

Addendum privacybeleid

Wet politiegegevens (Wpg)

Datum:	2025-08-18
Versie:	0.3
Status:	Definitief
Auteur:	FB
Opdrachtgever:	Directie

Inhoudsopgave

1	Administratie	3
1.1	Versiebeheer document.....	3
1.2	Goedkeuring	3
1.3	Distributie.....	3
1.4	Afkorting	3
2	Inleiding	4
2.1	Doel dit document.....	4
2.2	Management samenvatting	4
3	Twee regimes voor de boa: de AVG en Wpg	5
4	Verwerkingsgrondslagen Wet politiegegevens	5
5	Het bewaren van politiegegevens	6
6	Het ter beschikking stellen en verstrekken van politiegegevens.....	6
7	Register van verwerkingen	7
8	Het melden van datalekken.....	7
9	Rechten van betrokkenen.....	7
10	Functionaris gegevensbescherming en bevoegd functionaris.....	8
11	Verantwoordingsplicht (accountability).....	9
12	Informatiebeveiligingsbeleid	9
13	Bewustwording	10
	Bijlage 1: Checklist Wet politiegegevens (Wpg)	11

1 Administratie

1.1 Versiebeheer document

Versie	Datum	Door	Omschrijving
0.1	03-04-2025	FB	Eerste opzet
0.2	08-06-2025	EV JH RK TH NT	Diverse redactionele wijzigingen
0.3	18-07-2025	FB	Laatste redactionele wijzigingen

1.2 Goedkeuring

Versie	Datum	Naam	Functie	Record te vinden in:
0.3	19-08-2025	AO		

1.3 Distributie

Versie	Datum	Ontvanger	Doel

1.4 Afkortingen

Afkorting	Omschrijving
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie Adressen en Gebouwen
BF	Bevoegd functionaris
Bibob.	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur.
BIO	Baseline Informatiebeveiliging Overheid
BOA	Buitengewoon opsporingsambtenaar
BRP	Basisregistratie personen
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris gegevensbescherming
MAS	Methodische Aanpak Schoolverzuim
Wpg	Wet politiegegevens

2 Inleiding

2.1 Doel dit document

Sinds 25 mei 2018 geldt in de hele EU dezelfde privacywetgeving: de Algemene verordening gegevensbescherming (AVG). Het doel van de verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie. De AVG geldt voor de verwerking van persoonsgegevens, maar niet voor de verwerking van persoonsgegevens die gaan over de voorkoming, opsporing en vervolging van strafbare feiten. Naast de AVG is er een aparte Europese Richtlijn gegevensbescherming politie en justitie, die tegelijk met de AVG tot stand kwam. In Nederland is deze richtlijn per 1 januari 2019 geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens. De belangrijkste verandering voor Nederland is dat de Wpg nu ook geldt voor buitengewoon opsporingsambtenaren (boa's). Het bestaande privacybeleid van de gemeente richt zich voornamelijk op de AVG. Het is daarom gewenst er de verplichtingen op grond van de Wpg aan toe te voegen.

2.2 Management samenvatting

De gemeente heeft buitengewoon opsporingsambtenaren (boa's) in dienst voor taken in het kader van toezicht en handhaving van de openbare orde en de sociale veiligheid. Voorbeelden van boa's in dienst bij de gemeente zijn: gemeentelijke handhavers, parkeercontroleurs en leerplichtambtenaren. Een boa houdt toezicht op de lokale veiligheid, leefbaarheid en de naleving van (specialistische) regels. Bij overtredingen treedt de boa handhavend op. Hiertoe verwerkt een boa persoonsgegevens.

Als een boa persoonsgegevens verwerkt bij het uitvoeren van zijn toezichthoudende taak is de AVG van toepassing. Verwerkt een boa persoonsgegevens voor zijn politietaak (zoals het opsporen van strafbare feiten en het handhaven van de openbare orde), dan geldt de Wpg. Net als de AVG stelt de Wpg eisen aan de verwerking van persoonsgegevens. De Wpg heeft het in dat verband over politiegegevens. AVG en Wpg kennen veel overeenkomsten, maar op onderdelen zijn er ook duidelijke verschillen. Zo kent de Wpg specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook zijn er aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacy-rechten van betrokkenen. Het is bijvoorbeeld mogelijk dat er soms (tijdelijk) wordt afgezien van het melden van een datalek aan de betrokken persoon of personen. Dit wanneer de belangen op het gebied van opsporen en vervolgen zwaarder wegen. In het kader van de Wpg is bovendien ook eens per 4 jaar een externe audit verplicht en moeten er elk jaar interne audits worden gehouden. De AVG kent een dergelijke audit-verplichting niet.

Met dit addendum op het privacybeleid willen we medewerkers bewust maken van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens en van het verschil in benadering op het snijvlak van AVG en Wpg. Uitgangspunt daarbij is dat we de rechten van betrokkenen maximaal willen respecteren en werken volgens de vastgestelde procedures.

3 Twee regimes voor de boa: de AVG en Wpg

Boa's hebben vaak meerdere taken en verwerken verschillende soorten gegevens. Persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder, bijvoorbeeld bij een inspectie, vallen onder de AVG. Maar de gegevens die de Boa als opsporingsambtenaar verwerkt, bijvoorbeeld het controleren van iemands identiteit als hij een verdachte aanhoudt of boetes uitdeelt, vallen onder de Wpg. Een boa heeft dus een 'twee-petten-uitdaging'. Soms lopen deze taken in elkaar over en is het niet altijd duidelijk of de AVG of Wpg van toepassing is. En dat kan voor problemen of, in sommige gevallen, voor boetes zorgen. De gegevenshuishouding, systemen en werkprocessen moeten daarom zodanig worden ingericht dat voor alle betrokkenen duidelijk is onder welk wettelijk regime de verwerkingen plaatsvinden en aan ter zake geldende specifieke eisen en verplichtingen kan worden voldaan.

In ieder boa-domein gelden - vaak landelijke - regels en werkafspraken over wanneer de boa van pet moet wisselen. Voor de sociale recherche geldt bijvoorbeeld dat een vermoed fraudebedrag boven vijftigduizend euro strafrechtelijk wordt onderzocht en afgehandeld. Deze regeling bepaalt in dit geval dan de knip wanneer gegevens onder de Wpg vallen. Leerplichtambtenaren werken volgens de Methodische Aanpak Schoolverzuim (MAS). Deze is ontwikkeld door een aantal instanties en de landelijke vereniging voor leerplichtambtenaren om schooluitval te voorkomen. Per soort verzuim is in de MAS vastgelegd wanneer er proces-verbaal moet worden opgemaakt. En daarmee ligt dus vast wanneer de overstap van AVG naar Wpg plaatsvindt.

4 Verwerkingsgrondslagen Wet politiegegevens

De Wpg onderscheidt verschillende grondslagen waarvoor politiegegevens mogen worden verwerkt. Deze staan in de artikelen 8 t/m 13. Voor boa's zijn echter alleen artikel 8, 9 en 13-verwerkingen van toepassing. Afhankelijk van de grondslag gelden er andere voorwaarden. In Hellendoorn kennen we op dit moment alleen artikel 8-verwerkingen. Politiegegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak vallen hieronder. Dit gaat over zaken als foutief aanbieden van afval, alcohol gebruiken op de openbare weg, foutief parkeren en loslopende honden. Ook proces-verbaal opmaken bij luxe-verzuim in het kader van leerplicht valt hieronder. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan. Het is belangrijk dat dit ook altijd duidelijk vastgelegd wordt.

Bij artikel 9-verwerkingen gaat het om gegevensverwerkingen die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto of stelselmatige observatie. In Hellendoorn kennen we dit soort onderzoeken niet.

Artikel 13 biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9, vaak landelijk, verder te verwerken ter ondersteuning van het werk. Denk bijvoorbeeld aan het verwerken van namen en adressen van mensen die vuurwapengevaarlijk zijn. Bij boa's zijn geen artikel 13-verwerkingen bekend.

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. Artikel 8-gegevens kunnen gedurende een periode van één jaar na de datum van de eerste verwerking worden verwerkt. In de vier daarop volgende jaren mogen de gegevens alleen met een gerichte zoekvraag worden geraadpleegd en verwerkt. Bijvoorbeeld door te zoeken op een naam, adres of kenteken. Daarna worden ze vijf jaar bewaard en daarna dienen ze te worden vernietigd.

Gedurende de bewaartermijn kunnen de gegevens gebruikt worden voor het afhandelen van klachten en voor audits of een controle door de Autoriteit Persoonsgegevens. Verder geldt dat deze gegevens onder bepaalde omstandigheden ter beschikking kunnen worden gesteld voor hernieuwde verwerking, maar dan alleen in opdracht van het bevoegd gezag. Ze komen dan als het ware opnieuw tot leven in een actueel opsporingsonderzoek. Gegevens in de bewaartermijn mogen ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.

6 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 houdt in dat deze in principe worden gedeeld met andere opsporingsambtenaren die de gegevens nodig hebben voor de uitoefening van hun 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.

Uit het beginsel van de "free flow of information" dat aan de wet ten grondslag ligt, vloeit voort dat de door de boa's verwerkte gegevens vrijelijk kunnen worden uitgewisseld met de politie, de Koninklijke marechaussee of een andere bijzondere opsporingsdienst. Andersom geldt dat de boa's vrijelijk kennis kunnen nemen van de gegevens die bij de politie, de Koninklijke marechaussee of een andere bijzondere opsporingsdiensten worden verwerkt, voor zover dit noodzakelijk is voor een goede uitvoering van hun taak. Slechts in bijzondere gevallen kan de ter beschikkingstelling worden geweigerd of aan voorwaarden worden gebonden.

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 daarop gebaseerde Besluit politiegegevens zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er altijd wordt voldaan aan de documentatieverplichting. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob.

Voor het overige is iedereen die over politiegegevens beschikt, verplicht tot geheimhouding. Dit geldt zowel voor gegevens die boa's zelf verwerken als voor gegevens van collega's waar de boa toegang toe heeft. Als gegevens verstrekt worden, reist de geheimhoudingsplicht mee. De ontvanger mag de gegevens dan alleen verwerken voor het doel waarvoor ze zijn verkregen.

7 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 autorisaties.

8 Het melden van datalekken

Bij een datalek gaat het om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden. Maar ook om situaties waarbij persoonsgegevens verloren zijn gegaan of waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben. Wanneer een datalek heeft plaatsgevonden dient dit in principe binnen 72 uur te worden gemeld bij de Autoriteit Persoonsgegevens (AP). En in sommige gevallen ook aan de betrokkenen zelf. Op deze mededelingsplicht zijn op grond van de Wpg enkele uitzonderingen van toepassing. Zo is het bijvoorbeeld mogelijk dat er soms (tijdelijk) wordt afgezien van het melden van een datalek aan de betrokken persoon of personen. Dit wanneer de belangen op het gebied van opsporen en vervolgen zwaarder wegen. De gemeente heeft een vastgestelde procedure datalekken waarin is beschreven op welke wijze datalekken binnen de gemeente worden afgehandeld. Die geldt zowel voor AVG als Wpg. Tevens is er een intern register van datalekken waarin alle geconstateerde beveiligingsincidenten worden geregistreerd.

9 Rechten van betrokkenen

De gemeente verstrekt aan de betrokkene informatie over de verwerking van politiegegevens in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt met passende middelen, waaronder elektronische, verstrekt en in het algemeen in dezelfde vorm als de vorm van het verzoek. De betrokkene krijgt binnen zes weken uitsluitel over de

verwerking van hem betreffende persoonsgegevens en, wanneer dat het geval is, over zijn verzoek om die persoonsgegevens in te zien. De Wpg schrijft voor dat de verwerkingsverantwoordelijke zijn beslissing voor ten hoogste vier weken kan verdagen, dan wel voor ten hoogste zes weken indien blijkt dat bij verschillende regionale eenheden of bij de landelijke eenheid van de politie politiegegevens over de verzoeker worden verwerkt. Van de verdaging wordt schriftelijk mededeling gedaan. De gemeente kan het verzoek van 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. De gemeente zorgt voor de afdoening van het verzoek door middel van een formeel besluit welke open staat voor rechtstreeks beroep bij de bestuursrechter. De gemeente verstrekt in principe 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 de gemeente geregistreerd heeft.

De betrokkene heeft daarnaast het recht op, op diens schriftelijke verzoek, rectificatie van de hem betreffende onjuiste politiegegevens te verkrijgen en, rekening houdend met het doel van de verwerking, het recht om onvolledige politiegegevens te laten aanvullen, onder meer door middel van een aanvullende verklaring. Het verzoek bevat de aan te brengen wijzigingen.

De betrokkene heeft verder het recht op diens schriftelijke verzoek zonder onnodige vertraging vernietiging van de hem betreffende politiegegevens te verkrijgen indien de gegevens in strijd met een wettelijk voorschrift worden verwerkt of om te voldoen aan een wettelijke verplichting. In plaats van vernietiging draagt de verwerkingsverantwoordelijke zorg voor afscherming als:

- a. de juistheid van de gegevens door de betrokkene wordt betwist en de juistheid of onjuistheid niet kan worden geverifieerd, in welk geval de verwerkingsverantwoordelijke de betrokkene informeert voordat de afscherming wordt opgeheven, of
- b. de gegevens moeten worden bewaard als bewijsmateriaal.

De gemeente stelt de betrokkene binnen vier weken schriftelijk in kennis van de opvolging van zijn verzoek en geeft de rectificatie van de onjuiste politiegegevens door aan de bevoegde autoriteit van wie de gegevens afkomstig zijn. Ook de ontvangers van die gegevens worden geïnformeerd.

10 Functionaris gegevensbescherming en bevoegd functionaris

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de Functionaris Gegevensbescherming (FG). In de basis is de FG de toezichthouder voor zowel de AVG en de Wpg. Alleen als sprake is van een groot aantal Wpg-verwerkingen, is het aan te raden om een

FG specifiek als toezichthouder voor de Wpg aan te wijzen. 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 bevoegd functionaris (BF) is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en toetst doelfwikkend gebruik op subsidiariteit en proportionaliteit. Iedere artikel 9-verwerking dient een bevoegd functionaris te hebben. Omdat we binnen de gemeente geen artikel 9-verwerkingen kennen, is er ook geen bevoegd functionaris aangewezen.

11 Verantwoordingsplicht (accountability)

Een van de belangrijkste uitgangspunten van de Wpg is – net als bij de AVG – het principe van accountability: organisaties die persoonsgegevens verwerken hebben een verantwoordingsplicht. Dit houdt in dat we actief moeten kunnen aantonen dat wij compliant zijn en voldoen aan de Wpg. Als gemeente zullen we dus zoveel mogelijk moeten documenteren, bijvoorbeeld bij de verstrekking of doorgifte van politiegegevens aan derden. Getroffen maatregelen dienen continu te worden geëvalueerd en indien nodig geactualiseerd.

Er geldt met ingang van 2021 bovendien een verplichting van een externe privacy-audit, die eens in de vier jaar wordt uitgevoerd. Deze audit richt zich onder andere op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn én de werking van deze maatregelen en procedures. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegevens (AP).

Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarna er binnen een jaar een her-controle plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de Wpg waar de tekortkomingen geconstateerd worden. De resultaten worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit. Ter voorbereiding op de externe audit wordt jaarlijks een interne audit uitgevoerd.

12 Informatiebeveiligingsbeleid

Informatiebeveiliging is cruciaal voor het naleven van de Wpg, omdat het de bescherming van deze gegevens tegen ongeautoriseerde toegang en misbruik waarborgt. Organisaties die onder de Wpg vallen, moeten daarom passende technische en organisatorische maatregelen nemen om problemen op dit gebied te voorkomen. De basis daarvoor is de Baseline Informatiebeveiliging Overheid (BIO). Vanaf 2020 is dit het normenkader op het gebied van informatieveiligheid voor alle overheden: Rijk, provincies, waterschappen en gemeenten. De BIO geldt voor alle activiteiten van de gemeente. Uitgangspunt is een risicogerichte benadering, om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd.

De gemeente heeft een informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de verplichtingen uit de BIO. Het informatiebeveiligingsbeleid is

een richtinggevend en kaderstellend document. De gemeente vult het aan met specifieke (beleids-) documenten, procedures en werkinstructies. Getroffen maatregelen worden bovendien periodiek geëvalueerd en zo nodig geactualiseerd. Het college verantwoordt zich jaarlijks over informatiebeveiliging door middel van de ENSIA zelfevaluatie.

13 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 en andere bij het proces betrokken medewerkers. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Elke nieuwe medewerker moet daarom naast de algemene introductietraining Informatieveiligheid en Privacy verplicht een Wpg-training doorlopen. 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, 'awareness'-campagne of een bijeenkomst over een specifiek Wpg-onderwerp.

Bestandsnaam	:	<i>Addendum Wet politiegegevens (Wpg)</i>
Kenmerk	:	<i>2025 - 011657</i>
Datum	:	<i>18 juli 2025</i>

Bijlage 1: Checklist Wet politiegegevens (Wpg)

Aanwijzen buitengewoon opsporingsambtenaar

1. De gemeente 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. Elke nieuwe medewerker die politiegegevens verwerkt moet naast de algemene introductie-training Informatieveiligheid en Privacy verplicht een Wpg-training doorlopen.
3. Organiseer daarnaast jaarlijks bewustwordingsactiviteiten dan wel cursussen over de omgang met politiegegevens, die door de buitengewoon opsporingsambtenaar verplicht worden bijgewoond.

Verlenen, wijzigen en beëindigen van de toegang tot politiegegevens (artikel 6 Wpg)

1. Verleen aan de buitengewoon opsporingsambtenaar – conform het gemeentelijke autorisatiebeleid – een autorisatie tot politiegegevens indien de toegang tot politiegegevens noodzakelijk is voor het uitvoeren van de aan de opsporingsambtenaar opgedragen opsporingstaak.
2. Wijs de buitengewoon opsporingsambtenaar ten aanzien van politiegegevens op de plicht tot geheimhouding en de consequenties bij de schending van deze plicht.
3. Wijzig of beëindig de autorisatie onmiddellijk als de buitengewoon opsporingsambtenaar van functie verandert dan wel uit dienst gaat.

De plicht tot loggen (artikel 32a Wpg)

1. De gemeente heeft de plicht om de toegang tot politiegegevens te loggen.
2. Gebruik logginggegevens 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.
3. Logginggegevens en het resultaat van de periodieke controle worden bewaard voor een periode van vijf jaar.

Het verwerken van politiegegevens

1. Voorzie 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 Wpg.
3. Er worden geen politiegegevens verwerkt, indien het gegevens betreft die niet noodzakelijk zijn voor de uitvoering van de aan hem of haar opgedragen opsporingstaak.
4. Bij het verwerken van politiegegevens wordt onderscheid gemaakt tussen:
 - a. de verschillende categorieën van betrokkenen zoals genoemd in artikel 6b Wpg;
 - b. gegevens die gebaseerd zijn op feiten en een persoonlijk oordeel zoals genoemd in artikel 4 Wpg.
5. Het hiervoor genoemde onderscheid wordt in de applicatie, waartoe de buitengewoon opsporingsambtenaar toegang heeft, mogelijk gemaakt.

6. Schenk voortdurend aandacht aan de volledigheid, actualiteit en juistheid van de verwerkte politiegegevens. Dit onder andere via adequate koppelingen met de BRP, BAG en de RDW. Gebruik bijzondere persoonsgegevens alleen als dat strikt noodzakelijk is.
7. Er worden geen besluiten genomen die uitsluitend gebaseerd zijn op geautomatiseerde verwerking zoals bedoeld in de Wpg, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem of haar in aanmerkelijke mate treft.
8. Politiegegevens mogen niet voor andere doelen worden verwerkt dan voor de in de Wpg genoemde doeleinden.

De termijnen van politiegegevens (artikel 14 Wpg)

1. Voorzie 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. Zorg ervoor dat de politiegegevens voor de uitvoering van de opsporingstaak zoals bedoeld in artikel 8 Wpg:
 - 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. Zorg ervoor dat de bewaartermijnen conform de wet geconfigureerd zijn, zodat gewaarborgd is dat de politiegegevens niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de opsporingstaak.

Het ter beschikking stellen en verstrekken van politiegegevens (artikel 15 Wpg)

1. Politiegegevens worden ter beschikking gesteld 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. Politiegegevens mogen ook aan partijen buiten het Wpg-domein worden verstrekt zoals beschreven in de verstrekkingenwijzer. Daarbij wijst de gemeente de ontvangende partij op de plicht tot geheimhouding die op de verstrekte gegevens van toepassing is. De gemeente legt deze verstrekking vast binnen de betreffende applicaties (artikel 32 Wpg).
3. Zorg ervoor dat de geautomatiseerde verstrekkingen, zoals bijvoorbeeld aan het Centraal Justitieel Incassobureau, conform de wet plaatsvinden en worden gedocumenteerd.
4. Het verstrekken van politiegegevens aan een ontvangende partij geschiedt altijd op veilige wijze (bijvoorbeeld via beveiligde mail).
5. De gemeente verstrekt geen politiegegevens aan ontvangers in derde landen of internationale organisaties.

De rechten van de betrokkenen (paragraaf 4 Wpg)

1. Zorg voor het informeren van de betrokkenen over de verwerking van politiegegevens. Dit vindt plaats conform paragraaf 4 Wpg. Daarbij heeft de gemeente 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 dit conform artikel 27 Wpg niet wenselijk is, bijvoorbeeld als de informatie-verstrekking de opsporing en vervolging belemmert.
2. Stel voor de behandeling van verzoeken van betrokkenen een procedure vast. Daarbij gaat het om het recht op informatie, inzage, correctie, verzet alsmede om het recht op bezwaar.

Het register van verwerkingen (artikel 31d Wpg)

1. De gemeente houdt een register van verwerkingen bij, waarin per verwerking minimaal de volgende informatie voorkomt:
 - a. de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
 - b. de doelen van de verwerking;;
 - c. de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
 - d. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
 - e. in voorkomend geval, het gebruik van profilering;
 - f. in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie;
 - g. een aanwijzing van de rechtsgrondslag van de verwerking;
 - h. zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;
 - i. zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging;
 - j. de toekenning van de autorisaties.
2. Het register van verwerkingen dient jaarlijks te worden geactualiseerd.

Het behandelen van datalekken (artikel 33a Wpg)

1. Stel 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 houdt een register bij van gemelde datalekken.

Uitvoeren Wpg-audit (artikel 33 Wpg)

1. De gemeente laat conform de wet, eenmaal in de vier jaren een externe audit uitvoeren.
2. Ter voorbereiding op de audit-verplichting wordt jaarlijks een interne audit uitgevoerd, waar een auditplan voor wordt opgesteld.
3. Betrokken verwerkers dienen ten behoeve van de audit een TPM-verklaring te overleggen die conform de 'Nederlandse Orde van EDP Auditors handreiking' wordt uitgevoerd..
4. Indien uit de resultaten van de externe audit blijkt dat de verwerking van de politiegegevens op onderdelen niet voldoet aan de wettelijke normen wordt een verbeterplan opgesteld. Daarnaast dient de gemeente binnen een jaar een hercontrole uit te laten voeren.
5. De Autoriteit Persoonsgegevens ontvangt een afschrift van de controleresultaten.

De functionaris gegevensbescherming (artikel 36 Wpg)

1. De gemeente stelt een functionaris gegevensbescherming aan ten behoeve van de controle

- en het toezicht op de naleving van de Wpg. Zonder expliciet besluit is dit automatisch de op grond van de AVG aangewezen functionaris gegevensbescherming
2. De functionaris gegevensbescherming is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de Wpg.
 3. De functionaris gegevensbescherming maakt jaarlijks een toezichtplan, voert dit uit en rapporteert zo nodig rechtstreeks aan het bestuur en hoogste management.
 4. De functionaris gegevensbescherming is contactpersoon voor de Autoriteit Persoonsgegevens.

De verplichtingen van de gemeente

1. De gemeente draagt zorg voor passende technische- en organisatorische maatregelen om ongeoorloofde of onrechtmatige verwerkingen, verlies, vernietiging of beschadiging van politiegegevens tegen te gaan (artikel 4a en 4b van de Wet politiegegevens).
2. De Wpg vereist dat alle bestanden waarin politiegegevens opgeslagen worden, gescheiden zijn van andere gegevensbestanden. Zorg bovendien dat politiegegevens alleen worden verwerkt in politiesystemen die van een Wpg keurmerk – dat wil zeggen een Wpg TPM van een RE – zijn voorzien.
3. Wanneer sprake is van een verwerking waarbij er sprake is van een hoog risico op de rechten en vrijheden van betrokkenen, is conform artikel 4c Wpg een Data protection impact assessment (DPIA), vereist. (Bijvoorbeeld het starten van een artikel 13 verwerking, of de aanschaf van een nieuw systeem waarin politiegegevens worden verwerkt).
4. De inzet van een verwerker vindt uitsluitend plaats indien de verwerker afdoende garandeert dat passende technische- en organisatorische maatregelen worden genomen en daarover verantwoording aflegt. Afspraken op dit punt worden vastgelegd in een schriftelijke overeenkomst (artikel 6c, tweede lid, Wpg).
5. De gemeente voldoet aan de documentatieplicht zoals genoemd in de wet (artikel 32 Wpg).