gemeente putten

GEMEENTEBLAD

Officiële uitgave van de gemeente Putten

Nr. 168008

9 april

2026

Beleidsregels Wet politiegegevens

Het college van burgemeester en wethouders van de gemeente Putten,
gelezen het voorstel van burgemeester en wethouders van 17 maart 2026, nr. 2112181;
gelet op het bepaalde in artikel 3, 4, 8 en 25 van de Wet politiegegevens, artikel 4, 6, 30 en 33 van het Besluit politiegegevens.

besluit:

vast te stellen de Beleidsregels Wet politiegegevens.

Artikel 1: Begripsbepalingen

In dit beleid wordt verstaan onder:

a. *gemeente Putten:*
het college van de burgemeester en wethouders als verwerkingsverantwoordelijke van de politiegegevens;

b. *buitengewoon opsporingsambtenaar:*
de buitengewoon opsporingsambtenaar (boa) als bedoeld in het Besluit buitengewoon opsporingsambtenaar;

c. *opsporingstaak :*
de opsporing van de strafbare feiten als bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering;

d. *akte van opsporingsbevoegdheid:*
de akte van opsporingsbevoegdheid als bedoeld in artikel 142, eerste lid, onder a, van het Wetboek van Strafvordering;

e. *wet:*
de Wet politiegegevens (Wpg), het Besluit politiegegevens, het Besluit politiegegevens voor buitengewoon opsporingsambtenaar en de Regeling periodieke audit politiegegevens;

f. *beschikbaar studiemateriaal:*
het Praktijkhandboek van de wet politiegegevens, de Verstrekkingenwijzer en het Naslagwerk Verstrekken op grond van de wet politiegegevens;

g. *Wpg-domein:*
domein bestaande uit de politie, marechaussee, rijksrecherche, Bijzondere Opsporingsdiensten en de buitengewoon opsporingsambtenaren;

h. *politiegegevens:*
persoonsgegevens die in het kader van de uitoefening van de politietaak worden verwerkt;

i. *verwerken van politiegegevens:*
elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens;

j. *autorisatiebeleid:*
het autorisatiebeleid voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens;

k. *verwerker van politiegegevens:*
degene die, niet werkzaam binnen de gemeentelijke organisatie, het geheel of een gedeelte van het geautomatiseerde systeem onder zich heeft waarmee de politiegegevens worden verwerkt.

Artikel 2: Het aanwijzen van de buitengewoon opsporingsambtenaar

1. De gemeente Putten wijst de buitengewoon opsporingsambtenaar aan, indien de buitengewoon opsporingsambtenaar in het bezit is van een:
   a. akte van opsporingsbevoegdheid;
   b. verklaring omtrent het gedrag;

2. De buitengewoon opsporingsambtenaar voldoet aan de her- en bijscholingsplicht.

3. De gemeente Putten organiseert ten aanzien van politiegegevens bewustwordingsactiviteiten dan wel cursussen over de omgang met politiegegevens, die door de buitengewoon opsporingsambtenaar jaarlijks verplicht worden bijgewoond.

Artikel 3: Het verlenen, wijzigen en beëindigen van de toegang tot politiegegevens
(artikel 6 van de Wet politiegegevens)

1. De gemeente Putten stelt ten aanzien van het verlenen, wijzigen- en beëindigen van toegang tot politiegegevens een autorisatiebeleid vast.
2. De gemeente Putten verleent aan de buitengewoon opsporingsambtenaar conform het vastgestelde autorisatiebeleid een autorisatie tot politiegegevens, indien de toegang tot politiegegevens noodzakelijk is voor het uitvoeren van de aan de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
3. De gemeente Putten wijst de buitengewoon opsporingsambtenaar ten aanzien van politiegegevens op de plicht tot geheimhouding en de consequenties bij de schending van deze plicht.
4. Indien de buitengewoon opsporingsambtenaar van functie verandert dan wel uit dienst gaat, wordt de autorisatie conform het autorisatiebeleid gewijzigd of beëindigd.

Artikel 4: De plicht tot loggen
(artikel 32a van de Wet politiegegevens)

1. De gemeente Putten controleert en evalueert periodiek de toegekende autorisaties van de buitengewoon opsporingsambtenaar met als doel om de integriteit en de rechtmatigheid van de toegang tot politiegegevens te waarborgen.
2. Indien de gemeente Putten een verwerker heeft ingeschakeld dan heeft deze ook ten aanzien van de periodieke controle de plicht om de toegang tot politiegegevens te loggen.
3. Deze verwerker verstrekt op verzoek van de gemeente Putten de logginggegevens zodat deze conform het autorisatiebeleid periodiek gecontroleerd kunnen worden.
4. De gemeente Putten gebruikt de logginggegevens (eigen en eventueel verwerker) uitsluitend voor de controle van de rechtmatigheid van de gegevensverwerking, ter ondersteuning van de verplichte audits en ter waarborging van de integriteit en de rechtmatigheid van de toegang tot politiegegevens.
5. De gemeente Putten legt het resultaat van de periodieke controle vast in een verslag van bevindingen, welke wordt gearchiveerd binnen het daartoe bestemde en beveiligde zaaksysteem.
6. De gemeente Putten bewaart de logginggegevens (eigen en eventueel verwerker) alsmede het resultaat van de periodieke controle voor een periode van vijf jaar.

Artikel 5: Het verwerken van politiegegevens

1. De gemeente Putten voorziet in werkinstructies per boa-domein, die de buitengewoon opsporingsambtenaar bij de uitvoering van de opsporingstaak in acht neemt.
2. De buitengewoon opsporingsambtenaar verwerkt politiegegevens ten behoeve van de uitvoering van de politietaak als bedoeld in artikel 8 van de Wet politiegegevens.
3. De buitengewoon opsporingsambtenaar verwerkt geen politiegegevens, indien het gegevens betreft die niet noodzakelijk zijn voor de uitvoering van de aan hem of haar opgedragen opsporingstaak.
4. De buitengewoon opsporingsambtenaar maakt bij het verwerken van politiegegevens onderscheid tussen:
   a. de verschillende categorieën van betrokkenen zoals genoemd in artikel 6b van de Wet politiegegevens;
   b. gegevens die gebaseerd zijn op feiten en een persoonlijk oordeel zoals genoemd in artikel 4 van de Wet politiegegevens.
5. Indien de gemeente Putten een verwerker heeft ingeschakeld dan heeft deze ook ervoor te zorgen dat het onderscheid zoals genoemd in het vierde lid en onder a van dit artikel in de applicatie, waartoe de buitengewoon opsporingsambtenaar toegang heeft, mogelijk wordt gemaakt.
6. De buitengewoon opsporingsambtenaar neemt geen besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking zoals bedoeld in artikel 7a van de Wet politiegegevens, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem of haar in aanmerkelijke mate treft.

gemeente putten

Artikel 6: De termijnen van politiegegevens
(artikel 14 van de Wet politiegegevens)

1. De gemeente Putten voorziet in voldoende waarborgen om te bewerkstelligen dat de politiegegevens conform de wet niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
2. De gemeente Putten zorgt ervoor dat de politiegegevens voor de uitvoering van de opsporingstaak zoals bedoeld in artikel 8 van de Wet politiegegevens:
   a. gedurende een jaar beschikbaar zijn in het kader van de uitvoering van de opsporingstaak;
   b. na een jaar slechts beschikbaar zijn voor het gericht zoeken;
   c. na vijf jaar worden verwijderd;
   d. na tien jaar worden vernietigd.
3. Indien de gemeente Putten een verwerker heeft ingeschakeld dan zorgt deze ook ervoor dat bewaartermijnen conform de wet en het tweede lid van dit artikel geconfigureerd zijn, zodat gewaarborgd is dat de politiegegevens niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de opsporingstaak.
4. De buitengewoon opsporingsambtenaar neemt de termijnen conform de wet en het tweede lid van dit artikel in acht.

Artikel 7: Het ter beschikking stellen en verstrekken van politiegegevens
(artikel 15 en paragraaf 3 van de Wet politiegegevens)

1. De gemeente Putten stelt de politiegegevens conform de wet ter beschikking op basis van het 'Free flow of information' principe, indien het ter beschikking stellen van politiegegevens noodzakelijk is voor de uitoefening van de taken binnen het Wpg-domein.
2. De gemeente Putten mag de politiegegevens verstrekken zoals beschreven in de verstrekkingenwijzer aan partijen buiten het Wpg-domein. Daarbij wijst de gemeente Putten de ontvangende partij op de plicht tot geheimhouding die op de verstrekte gegevens van toepassing is.
3. De gemeente Putten legt de verstrekking zoals genoemd in het tweede lid van dit artikel vast. (artikel 32, eerste lid aanhef en onder b, van de Wet politiegegevens)
4. Indien de gemeente Putten een verwerker heeft ingeschakeld dan heeft deze ook ten aanzien van het tweede lid van dit artikel de plicht om binnen de gebruikte applicaties, technische mogelijkheden te creëren, waarmee verstrekkingen kunnen worden vastgelegd. (artikel 32, eerste lid aanhef en onder b van de Wet politiegegevens)
5. Indien de gemeente Putten een verwerker heeft ingeschakeld dan dient deze ervoor te zorgen dat de geautomatiseerde verstrekkingen, zoals bijvoorbeeld aan het Centraal Justitieel Incassobureau, conform de wet plaatsvinden en worden gedocumenteerd.
6. De gemeente Putten alsmede de verwerker voorzien in de technische mogelijkheden om ervoor te zorgen dat de politiegegevens door middel van een beveiligde wijze worden verstrekt aan de ontvangende partij.
7. De gemeente Putten verstrekt geen politiegegevens aan ontvangers in derde landen of internationale organisaties.

Artikel 8: De rechten van de betrokkenen
(paragraaf 4 van Wet politiegegevens)

1. De gemeente Putten draagt zorg voor het informeren van de betrokkenen over de verwerking van politiegegevens. Dit vindt plaats conform paragraaf 4 van de Wet politiegegevens. Daarbij heeft de gemeente Putten de plicht tot:
   a. actieve informatieverstrekking waarbij de informatievoorziening op de website conform de wet plaatsvindt;
   b. passieve informatieverstrekking; waarbij de informatie op verzoek wordt verstrekt, tenzij het verzoek conform artikel 27 van de Wet politiegegevens geheel of gedeeltelijk kan worden afgewezen, bijvoorbeeld als de informatieverstrekking de opsporing en vervolging belemmert.
2. De gemeente Putten stelt conform de wet een procedure vast de behandeling van verzoeken van betrokkenen, bestaande uit:
   a. recht op informatie;
   b. inzagerecht;
   c. correctierecht;
   d. recht van verzet;
   e. recht op bezwaar.

gemeente putten

Artikel 9: Het behandelen van datalekken
(artikel 33a van de Wet politiegegevens)

1. De gemeente Putten stelt conform de wet een procedure vast voor het melden van een (vermoedelijke) inbreuk op de beveiliging op politiegegevens, waaronder voor het melden van datalekken.
2. De gemeente Putten houdt een register bij van gemelde datalekken.

Artikel 10: Het register van verwerkingen
(artikel 31d van de Wet politiegegevens)

1. De gemeente Putten houdt een register van verwerkingen bij, waarin per verwerking minimaal de volgende informatie voorkomt:
   a. de naam en contactgegevens van de gemeente Putten;
   b. de verwerkingsdoeleinden;
   c. een beschrijving van de categorieën persoonsgegevens die worden verwerkt;
   d. een beschrijving van de categorieën betrokkenen;
   e. een beschrijving van de categorieën van ontvangers aan wie de politiegegevens ter beschikking worden gesteld of worden verstrekt;

2. De gemeente Putten actualiseert jaarlijks het register van verwerkingen.

Artikel 11: Het uitvoeren van een audit
(artikel 33 van de Wet politiegegevens)

1. De gemeente Putten laat conform de wet, eenmaal in de vier jaren een externe audit uitvoeren.
2. De gemeente Putten voert ter voorbereiding op de verplichting in het eerste lid van dit artikel, jaarlijks een interne audit uit.
3. De gemeente Putten stelt ten behoeve van het tweede lid van dit artikel een auditplan vast.
4. De betrokken verwerkers dienen ten behoeve van de audit een Third Party Memorandum verklaring te overleggen die conform de 'Nederlandse Orde van EDP Auditors handreiking' wordt uitgevoerd, zodat deze verklaring betrokken kan worden bij de beoordeling van de audit.
5. Indien uit de resultaten van de audit, zoals bedoeld in het eerste lid van dit artikel, blijkt dat de verwerking van de politiegegevens op onderdelen niet voldoet aan de wettelijke normen, dient de gemeente Putten binnen een jaar zorg te dragen voor deze tekortkomingen, met als doel dat deze worden verholpen. Daarnaast voert de gemeente Putten binnen één jaar een hercontrole uit, binnen de onderdelen waarvan het resultaat onvoldoende bleek te zijn.
6. Indien blijkt dat de beheersmaatregelen ten aanzien van de gebruikte applicatie(s) niet voldoen aan de wettelijke normen, dan draagt de verwerker verantwoordelijkheid voor het verhelpen van de tekortkomingen binnen een periode van één jaar.
7. De gemeente Putten zendt een afschrift van de controleresultaten van de audit zoals bedoeld in het eerste lid van dit artikel aan de Autoriteit Persoonsgegevens.

Artikel 12: De functionaris gegevensbescherming
(artikel 36 van de Wet politiegegevens)

1. De gemeente Putten stelt een functionaris gegevensbescherming aan ten behoeve van de controle en het toezicht op het verwerken van politiegegevens conform de wet en het beleid van de gemeente Putten.
2. De functionaris gegevensbescherming voert daarbij periodiek controles uit op het naleven van de wettelijke verplichtingen, waaronder de controle op:
   a. de bewustwordingsverplichting conform het derde lid van artikel 1 van dit beleid;
   b. het autorisatieproces conform artikel 2 van dit beleid;
   c. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
   d. het verwerken van politiegegevens conform artikel 5 van dit beleid;
   e. de bewaartermijnen conform artikel 6 van dit beleid;
   f. het ter beschikking stellen en verstrekken van politiegegevens zoals bedoeld in artikel 7 van dit beleid;
   g. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse zoals genoemd artikel 8 van dit beleid;
   h. het register voor verwerkingen conform artikel 11 van dit beleid;

gemeente putten

i. de verplichtingen ten aanzien van de audit conform artikel 12 van dit beleid;

3. De functionaris gegevensbescherming stelt periodiek rapportages op en rapporteert zo nodig rechtstreeks aan de gemeente Putten.

Artikel 13: De verplichtingen van de gemeente Putten

1. De gemeente Putten draagt zorg dat de procesinrichting voor de verwerking van politiegegevens in opzet, bestaan en dat de werking voldoet zoals genoemd in de wet, zodat hierop door de auditor en de functionaris gegevensbescherming toezicht kan worden gehouden.
2. De gemeente Putten treft daarbij conform de wet passende technische- en organisatorische maatregelen om ongeoorloofde of onrechtmatige verwerkingen, verlies, vernietiging of beschadiging van politiegegevens tegen te gaan, met als doel om de rechtmatigheid en beveiliging van politiegegevens te waarborgen. (artikel 4a en 4b van de Wet politiegegevens)
3. Indien er sprake is van een hoog risico op de rechten en vrijheden van betrokkenen, dan voert de gemeente Putten conform artikel 4c van de Wet politiegegevens een risicoanalyse, zoals een Data protection impact assessment (DPIA), uit.
4. De gemeente Putten maakt uitsluitend gebruik van een verwerker, indien de verwerker afdoende garandeert dat de passende technische- en organisatorische maatregelen en procedures zodanig worden geïmplementeerd dat voldaan wordt aan het bij of krachtens de wet bepaalde (Artikel 6c, 4a en 4b van de Wet politiegegevens).
5. Deze verwerker verstrekt op verzoek van de gemeente Putten alle informatie die nodig is om de nakoming van de verplichtingen uit artikel 6, 32 en 32a van de Wet politiegegevens aan te tonen.
6. De gemeente Putten legt de verplichtingen zoals genoemd in het vijfde lid van dit artikel, vast in een schriftelijke overeenkomst, welke door beide partijen wordt ondertekend. (artikel 6c, tweede lid, van de Wet politiegegevens)
7. De gemeente Putten voldoet aan de documentatieplicht zoals genoemd in de wet. (artikel 32, eerste lid, van de wet Politiegegevens)

Artikel 14: Slotbepaling

Dit besluit treedt in werking op de dag na publicatie.

Putten, 17 maart 2026.

Burgemeester en wethouders van Putten,
R. 't Hoen
gemeentesecretaris
H.A. Lambooij
burgemeester

gemeente putten

Bijlage 1 Privacybeleid Wet politiegegevens

Gemeente Putten

1 Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente heeft in haar privacybeleid en informatiebeveiligings-beleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.
De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.
Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.
Het huidige privacybeleid van de gemeente gaat alleen uit van de AVG. Het is daarom wenselijk de verplichtingen uit de Wpg hier aan toe te voegen. Dit wordt vastgelegd in dit beleidsdocument.

2 Doelstellingen van het WPG privacybeleid

Het privacybeleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen;
- Gedrag vertonen dat past bij goed werknemerschap;
- De kans op financiële en imagoschade minimaliseren.

3 Wpg kader

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd binnen CityControl;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden binnen CityControl;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de

wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

3.1 Register van verwerkingen
Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

3.2 Strategisch informatiebeveiligings- en privacy beleid
Het **strategisch informatiebeveiligings- en privacy beleid (IB&P- beleid) van de gemeente Putten** is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.
Het IB&P-beleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

3.3 FG en bevoegd functionaris
<u>De Functionaris Gegevensbescherming (FG)</u>
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.
De taken van de FG (artikel 36 van de Wet politiegegevens) met betrekking tot de Wpg kunnen als volgt worden samengevat. De FG voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op:

1. het beleid voor de uitvoering van de Wpg;
2. de bewustwordingsverplichting;
3. het autorisatieproces met betrekking tot het vastleggen van politiegegevens;
4. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
5. het verwerken van politiegegevens;
6. de bewaartermijnen;
7. het ter beschikking stellen en verstrekken van politiegegevens;
8. de informatiebeveiliging en het uitvoeren van een risicoanalyse;
9. de gegevensbeschermingseffectbeoordelingen;
10. het register voor verwerkingen;
11. de verplichtingen ten aanzien van de audit;

Daarnaast is het de taak van de FG om samen te werken met de Autoriteit persoonsgegevens en op te treden als contactpunt voor de Autoriteit Persoonsgegevens inzake aangelegenheden in verband met de verwerking van persoonsgegevens en indien nodig overleg te plegen.
<u>De bevoegd functionaris</u>
Indien er sprake is van verwerking onder artikel 9 wordt er een functie aangewezen die verantwoordelijk is voor het uitvoeren van de taak bevoegd functionaris. Dit is de ‘hoeder’ van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type

gemeente putten

gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt.

3.4. Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan beschreven in het privacybeleid van de gemeente en in aanvullend specifiek beleid. Dat beleid voorziet ook in de verplichtingen die voortvloeien uit de Wpg. Op hoofdlijnen zijn de rechten op grond van de Wpg gelijkluidend aan die van de AVG. Op een aantal punten verschilt dit. Voor de Wpg zijn de rechten van betrokkenen separaat uitgewerkt in een protocol. Betrokkenen kunnen de volgende verzoeken/bezwaren bij de gemeente doen:

- recht op informatie (Wpg art 24);
- recht op inzage (Wpg art 25);
- recht op rectificatie en/of aanvulling en/of vernietiging (Wpg art 28).

De gemeente kan het verzoek m.b.t. politiegegevens (Wpg) van de betrokkene afwijzen als:

- Het gerechtelijke onderzoeken of procedures zou belemmeren.
- Dat nadelige gevolgen heeft voor het voorkomen van het begaan van strafbare feiten, voor opsporing, onderzoek, vervolging of het opleggen van straffen.
- De openbare veiligheid in het geding is.
- De rechten en vrijheden van derden worden geschonden.
- De nationale veiligheid in het geding is.
- Een verzoek kan ook worden afgewezen als het kennelijk een ongegrond of buitensporig verzoek is.

Bij een inzageverzoek op basis van de Wpg verstrekt de gemeente geen documenten, maar stelt de betrokkene in de gelegenheid om op inzage te komen. Hierbij mogen geen foto's en of kopieën gemaakt worden van deze afschriften. In het besluit wordt opgenomen welke gegevens Gemeente Putten geregistreerd heeft (Wpg art 29 lid 5).

3.5 Het bewaren van politiegegevens

Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.
Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

3.6. Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg maakt een onderscheid tussen het *ter beschikking stellen* van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.
Bij het *verstrekken* van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.
De gemeente Putten verstrekt *geen* Wpg gegevens aan landen buiten de EER (derde landen).

3.7. Het melden van datalekken

De gemeente Putten heeft separaat een procedure voor datalekken. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:

- Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

3.8. Bewustwording

Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
Elke nieuwe medewerker moet daarom verplicht een Wpg training doorlopen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

3.9. Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden: https://www.putten.nl/Home/Over_deze_website/Privacyverklaring