gemeente Zoeterwoude

GEMEENTEBLAD

Officiële uitgave van de gemeente Zoeterwoude

Nr. 332600

4 augustus 2025

Intern regionaal privacybeleid

1 Inleiding

Binnen de gemeente Leiden, Leiderdorp, Oegstgeest en Zoeterwoude (hierna: de gemeente), gezamenlijk ook wel de Leidse regio, werken we veel met persoonsgegevens. Persoonsgegevens van inwoners, ondernemers, medewerkers en (keten)partners (hierna: betrokkenen). Een persoonsgegeven is alle informatie die iets zegt of kan zeggen over een persoon. Bijvoorbeeld een naam, rekeningnummer of Burgerservicenummer (BSN). De gemeente verzamelt persoonsgegevens om haar gemeentelijke wettelijke taken goed uit te voeren. Betrokkenen moeten erop kunnen vertrouwen dat de gemeente goed omgaat met hun persoonsgegevens. Zo wordt hun privacy geborgd.

Wat is Privacy?
Privacy is een recht dat is vastgelegd in het Europees Verdrag tot bescherming van de rechten van de mens (EVRM). In het EVRM staat dat 'een ieder het recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie'. De Algemene verordening gegevensbescherming (AVG) versterkt dit door specifieke regels te stellen voor de bescherming van persoonsgegevens.

Waarom een privacybeleid?
Dit Privacybeleid geeft invulling aan de wettelijke eisen op het gebied van de bescherming van persoonsgegevens. Daarbij gaat het vooral om de eisen uit de volgende wetten:

- Algemene verordening gegevensbescherming (AVG).
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).
- Wet politiegegevens (Wpg).

Dit Privacybeleid is van toepassing op alle persoonsgegevens die de gemeente gebruikt, laat gebruiken of met andere partijen uitwisselt. Voor sommige onderwerpen is het mogelijk om specifieker beleid, reglementen, protocollen of procedures op te stellen. Specifieke beleidsstukken moeten voldoen aan de uitgangspunten van dit algemene Privacybeleid.

Wat is de visie in de Leidse regio als het gaat om privacy?
De wereld om ons heen wordt steeds meer digitaal. Ook zijn er steeds meer innovatieve voorzieningen zoals Artificiële Intelligentie (AI). Hierdoor worden steeds andere eisen gesteld aan gegevensbescherming. Hoe dit gebeurt is vastgesteld in dit document. De gemeente is zich hiervan bewust en zet zich in voor een organisatie waarin privacy een fundament is. In het Strategisch Plan Bedrijfsvoering Leidse regio staan thema's zoals digitale transformatie en wendbare bedrijfsvoering centraal. In lijn met dat plan zorgt de gemeente altijd voor een veilige en vertrouwelijke omgang met persoonsgegevens. Daarbij wil de gemeente open en transparant zijn over hoe er met persoonsgegevens wordt omgegaan. De gemeente legt alleen persoonsgegevens vast als dit mag van de wet en als dat noodzakelijk is.

Leeswijzer

- Hoofdstuk 2: een beschrijving van de uitgangspunten die gemeente heeft als er met persoonsgegevens wordt gewerkt.
- Hoofdstuk 3: een beschrijving hoe de gemeente voldoet aan de wettelijke eisen uit de AVG.
- Hoofdstuk 4: een beschrijving van de rollen en verantwoordelijkheden per functie bij het naleven van dit Privacybeleid.
- Hoofdstuk 5: een beschrijving van de aanvullende eisen als de gemeente politiegegevens vastlegt.
- Hoofdstuk 6: een beschrijving van de aanvullende eisen als persoonsgegevens in een AI-toepassing worden gebruikt.

Waar kun je terecht met vragen over dit beleid?
Bij de Privacy Officers van Team Informatiebeveiliging & Privacy (IB&P) via de Zelf-servicedesk.

Hoelang is dit Privacybeleid geldig?
Dit Privacybeleid is vastgesteld door het college van burgemeester & wethouders op 1 juli 2025. Het beleid wordt tenminste een keer per drie jaar beoordeeld en zo nodig herzien. Als daar aanleiding voor bestaat kan het college besluiten tot een tussentijdse herziening van het Privacybeleid. Dit beleid blijft van toepassing tot het volgende Privacybeleid is vastgesteld.

2 Uitgangspunten

De gemeente houdt zich bij het verwerken van persoonsgegevens altijd aan de uitgangspunten uit dit hoofdstuk.

1. Rechtmatigheid
De gemeente gebruikt persoonsgegevens alleen in overeenstemming met de wet. Zo moet er altijd een verwerkingsgrondslag zijn om persoonsgegevens te gebruiken. Ook gaat de gemeente altijd behoorlijk en zorgvuldig om met persoonsgegevens.

2. Doelbinding
De gemeente gebruikt alleen persoonsgegevens als vooraf een duidelijk omschreven en gerechtvaardigd doel is bepaald. De gemeente gebruikt persoonsgegevens vervolgens niet verder voor andere doeleinden. Tenzij het nieuwe doel verenigbaar is met het oorspronkelijke doel en aan de wettelijke eisen wordt voldaan.

3. Minimale gegevensverwerking
De gemeente gebruikt alleen persoonsgegevens die noodzakelijk zijn om een bepaald doel te bereiken. Als de gemeente een doel kan bereiken zonder bepaalde persoonsgegevens vast te leggen is het niet toegestaan om die persoonsgegevens vast te leggen. Daarbij gelden altijd de beginselen van proportionaliteit en subsidiariteit:

- Proportionaliteit: de inbreuk op de rechten en vrijheden van betrokkenen moet in verhouding staan tot het doel.
- Subsidiariteit: Als er een mogelijkheid is om minder inbreuk te maken wordt voor die optie gekozen. Bijvoorbeeld door minder of geen persoonsgegevens vast te leggen.

4. Juiste en actuele gegevens
Het gebruiken van onjuiste persoonsgegevens kan nadelige gevolgen hebben voor betrokkenen. De gemeente neemt daarom alle redelijke maatregelen om te zorgen dat persoonsgegevens juist en actueel zijn. Indien blijkt dat persoonsgegevens niet juist of actueel zijn, worden deze hersteld.

5. Gegevens worden op tijd vernietigd
De gemeente bewaart persoonsgegevens in lijn met wettelijke bewaartermijnen en de Selectielijst gemeenten en intergemeentelijke organen. In sommige gevallen staat er in de wet of in de Selectielijst geen bewaartermijn. Alleen in die gevallen bepaalt de gemeente een bewaartermijn op basis van noodzakelijkheid. De gemeente bewaart persoonsgegevens niet langer dan noodzakelijk is om het vooraf bepaalde doel te bereiken.

6. Beveiliging van persoonsgegevens
De gemeente zorgt ervoor dat persoonsgegevens altijd goed worden beveiligd. En dat medewerkers integer en vertrouwelijk omgaan met persoonsgegevens. Daarbij geldt dat hoe gevoeliger persoonsgegevens zijn, hoe meer technische en organisatorische maatregelen worden genomen om deze te beschermen. Dit is verder uitgewerkt in het *Informatiebeveiligingsbeleid* van de gemeente.

7. Informatieplicht
De gemeente informeert betrokkenen altijd tijdig en in begrijpelijke taal over de omgang met hun persoonsgegevens en de rechten die zij hebben. Daarbij communiceert de gemeente altijd in Nederlands taalniveau B1. Alleen als in de wet een uitzondering op de informatieplicht staat, kan de gemeente hier vanaf wijken.

8. Toegang tot gegevens
Uitsluitend geautoriseerde medewerkers voor wie het noodzakelijk is om persoonsgegevens in te zien hebben toegang tot voor hen relevante persoonsgegevens. Ook hebben alleen geautoriseerde medewerkers de bevoegdheid om persoonsgegevens in te voeren, te wijzigen of te verwijderen.

9. Geen doorgifte buiten Europa (EER)
De gemeente geeft geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER), tenzij wordt voldaan aan de eisen uit de AVG die hiervoor gelden.

10. Profilering en geautomatiseerde besluitvorming
De gemeente doet niet aan profilering en neemt geen geautomatiseerde besluiten die gevolgen hebben voor betrokkenen. Een medewerker van de gemeente zal altijd de computer controleren. Een eventueel besluit neemt de medewerker ook altijd zelf.

3 Borging en beheersing privacy

De gemeente moet aantoonbaar voldoen aan de (U)AVG en Wpg. Dit brengt verschillende verplichtingen met zich mee.

1. Privacy by design en Privacy by default naleven
Privacy by design betekent dat in de 'ontwerpfase' van een werkproces, applicatie of dienst wordt nagedacht over het zo privacyvriendelijk mogelijk inrichten daarvan. Bijvoorbeeld dat alleen die persoonsgegevens worden vastgelegd die nodig zijn om een verzoek af te handelen. Privacy by default betekent dat standaardinstellingen zo privacyvriendelijk mogelijk worden ingesteld. De gemeente heeft dit vastgelegd in het *Beleid Privacy by Design*. Naast dat deze beginselen wettelijk verplicht zijn, zijn deze beginselen ook erg efficiënt. Achteraf bijstellen is minder efficiënt en kostbaarder. Deze beginselen worden bij leveranciers afgedwongen door de toepassing ervan als eis op te nemen in een programma van eisen bij een aanbestedingsprocedure.

2. Data Protection Impact Assessment uitvoeren
De gemeente voert een Data Protection Impact Assessment (DPIA) uit voor processen waar waarschijnlijk een verhoogd privacyrisico is. Dit is bijvoorbeeld het geval voor gemeentelijke taken waar met veel gevoelige persoonsgegevens van kwetsbare personen wordt gewerkt. Een DPIA is een vragenlijst om voor een bepaald proces in kaart te brengen of er privacyrisico's zijn. Voor die risico's worden maatregelen bedacht om ze weg te nemen. De Autoriteit Persoonsgegevens heeft een lijst opgesteld voor gevallen waarin wettelijk verplicht een DPIA moet worden uitgevoerd. Als er twijfel is of een DPIA wettelijk verplicht is voert de gemeente een pre-DPIA uit. Aan de hand van die vragenlijst adviseert een Privacy Officer of een DPIA wettelijk verplicht is. Dit is uitgewerkt in de Procedure risicoanalyses (DPIA). De gemeente houdt de uitgevoerde DPIA's bij in een register.

3. Register van verwerkingen bijhouden
De gemeente houdt een register van verwerkingen bij. Dit is een overzicht van alle activiteiten waarbij de gemeente werkt met persoonsgegevens. Per activiteit is aanvullende informatie te vinden over de gegevensverwerking. Bijvoorbeeld:
- welke persoonsgegevens de gemeente gebruikt.
- wat daarvan het doel is.
- hoe lang de persoonsgegevens worden bewaard.
- of deze persoonsgegevens worden gedeeld met andere partijen.

Dit overzicht moet altijd volledig en actueel zijn. In het kader van transparantie streeft de gemeente ernaar dit register van verwerkingen zoveel mogelijk openbaar te maken. Dit is verder uitgewerkt in de Procedure beheren en publiceren register van verwerkingen.

4. Datalekken melden
Bij een datalek hebben personen toegang tot andermans persoonsgegevens zonder dat dit de bedoeling is. Er is ook sprake van een datalek als persoonsgegevens worden gewijzigd of verwijderd zonder dat dit de bedoeling is. Als er sprake is van een risico voor de betrokkene moet een datalek binnen 72 uur worden gemeld bij de Nederlandse toezichthouder: de Autoriteit Persoonsgegevens. Als er sprake is van een hoog risico moet ook zo snel als mogelijk de betrokkene worden geïnformeerd. De gemeente legt alle datalekken vast in een intern datalekregister. Ieder kwartaal vindt er een evaluatie plaats van alle datalekken die hebben plaatsgevonden. Dit is verder uitgewerkt in de Procedure datalekken.

5. Zorgvuldig samenwerkingen
De gemeente wisselt persoonsgegevens uit met andere partijen. Dit gebeurt alleen als het is toegestaan en er vooraf contractuele afspraken over zijn gemaakt. Afhankelijk van de situatie worden de afspraken vastgelegd in een van de volgende overeenkomsten:
- Verwerkersovereenkomst.
- Overeenkomst gezamenlijk verwerkingsverantwoordelijken.
- Convenant.
- Gegevensuitwisselingsovereenkomst tussen zelfstandig verwerkingsverantwoordelijken.

De gemeente gebruikt daarbij zoveel als mogelijk haar eigen sjablonen. Dit en een uitleg van de type overeenkomsten is verder uitgewerkt in de Procedure privacy overeenkomsten.

6. Rechten van betrokkenen uitvoeren
De AVG en Wpg brengen niet alleen verplichtingen mee voor de gemeente. Ze brengen ook mee dat betrokkenen verschillende rechten hebben:
- Het recht op informatie.

- Het recht op inzage.
- Het recht op rectificatie of aanvulling.
- Het recht op verwijdering.
- Het recht op beperking van de verwerking.
- Het recht op dataportabiliteit.
- Het recht op bezwaar.
- Het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.

Hoe de gemeente deze verzoeken van betrokkenen afhandelt is vastgelegd in de Procedure rechten van betrokkenen.

Als een betrokkene een klacht indient over de omgang met zijn persoonsgegevens is de Functionaris Gegevensbescherming (FG) hiervoor het eerste aanspreekpunt.

7. Bewustwording vergroten
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 binnen de gemeente voortdurend aan te scherpen. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens. Bijvoorbeeld via een e-learning. De Privacy Officers stellen daarnaast ieder jaar een bewustwordingsplan op en voeren daarin opgenomen acties uit. Ieder kwartaal evalueren ze deze acties. Het onderwerp bewustwording is verder uitgewerkt in het *Beleid veilig personeel*.

8. Evaluatie uitvoeren
De gemeente streeft ernaar om in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control zijn betekent dat de gemeente weet welke 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. Daarom vinden er verschillende evaluaties plaats:
- Kwartaalevaluatie: ieder kwartaal evalueren de Privacy Officers de datalekken, inzageverzoeken, DPIA's, bewustwording en procedures.
- Jaarlijkse evaluatie: jaarlijks wordt er een (privacy)nulmeting gedaan. Uit de nulmeting wordt duidelijk wat het volwassenheidsniveau van de gemeente is. Aan de hand van de nulmeting wordt een rapportage en jaarplan opgesteld om verbeteringen door te voeren.

4 Rollen en verantwoordelijkheden

Om aan de verplichtingen uit de (U)AVG en Wpg te voldoen is het van belang om taken en verantwoordelijkheden duidelijk af te bakenen en te beleggen. In dit hoofdstuk wordt per functie beschreven wat de rollen en verantwoordelijkheden zijn.
Heb je vragen over de rollen en verantwoordelijkheden of heb je hulp nodig bij de uitvoering? Dan kun je terecht bij de Privacy Officers van Team Informatiebeveiliging & Privacy (IB&P) via de Zelf-servicedesk.

1. College van burgemeester & wethouders
Het college van burgemeester en wethouders, waar de burgemeester onderdeel van is, is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. De gemeentesecretaris is belast met de ambtelijke uitvoering namens het college. Het college heeft de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente.
- Stelt het Privacybeleid vast.
- Geeft sturing aan privacy beleidsvoering.
- Evalueert de toepassing en werking van het Privacybeleid op basis van de rapportage van de FG.
- Stelt voldoende middelen beschikbaar voor de naleving van het Privacybeleid en bevordert een duurzame privacycultuur.

2. Clustermanagers
De clustermanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen hun cluster. Zij hebben de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen cluster.
- Verantwoordelijk voor implementatie en uitvoering van het Privacybeleid binnen het eigen cluster.
- Informeert op verzoek van de FG op welke manier de eigen cluster voldoet aan de privacywetgeving.
- Bevordert een duurzame privacycultuur.

De Griffier voert deze taken bij de Griffie uit.

3. Teammanagers

Elke teammanager is binnen het eigen team verantwoordelijk voor de naleving van het Privacybeleid en een zorgvuldige omgang met persoonsgegevens. Een teammanager is vaak proceseigenaar. Als een team geen teammanager, maar een coördinator heeft gaan deze verantwoordelijkheden over op de clustermanager. De clustermanager kan bepaalde taken beleggen bij de programmamanager, een projectleider of coördinator, maar blijft zelf wel eindverantwoordelijk. De Griffier voert deze taken bij de Griffie uit.

Teammanagers hebben de volgende rollen en verantwoordelijkheden als het gaat om hun eigen team:
- Het tijdig betrekken van een Privacy Officer bij een nieuwe of wijziging van een activiteit waarbij persoonsgegevens worden vastgelegd.
- Het maken van contractuele afspraken over gegevensuitwisseling bij een nieuwe samenwerking.
- Het (laten) uitvoeren van een Data Protection Impact Assessment (DPIA) voor hoog risico activiteiten. Bijvoorbeeld als er veel gevoelige persoonsgegevens worden vastgelegd. Ook verantwoordelijk voor het opvolgen van maatregelen volgend uit een DPIA of het accepteren van risico's.
- Het registreren van nieuwe activiteiten in het register van verwerkingen en het doorvoeren van wijzigingen van bestaande activiteiten.
- Het verstrekken en intrekken van autorisaties van medewerkers.
- Het tijdig (laten) melden van datalekken binnen het team.
- Het tijdig oppakken van verzoeken van betrokkenen die hun rechten uitoefenen onder coördinatie van de Privacy Officer.
- Bevordert een duurzame privacycultuur binnen de afdeling, door periodiek beleid, procedures en privacygerelateerde onderwerpen onder de aandacht te brengen.

Teammanagers kunnen bij deze taken altijd hulp krijgen van de Privacy Officers, maar blijven wel verantwoordelijk voor de uitvoering van deze taken. Ook kunnen ze bepaalde taken laten uitvoeren door medewerkers binnen de afdeling. Bijvoorbeeld het uitvoeren van een DPIA of het bijhouden van het register van verwerkingen.

4. Functionaris Gegevensbescherming
Op basis van de AVG en de Wet politiegegvevens (Wpg) is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG en Wpg. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG stelt bij de uitoefening van zijn taak prioriteiten en richt zijn inspanningen op aangelegenheden waarbij sprake is van grotere risico's.

De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
- Interne toezichthouder op de naleving van de AVG en Wpg.
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan.
- Draagt Privacybeleid actief uit binnen de gehele gemeente en bevordert een duurzame privacycultuur.
- Adviseert de gemeente bij privacy klachten en verzoeken van betrokkenen.
- Adviseert de gemeente ten aanzien van het wegnemen of verminderen van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog risico dossiers.
- Adviseert de gemeente indien nodig bij datalekken.
- Ziet toe op bewustwording en opleiding van medewerkers.
- Ziet toe op het uitvoeren van audits.
- Treedt op als contactpunt voor de toezichthouder (Autoriteit Persoonsgegevens) en betrokkenen.
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie).
- Rapporteert aan het college van burgemeester & wethouders, de directie en de Gemeenteraad.

5. Privacy Officer
De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vragen. De Privacy Officer heeft een monitorende en ondersteunende functie bij het naleven en uitvoeren van het Privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:
- Adviseert en faciliteert de gemeente ten aanzien van het naleven en de uitvoering van het Privacybeleid.
- Opstellen Privacybeleid, procedures, formats en standaardovereenkomsten.
- Monitort en ondersteunt bij het registreren of wijzigen van verwerkingen in het register van verwerkingen.
- Adviseert en ondersteunt de gemeente bij het uitvoeren van Data Protection Impact Assessments (DPIA's).
- Adviseert over de bepalingen in verwerkersovereenkomsten en ondersteunt bij het opstellen, aanpassen en uitonderhandelen daarvan.

- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER.
- Adviseert over de verwerkingsgrondslag en rechtmatigheid van verwerkingen van persoonsgegevens.
- Ontwikkelt, organiseert en voert bewustwordingsprogramma's en privacytrainingen voor medewerkers uit.
- Adviseert en coördineert verzoeken van betrokkenen die hun rechten uit de AVG en Wpg uitoefenen.
- Adviseert de gemeente over privacy-by-design en privacy by default bij ontwikkeling van nieuwe systemen en processen. Ook adviseert de Privacy Officer bij aanbestedingen.
- Het inrichten van een privacyboekhouding zodat aan de verantwoordingsplicht wordt voldaan. Dit betekent het bijhouden van de administratie. Bijvoorbeeld het DPIA-register en Register datalekken.
- Toezichthouden op het BRP-domein (Basisregistratie Personen).
- Ondersteunt en faciliteert de gemeente bij het afhandelen van datalekken (volgens de meldprocedure).

6. De (Chief) Information Security Officer ((C)ISO)
De (C)ISO draagt zorgt voor de informatiebeveiliging binnen de gemeente. De (C)ISO zorgt voor een actueel informatiebeveiligingsbeleid. De rollen en verantwoordelijkheden van de (C)ISO staan in het *informatiebeveiligingsbeleid*.

7. Medewerkers
Medewerkers hebben een grote rol in de manier waarop de gemeente omgaat met persoonsgegevens. Alle medewerkers hebben een eigen verantwoordelijkheid hierin. Van hen wordt verwacht dat zij zorgvuldig en integer omgaan met persoonsgegevens en kennisnemen van dit Privacybeleid. Ook wordt verwacht dat zij actief hun kennis up-to-date houden door de aangeboden (digitale) trainingen te volgen.

5 Aanvullende eisen Wet politiegegevens

In dit hoofdstuk staan de aanvullende eisen die gelden als de gemeente politiegegevens vastlegt. Dit zijn vooral de gegevens die buitengewoon opsporingsambtenaren (hierna: boa's) vastleggen bij hun handhavingstaken. Voor die gegevens geldt de Wet politiegegevens (hierna: Wpg) en niet de AVG.

1. Werkinstructies vastleggen
De gemeente voorziet in werkinstructies per domein waarin boa's politiegegevens vastleggen. De boa's werken in lijn met die werkinstructie bij de uitvoering van hun opsporingstaken. De werkinstructies bevatten onder andere de volgende onderwerpen: Principes, vastlegging van gegevens (feiten/persoonlijk oordeel en categorie van betrokkene), delen van gegevens, bewaartermijnen, melden van datalekken en onderzoeken.

2. Bewaartermijn van politiegegevens hanteren
In de Wet politiegegevens staan bewaartermijnen voor politiegegevens. De gemeente hanteert altijd deze bewaartermijnen.

3. Het verstrekken en ter beschikking stellen van politiegegevens
Binnen het Wpg-domein stelt de gemeente politiegegevens ter beschikking op basis van het 'free flow of information'-principe. Dit betekent dat politiegegevens beschikbaar worden gesteld als dit noodzakelijk is voor de uitoefening van de taken binnen het Wpg-domein. Buiten het Wpg-domein verstrekt de gemeente alleen politiegegevens als dit volgens de Wpg is toegestaan. Daarbij wijst de gemeente de ontvangende partij op de plicht tot geheimhouding van de politiegegevens. De gemeente legt alle verstrekkingen vast.

4. Autorisaties inregelen
De gemeente stelt ten aanzien van het verlenen, wijzigen- en beëindigen van toegang tot politiegegevens een Autorisatieprocedure Wpg vast. De gemeente autoriseert een boa als de toegang noodzakelijk is voor het uitvoeren van de opgedragen opsporingstaken. Als niet-boa's toegang nodig hebben tot politiegegevens neemt de gemeente een autorisatiebesluit. De gemeente wijst een boa op de plicht tot geheimhouding en de gevolgen bij de schending van deze plicht. Als een boa van functie verandert of uit dienst gaat, wijzigt of beëindigt de gemeente de autorisaties.

5. Logging bijhouden
Loggegevens zijn automatische registraties van acties en gebeurtenissen in een systeem, zoals wie wanneer een bestand heeft geopend en gegevens heeft gewijzigd. De gemeente controleert en evalueert periodiek de toegekende autorisaties van de boa's. Het doel hiervan is de integriteit en de rechtmatigheid van de toegang tot politiegegevens waarborgen. De gemeente gebruikt de loggegevens alleen om te controleren of de gegevensverwerking op een juiste en rechtmatige manier gebeurt. Deze gegevens

helpen bij verplichte controles (audits) en zorgen ervoor dat toegang tot politiegegevens eerlijk en volgens de regels verloopt. De gemeente legt het resultaat van de periodieke controle vast in een verslag van bevindingen. De gemeente bewaart deze gegevens 5 jaar.

6. Audits uitvoeren
In de Wet politiegegevens staan wettelijk verplichte audits. De gemeente volgt deze wettelijke auditcyclus. Dit betekent elke vier jaar een externe audit en ieder jaar een interne audit. De resultaten van een externe audit worden gedeeld met de Autoriteit Persoonsgegevens. De gemeente stelt hiervoor een auditplan vast en zorgt dat het omgaan met politiegegevens in opzet, bestaan en in de werking voldoet aan de wet. De FG en auditor houden hier toezicht op. Als uit de externe audit blijkt dat de verwerking van politiegegevens op onderdelen niet voldoet aan de wet volgt er een hercontrole. Hierin staan de tekortkoming en verbeteringen centraal.

6 Aanvullende eisen inzet Artificiële Intelligentie (AI)

Bij de inzet van AI worden soms persoonsgegevens gebruikt. Zowel in de ontwikkel-, als ook in de test- en prodcutiefase. Als bij de inzet van AI persoonsgegevens worden gebruikt zijn de eisen uit dit Privacybeleid van toepassing. Naast de eisen uit dit Privacybeleid gelden ook andere eisen. Bijvoorbeeld wettelijke verplichtingen uit de AI-verordening. Die eisen vallen buiten de reikwijdte van dit Privacybeleid. De belangrijkste eisen uit het Privacybeleid zijn:

1. Rechtmatigheid
De gemeente gebruikt persoonsgegevens alleen in overeenstemming met de wet. Zo moet er altijd een verwerkingsgrondslag zijn om persoonsgegevens te gebruiken bij het trainen en gebruiken van AI.

2. Geautomatiseerde besluitvorming
De gemeente doet niet aan profilering en neemt geen geautomatiseerde besluiten die gevolgen hebben voor betrokkenen. Een medewerker controleert altijd de computer of AI en neemt zelf een besluit.

3. Dataminimalisatie
Om een AI te trainen is data nodig. Voor deze data geldt altijd het beginsel van dataminimalisatie als het gaat om persoonsgegevens. Dit betekent dat alleen persoonsgegevens worden gebruikt die noodzakelijk zijn om het doel te bereiken.

4. Transparantie
De gemeente informeert betrokkenen op een heldere en duidelijke manier over wat er met hun persoonsgegevens gebeurt. Als daarbij AI wordt gebruikt, legt de gemeente in duidelijke taal uit wat een AI doet en welke persoonsgegevens daarbij zijn gebruikt.

5. Rechten van betrokkenen
De gemeente zorgt ervoor dat betrokkenen hun rechten kunnen uitoefenen. Dit betekent dat altijd duidelijk moet zijn waar persoonsgegevens van betrokkenen zijn opgeslagen. In de gehele levenscyclus van data in AI moet duidelijk zijn welke persoonsgegevens zijn gebruikt.

6. Data Protection Impact Assessment
Bij complexe AI-systemen waar persoonsgegevens worden gebruikt voert de gemeente altijd een Data Protection Impact Assessment (DPIA) uit.

7. Persoonsgegevens op tijd verwijderen
De gemeente verwijdert persoonsgegevens als deze niet meer nodig zijn. Dit geldt voor gehele levenscyclus van persoonsgegevens in relatie tot een AI-systeem.