Privacy Statement

Inhoudsopgave

0. Algemeen

De politie verzamelt en verwerkt gegevens, dat is de kern van ons werk. Daarmee kunnen we waakzaam en dienstbaar zijn. Met al die gegevens gaan wij integer om, met respect voor ieders privacy en met de grootst mogelijke zorgvuldigheid. In dit privacy statement laten we zien met welk doel we gegevens verzamelen, hoe we ze gebruiken en wat uw rechten zijn. Dit privacy statement kan ook wijzigen. In dat geval informeren wij u daarover op onze website.

De politie heeft op dit gebied te maken met twee wetten:

- Wet Politiegegevens (Wpg)

Voor het verwerken van persoonsgegevens voor de uitvoering van de politietaak: handhaven van de openbare orde, strafrechtelijke handhaving en het verlenen van hulp.

- Algemene verordening gegevensbescherming (AVG)

Voor het verwerken van persoonsgegevens voor andere taken dan de politietaak, zoals interne bedrijfsvoering.

1. Verwerkingsverantwoordelijke

De Korpschef is belast met de leiding over de politieorganisatie. Hij is zoals we dat noemen, de verwerkingsverantwoordelijke. De korpschef bepaalt met welk doel en met welke middelen, hoe en welke gegevens worden verwerkt. De verwerkingsverantwoordelijke moet voldoen aan privacywet- en regelgeving.

Naast de politie zijn er andere organisaties die zich bezighouden met opsporing. Zij hebben hun eigen verwerkingsverantwoordelijke.
De korpschef wordt in zijn werk bijgestaan door leidinggevenden van de eenheden en het bedrijfsvoeringsonderdeel.

Dat zijn de:
- CIO (Chief Information Officer), tevens lid korpsleiding
- Politiechefs van de eenheden
- Directeuren
- Kwartiermaker LMO (Landelijke Meldkamer Organisatie).

De korpschef geeft hen mandaat en volmacht om bepaalde taken over te nemen. Dat betekent dat zij in naam van de korpschef beslissingen nemen en bepalen op welke manier en voor welk doel persoons- en politiegegevens worden verwerkt.

Bijzondere opsporingsdiensten (bod'en)
Bijzondere opsporingsdiensten zijn ondergebracht bij de:
- FIOD (ministerie van Financiën)
- Inspectie Leefomgeving en Transport (ministerie van Infrastructuur en Waterstaat)
- Nederlandse Voedsel- en Waren Autoriteit (ministerie van Landbouw, Natuur en Voedselkwaliteit)
- Inspectie SZW (ministerie Sociale Zaken en Werkgelegenheid)

Bod'en hebben de taak om zware of middelzware vergrijpen op te sporen en strafrechtelijk te vervolgen. Ze mogen dat alleen doen op het werkterrein van het ministerie waartoe ze behoren. De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door medewerkers van de bijzondere opsporingsdiensten.

Buitengewoon opsporingsambtenaren
Buitengewoon opsporingsambtenaren (boa's) sporen strafbare feiten op. Ze vullen de politie, KMar en rijksrecherche aan bij het handhaven van de rechtsorde. Hun opsporingsbevoegdheden beperken zich tot één bepaald werkterrein (domein). Een parkeerwachter bijvoorbeeld, mag alleen controleren of mensen zich aan de parkeerregels houden, niets meer en niets minder.

Als een buitengewoon opsporingsambtenaar optreedt als boa, dus onder gezag van de officier van justitie, dan is de Wet politiegegevens (Wpg) van toepassing. Sommige boa's hebben ook andere functies of taken. Denk hierbij aan toezicht en handhaving binnen hun domein. De Wpg is daarop niet van toepassing.

1.a. Verwerkers en verwerkersovereenkomsten
De politie kan niet alle verwerkingen van gegevens zelf uitvoeren. Soms besteden wij dit uit aan een andere partij: de verwerker. Om ervoor te zorgen dat deze verwerker voldoet aan de privacywet- en regelgeving en de beleidsnormen van de politie, stellen we een verwerkersovereenkomst op.

De verwerker is degene die de verwerking van gegevens daadwerkelijk uitvoert. Maar de korpschef blijft de verantwoordelijke en kan de verwerker dus ook aanwijzingen en opdrachten geven. Denk hierbij aan KPN, die websites van de politie host, waaronder politie.nl.

Als verwerkingsverantwoordelijke is de korpschef verantwoordelijk voor de verwerkingen die de verwerker heeft uitgevoerd.

De verwerkingsverantwoordelijke mag alleen een beroep op een verwerker doen als die voldoende maatregelen heeft genomen om aan de privacywetgeving te voldoen (art. 28 AVG en art. 6c Wpg). Dit houdt in dat de verwerker passende technische en organisatorische maatregelen moet nemen om de privacy van de betrokkenen te waarborgen.

2. Waarvoor verwerkt de politie persoonsgegevens?

In de wet staat dat persoonsgegevens rechtmatig moeten worden verwerkt. Als politie hebben wij te maken met twee wetten: de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Naast deze twee zijn er nog andere wetten die iets zeggen over het verwerken van persoonsgegevens in bijzondere situaties.

Wet politiegegevens (Wpg): politietaak
Het verwerken van persoonsgegevens voor het uitvoeren van onze politietaak valt onder de Wpg. Denk hierbij aan gegevens die we verzamelen voor het opsporen van strafbare feiten, het handhaven van de openbare orde of hulpverlening. We kunnen deze gegevens ook gebruiken voor bigdata-analyses, profileringen en gegevensverwerking met behulp van sensoren. Uiteraard doen we dit allemaal binnen de kaders van de wet.

Algemene verordening gegevensbescherming (AVG): interne bedrijfsvoering
Naast het uitvoeren van politietaken, zijn we ook een 'gewoon' bedrijf. Voor het verwerken van gegevens voor onze

interne bedrijfsvoering is de AVG van toepassing, zoals de personeelsadministratie, klachtenafhandeling, ICT-voorzieningen, marketing en communicatie.

Dan zijn er nog meer taken die onder de AVG vallen: het verlenen van vergunningen door de korpschef, de vreemdelingentaak van de politie, en het beheer van de 1-1-2 alarmcentrale door de korpschef.

De Wpg en de AVG geven aan op welke gronden de politie verkregen gegevens mag verwerken. Dat zijn de limitatieve verwerkingsgrondslagen. Alleen als het gebruik van persoonsgegevens onder een van deze grondslagen valt, is de verwerking rechtmatig.

Overzicht van de verwerkingsgrondslagen en de redenen waarvoor de politie persoonsgegevens verwerkt.

Wet politiegegevens (Wpg)

Op basis van deze grondslagen in de Wpg verwerkt de politie persoonsgegevens (artikel 8 tot en met 10, artikel 12 en artikel 13 Wpg)

Dagelijkse politietaak (art. 8): politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak: handhaving van wetten en regels, hulpverlening, surveillance, verkeerszaken en eenvoudige opsporingsonderzoeken.

Uitgebreidere opsporingsonderzoeken en veelplegersdossiers (art. 9): politiegegevens kunnen gericht worden verwerkt voor onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval. Denk hierbij aan het verzamelen van gegevens over een bepaalde persoon of naar aanleiding van een specifieke gebeurtenis.

Opbouw informatieposities opsporingsonderzoeken en veelplegersdossiers (art.10): politiegegevens kunnen gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde. Het gaat hier om het opbouwen van een informatiedossier over mensen, maar los van concrete handhavings- of opsporingsacties.

Informanten (art.12): politiegegevens kunnen worden verwerkt voor de controle op en het beheer van gegevens die door een informant zijn verstrekt. Ook geeft dit artikel aan hoe het gebruik van informantengegevens beoordeeld en verantwoord dient te worden.

Ondersteuning van de politietaak (art.13): politiegegevens die zijn verwerkt op basis van artikel 8, 9 of 10 kunnen ook voor andere doeleinden worden gebruikt. Bijvoorbeeld om verdachten of betrokkenen te identificeren, of voor specialistische onderwerpen, zoals de forensische opsporing.

We kunnen als dat nodig is meerdere soorten persoonsgegevens verzamelen, afhankelijk van het soort onderzoek en het doel, zoals:

- personalia (naam, voornaam, adres, geboortedatum)
- IP-adres, kenteken
- financiële gegevens
- bijzondere persoonsgegevens, zoals biometrische gegevens, zoals DNA.

Onze informatiesystemen maken gebruik van basisregistraties van overheidsinstellingen met publiekrechtelijke taken, zoals:

- Basisregistratie Personen (BRP) van de Rijksdienst voor identiteitsgegevens (RvIG)
- Kentekenregister van de (Rijksdienst voor het Wegverkeer) RDW
- Basisregistraties Adressen en Gebouwen (BAG) van het Kadaster
- Handelsregister van de Kamer van Koophandel (KvK)

Uit deze basisregistraties kunnen we ook persoonsgegevens halen. Wanneer we die gegevens hebben verwerkt zijn het voor ons politiegegevens geworden.

Sommige (persoons)gegevens verzamelen we op grond van een andere wet. Drie wetten lichten we eruit:

Wetboek van Strafvordering

Volgens het Wetboek van Strafvordering is de politie verplicht om de identiteit van een verdachte vast te stellen. De Wet identiteitsvaststelling verdachten, veroordeelden en getuigen – en het daarbij horende besluit – geven aan welke gegevens we daarvoor moeten gebruiken. Op grond hiervan verwerken we de naam, voornaam, geboorteplaats- en datum, het adres (zoals vermeld in de gemeentelijke basisadministratie), en iemands feitelijke verblijfplaats. In speciale gevallen worden ook bijzondere categorieën persoonsgegevens verzameld.

Iemands identiteit kan ook worden vastgesteld door het afnemen van vingerafdrukken en het maken van foto's. Dit doen we bij een verdachte van een misdrijf waar voorlopige hechtenis op staat.

Wet bijzondere opsporingsdiensten
De bijzondere opsporingsdiensten FIOD, Inspectie Leefomgeving en Transport, Nederlandse Voedsel- en Waren Autoriteit en Inspectie SZW kunnen voor hun opsporingstaken ook persoonsgegevens verwerken. Het verwerken van deze persoonsgegevens valt onder de Wpg.

APV (Algemeen Plaatselijke Verordening)
Een APV is gemeentelijke verordening die voor iedereen geldt binnen die gemeente. In een APV kunnen bepalingen staan die moeten worden gehandhaafd door boa's, maar ook door de politie.

Algemene verordening gegevensbescherming (AVG)

Op basis van de volgende grondslagen in de AVG verwerkt de politie persoonsgegevens (art. 6 lid 1 AVG):

a) de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden Toestemming moet altijd uit vrije wil worden gegeven. De verwerkingsverantwoordelijk moet dit later ook kunnen aantonen;

b) de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

c) de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** die op de verwerkingsverantwoordelijke rust;

d) de verwerking is noodzakelijk om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen;

e) de verwerking is noodzakelijk voor het **vervullen van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen. Dat is bijvoorbeeld het geval bij uitvoering van de korpscheftaken, zoals het verlenen van een jachtakte;

f) de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen van de verwerkingsverantwoordelijke** oof van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De AVG is binnen de politieorganisatie van toepassing op de volgende onderdelen:

Personeelsadministratie
Alle informatie over werknemers valt onder de AVG. Daarnaast zijn er aanvullende wetten van kracht, zoals de verplichting om iemands identiteit te controleren of gegevens door te geven aan de Belastingdienst.

Sollicitanten
De gegevens van sollicitanten worden verwerkt zolang dat noodzakelijk is. Het is denkbaar dat we CV's langer bewaren om sollicitanten in een later stadium te kunnen benaderen. Op het moment dat we een sollicitant hebben aangenomen, gaat de verwerking over naar de personeelsadministratie.

Screening
Iedereen die bij de politie komt werken ondergaat een betrouwbaarheids- en geschiktheidsonderzoek. Deze screening start pas als uit het sollicitatieproces blijkt dat een kandidaat geschikt is voor de functie.

Inkoop en (leveranciers)contracten
De politieorganisatie sluit contracten af met verschillende partijen, een schoonmaakbedrijf bijvoorbeeld, het bedrijfsrestaurant of voor het aanschaffen van werkkleding. Voor deze transacties leggen we persoonsgegevens vast.

Bezoek aan het politiebureau
Op de politiebureaus bewaken camera's onze eigendommen en die van bezoekers. Deze beelden blijven bewaard zo lang noodzakelijk is voor dit doel.

Marketing, PR, social media en websites
Als het om communicatie gaat, is er een tweedeling bij de politie. Communicatie in het kader van de uitvoering van de politietaak valt onder de Wpg. Denk aan opsporingsberichten van verdachten of vermiste personen op websites, social media of via andere communicatiekanalen.
De berichten die daaruit voortvloeien, zijn verder geen uitvoering van de politietaak en vallen onder de AVG. Een nieuwsbericht bijvoorbeeld, over een opgepakte dader.

- *Social media*

Politieagenten zijn steeds vaker op social media te vinden. Op die manier kan op een unieke manier een inkijk worden gegeven in het werk van de politie. Om te voorkomen dat personen, locaties of voorwerpen op een herkenbare manier in beeld worden gebracht en daardoor herleidbaar zijn, heeft de politie interne instructies opgesteld voor het gebruik van social media. Op die manier proberen we te voorkomen dat personen ongewenst in verband worden gebracht met de politie. Bent u toch herkenbaar in beeld gekomen? Neem contact op met de betreffende eenheid.

- *Websites*

De politie heeft verschillende websites, zoals politie.nl. en kombijdepolitie.nl Om onze dienstverlening te optimaliseren maakt de politie gebruik van webstatistieken. We gebruiken deze gegevens niet voor een ander doel en stellen ze ook niet aan derden ter beschikking. Wilt u een webformulier invullen, dan wordt u gevraagd om naam, adres, postcode, woonplaats, telefoon en e-mailadres. Alleen het e-mailadres is verplicht om in te vullen. Om u zo goed mogelijk van dienst te zijn, wil de politie contact met u opnemen naar aanleiding van het door u ingevulde formulier. Uw internetprovider stuurt automatisch uw IP-adres mee met het formulier, ook dit is een persoonsgegeven.

Online aangifte doen valt onder de Wpg. Het opnemen van aangifte is namelijk een politietaak. Indien u anoniem informatie wil delen, kunt u contact opnemen met Meld Misdaad Anoniem.

Daarnaast gebruiken we Google Analytics voor managementrapportages op Politie.nl. Op basis van de maandcijfers over het aantal bezoekers aan (speciale onderdelen van) de website, zien we op welke berichten het meest wordt geklikt. Met statistieken kunnen we meten hoe lang de bezoeker op de website blijft.

Werkzaamheden niet zijnde de politietaak
Naast de uitvoering van de politietaak handelt de politie ook als een ‘gewone’ organisatie. Dus verrichten we ook andere werkzaamheden dan politietaken. Denk hierbij aan de (e-mail) communicatie tussen werknemers, maar ook het opstellen van beleidsstukken.

Korpscheftaken
Korpscheftaken vallen niet onder de Wet politiegegevens, dus is de Algemene verordening gegevensbescherming daarop van toepassing. Het gaat om de volgende taken:
- Het verlenen van een jachtakte.
- Het verlenen van een (vuur)wapenverlof.
- Het verlenen van een vergunning in het kader van de Wet explosieven voor civiel gebruik.
- Toestemming geven voor het laten werken van personen in de beveiliging.
- Toestemming geven voor het verstrekken van een legitimatiebewijs voor beveiligers.
- Taken die de korpschef krijgt opgedragen volgens de Wet precursoren op explosieven.
- Toezicht houden op boa’s.

Vreemdelingenzaken
De politie voert werkzaamheden uit in verband met de Vreemdelingenwet 2000. Ook op deze werkzaamheden is de Algemene verordening gegevensbescherming van toepassing.

3. Privacy by design en gegevensbeschermingseffectbeoordeling

Bij het ontwikkelen van nieuwe producten en diensten is privacybescherming een belangrijk aandachtspunt. Dat wil zeggen dat we al in de beginfase van een ontwerp nadenken over privacy verhogende maatregelen: privacy by design.

Als dat nodig is, voeren we een gegevensbeschermingseffectbeoordeling uit. We toetsen dan vooraf wat de effecten van de gegevensverwerking zijn op de gegevensbescherming van burgers. Blijkt er een hoog risico te zijn op inbreuk op de persoonlijke levenssfeer en dit risico kan niet worden afgedekt, dan leggen we de verwerking voor advies voor aan de Autoriteit Persoonsgegevens.

4. Autorisaties en informatiebeveiliging

Autorisaties
Alleen medewerkers die daartoe bevoegd zijn krijgen toegang tot gegevens. Zij mogen alleen die gegevens inzien die zij nodig hebben om hun werk te kunnen doen.

Het is mogelijk dat we toegang verlenen aan medewerkers van andere organisaties met opsporingstaken. Ook zij krijgen alleen toegang tot die gegevens die zij nodig hebben om hun werk te kunnen doen.

Logging
De handelingen van medewerkers in politiesystemen worden gelogd. We houden bij wie welke handeling op welk tijdstip uitvoert in een bepaald bestand. De Wet politiegegevens verplicht logging. De Algemene verordening gegevensbescherming verplicht logging weliswaar niet, maar legt wel de nadruk op verantwoording en documentatie.

Logging-gegevens worden gebruikt:
- ter controle van de rechtmatigheid van de gegevensverwerking;
- voor interne controles;
- voor het waarborgen van de integriteit en de beveiliging van politiegegevens;
- voor strafrechtelijke procedures.

Hoewel de loggingsverplichting uit de Wpg voortvloeit, is op de logginsgegevens de AVG van toepassing. Ze zijn immers niet bedoeld voor de uitvoering van de politietaak.

Logging is van toepassing op de volgende verwerkingen van politiegegevens:
- verzameling
- wijziging
- raadpleging
- verstrekking onder meer in de vorm van doorgifte
- een combinatie van een van de hiervoor genoemde opties
- vernietiging

Logbestanden gebruiken we voor beveiligingsdoeleinden en voor (intern) onderzoek achteraf. Denk aan onderzoek naar hacking. Ook kan met behulp van logging a-typisch gedrag van gebruikers en mogelijk onrechtmatig gebruik worden vastgesteld.

De logginggegevens kunnen verder worden gebruikt om de Autoriteit Persoonsgegevens (AP) te informeren in het geval van een datalek of om de burger of medewerker zijn of haar recht op inzage uit te oefenen

Informatiebeveiliging
De politie neemt passende maatregelen - technisch en organisatorisch - om politie- of persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking, tegen opzettelijk verlies, vernietiging of beschadiging.

Autorisaties
Medewerkers van de Koninklijke Marechaussee, Rijksrecherche, bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren kunnen toegang krijgen tot politiegegevens. Zij krijgen alleen toegang tot die politiegegevens die zij nodig hebben voor het opsporingswerk. Net als de politie, is de marchaussee belast met het uitvoeren van politietaken (artikel 4 lid 1 Politiewet 2012.)

5. Bewaartermijnen

Wet politiegegevens (Wpg)
In de Wpg staan vaste bewaartermijnen voor persoonsgegevens. Ook maakt de Wpg onderscheid tussen verwijderen en vernietigen van gegevens. Als we gegevens verwijderen, zijn deze nog niet definitief weg. We zetten ze als het ware achter een digitaal schot en zijn in principe niet meer in te zien. Dat is alleen mogelijk als daar dringende redenen voor zijn en onder strikte voorwaarden.

Vernietigen is een definitieve handeling. De gegevens zijn niet meer terug te halen.

Artikel 13 is een apart artikel in de Wpg en gaat over de verdere verwerking van gegevens. Dat betekent dat er sprake is van een ander doel dan waarvoor de gegevens zijn verzameld. De bewaartermijnen voor het doel uit artikel 13 Wpg zijn vastgelegd in een apart protocol.

Bewaartermijn logging-gegevens voor WPG-gegevens
De bewaartermijn voor logging-gegevens is gekoppeld aan de periodieke privacy audits waartoe de politie wettelijk is verplicht. Deze externe audits worden iedere 4 jaar uitgevoerd, waarna eventueel nog een hercontrole kan plaatsvinden. Voor het bewaren van logging-gegevens is daarom een maximale termijn van 5 jaar vastgesteld.

Doel verwerking	Verwerken	Verwijderen	Vernietigen
Dagelijkse politietaak (artikel 8)	Tot 5 jaar na de datum van eerste verwerking	Na 5 jaar	5 jaar na verwijdering
Recherche-onderzoeken (artikel 9)	Zolang het onderzoek loopt	Een half jaar na afloop van het onderzoek + max. een half jaar om te kijken of er aanleiding is voor een nieuw onderzoek.	5 jaar na verwijdering
Opbouwen informatie-positie (artikel 10)	Zolang het onderzoek loopt	Zodra niet meer nood-zakelijk voor het onderzoek	5 jaar na verwijdering
Beheer informanten (artikel 12)	Zolang het noodzakelijk is	n.v.t.	Op het moment dat zij niet langer noodzakelijk zijn voor het doel van de verwerking. Dit wordt periodiek getoetst Uiterlijk 10 jaar na de datum van de laatste verwerking
Ondersteunende taken (artikel 13)	Afhankelijk van het protocol	n.v.t.	Afhankelijk van het protocol

Aanvulling op de tabel wpg bewaartermijnen

- Artikel 13-gegevens volgen de bewaartermijn van het voor hun verwerking opgesteld protocol. Een voorbeeld hierbij is de verwerking van gegevens door de forensische opsporing. De bewaartermijnen zijn gekoppeld aan de verjaringstermijn van het misdrijf waarvoor de gegevens zijn verzameld.

- Cold cases zijn zaken die nog niet zijn opgelost. Zolang het onderzoek nog loopt, worden de gegevens niet verwijderd

- Gegevens met culturele of historische waarde kunnen voor vernietiging worden behoed door ze over te brengen naar een archief. Het gaat hier om bijzondere zaken die een grote impact hebben gehad op de maatschappij, zoals de moorden op Theo van Gogh en Pim Fortuyn. Op deze stukken is de Archiefwet van toepassing.

- Overigens kan de politie wel langer gebruikmaken van geanonimiseerde gegevens. Dat zijn gegevens die niet meer herleidbaar zijn tot een persoon. Een voorbeeld hiervan is het aantal inbraken in een bepaalde regio.

Algemene verordening gegevensbescherming (AVG)

In de AVG staan geen concrete bewaartermijnen genoemd. Bij de politie bewaren we persoonsgegevens zolang als dat noodzakelijk is voor het doel waarvoor ze verzameld zijn, of op grond van de archiefwet is vereist. Gegevens worden niet langer bewaard dan wettelijk is toegestaan. Soms gelden er andere wetten die een specifieke bewaartermijn vaststellen.

Bewaartermijn logging-gegevens voor AVG-gegevens

Ook AVG-gegevens worden in principe 5 jaar bewaard, maar het kan zijn dat de logging-gegevens van bepaalde (interne bedrijfsvoeringsapplicaties) korter worden bewaard. Het gaat dan om gevallen waarvan het bewaren van de gegevens die niet noodzakelijk meer zijn voor verantwoording. Denk hierbij aan de logging op zaalreserveringssystemen.

Bewaartermijn klachten

De maximale bewaartermijn van de AVG gegevens is in principe 5 jaar vanaf het moment van afsluiten van de klacht.

Persoonsgegevens mogen langer worden bewaard als archivering een algemeen belang dient; of voor wetenschappelijk of historisch onderzoek en statistische doeleinden. Om inbreuk op de privacy te beperken, moeten aanvullende maatregelen worden genomen. Bijvoorbeeld door de gegevens te pseudonimiseren, een techniek waarbij het moeilijker wordt om de informatie naar een persoon te herleiden.

6. Verwijderen en vernietigen

Wet politiegegevens (Wpg)

De Wpg maakt onderscheid tussen verwijderen en vernietigen van gegevens. Als we gegevens verwijderen, zijn zij nog niet definitief weg. Ze komen als het ware achter een digitaal schot te staan en zijn niet meer in te zien. Alleen als mocht blijken dat we de gegevens nodig hebben voor een klachtenprocedure of omdat er verantwoording over moet worden afgelegd, dan kunnen we ze opvragen.

Als er een groot opsporingsonderzoek moet worden verricht wat een grote impact heeft op de rechtsorde, dan mogen deze gegevens opnieuw verwerkt, en dus ook geraadpleegd, worden. Dit kan alleen als de officier van justitie daar opdracht voor geeft.

Vernietigen is een definitieve handeling. De gegevens zijn niet meer terug te halen.

Algemene verordening gegevensbescherming (AVG)

De AVG maakt geen onderscheid tussen verwijderen en vernietigen en spreekt alleen van vernietigen. We mogen gegevens niet langer bewaren dan noodzakelijk voor het doel van de verwerking. Daarna moeten we ze vernietigen. Hoe lang we de gegevens bewaren verschilt per geval.

7. Delen van gegevens

Wet politiegegevens (Wpg)

Naast de politie is de Wpg ook van toepassing op de Koninklijke Marechaussee en de rijksrecherche:

Daarnaast is de Wpg van overeenkomstige toepassing op de verwerking van persoonsgegevens door de buitengewoon opsporingsambtenaren (boa's) en de vier bijzondere opsporingsdiensten:

- De Fiscale Inlichtingen- en Opsporingsdienst (FIOD),
- De Inspectie Sociale Zaken en Werkgelegenheid, Directie Opsporing (ISZW-DO)
- De Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport (ILT/IOD)
- De Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Waren Autoriteit (NVWA-IOD)

Het motto voor de politie en die organisaties die aan de Wpg moeten voldoen is "delen tenzij". Dat betekent dat we in bepaalde gevallen verplicht zijn om politiegegevens beschikbaar te stellen aan die andere organisaties en andersom. Dit motto geldt niet voor instanties die niet aan de Wpg zijn gebonden.

De politie mag gegevens uitsluitend verstrekken aan andere partijen als daar een wettelijke basis voor is. Denk hierbij aan het Openbaar Ministerie of de gemeente.

Gegevens mogen niet altijd voor een ander doel worden gebruikt dan waarvoor zij zijn verzameld.

Grondslagen verstrekking Wpg
Op basis van de volgende grondslagen in de Wpg en het Besluit politiegegevens verstrekt de politie persoonsgegevens (art. 16-24 Wpg):

Verstrekking aan gezagsdragers (art. 6):
Op basis van dit artikel moeten we politiegegevens verstrekken aan het Openbaar Ministerie en de burgemeesters (het bevoegd gezag) en de korpschef voor disciplinaire onderzoeken.

Verstrekking aan inlichtingendiensten (art. 17):
Politiegegevens worden verstrekt voor zover dit voortvloeit uit de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Doorgiften aan derde landen (art. 17a):
Gegevens kunnen alleen aan derde landen worden doorgegeven als er sprake is van een toereikend beschermingsniveau. De Europese Commissie moet dit hebben vastgesteld. Als dat niet het geval is moeten er juridisch afdwingbare passende waarborgen zijn voor de bescherming van persoonsgegevens. Of de verwerkingsverantwoordelijke moet zelf hebben geconcludeerd dat er passende waarborgen worden geboden door het derde land.

Aangezien Bonaire, Saba en Sint-Eustatius (BES-eilanden) niet behoren tot het Europese grondgebied, vallen zij in de categorie 'derde landen'. De doorgifte aan de BES is geregeld doordat in de Wpg een paragraaf is opgenomen waarin voorwaarden staan voor het van toepassing zijn van de Wpg. Hierdoor is voldaan aan artikel 17a lid 2 sub a Wpg.
Er is een juridisch bindend instrument waarin passende waarborgen voor de bescherming van persoonsgegevens zijn geboden.

Verstrekking aan derden structureel (art. 18):
Als er structureel politiegegevens aan derden worden verstrekt, moet dat zijn vastgelegd in een Algemene maatregel van bestuur. Het Besluit politiegegevens is zo'n Algemene maatregel van bestuur. Daar staat in artikel 4:1-4:4 aan wie de gegevens structureel kunnen worden verstrekt.

Verstrekking aan derden incidenteel (art. 19):
Politiegegevens kunnen in bijzondere gevallen worden verstrekt aan personen of instanties. De gegevens moeten dan nodig zijn voor een van de volgende doelen:

- Het voorkomen en opsporen van strafbare feiten.
- Het handhaven van de openbare orde.
- Hulp verlenen aan hen die dat behoeven.
- Het uitoefenen van toezicht op het naleven van de regelgeving.

Verstrekking aan derden structureel voor samenwerkingsverbanden (art. 20):
De politie heeft met sommige partijen een samenwerkingsverband. Politiegegevens kunnen aan deze partijen worden verstrekt als daar een zwaarwegend algemeen belang voor is. Hierbij kan worden gedacht aan zowel publieke als private partijen, zoals gemeenten, woningbouwverenigingen, de belastingdienst, banken en scholen.

Verwerking voor wetenschappelijk onderzoek en statistiek (art. 22):
Politiegegevens kunnen worden verwerkt voor beleidsinformatie, wetenschappelijk onderzoek of statistiek zolang de gebruikte resultaten geen persoonsgegevens bevatten. Het gaat dan om geanonimiseerde bestanden.

Rechtstreekse verstrekking (art. 23):
Het verstrekken van politiegegevens aan het Openbaar Ministerie en de korpschef kan rechtstreeks gedaan worden.

Dit betekent dat deze geautomatiseerd (via een systeem) kunnen worden verstrekt.

Rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten (art. 24):
De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) kunnen politiegegevens rechtstreeks geautomatiseerd vergelijken als dat noodzakelijk is voor de uitvoering van hun taak.

Algemene verordening gegevensbescherming (AVG)
Indien persoonsgegevens niet verder worden verwerkt, moet worden gekeken of het nieuwe doel verenigbaar is met het oorspronkelijke doel. Dit houdt in dat het nieuwe doel niet te veel van het oorspronkelijke doel mag afwijken. In sommige gevallen moet de betrokkene echt toestemming geven. Gegevens over het slachtoffer verstrekt de politie alleen aan Slachtofferhulp Nederland wanneer het slachtoffer daarmee akkoord is gegaan.

8. Rechten van betrokkenen

De persoon op wie de persoons- of politiegegevens betrekking hebben, noemen we de betrokkene. De betrokkene heeft een aantal rechten, zoals het recht op:
- inzage
- rectificatie
- gegevenswissing/vernietiging
- beperking van de verwerking van gegevens
- overdraagbaarheid (alleen AVG)
- bezwaar/beroep

We hebben als politie de plicht om u te informeren over de verwerkingen. Daarnaast stellen wij u op de hoogte als er is voldaan aan uw verzoek van rectificatie of gegevenswissing of de beperking van de verwerking van gegevens.

Wilt u informatie over de verwerking van uw persoonsgegevens, dan kunt u een schriftelijk verzoek indienen. Als u van mening bent dat de gegevens niet kloppen, dan kunt u een schriftelijk verzoek bij ons indienen waarin u aangeeft wat er gewijzigd moet worden.

We hebben het recht uw verzoek af te wijzen 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.

Zie verder punt 14. Vragen over het gebruik van uw gegevens

Wet politiegegevens (Wpg)

Recht op inzage (art. 25): U mag vragen of de politie politiegegevens van u verwerkt. U moet dit schriftelijk doen.

Zijn die gegevens er, dan kunt u ze inzien. U krijgt dan informatie over in ieder geval:
- Doelen en rechtsgrond van de verwerking.
- De betrokken categorieën van politiegegevens.
- De vraag of deze politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt. Ook krijgt u informatie over de ontvangers of categorieën ontvangers van uw gegevens. Met name ontvangers in derde landen of internationale organisaties.
- De voorziene periode van opslag. Of, als dat niet mogelijk is, de criteria voor het bepalen van de bewaartermijn.
- Het recht om te vragen om rectificatie, vernietiging of afscherming van de verwerking van uw gegevens.
- Het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- De herkomst van de politiegegevens.

Recht op rectificatie en vernietiging van politiegegevens (art. 28): na schriftelijk verzoek heeft u het recht onjuiste politiegegevens te rectificeren of, indien nodig, aan te vullen.

Als uw gegevens: feitelijk onjuist, onvolledig, niet nodig voor het doel of in strijd met een wettelijk voorschrift worden verwerkt, kunt u een verzoek indien om deze gegevens te verbeteren, aan te vullen, te verwijderen, af te schermen of te markeren.

De beslissing op zowel het verzoek uit artikel 25 als 28 Wpg is een besluit in de zin van de Algemene Wet Bestuursrecht.

U kunt hiertegen in beroep gaan. Ook kunt u zich wenden tot de Autoriteit Persoonsgegevens en vragen om bemiddeling of advies. Tegelijkertijd kan beroep worden ingesteld.

Algemene verordening gegevensbescherming (AVG)

Recht op inzage (art. 15):
U mag zien welke gegevens de politie van u heeft, waarvoor deze zijn verwerkt en aan wie ze eventueel zijn doorgegeven.

Recht op rectificatie (art. 16):
Dit houdt in dat de verwerkingsverantwoordelijke direct onjuiste persoonsgegevens moet aanpassen.

Recht op wissing/vergetelheid (art. 17):
De politie moet uw persoonsgegevens wissen als voldaan is aan de in de wet opgenomen eisen.

Recht op beperking van de verwerking (art.18):
Als voldaan wordt aan de eisen die wet stelt, mag u de politie verzoeken de verwerking te beperken.

Recht op overdraagbaarheid van de gegevens (art. 20):
U mag uw gegevens meenemen naar een andere verwerkingsverantwoordelijke.

Recht van bezwaar (art. 21):
U heeft het recht bezwaar te maken tegen het verwerken van persoonsgegevens door de politie.

9. Toezicht

9.a. Functionaris voor gegevensbescherming (FG)

De politie heeft een functionaris voor gegevensbescherming (FG). Deze houdt intern toezicht op de toepassing en naleving van de privacywetgeving.

De functionaris voor gegevensbescherming (FG) heeft de volgende taken:
- De FG informeert en adviseert de verwerkingsverantwoordelijke over de verplichting op grond van de privacy-wetgeving.
- Houdt toezicht op de naleving van de privacywetgeving.
- Geeft advies over de gegevensbeschermingseffectbeoordeling en ziet toe op de uitvoering ervan.
- Werkt samen met de Autoriteit Persoonsgegevens (AP) en is het contactpunt voor de AP.

Contactgegevens:
Let op, voor het inzien van uw gegevens richt u een verzoek aan de privacyfunctionaris van uw regio. Zie ook onderdeel 15.

U kunt de functionaris gegevensbescherming bereiken via het contactformulier op de website.

9.b. Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is de nationale toezichthouder die toezicht houdt op de toepassing van de privacywetgeving. Wie klachten heeft over het gebruik van persoons- of politiegegevens door de politie kan bij de AP terecht.

10. Schengen Signaleringen / Schengen Alert

De politie kan uw persoonsgegevens controleren of verwerken in het Schengen Informatie Systeem.

11. Landelijk Meldkamer Samenwerking 1-1-2 alarmcentrale

Politie, brandweer, ambulancezorg en Koninklijke Marechaussee (KMar) krijgen tien meldkamers die samenwerken. Om dit te bereiken wordt binnen de politie een ‘dedicated’, organisatieonderdeel ingericht, de Landelijke Meldkamer Samenwerking (LMS). De LMS gaat feitelijk het beheer van de 1-1-2 alarmcentrale uitvoeren. Ook treedt de LMS op als verwerker van persoonsgegevens binnen de meldkamersamenwerking. Hier zijn de Regionale Ambulancevoorzieningen, de brandweerregio’s (Veiligheidsregio’s) en de KMar de verwerkingsverantwoordelijken.

12. Waarom wil de politie op deze website uw persoonsgegevens weten?

In de formulieren op Politie.nl wordt standaard gevraagd naar uw naam, adres, postcode, woonplaats, telefoon en e-mailadres. Alle velden zijn optioneel, het is dus niet verplicht om uw persoonsgegevens in te vullen. Voor het e-mail adres is een uitzondering gemaakt. Om u zo goed mogelijk van dienst te kunnen zijn, wil de politie contact met u kunnen opnemen. Bijvoorbeeld om u een vraag te kunnen stellen en natuurlijk om antwoord te kunnen geven als u zelf een vraag hebt gesteld.

Uw internetprovider stuurt automatisch uw IP adres mee met het formulier dat u via Politie.nl verstuurt. Als u anoniem informatie met de politie wil delen, kunt u contact opnemen met Meld Misdaad Anoniem.

13. Gebruik van anonieme bezoekersgegevens

Voor de meting van webstatistieken verzamelt de politie anonieme gegevens over het gebruik van deze website. Door analyse van de verzamelde gegevens kan de website worden verbeterd, zodat de bezoeker gezochte informatie zo gemakkelijk mogelijk kan vinden. Daarnaast kan de politie door de webstatistieken haar dienstverlening verder optimaliseren. Het gaat om de volgende gegevens: uw IP-adres, het adres van uw internetprovider, de browser die u gebruikt (zoals Chrome, Firefox, Internet Explorer of Safari), het tijdstip en de duur van uw bezoek en welke pagina's u heeft bezocht.

Google Analytics wordt gebruikt voor managementrapportages met daarin maandcijfers over bezoekersfrequentie aan de website en specifieke onderdelen van de website, zoals interesse voor nieuws, aangifte doen, gezochte verdachten, vermiste personen etc. Daarnaast worden de statistieken gebruikt in gebruikersonderzoek, bijvoorbeeld de gemiddelde verblijfsduur op een pagina. Het gaat hier nadrukkelijk om statistieken en niet om informatie over individuele bezoekers.

Google Tagmanager wordt gebruikt voor de koppeling met de Feedback tool van Usabilla. Dit is een passief onderzoeksinstrument, bezoekers aan de website kunnen kiezen om een feedbackformulier via Politie.nl naar de politie te sturen met commentaar of complimenten over (onderdelen) van de website. Er worden geen persoonsgegevens of bereikbaarheidsinformatie uitgevraagd.

De verzamelde gegevens worden niet voor een ander doel gebruikt of aan derden ter beschikking gesteld. Ook wordt gebruikgemaakt van cookies.

14. Privacy en solliciteren

U kunt via deze website solliciteren op vacatures bij de politie. De politie onderschrijft de NVP-Sollicitatiecode. Deze sollicitatiecode bevat basisregels die arbeidsorganisaties naar het oordeel van de Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling (NVP) in acht behoren te nemen bij werving en selectie.
Als sollicitant heeft u recht op:

- een eerlijke kans op aanstelling
- informatie
- privacy
- een vertrouwelijke behandeling van uw persoonlijke gegevens
- een doelmatige sollicitatieprocedure
- toegang tot een geschillenregeling

15. Vragen over het gebruik van uw gegevens

Heeft u vragen over het gebruik van persoons- of politiegegevens? Dien een schriftelijk verzoek in bij de privacyfunctionaris uit uw regio. Stuur hierbij wel een kopie van een geldig legitimatiebewijs mee ter verificatie van uw identiteit. Uw foto en Burgerservicenummer (BSN) mag u afschermen.

Dit privacy statement is gepubliceerd op 23 maart 2021.