
2.0def	18-10-2024	Jasmijn de Pruis Jan Lemstra	Voorstel aan B&W

Distributielijst

Naam	Organisatiedeel / Functie|Rol
Jasmijn de Pruis	PO
Jan Lemstra	CISO

Review

Naam	Functie	Datum	Hoofdstukken/ onderwerpen
Jasmijn de Pruis	PO	20-04-2023	Geheel
Jan Lemstra	CISO	04-11-2023	Geheel

Classificatie

Classificatie	Niveau
X	**Openbaar**
	Intern (bedrijfsvertrouwelijk)
	Vertrouwelijk
	Geheim

1. Inleiding

1.1 Algemeen

De gemeente werkt met een grote hoeveelheid persoonsgegevens van inwoners, ondernemers en (keten)partners. Persoonsgegevens zijn alle gegevens die (in)direct herleidbaar zijn tot een persoon. Deze gegevens verzamelt de gemeente om de wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor inwonerzaken.
Het college van burgemeester en wethouders is (vanuit de Algemene verordening gegevensbescherming (AVG)) verwerkingsverantwoordelijke en heeft de taak om de persoonsgegevens goed te beschermen.

De gemeente hecht waarde aan de privacy van haar inwoners en wil op een verantwoorde manier omgaan met de verwerking van persoonsgegevens.
In dit beleid worden hiervoor kaders gesteld, gebaseerd op de AVG.

1.2 Begripsbepalingen

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

1.3 Doel

Het doel van dit privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens. De AVG is het centrale kader en houvast voor de wijze waarop we omgaan met persoonsgegevens. Dit beleid is een nadere uitwerking hiervan en dient als uitgangspunt bij de gegevensverwerkingen binnen de gehele gemeentelijke organisatie.

Aan de hand van dit beleid wil de gemeente de rechten van betrokkenen – waarvan zij gegevens verwerkt of laat verwerken – waarborgen. De verdere uitwerking van dit beleid is – waar relevant – vastgelegd in organisatiebrede procedures voor bijvoorbeeld datalekken en rechten van betrokkenen. Tevens zijn er domeinspecifiek afspraken vastgelegd over bijvoorbeeld gegevensdeling binnen het sociaal domein.

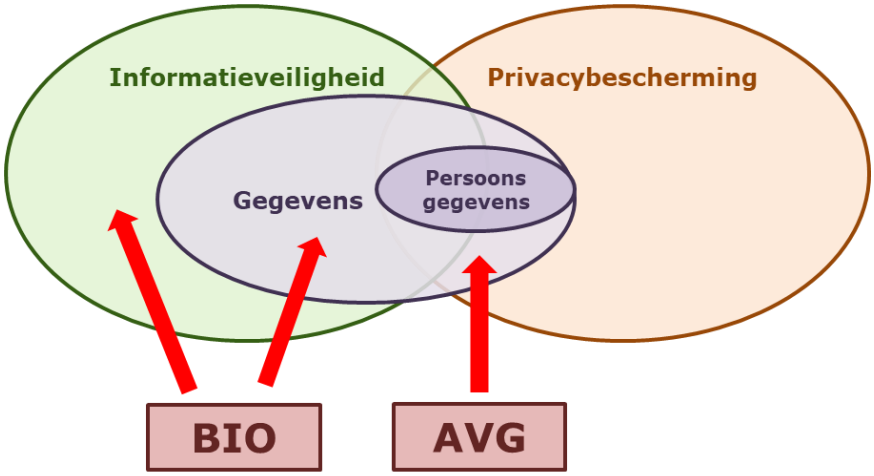
Iedereen werkzaam in of voor de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De organisatie verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de organisatie dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

Hiermee leggen we als gemeente de basis voor eenduidige aantoonbare naleving van de AVG. Daarnaast sluiten we aan bij de vier kernwaarden in de manier waarop de gemeentelijke organisatie werkt:

- *Eenvoud*
  We maken het zakendoen met de gemeente gemakkelijk van aanvraag tot afhandeling. Dit geld onder andere bij het doen van AVG-verzoeken.
- *Maatwerk*
  Bij initiatieven en vraagstukken kijken we altijd naar een oplossing die het beste past voor die specifieke situatie.
- *Samen*
  Als organisatie werken we samen vanuit het belang van de klant samen voor de klant.
- *Vertrouwen*
  Klanten kunnen op ons rekenen en erop vertrouwen dat we doen wat we beloven en dat we de dingen goed doen.

1.4 Positionering beleid

Het privacybeleid is onderdeel van de Visie, het Strategisch en Tactisch beleid Informatiebeveiliging & Privacy. Dit privacybeleid heeft grote samenhang met het informatiebeveiligingsbeleid. Hierin zijn maatregelen opgenomen om alle informatie te beschermen. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens.



De komende jaren zet de gemeente in op verdere professionalisering van de privacy volwassenheid in de organisatie. Een privacy volwassen organisatie is noodzakelijk voor het beschermen van de rechten van betrokkenen. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle personen die werkzaam zijn voor de gemeente essentieel voor privacy binnen de organisatie.

1.5 Reikwijdte

Dit privacybeleid is expliciet van toepassing op alle verwerkingen van persoonsgegevens van inwoners, ondernemers, leveranciers, ketenpartners, medewerkers en andere derden door of namens de gemeentelijke organisatie, waaronder:

- De verwerking van persoonsgegevens binnen de bedrijfsprocessen;
- Alle locaties en devices die door de gemeentelijke organisatie worden gebruikt waar(op) persoongegevens worden verwerkt;
- De gegevensuitwisseling met derde partijen zoals ketenpartners en leveranciers.

1.6 Geldigheidsduur

Dit beleid is vastgesteld door het college van burgemeester en wethouders als verwerkingsverantwoordelijke. Het beleid wordt tenminste eenmaal per drie jaar beoordeeld en zo nodig herzien. Als er een aanleiding is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van data protection impact assessments), kan het college besluiten tot een tussentijdse herziening.

2. Beleidsuitgangspunten bij de verwerking van persoonsgegevens

Persoonsgegevens worden enkel verwerkt in overeenstemming met de volgende beleidsuitgangspunten.

2.1 Rechtmatige grondslag, behoorlijkheid en transparantie

Persoonsgegevens worden slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Hiervan is sprake indien gegevens worden verwerkt op basis van een verwerkingsgrondslag. De grondslagen zijn limitatief opgesomd in de AVG:

- Op basis van toestemming van de betrokkene;
- Voor de uitvoering van een overeenkomst waarin de betrokkene een partij is;
- Voor het nakomen van een verplichting die in de wet staat;
- Voor het behartigen van vitale belangen;
- Voor een goede vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag;
- Voor het behartigen van gerechtvaardigde belangen.

Vaak vloeit de grondslag voor een verwerking bij een gemeentelijke organisatie voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak. Indien de verwerking op toestemming is gebaseerd, wordt toestemming gevraagd in begrijpelijke en duidelijke vorm, bijvoorbeeld schriftelijk via een toestemmingsformulier of digitaal middels opt-in. Daarnaast krijgt de betrokkene de gelegenheid om te allen tijde zijn toestemming in te trekken. In de uitvoering van gemeentelijke taken kan de verwerking nooit gebaseerd worden op basis van een gerechtvaardigd belang. Indien de gemeente handelt als private partij – en de verwerking wordt gebaseerd op het gerechtvaardigd belang – wordt er altijd vooraf een belangenafweging gemaakt. Het belang van de gemeente om persoonsgegevens te verwerken wordt daarbij afgewogen tegen het belang van privacy van de betrokkene.

2.2 Doelbinding

De gemeente mag persoonsgegevens enkel verwerken als hiervoor een doel is vastgesteld. De uitvoerende organisatie stelt het doel voor de gegevensverwerking vast en zorgt ervoor dat dit wordt opgenomen in het verwerkingsregister. Zonder doel mogen persoonsgegevens niet worden verwerkt. De gemeente verwerkt alleen persoonsgegevens die noodzakelijk zijn om het vastgestelde doel te kunnen bereiken. De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door geen persoonsgegevens te verwerken.

2.3 Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De proceseigenaar laat – voorafgaand aan de start van de gegevensverwerking – een toets uitvoeren door de Privacy Officer om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving. Bij twijfel over de verenigbaarheid van de doeleinden wordt advies ingewonnen van de Functionaris Gegevensbescherming (FG).

2.4 Minimale gegevensverwerking

Waar mogelijk worden minder of geen persoonsgegevens verwerkt. De gemeente kiest altijd voor een manier van gegevensverwerking waarbij zo min mogelijk inbreuk wordt gemaakt op de privacy van de betrokkene. Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel (proportionaliteit). De gegevensverwerking is alleen toegestaan als het doel niet op een andere manier kan worden bereikt (subsidiariteit).

2.5 Juiste en actuele gegevens

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt.
De organisatie neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.
Proceseigenaren zijn verantwoordelijk om passende maatregelen te implementeren in hun werkprocessen.

2.6 Gegevens worden op tijd vernietigd

De gemeente bewaart persoonsgegevens niet langer dan noodzakelijk. De AVG schrijft geen concrete bewaartermijnen voor, de verwerkingsverantwoordelijke moet zelf bewaartermijnen vaststellen.

De gemeente stelt waar mogelijk 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.

Als het doel is bereikt en de gegevens niet meer noodzakelijk zijn worden de gegevens vernietigd of zo aangepast dat de gegevens niet meer terug te herleiden zijn tot een persoon. Gegevens kunnen bijvoorbeeld worden geanonimiseerd tot statistische informatie die kan bijdragen aan de gemeentelijke beleidsvorming.

Vragen ter bepaling van de bewaartermijn zijn:
- Wanneer is het (proces)doel bereikt?
- Is er een wettelijke plicht om de gegevens te bewaren?
- Kunnen de persoonsgegevens worden vernietigd zonder afbreuk te doen aan het proces?
- Kunnen de persoonsgegevens worden geanonimiseerd zonder afbreuk te doen aan het proces?
- Is het langer bewaren van persoonsgegevens een grotere inbreuk op de privacy van betrokkenen?
- Kunnen persoonsgegevens gedurende de bewaartermijn actueel, juist en volledig worden bewaard?
- Kan de betrokkene toegang worden verleend tot de persoonsgegevens tijdens de gehele bewaartermijn?

2.7 Beveiliging

De gemeente neemt passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De organisatie handelt hierbij in overeenstemming met wet- en regelgeving (waaronder de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene verordening gegevensbescherming (AVG)) en het intern vastgestelde beleid Informatiebeveiliging & Privacy. Deze wet- en regelgeving en beleid verplicht de organisatie om gegevens te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

2.8 Privacy by Default en Privacy by Design

De gemeente houdt bij de ontwikkeling en implementatie van nieuwe diensten, systemen of processen rekening met de aspecten van privacy en gegevensbescherming (Privacy by Design). Zo wordt bij het opstellen van een wijzigingsverzoek of businesscase vooraf nagedacht over maatregelen die de organisatie moet nemen om de gegevens van betrokkenen te beschermen. Bij alle aanbestedingen van oplossingen en diensten waarbij persoonsgegevens worden verwerkt, wordt de privacy officer vooraf geconsulteerd voor een advies over hoe in dat specifieke proces persoonsgegevens worden gewaarborgd. Privacybescherming wordt proactief geïntegreerd in diensten, systemen en processen.

Tevens richt de gemeente werkprocessen en standaardinstellingen in informatiesystemen altijd zo privacy-vriendelijk mogelijk in (Privacy by Default). Dit betekent dat de principes voor de verwerking van persoonsgegevens worden meegenomen in iedere gegevensverwerking.

Dit wordt onder andere gerealiseerd door middel van het uitvoeren van gegevensbeschermingseffectbeoordeling (een *Data Protection Impact Assessment* (DPIA)). De gemeente voert een DPIA uit indien de gegevensverwerking (mogelijk) een hoog risico inhoudt voor de betrokkene. De verwerkingsverantwoordelijke moet op basis van de uitkomsten van de DPIA maatregelen nemen om de impact van de gegevensverwerking te mitigeren. Wanneer de gemeente voornemens is om een algoritmisch systeem in te zetten of te ontwikkelen wordt er altijd een zogeheten impact assessment voor mensenrechten bij de inzet van algoritmen (IAMA) uitgevoerd.

De uitkomsten van de DPIA of IAMA worden altijd voorgelegd aan de interne toezichthouder, de Functionaris Gegevensbescherming (FG). De FG zal voorziet de verwerkingsverantwoordelijke van een advies over de te nemen maatregelen. Indien het niet mogelijk is om (voldoende) maatregelen te nemen raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de gegevensverwerking de Autoriteit Persoonsgegevens (AP).

2.9 Toegang tot gegevens

Uitsluitend geautoriseerde medewerkers hebben toegang tot persoonsgegevens en zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend.
Deze bevoegdheden worden verleend op grond van het binnen de organisatie geldend beleid voor logische en fysieke toegang tot gegevens. Deze bevoegdheden worden periodiek gecontroleerd. De organisatie hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en te corrigeren. Toegang tot persoonsgegevens houdt altijd verband met een welbepaald doel (doelbinding) en proportionaliteit (niet meer dan noodzakelijk).

2.10 Inbreuk in verband met persoonsgegevens

Bij ongeoorloofde toegang tot, verlies of wijziging van persoonsgegevens spreken we van een inbreuk op de beveiliging van persoonsgegevens, oftewel een datalek.
Bijvoorbeeld wanneer persoonsgegevens zijn ingezien of gewijzigd door iemand die daar geen recht toe heeft. Een datalek moet afhankelijk van het risico voor de betrokkene(n) worden gemeld bij de Autoriteit Persoonsgegevens (AP) en soms bij de getroffen betrokkene(n).
De gemeente registreert datalekken, ziet toe op de opvolging hiervan en zet de bevindingen om in verbeterpunten. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure Beveiligingsincident melden.

2.11 Gegevens delen met derden

De gemeente schakelt soms derden in die in opdracht van of samenwerking met de gemeente persoonsgegevens verwerken. De AVG spreekt van verschillende rollen:

- Verwerkingsverantwoordelijke: de partij die eigenstandig het doel van en de middelen voor de gegevensverwerking vaststelt;
- Verwerker: de partij die in opdracht van de verwerkingsverantwoordelijke gegevens verwerkt;
- Gezamenlijk verwerkingsverantwoordelijke: twee of meer partijen die gezamenlijk het doel van en de middelen voor de gegevensverwerking vaststellen.

Voorafgaand aan iedere gegevensdeling worden de rollen van partijen duidelijk vastgesteld, de proceseigenaar kan hiervoor de Privacy Officer consulteren. Nadat duidelijk is welke partij welke rol inneemt worden afspraken omtrent gegevensverwerking vastgelegd in een (gezamenlijke) verwerkersovereenkomst. Hiervoor hanteert de gemeente het model van de VNG. In de (gezamenlijke) verwerkersovereenkomst worden ten minste afspraken over het volgende gemaakt:

- Omschrijving van de persoonsgegevens, betrokkenen, doeleinden, duur en de aard van de gegevensverwerking;
- De verplichtingen van de partij(en) ten aanzien van de gegevensverwerking;
- Personen in dienst van of werkzaam voor de partij(en) hebben een geheimhoudingsplicht;
- Het terugleveren of vernietigen van persoonsgegevens na afloop van de verwerkersovereenkomst;
- Aansprakelijkheid van de partij(en).

2.12 Doorgifte buiten de EER

In principe worden persoonsgegevens niet doorgegeven aan landen buiten de Europese Economische Ruimte (EER). Indien het voor de gegevensverwerking noodzakelijk is om persoonsgegevens door te geven wordt er altijd een toets uitgevoerd door de Privacy Officer om te bepalen of het mogelijk is om persoonsgegevens door te geven middels doorgifteinstrumenten als bepaald in toepasselijke wet- en regelgeving.

2.13 Rechten van betrokkenen

Elke betrokkene heeft het recht om te vernemen welke persoonsgegevens de organisatie over de betrokkene heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht op informatie, recht van inzage, recht op rectificatie, recht op verwijdering, recht van bezwaar, recht op beperking en recht op overdraagbaarheid.

Recht op informatie
Betrokkenen hebben het recht om te weten of en op welke wijze de gemeente persoonsgegevens van hen verwerkt. De gemeente informeert de betrokkenen over de verwerking van hun persoonsgegevens via de privacyverklaring op de gemeentelijke website.

Recht van inzage
Betrokkenen hebben het recht om in te zien welke persoonsgegevens de gemeente over hen verwerkt en voor welke doeleinden. Rechtenverzoeken worden in behandeling genomen via de procedure voor inzageverzoeken.

Recht op rectificatie
Betrokkenen hebben het recht om hun persoonsgegevens te laten aanpassen als deze onjuist of onvolledig zijn. Rechtenverzoeken worden in behandeling genomen via de procedure voor rectificatieverzoeken.

Recht op verwijdering
Betrokkenen hebben het recht om hun persoonsgegevens te laten vernietigen indien het doel van de verwerking is behaald. Rechten verzoeken worden in behandeling genomen via de procedure voor vernietigingsverzoeken.

Recht van bezwaar
Betrokkenen hebben het recht om bezwaar te maken tegen de gegevensverwerking. Rechtenverzoeken worden in behandeling genomen via de procedure voor bezwaarverzoeken.
Recht op beperking
Betrokkenen hebben het recht om de verwerking van hun persoonsgegevens te laten beperken, bijvoorbeeld wanneer de betrokkene betwist of zijn persoonsgegevens juist zijn. Rechtenverzoeken worden in behandeling genomen via de procedure voor beperkingsverzoeken.

Recht op overdraagbaarheid
Betrokkenen hebben het recht om hun persoonsgegevens te laten overdragen. Dit houdt in dat de betrokkene zijn gegevens door de gemeente overgedragen krijgt in een gestructureerde, gangbare en machine leesbare vorm. Rechtenverzoeken worden in behandeling genomen via de procedure voor dataportabiliteitsverzoeken.

Recht op menselijke blik bij besluiten
De AVG staat geautomatiseerde besluiten, waaronder profilering, in principe niet toe. Betrokkenen hebben daarom altijd het recht op een menselijke blik bij besluiten die een rechtsgevolg heeft voor de betrokkene.

2.14 Monitoring van burgers in de openbare ruimte

In het geval van verwerking van persoonsgegevens door het (digitaal) monitoren van burgers in de openbare ruimte vraagt dit expliciete bestuurlijke besluitvorming door het college vooraf aan de start van dergelijke verwerkingen.

2.15 Geschillenbeslechting

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

2.16 Verantwoording en toezicht

Binnen de gemeentelijke organisatie vindt een groot aantal gegevensverwerkingen plaats waar intern en extern toezicht op wordt houden. De Autoriteit Persoonsgegevens is de nationale toezichthouder op gebied van privacy en gegevensbescherming. Daarnaast beschikt de gemeentelijke organisatie over een onafhankelijke, interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De organisatie stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren. De FG brengt jaarlijks een verslag uit aan het college en de gemeenteraad over zijn verrichte werkzaamheden, bevindingen en aanbevelingen.

2.17 Verwerkingsregister

De gemeente beschikt over een register van alle gegevensverwerkingen waarvoor ze verantwoordelijk is. Het gaat dan om alle incidentele (bijvoorbeeld pilots) en structurele verwerkingen. Per gegevensverwerking wordt in ieder geval omschreven:

- Naam en contactgegevens van de verwerkingsverantwoordelijke;
- Naam van de verwerker(s) en andere verwerkingsverantwoordelijke(n);
- Wat het doel is van de verwerking;
- De grondslag voor gegevensverwerking;
- Welke persoonsgegevens worden verzameld;
- De categorieën van betrokkenen;
- Beschrijving van ontvangers van persoonsgegevens;
- Beschrijving van doorgifte van persoonsgegevens;
- Hoe lang persoonsgegevens worden bewaard;
- Welke beveiligingsmaatregelen zijn genomen.

Bij iedere nieuwe of wijzigende verwerking van persoonsgegevens wordt de Privacy Officer op de hoogte gesteld door de uitvoerende organisatie. De Privacy Officer voert vervolgens een toets uit om te bepalen of de gegevensverwerking rechtmatig is. De toets wordt uitgevoerd aan de hand van de bepalingen in de AVG. Gegevensverwerkingen die binnen een bepaald proces plaatsvinden en waarvan de doelen hetzelfde zijn worden samengevoegd onder één categorie in het verwerkingsregister. De verwerkingsverantwoordelijke moet ervoor zorgen dat het register altijd actueel en volledig is. Het register wordt minimaal eenmaal per zes maanden gecontroleerd op actualiteit. Het verwerkingsregister van de gemeente wordt gecoördineerd en beheerd door de Privacy Officer. Het verwerkingsregister moet worden op de website van de gemeente.

2.18 Bewustwording

Alleen beleid en technische maatregelen zijn niet voldoende om risico’s bij het verwerken van persoonsgegevens uit te sluiten of minimaliseren. Essentieel is het bewustzijn over privacy en informatiebeveiliging in de organisatie voortdurend aan te scherpen, zodat kennis van dreigingen en risico’s wordt verhoogd. De organisatie moet (veilig en verantwoord) gedrag om gegevens zorgvuldig te verwerken aanmoedigen. Van bestuurder tot medewerker: iedereen wordt aantoonbaar geïnformeerd en getraind over het zorgvuldig omgaan met persoonsgegevens. Bewustwording omtrent informatiebeveiliging en privacy is een structureel programma binnen de organisatie en krijgt extra aandacht bij de indiensttreding van nieuwe medewerkers. Alle medewerkers worden geschoold op dit onderwerp via bijvoorbeeld mailings, cursussen, phishing simulaties en workshops. Dit gebeurt passend binnen de context van en bij het domein waarbinnen de persoonsgegevens worden verwerkt.

2.19 PDCA-cyclus

De gemeente wil in control zijn op de verwerking van persoonsgegevens. *In control* betekent in dit verband dat de organisatie weet welke risico's er zijn, welke mitigerende maatregelen genomen zijn, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus. Daarnaast gebruikt de gemeentelijke organisatie het AVG-borgingsproduct van de VNG als jaarlijks beoordelingskader voor het waarborgen van privacy compliance binnen de organisatie. Het AVG-borgingsproduct is een normenkader dat door de organisatie gebruikt wordt voor het duiden van privacy risico’s en de daarbij behorende beheersmaatregelen binnen de organisatie. De Functionaris Gegevensbescherming rapporteert jaarlijks over de stand van zaken op het gebied van gegevensbescherming in het FG-rapport.