Privacybeleid

Gemeente Apeldoorn

Inhoud

1 Inleiding

De gemeente Apeldoorn werkt met (persoons)gegevens van onder andere inwoners, ondernemers, medewerkers en (keten)partners (ook wel betrokkenen genoemd). Deze gegevens verzamelt de gemeente om (wettelijke) taken goed uit te kunnen voeren. Denk hierbij aan het verlengen van een rijbewijs, het uitschrijven van een parkeerboete en het tegengaan van illegale prostitutie. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De betrokkene moet erop kunnen vertrouwen dat de gemeente zorgvuldig, veilig en rechtmatig met de persoonsgegevens omgaat.

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

Geldigheidsduur
Dit beleid is vastgesteld op 21 mei 2024 door het college van B&W (hierna: college) als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.

Dit privacybeleid treed in werking na vaststelling ervan door het college van B&W. Het eerder vastgestelde 'Privacybeleid 2015' en het 'Privacybeleid 2018' komen daarmee te vervallen.

Het privacybeleid wordt na vaststelling actief gedeeld met het (lijn)management en wordt organisatie breed beschikbaar gesteld.

Begripsbepalingen
De definities uit art. 4 AVG en art. 1 Wpg hebben in dit beleid dezelfde betekenis.

2 Reikwijdte

De gemeente verwerkt dagelijks enorme hoeveelheden persoonsgegevens van verschillende betrokkenen om (wettelijke) taken uit te kunnen voeren. Dit vraagt van de gemeente om zorgvuldig, veilig en rechtmatig om te gaan met de persoonsgegevens. Daarom dient de gemeente te voldoen aan de AVG en de Wpg.

Om te beginnen: binnen de Europese Unie (EU) is de General Data Protection Regulation (GDPR) van toepassing. De AVG is hiervan een Nederlandse vertaling. Alle bedrijven en organisaties die persoonsgegevens verwerken dienen aan de verordening te voldoen. De AVG heeft daarom een breed toepassingsgebied en het bestaat veelal uit open normen. Dit maakt dat naast overheden bijvoorbeeld ook onderwijsinstellingen en winkelketens volgens de AVG kunnen werken. Het is aan de gemeente Apeldoorn om de AVG te interpreteren binnen andere geldende wet- en regelgeving zoals de Wet maatschappelijk ondersteuning (Wmo) en de Kieswet.

Naast de AVG is ook de Wpg van toepassing op de gemeente. Processen of delen van processen vallen *of* onder de AVG *of* onder de Wpg.

Beide privacywetten hebben als doel het beschermen van de persoonsgegevens.

De Wpg is Nederlandse wetgeving en van toepassing op de politie, marechaussee, de rijksrecherche en boa-organisaties, waaronder de gemeente Apeldoorn. In tegenstelling tot de AVG, is de Wpg een gesloten keten waarin domeinen zijn gedefinieerd:

- Domein I – Openbare ruimte
- Domein II – Milieu, welzijn en infrastructuur
- Domein III – Onderwijs
- Domein IV – Openbaar vervoer
- Domein V – Werk, inkomen en zorg
- Domein VI – Generieke opsporing

Bij de gemeente Apeldoorn werken boa's in domein I, II, III en V. Zowel intern als extern geldt binnen de Wpg-domeinen de *free flow of information.* Persoonsgegevens die het Wpg-domein verlaten, kunnen alleen onder voorwaarden worden gedeeld.

De reikwijdte van dit privacybeleid en de naleving ervan geldt daarmee voor de gehele gemeente. Dit privacybeleid geldt ook voor externe partijen die namens de gemeente Apeldoorn persoonsgegevens verwerken, waaronder:

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

2.1 Wet- en regelgeving

Naast privacywetgeving moet de gemeente aan een tal van andere wet- en regelgeving voldoen. Hierin wordt onderscheid gemaakt tussen kaderwetten en materiewet- en regelgeving. Voorbeelden van kaderwetten zijn:

- De Archiefwet
- De Wet open overheid (Woo), en
- De richtlijn Network and Information Security directive (NIS2)

Voorbeelden van materiewet- en regelgeving:

- De Participatiewet
- De Wet arbeid en zorg
- De wet Bevordering integriteitsbeoordeling door het openbaar bestuur (Bibob-wet)

Een goede naleving van privacywetgeving vraagt om een continue afweging waarbij kaderwetten en materiewet- en regelgeving zijn meegewogen.

2.2 Specifieke uitwerkingen

Dit beleid is het kader voor verdere uitwerking in deelonderwerpen. Dit kan zijn omdat het op een beperkt aantal verwerkingen van toepassing is of omdat het gaat om tactische en operationele stukken. Onderstaande opsomming is niet limitatief maar geeft een overzicht van (wettelijke) uitwerkingen op basis van dit beleid. Van een aantal van onderstaande uitwerkingen is ten tijde van schrijven een (concept)uitwerking aanwezig maar deze zijn niet geformaliseerd en vastgesteld.

- Beleid/procedure voor de rechten van betrokkenen;
- Beleid/procedure voor het afhandelen van gemelde datalekken;
- Beleid/procedure voor het delen van persoonsgegevens met derden;
- Beleid/procedure voor het uitvoeren van een risicoanalyse (DPIA);
- Beleid/procedure/werkwijze voor het beheer van het verwerkingsregister;
- Beleid/procedure/werkwijze voor de toepassing van Privacy by Design/en – Default;
- Beleid/procedure/werkwijze voor de inzet van cameratoezicht;
- Jaarlijks communicatie- en/of bewustzijnsplan.

De vaststelling ven bovengenoemde tactische uitwerkingen, vindt plaats volgens de verantwoordelijkheden en bevoegdheden in het mandaatregister van gemeente Apeldoorn. Dit is veelal op niveau van de gemeentesecretaris belegd.

2.3 Informatiebeveiliging

In de AVG en Wpg is opgenomen dat persoonsgegevens goed beveiligd moeten zijn als het toegestaan is ze te verwerken. Binnen de gemeente ondersteunen de security medewerkers de organisatie bij het beveiligen van informatie. Voor een goede bescherming van persoonsgegevens is het belangrijk dat de informatiebeveiliging van de gemeente op orde is en voldoet aan de Baseline Informatiebeveiliging Overheid. De vakgebieden privacy en informatiebeveiliging zijn daarmee nauw met elkaar verbonden.

Het doel van informatiebeveiliging is het realiseren van een betrouwbare dienstverlening naar bijvoorbeeld inwoners, bezoekers, ondernemers en medewerkers van gemeente Apeldoorn en de kans op verstoringen hierin zoveel mogelijk te beperken.

3 Wettelijke kaders en principes

De AVG en Wpg zijn gebaseerd op meerdere kaders en principes voor de verwerking van persoonsgegevens. De gemeente heeft het doel persoonsgegevens slechts te verwerken in overeenstemming met deze kaders en principes.

3.1 Privacy kaders

In deze paragraaf staan de wettelijk verplichte kaders die in zowel de AVG als de Wpg beschreven staan en overeenkomen. Opvolgend staan specifieke kaders voor de AVG en Wpg.

Register
De gemeente is verplicht om registers bij te houden zoals het datalekregister en het verwerkingsregister. In het verwerkingsregister staan alle verwerkingen van/processen met persoonsgegevens. Vanuit de Wpg is naast het datalek- en verwerkingsregister ook een register met daarin de ingediende verzoeken om inzage van de betrokkenen, en een verstrekkingenregister, verplicht.

Naast de wettelijk verplichte registers houdt gemeente Apeldoorn een Data Protection Impact Assessment (DPIA)-register bij en een register waarin externe partijen staan waarmee de gemeente samenwerkt en persoonsgegevens deelt.

Data Protection Impact Assessment
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een analyse uitvoeren op het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een Data Protection Impact Assessment (hierna: DPIA) uit. Deze risicoanalyse wordt voorafgaand aan de verwerking van persoonsgegevens uitgevoerd. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Verwerkingen waarop een DPIA noodzakelijk is, worden geprioriteerd op basis van het risico. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[1] genoemd.

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

De gemeente Apeldoorn maakt gebruik van het Borgingsproduct van de VNG voor het uitvoeren van een analyse op de naleving van de AVG. Voor de Wpg geldt de wettelijke verplichting om jaarlijks een audit uit te (laten) voeren.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet intern worden gemeld en bij een hoger risico ook bij Autoriteit Persoonsgegevens en/of de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de datalekprocedure.

Samenwerking
De gemeente schakelt soms derden in om persoonsgegevens in opdracht te verwerken, een fictief voorbeeld hiervan is een administratiekantoor dat voor gemeente salarisverwerking uitvoert. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG en ook de Wpg verplichten

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

de gemeente tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Rechten van betrokkenen
Iedereen heeft het recht om te weten welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG en §4 uit de Wpg, uit te oefenen.

De gemeente informeert actief de betrokkene voorafgaand aan de verwerking van zijn/haar persoonsgegevens. Dit doet de gemeente in bijvoorbeeld een privacyverklaring. Daarnaast worden de volgende rechten gefaciliteerd: het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.
Voor de Wpg gaat het om: het recht op informatie, het recht op inzage en het recht op rectificatie en vernietiging van persoonsgegevens. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn/haar persoonsgegevens is omgegaan, kan de betrokkene een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. 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.

Functionaris Gegevensbescherming (FG)
De gemeente is verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het college van zijn/haar werkzaamheden, bevindingen en geeft adviezen.

3.1.1 AVG kader

In deze paragraaf staan specifieke wettelijke kaders uit de AVG beschreven, deze kaders wijken af of staan niet beschreven in de Wpg en daarom worden ze in deze paragraaf apart genoemd.

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

3.1.2 Wpg kaders

In deze paragraaf staan specifieke wettelijke kaders uit de Wpg beschreven, deze kaders wijken af of staan niet beschreven in de AVG en daarom worden ze in deze paragraaf apart genoemd.

Ter beschikking stellen en verstrekken van persoonsgegevens
Wanneer persoonsgegevens worden gedeeld wordt afhankelijk van de ontvanger, onderscheid gemaakt tussen het *ter beschikking stellen van persoonsgegevens* en het *verstrekken van persoonsgegevens*.

Als persoonsgegevens binnen het Wpg-domein worden gedeeld (bijvoorbeeld met boa's van andere afdelingen of met de politie) wordt dit *ter beschikking stellen* genoemd. De gemeente stelt persoonsgegevens alleen ter beschikking wanneer dit noodzaak is voor de uitvoering van de taak van de ontvanger. De gemeente besluit of dit inderdaad noodzakelijk is. Deze vorm van gegevensdeling wordt ook wel 'free-flow-of-information' genoemd.

Bij het *verstrekken* van persoonsgegevens verlaten de gegevens het Wpg-domein, bijvoorbeeld wanneer de gemeente persoonsgegevens deelt met bureau HALT. De gemeente verstrekt alleen persoonsgegevens wanneer dit aan de gestelde voorwaarden in de Wpg voldoet. Eventuele verstrekkingen staan in het verstrekkingenregister.

Audit
De gemeente Apeldoorn voert jaarlijks de wettelijk verplichte audit uit. Resultaten van de audit laten zien waar de gemeente moet verbeteren. Indien noodzakelijk wordt de auditrapportage gedeeld met de AP.

3.2 Privacy principes

In deze paragraaf staan de principes die in zowel de AVG als de Wpg beschreven staan. Verderop in dit hoofdstuk is aandacht voor specifieke principes alleen voor de AVG of Wpg.

Welbepaalde doeleinden
De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden, bijvoorbeeld voor het uitschrijven van parkeerboete, het behandelen van een bezwaarschrift en het verlengen van een rijbewijs. Zonder specifiek doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om het doel te bereiken waarvoor de gegevens zijn verkregen.

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

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 gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te vernietigen.

Gegevens worden op tijd vernietigd
De AVG en Wpg bepalen dat persoonsgegevens niet langer mogen worden bewaard dan voor het doel noodzakelijk is. Voor de AVG geldt dat de gemeente de bewaartermijn van een verwerking vast stelt 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.

Alleen 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. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Voor de Wpg gelden de maximale bewaartermijnen die daarin zijn opgenomen. Anders dan in de AVG stelt de Wpg dat persoonsgegevens binnen het gestelde bewaartermijn na een periode (afhankelijk van het doel), niet meer raadpleegbaar zijn, maar wel bewaard moeten blijven. De bewaartermijnen zijn (net als in de AVG) afhankelijk van het beoogde doel.

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

Privacy by Default en Privacy by Design
De gemeente houdt bij de ontwikkeling en/of aanschaf van nieuwe diensten, systemen of processen rekening met aspecten van privacy om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie wordt zoveel mogelijk beperkt. Wanneer de doorgifte onoverkomelijk is, wordt dit gedaan wanneer dit in overeenstemming is met de relevante bepalingen in de AVG of Wpg en dit privacybeleid.

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

Verantwoording
Onder de verantwoordelijkheid van zowel het college, de burgermeester als ook de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. De verantwoordelijken moeten aan betrokkenen maar ook aan de Autoriteit Persoonsgegevens, kunnen verantwoorden wat er met welke persoonsgegevens, voor welk doel wordt gedaan. Het afleggen van verantwoording wordt zowel actief als reactief gedaan.

Bewustwording
Beleid en maatregelen alleen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken, wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Hiervoor heeft gemeente Apeldoorn een communicatieplan/bewustzijnscampagne ontwikkeld. Dit gebeurt passend binnen de context van en bij het thema en de afdeling waarbinnen die worden verwerkt.

3.2.1 AVG principes

In deze paragraaf staan specifieke principes uit de AVG beschreven, deze principes wijken af of staan niet beschreven in de Wpg en daarom worden ze in deze paragraaf apart genoemd.

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

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

Toegang tot gegevens
Uitsluitend geautoriseerde medewerkers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en vernietigen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid.

Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken. De gemeente heeft hiervoor logging- en monitoringsbeleid opgesteld.

3.2.2 Wpg principes

In deze paragraaf staan specifieke principes uit de Wpg beschreven, deze principes wijken af of staan niet beschreven in de AVG en daarom worden ze in deze paragraaf apart genoemd.

Geheimhouding
De Wpg regelt een strikte geheimhouding op de verwerking van persoonsgegevens. Bij het schenden van deze geheimhouding wordt een sanctie opgelegd. Hier is voorafgaand en tijdens het dienstverband van de boa voldoende aandacht voor. De geheimhouding beperkt zich overigens niet tot de organisatie die de persoonsgegevens heeft verzameld, maar wordt ook doorgegeven aan eventuele ontvangers van binnen en buiten de organisatie.

Autorisaties en logging
In de wet zijn voorwaarden gesteld voor het geven van autorisaties aan boa's en niet-boa's. Het uitgangspunt is dat boa's slechts autorisatie en rechten krijgen tot persoonsgegevens die voor hen noodzakelijk zijn voor de uitoefening van de taak. Autorisaties voor niet-boa's kunnen alleen worden toegekend wanneer de autorisatie verklaring positief is beoordeeld door de verwerkingsverantwoordelijke.

4 Visie

De komende jaren zet de gemeente in op verdere implementatie en professionalisering van privacy in de organisatie. Dit is noodzakelijk voor het goed functioneren van de gemeente en is de basis voor het beschermen van rechten van betrokkenen. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder thema en elke afdeling is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

4.1 Ambitie

De gemeente Apeldoorn zet een spreekwoordelijke stip op de horizon en heeft onderstaande ambitie geformuleerd.

De gemeente verankerd privacy in de organisatie(cultuur)
Privacy is onderdeel van nieuwe ontwikkelingen en is een belangrijke onderdeel bij (zowel dagelijkse als bestuurlijke) besluitvorming. Medewerkers die persoonsgegevens verwerken zijn zich bewust van mogelijke risico's en herkennen risico's in het eigen werk.

De gemeente zet de betrokkene centraal
De gemeente is zich bewust van haar (sterke) positie ten opzichte van de betrokkene. De gemeente gaat daarom zorgvuldig, veilig en rechtmatig om met persoonsgegevens. De betrokkene heeft een centrale plek in het proces en wordt tijdig en op een passende manier geïnformeerd over de verwerking van persoonsgegevens. De gemeente is in staat om ten behoeve van de betrokkene, een goede afweging te maken tussen doelmatigheid en rechtmatigheid. Ook wordt de betrokkene (uiteraard binnen de kaders van geldende wet- en regelgeving) in staat gesteld om regie te voeren op eigen persoonsgegevens.

De gemeente reflecteert op eigen handelen en verbetert waar nodig
De gemeente zoekt voorafgaand aan een verwerking actief naar mogelijke risico's en sluit deze zoveel mogelijk uit. Door de snelheid van (technologische) ontwikkelingen wordt periodiek geëvalueerd en worden er (waar nodig aanvullende) maatregelen genomen. Medewerkers die persoonsgegevens verwerken en verantwoordelijken kunnen rekenen op voldoende handvatten om hun verantwoordelijkheid ook daadwerkelijk te nemen.

De gemeente is open en transparant over de verwerking en bescherming van persoonsgegevens
De betrokkene wordt actief geïnformeerd over de verwerking van persoonsgegevens. De gemeente is op haar beurt in staat om (ook reactief) verantwoording af te leggen naar zowel de betrokkene, als ook de gemeenteraad en de Autoriteit Persoonsgegevens (hierna: AP) over de verwerking en bescherming van persoonsgegevens.

4.2 Vertrekpunt

Een algemene beschrijving van de bevindingen uit metingen in Q4 2023 geeft inzicht in het vertrekpunt van de gemeente Apeldoorn. Zo worden persoonsgegevens verzamelt en verwerkt, waarbij de keuzes per gegevensverwerking op verwerkingsniveau worden gemaakt vanuit persoonlijk perspectief en afhankelijk zijn van de kennis en kunde van individuele medewerkers. Hierbij ontbreekt het aan formele processen om eisen te stellen aan de verwerking van persoonsgegevens en worden er informeel keuzes gemaakt over hoe er in een concreet geval wordt omgegaan met persoonsgegevens en op welke wijze de gegevens worden verzameld en (verder) verwerkt. Dit betekent dat op dit niveau wel vastlegging kan plaatvinden, maar dat er geen sprake is van vast*stelling*. Er is geen managementcyclus, waardoor reactief wordt gereageerd op keuzes en incidenten die zich voordoen.

4.3 Aanpak

De noodzaak voor verdere implementatie van privacywetgeving en het verbeteren van de naleving wordt erkent. De gemeente Apeldoorn wil formaliseren en professionaliseren door de basis (met o.a. beleid en standaarden) te verstevigen, de implementatie ervan in de primaire processen te borgen, verantwoordelijkheden te beleggen en de kennis en het bewustzijn te vergroten. Centrale kernwaarden om dit succesvol te kunnen doen, zijn:

- Oplossingen zijn gericht op groei;
- Oplossingen zijn toepasbaar;
- Oplossingen zijn van hoge en gelijkwaardige kwaliteit;
- Oplossingen zijn duurzaam.

4.4 Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

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

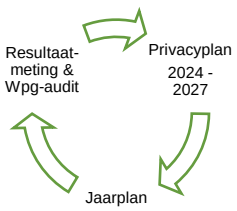
4.5 PDCA-cyclus

De naleving van privacywetgeving is geen eenmalige actie, het vraagt voortdurend om aandacht en is dynamisch. Mede daardoor is het inrichten van een PDCA-cyclus van groot belang. Hiermee worden de resultaten van uitgevoerde acties gemeten, hierop te reflecteren en het is mogelijk om tijdig bij te sturen. Onderstaande cyclus wordt daarom gehanteerd bij het verbeteren van de naleving van privacywetgeving en dit beleid.

Privacyplan 2024 – 2027
Dit plan beschrijft de richting voor het verder implementeren en professionaliseren van privacy bij gemeente Apeldoorn. Op basis van wensen, behoeften en input van in ieder geval de verwerkingsverantwoordelijken en de verplichtingen vanuit de AVG en Wpg, is de vertaalslag gemaakt naar kernwaarden, speerpunten en doelen. Dit plan wordt vastgesteld door het College van Burgermeester en Wethouders.

Jaarplan
Het jaarplan vertaalt kernwaarden, speerpunten en doelen naar concrete acties voor 1 jaar. Dit jaarplan wordt vastgesteld door de directieraad.

Resultaatmeting en audits
Voorafgaand aan het jaarplan wordt jaarlijks voor de AVG een resultaatmeting (o.b.v. het Borgingsproduct van de VNG) en een wettelijk verplichte Wpg-audit uitgevoerd. De meting en de audit geven inzicht in de resultaten van de uitgevoerde acties en of dit (nog) in lijn is met de uitgezette richting van het privacyplan. Door de resultaten jaarlijks meetbaar te maken kan tijdig worden bijgestuurd in het opvolgende jaarplan.



5 Verantwoordelijkheden

Het governancemodel van de gemeente biedt een overkoepelend beeld hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Aan de hand van het RASCI-model zijn de taken en verantwoordelijkheden voor de naleving van privacywetging beschreven. De beschrijving is in lijn met de vastgestelde Organisatieregeling en het mandaatregister van gemeente Apeldoorn en komt overeen met de huidige situatie.

In specifieke uitwerkingen van dit beleid, zijn verantwoordelijkheden eveneens benoemd en verder uitgewerkt.

5.1 Beschrijving van functies en rollen

College van Burgermeester en Wethouders
Het college is voor de meeste verwerkingen van persoonsgegevens bestuurlijk eindverantwoordelijk. Zij dienen dan ook uitvoering te (laten) geven aan privacywetgeving en dit -beleid.

Gemeentesecretaris
De gemeentesecretaris is ambtelijk eindverantwoordelijk voor de verwerking en bescherming van persoonsgegevens. De gemeentesecretaris dient uitvoering te (laten) geven aan privacywetging en dit -beleid. Hij/zij is ambtelijk verantwoordelijk voor het aanjagen en vergroten van de privacycultuur bij de gemeente Apeldoorn.

Lijnmanager / afdelingshoofd
Het lijnmanagement, veelal het afdelingshoofd, is middels mandaat verantwoordelijk voor de daadwerkelijke uitvoering van privacywetging en -beleid binnen het organisatieonderdeel. Van hen wordt verwacht dat zij wettelijke privacy taken (laten) implementeren in de primaire processen, privacy functionarissen tijdig betrekken bij ontwikkelingen en actief sturen op het vergroten van kennis en bewustzijn binnen het organisatieonderdeel.

Functionaris Gegevensbescherming
De FG is de onafhankelijk en interne toezichthouder bij gemeente Apeldoorn. De FG houdt zich primair bezig met toezicht en het adviseren van de (bestuurlijk) verwerkingsverantwoordelijke. De FG is bevoegd onderzoek te doen naar de naleving van privacywetgeving en moet daarin gefaciliteerd worden (bijvoorbeeld door toegang te krijgen tot systemen en bestanden). De taken van een FG zijn beschreven in art. 39 van de AVG en art. 36 van de Wpg. Vanwege de onafhankelijke positie van de FG, kan hij/zij niet verantwoordelijk worden gehouden voor de uitvoering en naleving van privacywetgeving bij de gemeente.

Concern Privacy Officer
De CPO werkt als onafhankelijk adviseur en houdt zich bezig met strategische, tactische en complexe privacyvraagstukken. De CPO is eveneens vakgroepleider van de vakgroep Privacy. De CPO is verantwoordelijk voor het opstellen en het beheer van privacykaders, -beleid, -processen/-procedures, -handvatten en -formats en faciliteert daarmee de verwerkingsverantwoordelijke. De CPO adviseert de verwerkingsverantwoordelijk over de naleving van privacywetgeving en bewaakt de PDCA-cyclus.

Privacy Officer
De PO’s geven (on)gevraagd advies en ondersteunen de verwerkingsverantwoordelijke. Dit doen zij op tactisch en operationeel niveau. Daarnaast realiseren en beheren zij tactische en operationele uitwerkingen van dit beleid. Zij zijn de schakel tussen beleid en de praktische toepassing.

5.2 Uitwerking RASCI-model

Bovenstaande toelichting is geconcretiseerd aan de hand van de RASCI-model. De afkorting ‘RASCI’, staat voor:

Responsible (verantwoordelijke)
Accountable (eindverantwoordelijke)
Supportive (ondersteunend)
Consulted (raadplegend)
Informed (geïnformeerd)

Op basis van de wettelijke privacytaken en de rollen vanuit het RASCI-model is onderstaande tabel gevuld met de verantwoordelijke functies. De afkortingen die zijn gebruikt, staan voor:

CvBW = College van Burgermeester en Wethouders
GC = Gemeentesecretaris
LM = Lijnmanager/afdelingshoofd
FG = Functionaris Gegevensbescherming
CPO = Concern Privacy Officer
PO = Privacy Officer

	R	**A**	**S**	**C**	**I**
Bevorderen van de privacycultuur	GC / LM	CvBW	CPO / PO	FG	
Uitvoering geven aan privacywetgeving/-beleid	GC / LM	CvBW	CPO / PO	FG	
Realisatie en beheer van privacybeleid, -procedures, -formats, -handleidingen	CPO / PO	CvBW		FG	
Uit (laten) voeren van DPIA’s	GC /LM	CvBW	PO	CPO / FG	
Beheer van het verwerkingsregister	GC / LM	CvBW	PO		CPO / FG
Afhandeling datalekken	GC / LM	CvBW	PO	CPO	FG
Afhandelen van verzoeken van betrokkenen	GC / LM	CvBW	PO		CPO / FG
Afhandelen privacy klachten	FG	FG			GC / LM
Maken van afspraken in samenwerkingen waarbij persoonsgegevens worden gedeeld	GC / LM	CvBW	PO		
Nemen van voldoende technische en organisatorische maatregelen	GC / LM	CvBW	CPO / PO	FG	
Uit (laten) voeren van (wettelijke) audits	GC / LM / CPO	CvBW	CPO / PO		FG
Signaleren en analyseren van ontwikkelen en risico’s op het gebied van gegevensbescherming	CPO / PO / FG	CvBW		GC / LM	
Toezicht op de naleving van priavcywetgeving/-beleid	FG	FG			CvBW

Andere rollen en verantwoordelijkheden

Functie	Betrokkenheid
CISO	Adviseert over de toepassing en implementatie van technische en organisatorische maatregelen. Ook wordt de (C)ISO betrokken bij de afhandeling van datalekken. Er is wederzijdse betrokkenheid bij beveiligingsincidenten en datalekken.
Communicatiemedewerker/-adviseur	In gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken.
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
Gemeentearchivaris	Stelt kaders en beleid is voor bewaren en vernietigen van informatie. Ook ziet de archivaris toe op de archivering ervan en adviseert de (verwerkings)verantwoordelijke.