Handleiding
Rechten van Betrokkene
Wpg

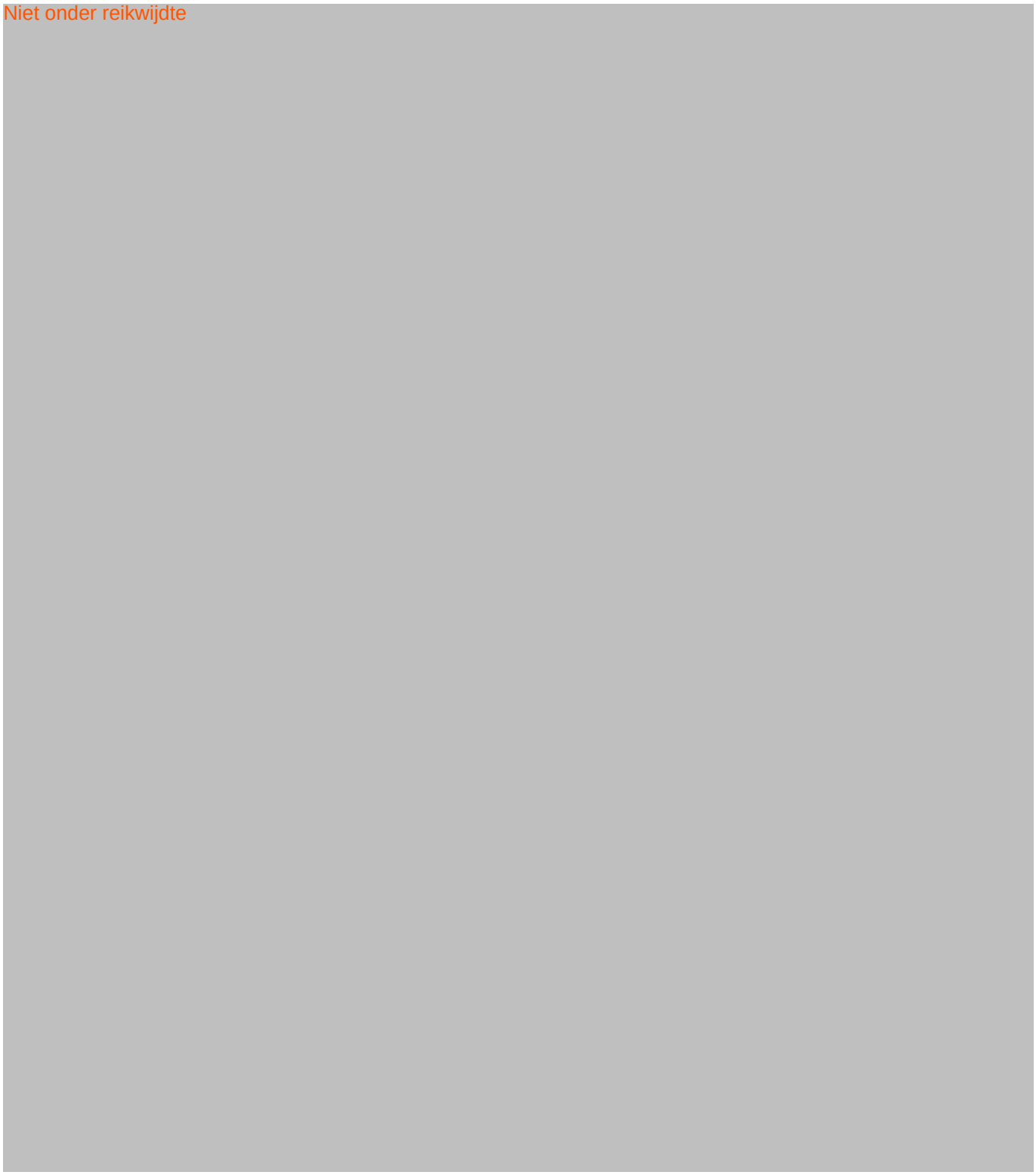
Uitgangspunten voor een uniforme werkwijze door de behandelaar

Door	5.1.2.e privacyfunctionaris eenheid Rotterdam
	5.1.2.e , adviseur privacy
Afdeling	Portefeuille privacy
Versienummer	2.0
Datum	28 januari 2026
Kenmerk	Handleiding RvB Wpg – versie 2.0
Status	Definitief
Rubricering	Politie Intern

Portefeuille Privacy
Typ Postadres Dienst of Postadres Eenheid

Documentinformatie nakijken

Niet onder reikwijdte



Inhoudsopgave

Documentinformatie **2**

Inhoudsopgave **3**

1 Algemeen **5**
1.1 Introductie 5
1.2 Doel 5
1.3 Algemene wet bestuursrecht 6
1.4 Behandelaar 6
1.5 Verzoeker 6
1.6 Verzoekschrift 7
1.7 Doorzendplicht 8
1.8 Opschorten 8
1.9 Verdagen 9
1.10 Termijnen 9
1.11 In gebreke stellen 10
1.12 Rechtsmiddelen 10
1.13 Mandatering 11
1.14 Tot slot 11

2 Inzage van politiegegevens **13**
2.1 Algemeen 13
2.2 Indienen verzoek 14
2.3 Registreren verzoek 14
2.4 Beoordelen formaliteiten 14
2.5 Verzamelen persoonsgegevens 17
2.6 Beoordelen besluit 19
2.7 Uitvoeren inzage 21
2.8 Afsluiten en archiveren 23
2.9 Specifiek: verzoek nabestaande(n) 24
2.10 Specifiek: verzoek loggingsgegeven(s) 25
2.11 Specifiek: verzoek foto- en camerabeelden 25
2.12 Specifiek: internationale signaleringen 27

3 Rectificatie en vernietiging van politiegegevens **29**
3.1 Algemeen 29
3.2 Indienen verzoek 29
3.3 Registreren verzoek 29
3.4 Beoordelen formaliteiten 30
3.5 Verzamelen persoonsgegevens 32
3.6 Beoordelen besluit 32
3.7 Uitvoeren verzoek 34
3.8 Afsluiten en archiveren 34
3.9 Specifiek: verwijderen identiteitsgegevens 35

Bijlage A: overzicht adressen eenheden ..... Fout! Bladwijzer niet gedefinieerd.

Bijlage B: overzicht bevragingen onder Wpg ..... Fout! Bladwijzer niet gedefinieerd.

Bijlage C: overzicht bevragingen onder de AVG ..... Fout! Bladwijzer niet gedefinieerd.

Bijlage D: overzicht …….. ..... Fout! Bladwijzer niet gedefinieerd.

Bijlage E: overzicht ..... Fout! Bladwijzer niet gedefinieerd.

1 Algemeen

1.1 Introductie

De Wpg is nationale wetgeving die voortkomt uit de Europese Richtlijn opsporing en vervolging en op 1 januari 2019 in werking is getreden. De Wpg heeft betrekking op de bescherming van persoonsgegevens van natuurlijke personen in verband met de verwerking van die persoonsgegevens voor de politietaak (= politiegegevens).

Deze handleiding geldt voor politiemedewerkers die betrokken zijn bij de behandeling van verzoeken in het kader van de 'Rechten van de betrokkene' uit de Wpg. Zo'n verzoek kan door een betrokkene ingediend worden bij de privacydesk van een eenheid[1].

De privacydesk maakt gebruik van landelijk vastgestelde brieven voor het nemen van besluiten en het voeren van correspondentie over het ingediende verzoek. Deze brieven staan in een Document Management Systeem (nu Documentum) voor de vastlegging van het dossier.

De AVG (EU/2016/L 119/1) en de Europese Richtlijn opsporing en vervolging (EU/2016/680) die is omgezet naar de Wet politiegegevens, sluiten elkaar wederzijds uit en hanteren verschillende termijnen bij de afhandeling van Rechten van betrokkene verzoeken. Hiervan uitgaande is het noodzakelijk om een algemeen verzoek om inzage (Wpg en AVG) gescheiden af te handelen. Zeker als de verzoeker later heeft aangegeven op grond van beide wetgevingen inzage te willen. Het gevolg is dat separate besluiten worden genomen, die wel naar elkaar verwijzen om tegemoet te komen aan het gehele verzoek. Ook kunnen beide feitelijke inzagen in het kader van klantvriendelijkheid op één moment worden afgehandeld.

1.2 Doel

Het doel van 'Rechten van betrokkene' is om de burger waarborgen te geven tegen ongerechtvaardigde inbreuk(en) op zijn persoonlijke levenssfeer. Hiermee wordt rechtsbescherming geboden tegen het (on)gevraagd verwerken van persoonsgegevens in (politie)systemen (= controle/ transparantie) en/of met het wijzigen of verwijderen van onjuiste verwerkingen (= correctie).

Het recht op inzage en rectificatie zijn geen absolute rechten. Deze rechten kunnen worden beperkt vanwege zwaarder wegende belangen. Er dient een afweging plaats te vinden, die wordt getoetst aan noodzakelijkheid en evenredigheid. Uit Tweede Kamerverslagen blijkt dat het recht op inzage een grondrecht van de betrokkene betreft. Als dat recht bij voorbaat wordt beperkt of zelfs uitgesloten dan vormt dit een ernstige aantasting van de rechten van burgers. De verplichting van de verwerkingsverantwoordelijke om inzage te geven in de persoonsgegevens die worden verwerkt en daarmee rekenschap af te leggen over de gegevensverwerking en de juistheid van de verwerkte gegevens, vormt daarvan het spiegelbeeld. Dit betekent dat je eerst toetst op het rechtsartikel zelf en daarna pas of een afwijzing noodzakelijk en evenredig is.

De Rechten van betrokkene betreffen specifiek voor de Wpg:

- het recht op inzage van politiegegevens (artikel 25 Wpg) en
- het recht op rectificatie en vernietiging van politiegegevens (artikel 28 Wpg).

[1] Zie link: https://www.politie.nl/algemeen/privacydesk-adressen.html

Naast bovenstaande rechten zijn er nog meer algemene verplichtingen in de Wpg[2] onder Rechten van betrokkene opgenomen, welke op politie.nl zijn gepubliceerd. Denk bijvoorbeeld aan de Functionaris Gegevensbescherming (FG), welke soorten verwerkingen er plaatsvinden, etc.

1.3 Algemene wet bestuursrecht

Bij de procedurele afhandeling van een Wpg-rechten van betrokkene verzoek – buiten behandeling stellen, vormvereisten, motiveringsplichten en bezwaar – is de Algemene wet bestuursrecht (Awb) van toepassing.

1.4 Behandelaar

Het verzoek wordt geregistreerd in de eenheid waar het verzoek wordt ingediend en in beginsel afgehandeld door de Privacydesk van de eenheid waar de betrokkene woonachtig is. Hiermee wordt tegemoetgekomen aan het feit dat die eenheid of politiechef ook meestal wordt aangeschreven en een feitelijke inzage daar het beste bijpast. Dit betekent dat bij een tijdelijke verblijfplaats, die ook als vervangende woonplaats wordt gezien. Denk bijvoorbeeld aan een Penitentiaire Inrichting waar een betrokkene verblijft. Verder geldt in beginsel dat een politie-eenheid alle Wpg-verzoeken Rechten van betrokkene afhandelt, die gerelateerd zijn aan de politietaak[3]. Dit zijn allemaal operationele verwerkingen. Verzoeken afkomstig uit het buitenland kunnen per post, maar ook per email worden toegezonden naar de Privacydesk van de Landelijke Eenheden. De mogelijkheid van de communicatie per email wordt hier toegestaan omdat het postverkeer niet met alle delen van de wereld even goed is gewaarborgd.

Bij verzoeken uit het buitenland wordt door de Privacydesk van de Landelijke Eenheden beoordeeld of er registraties van betrokkene in Nederland bekend zijn. Zitten de meeste registraties in de regionale eenheid dan stuurt de Privacydesk van de Landelijke Eenheden het verzoek ter behandeling door naar die regionale eenheid.

In afwijking op alle bovenstaande uitgangspunten blijft altijd het adagium: zoek elkaar op en stem af met de andere eenheid/dienst als je moverende redenen hebt om een verzoek over te dragen. Bijvoorbeeld als blijkt dat de meeste verwerkingen in andere eenheid plaatsvinden, kan die eenheid er mogelijk belang bij hebben om het verzoek over te nemen en zelf af te handelen

1.5 Verzoeker

Uitgangspunt is dat bij een verzoek in het kader van Rechten van betrokkene vanuit het bestuursorgaan altijd wordt gecorrespondeerd met de verzoeker. Ook als dat niet de betrokkene zelf betreft.

In de formaliteiten voor een verzoek Rechten van betrokkene is opgenomen dat de identiteit van de verzoeker ‘deugdelijk moet worden vastgesteld’. Er zijn richtlijnen opgesteld vanuit de EDPB[4] om een ongeoorloofde of onwettige verwerking van identificatie van verzoekers te voorkomen:

- gebruik een alternatieve methode voor identificatie, zoals het versturen van een e-mail of sms met een bevestigingslink, of stel beveiligingsvragen, of gebruik multi-factor authenticatie;
- vraag alleen een kopie van een identiteitsbewijs op in uitzonderlijke gevallen en zorg voor een passend beveiligingsniveau;
- vraag alleen noodzakelijke identiteitsgegevens en laat de rest weg of laat die onzichtbaar maken (denk aan BSN nummer, nationaliteit, of foto) en

[2] Zie artikel 24a en 24b Wpg
[3] Zie artikel 3 Politiewet
[4] EDPB is de European Data Protection Board; de Europese Raad van Toezichthouders Privacy

- bouw waarborgen in om onrechtmatige verwerking van het identiteitsbewijs bewijs te voorkomen.

Op grond van bovenstaande worden de volgende uitgangspunten gehanteerd:

1. als een kopie identiteitsbewijs wordt meegestuurd geef dan altijd vooraf aan dat de foto en/of BSN-nummer niet zichtbaar moeten zijn
2. maak vervolgens een notitie van de verificatie (welk identiteitsbewijs en bijbehorend nummer)
3. en vernietig vervolgens de kopie zelf[5].

Tip: maak in het betreffende dossier altijd een aantekening hoe de identiteit van verzoeker is vastgesteld. Leg ook bij een feitelijke inzage aan het politiebureau de documentsoort en het bijbehorende nummer vast en bewaar dus geen kopieën en sla die ook niet op in een systeem. Hiertoe is geen noodzaak meer.

Voor de Wpg geldt dat een verzoek ex artikel 25 of 28 Wpg namens de betrokkene alléén kan worden gedaan door een advocaat of de wettelijk vertegenwoordiger van betrokkene (denk hierbij aan minderjarigen of onder curatele gestelde). De advocaat moet door betrokkene zijn gemachtigd om namens hem/haar dit recht te kunnen uitoefenen. De advocaat doet het verzoek uitsluitend met de bedoeling om de belangen van betrokkene als cliënt te behartigen. De advocaat of wettelijk vertegenwoordiger van betrokkene wordt tijdens de procedure verder geïnformeerd en niet de betrokkene zelf.

Voor een advocaat geldt dat diens identiteit kan blijken uit navraag of controle bij de orde van advocaten, via het briefpapier en/of website. Naar het oordeel van de AP is daarmee gewaarborgd dat een advocaat is wie hij zegt te zijn[6] en is een kopie identiteitsbewijs van de advocaat daarom in beginsel niet nodig. Bij een schriftelijk inzageverzoek door een advocaat namens betrokkene blijft wel staan dat een kopie identiteitsbewijs en machtiging van betrokkene wel overlegd moeten worden.

Een ander (niet zijnde advocaat of wettelijk vertegenwoordiger) machtigen om kennis te nemen van politiegegevens wordt dus **niet** toegestaan. Het is een persoonlijk recht en mogelijk is er sprake van een bepaalde gezagsverhouding tot de betrokkene (denk aan werkgever en werknemer). De politie gaat hier geen nader onderzoek naar instellen, omdat artikel 26 Wpg het gesloten karakter hiervan weergeeft. Dit geldt dus eveneens voor het vergezellen bij een inzage.

Tip: uitzonderingen en maatwerk blijven altijd mogelijk. Denk bijvoorbeeld aan een zoon of dochter van een dementerende ouder. Als je afwijkt neem dan de feiten en/of omstandigheden op in het besluit, zodat duidelijk is dat en waarom een uitzondering wordt gemaakt in verband met eventuele precedentwerking.

1.6 Verzoekschrift

Het verzoekschrift moet duidelijkheid geven over de concrete vraag van de verzoeker. In de praktijk blijkt dit lastig, omdat enerzijds de verzoeker niet precies aangeeft wat hij wil of de kennis niet heeft en anderzijds er gebruik wordt gemaakt van standaardbrieven die van websites worden afgehaald. Uitgangspunt hierbij is dat de behandelaar vanuit de politie het verzoek **niet** zelf interpreteert, maar om duidelijkheid vraagt aan de verzoeker en dit vastlegt in het dossier en in de correspondentie.

[5] Voor de LE's geldt dat bij verzoeken per mail uit het buitenland eerst nog een extra handtekening oid wordt gevraagd en wordt vergeleken met die van het ID. Een andere manier om een identiteit vast te stellen is niet mogelijk.
[6] Uitspraak CBP van *4 februari 2003 (nummer z2002-01511)*

Tip: vraag om verduidelijking, want het eigenstandig interpreteren van een algemeen verzoek en daarop nemen van een besluit op grond van artikel 25 Wpg is in een casus al door een rechterlijke uitspraak tenietgedaan.

Het uitgangspunt is dat er schriftelijk of elektronisch op een begrijpelijke wijze wordt gecorrespondeerd met de verzoeker en ook op dezelfde wijze als het verzoekschrift is gedaan.
Per 1 januari 2026 is de Wet elektronisch bestuurlijk verkeer (WEBV) in werking getreden. Deze wet verplicht overheidsorganisaties om burgers de mogelijkheid te bieden elektronisch te communiceren met de overheid, naast de bestaande mogelijkheid per post. Vanaf 1 januari 2026 wordt de mogelijkheid om een verzoek in te dienen uitgebreid met een elektronisch route via politie.nl. Hiermee wordt voldaan aan een wettelijke verplichting, namelijk het moeten aanbieden van een elektronisch weg. Dit is een nieuw recht voor de burger. Daarnaast wordt er meer duiding gevraagd over het verzoek om het beter te kunnen behandelen. Het verzoek mag elektronisch, maar ook schriftelijk worden beantwoord.

De betrokkene moet informatie over de verwerking van zijn politiegegevens in beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal kunnen verkrijgen. Deze informatie wordt met passende middelen, waaronder elektronische, verstrekt en in het algemeen in dezelfde vorm als het verzoek zelf (artikel 24a Wpg).

1.7 Doorzendplicht

Als redelijkerwijze de verzoeker niet kan weten dat hij bij een ander bestuursorgaan zijn verzoek moet indienen, dan geldt de doorzendplicht ex artikel 2:3 Awb.

Aan het bestuursorgaan dat bevoegd is om de inzage verder in behandeling te nemen wordt het verzoek schriftelijk overgedragen en de verzoeker wordt hiervan schriftelijk in kennis gesteld. Dit geldt niet voor een advocaat of juridisch adviseur, waaraan je het verzoek gewoon terug kan sturen met de mededeling dat een ander bestuursorgaan bevoegd is.

1.8 Opschorten

De wettelijke termijn voor afhandeling van een verzoek Rechten van betrokkene voor de Wpg wordt opgeschort, als het verzoek niet voldoet aan de daaraan gestelde vormvereisten (= formaliteiten). Bijvoorbeeld een deugdelijke identificatie van de verzoeker is niet mogelijk, omdat er geen kopie legitimatiebewijs is meegezonden. De verzoeker krijgt dan de gelegenheid om dit verzuim te herstellen. De afhandeltermijn wordt dan opgeschort vanaf de dag nadat het verzoek om aanvulling is verstuurd (artikel 4:15 Awb) en vangt weer aan op het moment dat het verzuim is hersteld.

Tip: reageer adequaat op het moment dat er sprake is van een vormvereiste, waar niet aan wordt voldaan (=verzuim). De afhandelingstermijn start namelijk al op het moment dat het verzoek is ontvangen door het bestuursorgaan.

Er is geen wettelijke termijn genoemd voor het opschorten, anders dan ‘redelijke termijn’. Een standaard termijn van twee weken is normaal, maar kan worden aangepast. Bijvoorbeeld na afstemming met verzoeker. Dit is maatwerk.
Indien niet (tijdig) wordt voldaan aan het verzuimherstel wordt de behandeling van het verzoek beëindigd en een besluit daartoe opgemaakt en verstuurd. Een voornemen hiertoe is al opgenomen in de reactie tot verzuim herstel.

1.9 Verdagen

Indien voor de afhandeling van een verzoek Rechten van betrokkene uit de Wpg **(alléén** inzage) meer tijd nodig is, kan de afhandeling worden verdaagd. Hiermee krijgt de behandelaar meer tijd om het verzoek binnen de gestelde termijn af te handelen. De termijn van verdaging is voor de Wpg vier weken, als blijkt dat de complexiteit en/of het aantal verwerkingen daarom vraagt en zes weken, als blijkt dat bij verschillende regionale eenheden of landelijke eenheid politiegegevens worden verwerkt.

Bovengenoemde verdaging is een procedurele beslissing, waarbij de betrokkene niet rechtstreeks in zijn belang is geschaad. Daarom is dit geen besluit en staat hier ook geen rechtsmiddel tegenover (zie artikel 6:3 Awb). Dit kan door de behandelaar zelf worden opgesteld en verstuurd.

1.10 Termijnen

In de Awb is een beslistermijn van maximaal 8 weken voor een bestuursorgaan opgenomen, tenzij in specifieke wetgeving beslistermijnen zijn voorgeschreven is. In dit geval geldt voor Rechten van betrokkene de termijnen uit de Wpg en daarin wordt gesproken over specifieke termijnen van weken, voor het afhandelen van een verzoek Rechten van betrokkene. Eén week wordt gelijkgesteld met zeven dagen en dit is ook ingericht in het digitale systeem voor termijnbewaking.

Tip: als de wettelijk gestelde termijn op een zaterdag, zondag of algemeen erkende feestdag eindigt, wordt die verlengd tot en met de eerstvolgende reguliere werkdag (artikel 1 lid 1 Algemene Termijnenwet). Het digitale systeem houdt hier géén rekening mee.

Voor het inzetten van rechtsmiddelen zijn er geen problemen bij het uitgangspunt dat één maand in het digitale systeem wordt gelijkgesteld met dertig dagen. Immers de termijn van bezwaar (of beroep) gaat in op de dag na die waarop het besluit op de voorgeschreven wijze bekend is gemaakt (artikel 6:8 Awb). Als wij op de 30ste dag het besluit toesturen aan betrokkene, terwijl het de maand februari is met 28 dagen, dan nog is het begin van de termijn de toezending of uitreiking (artikel 3:41 Awb). Dus toezending op 3 april, dan gaat de termijn voor bezwaar en beroep in op 4 april, ongeacht de tijd die wij hebben genomen om het besluit op te maken.

Er kan wel een discrepantie ontstaan bij het toepassen van de zogenaamde ‘wet dwangsom’ (artikel 4:17 Awb). Als een betrokkene op 1 februari zijn verzoek doet, kan hij/zij formeel op 1 maart een in gebreke stelling sturen, terwijl de 30 dagen termijn nog niet is verlopen. Er geldt dan altijd nog een termijn van twee weken om alsnog een besluit te nemen. (zie ook 3.9).

Tip: mede in verband met hanteren van verschillende termijnen is het noodzakelijk om een algemeen verzoek om inzage gescheiden (Wpg en AVG) af te handelen. Zeker als de verzoeker later heeft aangegeven op grond van beide wetgevingen inzage te willen. Het gevolg is dat separate besluiten worden genomen, die wel naar elkaar verwijzen om tegemoet te komen aan het gehele verzoek. Ook kunnen beide feitelijke inzagen op één moment worden afgehandeld (= klantgericht).

In algemene zin geldt dat de termijn start vanaf de dag dat het bestuursorgaan het verzoek heeft ontvangen en de dag na ontvangst van het verzoek telt als 1e dag.

Tip: let op dat de dag van ontvangst van het verzoek kan afwijken van de registratie in het (post)verwerkings- systeem. Bijvoorbeeld bij afgifte van een verzoek aan een politiebureau. De ontvangstdatum is te allen tijde leidend en vaak herkenbaar aan het stempel van ontvangst.

1.11 In gebreke stellen

Als er niet tijdig een besluit wordt genomen op het verzoek Rechten van betrokkene kan de verzoeker de politie in gebreke stellen ex artikel 4:17 Awb. Op basis hiervan verbeurt de politie voor elke dag dat het in gebreke is een dwangsom[7]. De eerste dag waarover de dwangsom verschuldigd is, is de dag waarop twee weken zijn verstreken na de dag waarop de termijn voor het geven van de beschikking is verstreken **en** de politie van de aanvrager een schriftelijke ingebrekestelling heeft ontvangen.
In gebreke stellen kan dus pas **na** het verstrijken van de beslistermijn en moet schriftelijk gebeuren. Premature ingebrekestellingen (ingediend voor het aflopen van de beslistermijn) zijn in principe (enkele uitzonderingen daargelaten) niet-ontvankelijk. De reactie op een (voortijdige) ingebrekestelling is overigens wel een besluit, waartegen ook weer bezwaar/beroep open staat.

Tip: zorg bij een ingebrekestelling dat je alsnog binnen veertien dagen een formeel besluit neemt en dat aangetekend verstuurt.

Voor de Wpg geldt dat als een verzoek Rechten van betrokkene ook na een in gebreke stelling zonder gevolg blijft (lees: geen reactie krijgt) de verzoeker hiertegen een beroep kan instellen bij de rechtbank (artikel 6:2 Awb). Dit beroep is niet aan een termijn gebonden (hoeft dus niet binnen 6 weken), maar op grond van lid 4 is het beroep niet-ontvankelijk indien dit onredelijk laat is ingediend. Voorwaarden zijn wel dat de beslistermijn moet zijn verstreken (1), de verzoeker het bestuursorgaan schriftelijk in gebreke moet hebben gesteld (2) en na de dag van ontvangst van de ingebrekestelling door het bestuursorgaan 2 weken moeten zijn verstreken (3). Het instellen van een beroep schort de dwangsom niet op. Niet alsnog besluiten betekent dat gedurende de lopende beroepsprocedure de dwangsomkosten opbouwen tot het wettelijk voorgeschreven maximum (42 dagen, zie de Algemene termijnenwet).

1.12 Rechtsmiddelen

Voor de Wpg geldt dat als op een verzoek Rechten van betrokkene een besluit is genomen[8] de verzoeker hierna rechtsmiddelen kan inzetten. In de besluiten is een uitgebreide rechtsmiddelen-verwijzing opgenomen.

De dagtekening van het besluit is niet altijd dezelfde is als de dag van verzending van het besluit. Dit is belangrijk omdat de termijn voor bezwaar of beroep ingaat op de dag na bekendmaking van het besluit (artikel 6:8 Awb). De Raad van State heeft in jurisprudentie vastgelegd dat dit wordt gelijkgesteld met de dag na verzending van het beluit. De (post)administratie van het bestuursorgaan is daarbij leidend.

*Tip: het verdient aanbeveling om **alle besluiten aangetekend te (laten) versturen**. Hierdoor zorg je ervoor dat in een formele procedure duidelijkheid bestaat over de verzenddatum van het besluit en*

[7] Zie artikel 4.17 lid 2 Awb; dwangsom in 2024 maximaal 1442 Euro (1 x 14 dagen a 23 Euro per dag, 1 x 14 dagen a 35 Euro per dag en 1 x 14 dagen a 45 Euro per dag).
[8] Besluit (gedeeltelijk) toekennen of (gedeeltelijk) weigeren.

kun je als bestuursorgaan aan je verplichting voldoen om aannemelijk te maken dat verzoeker het besluit heeft ontvangen.[9]

De verzoeker die het niet eens is met zijn Wpg besluit kan binnen zes weken na de dag van verzending van dat besluit direct beroep instellen bij de rechtbank binnen het rechtsgebied waarvan de verzoeker van het beroepschrift zijn woonplaats in Nederland heeft. Als de verzoeker van het beroep geen woonplaats in Nederland heeft, is de rechtbank in Den Haag bevoegd. Dit geldt alleen voor besluiten op verzoeken ex artikel 25 of 28 Wpg die als Awb besluiten zijn aangewezen[10].

Als de politie onder geheimhouding de geweigerde politiegegevens in een kwestie aan de bestuursrechter verstrekt (in de zin van artikel 8:29 lid 1 Awb) dan draagt de verzoeker het risico voor weigeren van de toestemming voor de geheimhoudingstoets door de bestuursrechter. Concreet betekent dit dat als de verzoeker geen toestemming geeft aan de rechter om de stukken te beoordelen, dan kan de rechter de juistheid van de gronden voor de niet-verstrekking van deze stukken niet zelf inhoudelijk beoordelen. De gevolgen hiervan moesten volgens de bestuursrechter voor rekening en risico van de verzoeker komen.

Ook kan de verzoeker die het niet eens is met zijn Wpg besluit desgewenst binnen zes weken na de dag van verzending van dat besluit zich wenden tot de Autoriteit Persoonsgegevens voor bemiddeling, advisering of het indienen van een klacht. Verzoeker krijgt na afhandeling van een klacht of bemiddelingsverzoek bij de AP een nieuwe termijn van zes weken voor het (alsnog) kunnen indienen van een beroepschrift bij de rechtbank of bezwaar bij het bestuursorgaan.

Tot slot kan de verzoeker die het niet eens is met de beëindiging van de behandeling van zijn verzoek Rechten van betrokkene op grond van de Wpg, omdat verzuimherstel niet of onvoldoende is uitgevoerd (zie 1.5), binnen zes weken na de dag van verzending van het Awb besluit een gemotiveerd bezwaarschrift indienen bij de politie-eenheid waar het besluit is genomen. Na de bezwaarprocedure kan de verzoeker eventueel een beroep instellen bij de rechtbank.

1.13 Mandatering

De Korpschef is de verantwoordelijke voor verwerking van politiegegevens onder de Wpg. Bij ondermandaat[11] is dit doorgeleid via de Politiechef naar elke eenheid.

Elke eenheid heeft vervolgens bij ondermandaat geregeld wie namens de politiechef besluiten ondertekent. Dit ligt soms bij het hoofd Staf en/of teamchef Bestuursondersteuning van een eenheid. Ook is in enkele eenheden bij ondermandaat geregeld dat gedeeltelijk negatieve of gewogen positieve besluiten door aangewezen functies (denk aan privacyfunctionaris of privacydesk medewerker) mogen worden genomen, na overleg met (een van) de bedrijfsvoering specialist(en) van de Staf die de Wpg en/of AVG in zijn takenpakket heeft.

Tip: kijk hoe de mandatering voor jouw eenheid is ingeregeld voor Wpg besluiten en raadpleeg zo nodig een stafjurist.

1.14 Tot slot

Met deze handleiding is geborgd dat binnen de politie uniform en eenduidig naar de betrokkene of

[9] De Privacydesk van de Landelijke eenheden heeft de mogelijkheid om per email besluiten te versturen omdat het postverkeer niet met alle landen van de wereld even goed gewaarborgd is.
[10] Zie artikel 29 Wpg
[11] Zie mandaatbesluit Politie, januari 2020

diens vertegenwoordiger toe wordt gecommuniceerd en gehandeld. Hiermee wordt ook tegemoetgekomen aan de beginselen van behoorlijk bestuur en tevens voldaan aan de eisen die de Algemene wet bestuursrecht (Awb) stelt aan het nemen van een beslissing op een verzoek.

De handleiding geeft de stappen weer die in het proces van afhandeling Rechten van betrokkene voor de Wpg aan de orde (kunnen) komen; van het indienen van een verzoek tot het nemen van een besluit en afsluiten va het verzoek. De twee Landelijke eenheden (LO en LX) vormen hier op onderdelen een uitzondering op, waar het betreft verzoeken die afkomstig zijn uit het buitenland.

2 Inzage van politiegegevens (Wpg)

2.1 Algemeen

Artikel 25 van de Wpg geeft de betrokkene of diens wettelijke vertegenwoordiger de mogelijkheid van de verwerkingsverantwoordelijke te horen te krijgen of over hem/haar politiegegevens worden verwerkt. En als dat het geval is, dan heeft de betrokkene recht op inzage van die politiegegevens of om specifieke informatie daarover te verkrijgen (zie 2.7).

Tip: let op dat het inzagerecht toeziet op het kennisnemen van politiegegevens die worden verwerkt en dus niet toeziet op documenten waarin politiegegevens worden verwerkt.

In de praktijk blijkt dat betrokkenen het recht op inzage vooral willen gebruiken om informatie over - of kopieën van - politiedocumenten verstrekt te krijgen voor andere doelen. Bijvoorbeeld voor het voeren van civiele procedures over burenruzies, gedragsaanwijzingen, voogdijschap, of omgangsregeling voor de kinderen. Het recht op inzage van politiegegevens ziet toe op transparantie en toetsen van verwerkingen en vormt daarmee geen grondslag voor het verstrekken van kopieën voor andere doeleinden[12]. Dit in aansluiting op jurisprudentie waarin dit wordt bevestigd[13].

Vandaar dat als uitgangspunt werd genomen dat alleen een feitelijke inzage werd toegestaan. In de Coronatijd is het mededelen van verwerkingen met een overzicht dat als bijlage bij het besluit werd gevoegd, de standaardnorm geworden. Hiermee werd een inzageverzoek schriftelijk afgehandeld door het versturen van een overzicht met de specifieke informatie over de verwerkingen van de betrokkene. Beide opties zijn mogelijk en dit betekent contact leggen met de betrokkene en daarna, of besluit nemen en overzicht versturen (1), of een besluit nemen en feitelijke inzage laten plaatsvinden (2). In beide gevallen wordt een formeel besluit opgemaakt. In geval de verzoeker in het buitenland verblijft en een feitelijke inzage om praktische redenen niet mogelijk is, kan ook met een overzicht worden volstaan. Dit laatste geldt zeker voor de Landelijke eenheden (LO en LX), die alle verzoeken uit het buitenland met betrekking tot signaleringen en andere verwerkingen over betrokkene afhandelt (zie 2.12).

Tip: let op dat ook bij het verstrekken van een overzicht met specifieke informatie over artikel 9 of 10-Wpg verwerkingen, vooraf de toestemming van de Bevoegd Functionaris is vereist en daarbij ook mogelijk tot een (gedeeltelijke) weigering kan worden besloten.

Er wordt bij inzage wel onderscheid gemaakt tussen het besluit nemen en overzicht versturen (paragraaf 4 Wpg) inzagerecht) en het verstrekken van politiegegevens voor andere doeleinden (paragraaf 3 Wpg). En neem bij twijfel hierover contact op met de verzoeker om duidelijkheid te verkrijgen, waar het verzoek toe bedoeld is. Eigen interpretatie over de aard van het verzoek is niet aan de orde en dienstbaarheid en behoorlijkheid zijn de uitgangspunten hierbij.

[12] Zie voormalig artikel 20 WPolR en diverse uitspraken van RvS op respectievelijk 27 mei 2015 (ECLI:NL: RVS:2015:1779), 9 september 2015 (ECLI:NL:RVS:2015:12803) en 6 juli 2016 (ECLI:NL:RVS:2016:1852).
[13] Zie bijvoorbeeld ECLI:NL: RVS:2015:2805

2.2 Indienen verzoek

In de wet staat: 'De betrokkene heeft het recht om op diens schriftelijk verzoek ….' (artikel 25 Wpg). Dit betekent dat het verzoek om inzage schriftelijk moet worden ingediend. Op de website politie.nl staat een overzicht van alle eenheden en adressen welke door de betrokkene of diens vertegenwoordiger kan worden gebruikt (zie bijlage B).

Tip: let ook op de dienstbaarheid en behoorlijkheid naar de verzoeker toe. Een handgeschreven briefje is ook een formeel verzoek. Op politie.nl is het nieuwe privacy statement gepubliceerd, waar bij Rechten van betrokkenen opgenomen is dat voor een dergelijk verzoek een kopie van een identiteitsbewijs meegestuurd moet worden. Daarbij is ook aangeven om de foto en BSN – in lijn met AVG en Wpg – af te schermen.

2.3 Registreren verzoek

Een verzoek wordt geregistreerd en krijgt een uniek kenmerk, zodat dit bij correspondentie steeds kan worden aangehaald. De wettelijke termijn voor afhandeling start met de datum van ontvangst van het betreffende verzoek. Dit is de eerste dag, nadat het verzoek bij de politie is ontvangen. Dit staat bijvoorbeeld los van een verwerkingstermijn bij de interne postverwerking.

Het ontvangen verzoek met bescheiden wordt ingeboekt en intern doorgezonden naar de Privacydesk, of andere afdeling die het verzoek in behandeling neemt. Het verdere proces van afhandeling en termijnbewaking wordt bijgehouden in het digitale systeem. In het systeem worden de volgende gegevens over het verzoek vastgelegd:

- ✓ de datum ontvangst bij de politie;
- ✓ de naam, adres en woonplaats van de verzoeker en de betrokkene (indien dit verschillende personen betreffen);
- ✓ wat voor verzoek het betreft;
- ✓ alle correspondentie over het verzoek.

Vervolgens wordt vanuit de behandelaar een ontvangstbevestiging verstuurd op het binnengekomen verzoek, met daarin opgenomen de termijn voor afhandelen van dit verzoek, mogelijkheid van een klacht bij de AP, het vernietigen van het meegestuurde kopie identiteitsbewijs en verwijzing naar privacy statement zijn opgenomen.

Tip: bij een gecombineerd verzoek in één brief (inzage in persoons- en politiegegevens) moet voor het "andere" verzoek een nieuwe registratie worden aangemaakt. Dit betekent dus ook een separate ontvangstbevestiging, omdat andere wetgeving, artikelen en termijnen gelden.

2.4 Beoordelen formaliteiten

Identiteit vaststellen. Bij behandeling van een verzoek om inzage moet de politie zorgen voor deugdelijke vaststelling van de identiteit van de betrokkene en eventueel de verzoeker als dat iemand anders is (artikel 26 Wpg). Daarom wordt standaard gevraagd bij een schriftelijk verzoek om inzage een kopie van een geldig identiteitsbewijs bij te voegen van betrokkene en (indien van toepassing) diens wettelijk vertegenwoordiger, waar het BSN en de foto onleesbaar van zijn gemaakt. Dit is een deugdelijke vaststelling, omdat de (adres)gegevens gecontroleerd kunnen worden met het BRP.

Als een advocaat als gemachtigde optreedt, zal in beginsel een machtiging van de betrokkene overlegd moeten worden. Het deugdelijk vaststellen van de identiteit van de advocaat zelf kan ook op andere wijze plaatsvinden (zie 1.4).

Ontbreekt een kopie van een identiteitsbewijs en/of machtiging, dan wordt de verzoeker in de gelegenheid gesteld, onder gelijktijdige opschorting, om dat verzuim te herstellen.

Verzoeker. Een verzoek om inzage van politiegegevens is een persoonlijk recht en kan niet worden ingediend door iemand anders, of door een minderjarige onder de16 jaar, of door iemand die onder curatele is gesteld. Een dergelijk verzoek kan formeel/juridisch worden geweigerd, maar vanuit dienstbaarheid en behoorlijkheid wordt de mogelijkheid tot verzuimherstel geboden. Er wordt daarbij vanuit gegaan dat de betrokken zelf ook belang heeft bij het verzoek. Indien het verzuim niet (tijdig) wordt hersteld is het verzoek daarmee niet-ontvankelijk en wordt besloten alsdan dat af te wijzen, waarmee niet wordt toegekomen aan de inhoudelijke behandeling

Het gaat voor de betrokkene 'om de hem betreffende politiegegevens' en niet die van een ander (artikel 25 Wpg), tenzij de verzoeker als advocaat is gemachtigd, of als wettelijk vertegenwoordiger optreedt. Voorts maakt dit artikel onderdeel uit van paragraaf 4 van de Wpg, die betrekking heeft op de rechten van de betrokkene. Ingevolge artikel 1, aanhef en onder g, van de Wpg wordt onder betrokkene verstaan degene op wie een politiegegeven betrekking heeft[14]. Een verzoek om inzage kan dus niet worden ingediend over iemand anders[15].

Het verzoek voor een minderjarige, die de leeftijd van 16 jaar nog niet heeft bereikt, moet worden gedaan door diens wettelijk vertegenwoordiger (artikel 26 Wpg). Dit is een wettelijk voorschrift. Als hier niet aan wordt voldaan, wordt verzoeker alsnog de mogelijkheid geboden, onder gelijktijdige opschorting, om dit te herstellen. Wordt hier wel aan voldaan dan wordt de wettelijke vertegenwoordiger tijdens de procedure verder geïnformeerd als verzoeker.

Tip: wees voorzichtig bij minderjarigen tot 16 jaar en check of de verzoeker ook daadwerkelijk als wettelijk vertegenwoordiger kan optreden. Er kunnen belangen spelen zoals scheiding, voogdijschap, zedenverhaal, ouderlijk gezag, etc. Een verzoek kan worden ingediend door één van de vertegenwoordigers en hoeft niet ondertekend te zijn door alle vertegenwoordiger(s).

Ook ten aanzien van een onder curatele gesteld persoon, kan het verzoek om inzage alleen worden gedaan door diens wettelijk vertegenwoordiger (artikel 26, lid 2 Wpg). Dit is een wettelijk voorschrift. Als hier niet aan wordt voldaan, wordt verzoeker alsnog de mogelijkheid geboden, onder gelijktijdige opschorting, om dit te herstellen. Wordt hier wel aan voldaan dan wordt de wettelijk vertegenwoordiger tijdens de procedure verder geïnformeerd als verzoeker.

Tip: check bij een vermoeden of de betrokkene onder curatele is gesteld in het landelijk register, dat is te vinden onder: https://curateleenbewindregister.rechtspraak.nl. Leg dit vast in het dossier.

Het verzoek kan worden gedaan door een advocaat aan wie de betrokkene een bijzondere machtiging heeft verleend., uitsluitend met de bedoeling de belangen van zijn cliënt te behartigen (artikel 26, lid 3 Wpg). Dit is een wettelijk voorschrift. Als hier niet aan wordt voldaan, wordt betrokkene alsnog de mogelijkheid geboden, onder gelijktijdige opschorting, om dit verzuim te herstellen. Als het verzuim wordt hersteld, dan wordt de advocaat tijdens de procedure verder geïnformeerd en niet de betrokkene. Een machtiging wordt in het dossier opgenomen.

Tip: in de praktijk blijkt dat verzoeken voor Rechtten van betrokkene ook worden ingediend door anderen, zoals een juridisch vertegenwoordiger. Deze worden afgewezen en niet in behandeling genomen, zodat hiermee het personen of instanties onmogelijk wordt gemaakt om via een omweg de

[14] Zie ook Kamerstukken II 2005/06, 30 327, nr. 3, blz. 27 waarin staat vermeld dat voor de definitie van betrokkene is aangesloten bij die in artikel 1, aanhef en onder f, van de Wet bescherming persoonsgegevens (Wbp).
[15] Derden kunnen zich derhalve niet op dit artikel beroepen (zie de uitspraak van de Afdeling van 22 november 2017, ECLI:NL:RVS:2017:3223).

beschikking te krijgen over persoonsgegevens van een persoon met wie men een bepaalde relatie heeft of wil aangaan[16]*.*

Zodra alle (gevraagde) benodigde bescheiden zijn aangeleverd en daarmee het verzuim is hersteld, wordt het verzoek verder in behandeling genomen en gaat de afhandelingstermijn weer (verder) lopen. Als de verzoeker het verzuim niet of onvoldoende heeft hersteld, dan wordt de behandeling beëindigd en een besluit ex artikel 4:5 Awb (buiten behandeling stellen) verstuurd. Tegen dit besluit staat bezwaar open en het voornemen tot een dergelijk besluit is al opgenomen in de verzuimbrief. Hierdoor kom je niet meer toe aan een inhoudelijk besluit (stap 5). Dit besluit moet binnen vier (4) weken na ontvangst van onvoldoende aanvullende informatie of het verstrijken van de gestelde termijn worden verstuurd. Als het verzoek buiten behandeling is gesteld en verzoeker dient opnieuw een incompleet (herhaald) verzoek in, dan kunnen we dat afwijzen op grond van “geen nieuwe feiten of omstandigheden” (artikel 4:6 Awb).

Tip: na die 4 weken kun je het verzoek ook nog afwijzen, maar dan is het een inhoudelijke afwijzing. Dit is voor de bezwaar-/beroepsprocedure van belang of er ex tunc of ex nunc beoordeeld moet worden.

Verzoekschrift. Een verzoek om inzage van politiegegevens kan alleen als zodanig worden afgehandeld als duidelijk is dat dit ook de bedoeling van het verzoekschrift is. Het gaat om de controle of de gegevens juist, volledig en actueel zijn en rechtmatig worden verwerkt. Dus niet voor het ontvangen van kopieën van meldingen of aangiftes. Het interpreteren van een verzoekschrift is niet aan de behandelaar van de politie voorbehouden. Verder mag (de korpschef) een redelijke vergoeding vragen of weigeren aan een verzoek gevolg te geven wanneer dat kennelijk ongegrond of buitensporig is. Met name als de betrokkene zonder goede reden en herhaaldelijk om informatie verzoekt, of wanneer de betrokkene zijn recht om informatie te verkrijgen misbruikt, bijvoorbeeld door bij het verzoek valse of misleidende informatie te verstrekken[17].

Tip: let wel op dat dit uitzonderlijke situaties zijn en de bewijslast hiervoor ligt bij de politie.

Bij een te algemeen gesteld inzageverzoek (“Ik wil alles”) en veel politiegegevens worden verwerkt, wordt aan de verzoeker gevraagd om zijn verzoek te specificeren en concreet aan te geven waar hij inzage over wil hebben. Hiermee wordt een onevenredige inspanning van de politie voorkomen. Communiceer hier schriftelijk over en leg dit goed vast in het dossier.

Bij een kennelijk ongegrond, of buitensporig verzoek, in het bijzonder vanwege de geringe tussenpozen[18] tussen opeenvolgende verzoeken, kan het verzoek dus worden geweigerd (zie 2.7). In beginsel wordt voor een herhalingsverzoek een termijn van 6 maanden gehanteerd.

Tip: een herhaald verzoek vraagt wel scherpte op de inhoud van het verzoek en een eventueel eerder genomen besluit. Bij een herhaling van een eerder verzoek waarbij een deel is geweigerd, ben je half jaar verder en zijn er dus eventueel nieuwe verwerkingen bijgekomen, gerekend vanaf de datum van

[16] Hiermee wordt aangesloten bij artikel 20, vierde lid, van de Wet justitiële en strafvorderlijke gegevens (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 85) en bij het beoogde doel van dit onderdeel uit artikel 26 Wpg (Kamerstukken II 1995/96, 24 797, nr. 3, blz. 28).
[17] Overweging 40 van de Europese Richtlijn 2016/680
[18] Overweging 43 van de Europese Richtlijn 2016/680 zegt dat een natuurlijke persoon het recht op inzage van de gegevens die over hem zijn verzameld met redelijke tussenpozen moet kunnen uitoefenen, zodat hij kennis kan nemen van de verwerking en de rechtmatigheid daarvan kan nagaan.

het vorige besluit. Tevens dienen eventueel eerder geweigerde politiegegevens opnieuw getoetst te worden.

Beslistermijn. De politie heeft de wettelijke verplichting het verzoek om inzage binnen zes (6) weken af te handelen. Deze termijn start vanaf het moment dat het verzoek is ontvangen. Indien blijkt dat niet aan alle vereisten wordt voldaan (= verzuim), dan wordt de behandeling opgeschort. De termijn van afhandeling gaat weer lopen als het verzuim is herteld (zie 2.5).

Er is éénmalig de mogelijkheid de beslistermijn – voor afloop daarvan – te verdagen, als blijkt dat het niet mogelijk is binnen de gestelde termijn een besluit te nemen op het verzoek om inzage van de politiegegevens. Of met uitstel van ten hoogste vier (4) weken, of met uitstel van zes (6) weken, als de politiegegevens in verschillende eenheden en/of bij de landelijke eenheden zijn verwerkt. Van de verdaging krijgt de verzoeker schriftelijk bericht en dit verlengt de afhandelingstermijn.

Doorsturen verzoek. Het verzoek wordt in principe in behandeling genomen door de eenheid waar de betrokken woonachtig is en als hiervan wordt afgeweken en een andere eenheid het verzoek overneemt, wordt de verzoeker hierover (schriftelijk) geïnformeerd.

Tip: check of bij andere eenheden eerdere of identieke verzoeken zijn ingediend en stem daarna af wie, wat doet en houdt er wel rekening mee dat een interne doorzending de beslistermijn niet opschort.

Als een dossier is ingezonden naar het OM, waar nog geen beslissing in is genomen, dan volgt altijd afstemming met het OM. Er is dan een verwerking bij het OM (= procesdossier) met als grondslag de Wet justitiële en strafvorderlijke gegevens (Wjsg) en een verwerking bij de politie (= onderzoek dossier) met als grondslag de Wpg. Mogelijk kunnen belangen, zoals bescherming van rechten of vrijheden van derde(n) of opsporings- of vervolgingsbelang, worden geschaad door een inzage bij de politie. In bestaande praktijk moet er dus altijd afstemming plaatsvinden met het OM[19] en kan het verzoek worden afgewezen en/of eventueel ook doorgezonden worden aan het OM, of in soortgelijke gevallen naar een ander bestuursorgaan. Aan het bestuursorgaan dat bevoegd is om de inzage verder in behandeling te nemen wordt het verzoek schriftelijk overgedragen en de verzoeker wordt hiervan schriftelijk in kennis gesteld.

Tip: let op dat bij een strafrechtelijk dossier dat is verstrekt aan het OM (= procesdossier) geldt nagenoeg altijd dat er meer informatie is verwerkt bij de politie (= onderzoek dossier). Alsdan moet de politie altijd een eigenstandig beluit nemen, dat vaak tot een afwijzing zal leiden, na afweging van belangen. Daarnaast geldt dat als betrokkene politiegegevens die in een processtuk zijn verwerkt, heeft ontvangen op grond van artikel 30 tot en met 34 Wetboek van Strafvordering (WvSv), voor die stukken is voldaan aan het kennis nemen ex artikel 25 Wpg[20] en hoeft de behandelaar dit niet meer mee te nemen bij de inzage.

2.5 Verzamelen persoonsgegevens

Verzamelen gegevens. Voor het verzamelen van de politiegegevens over betrokkene en gerelateerd aan het inzageverzoek doet de behandelaar of zelf een zoekslag in systemen en/of een verzoek aan de afdeling DRIO met een Poortwachtersautorisatie in verband met ‘oude’, reeds verwijderde politiegegevens. Al dan niet in samenwerking met DRIO wordt een overzicht gegenereerd van alle

[19] Zie ‘Aanwijzing Wpg’ en doorzendplicht in kader van artikel 2:3 Awb
[20] Zie artikel 24a, lid 5 Wpg

verwerkingen voor de politietaak. Dit betreft de verwerkingen onder artikel 8, 9, 10 en/of 13 Wpg, met uitzondering van artikel 12 Wpg verwerking die is uitgesloten. Over de betrokkene wordt de daarbij behorende inhoudelijke informatie verzameld die voor de politietaak mogelijk in diverse systemen, waaronder BVH, Summ IT, GMS, RSC (LSM-meldingen), LJP, OPS, NSIS en KA-omgeving is verwerkt. Deze informatie wordt opgevraagd met behulp van zoekapplicaties Blue Spot Monitor, Blue View en BVI-IB. Verder worden de bevoegde functionarissen bevraagd voor een gerichte verwerking onder artikel 9 en/of 10 Wpg. Een overzicht van systemen, applicaties en/of registers die wel/niet onder de uitvraag voor inzage onder de Wpg vallen is onder bijlage A opgenomen.

Tip: neem in het besluit op welke zoekslagen je in welke systemen hebt gedaan of hebt laten doen. Er is steeds meer jurisprudentie waaruit blijkt dat de politie moet aantonen hoe en in welke systemen is gezocht. Zoek niet alleen op naam of keno, maar in brede zin op naam en adres. Niet altijd is een personenkaart aangemaakt en gekoppeld en is er in het vrije tekstveld van een toelichting of verklaring iets over de betrokkene opgenomen en dus verwerkt.

Verder kun je het systeem BosZ raadplegen als bijvoorbeeld wordt gevraagd naar de wijze of mate van afdoening in een bepaalde zaak. Of de Landelijke Service Module (LSM) als het over meldingen gaat die betrokkene heeft gedaan. Tot slot is het van belang om de kantoorautomatiseringsomgeving en dan specifiek de O-schijf mee te nemen als daar aanleiding voor is, of naar wordt verwezen. Denk hierbij bijvoorbeeld aan het verwerken van foto's of digitale informatie, aanvullende op een basisregistratie in BVH of Summ IT.

Tip: let op dat er mogelijk ook politiegegevens op andere dan de O:schijf worden verwerkt binnen de KA-omgeving, ook als is dat niet de bedoeling.

Het overzicht van politiegegevens wordt samengesteld uit BVH met behulp van de applicatie Blue Spot Monitor en uit Summ-IT met de applicatie 'zoeken en vinden'. Dit is wat redelijkerwijs van medewerkers van de Privacydesk en DRIO verwacht mag worden bij het zoeken op naam en/of 'keno'-sleutel. Ook de verwijderde en nog niet vernietigde politiegegevens (artikel 14 Wpg) moeten worden meegenomen, alsmede de verstrekking aan derde(n) van politiegegevens over betrokkene in de afgelopen vier jaar conform artikel 25 Wpg. Een overzicht van de zoeksystemen en bijbehorende autorisaties is onder bijlage D opgenomen.

*Tip: bij een zoekvraag via Blueview krijg je mogelijk ook informatie te zien van verwerkingen over de betrokkene bij andere Wpg verantwoordelijken en daar ziet het verzoek aan de politie **niet** op toe. Dit betekent dat je informatie uit die bestanden niet mag betrekken in de beantwoording van het verzoek om inzage. Vink die bestanden dan ook uit voor je de zoekslag maakt.*

Formeel valt ook de correspondentie over betrokkene met de feitelijke persoonsgegevens onder het inzagerecht, zowel voor de Wpg als de AVG. Denk hierbij aan brieven of mailverkeer. Dit vergt extra tijd en capaciteit om uit te zoeken en de cruciale vraag hierbij is wat de verzoeker uiteindelijk wil. Uitgangspunt is dan ook om bij het verzamelen ten minste de concrete verwerkingen in de basis applicaties te gebruiken voor beantwoording van het inzageverzoek. Mocht uit het verzoek of aanvulling anders blijken, neem dan de correspondentie mee in het verzamelen en overzicht.

Toestemming Bevoegd Functionaris. Voor zover blijkt van artikel 9 en 10 Wpg-verwerkingen vraagt de behandelaar toestemming van de Bevoegd Functionaris om de betrokkene van die gegevensverwerking inzage te geven. Er is een format met uitleg, waarmee informatie over de verwerkte politiegegevens ex artikel 9 of 10 Wpg bij een Bevoegd Functionaris kan worden opgevraagd (brief 10). De Bevoegd Functionaris kan dit gemotiveerd weigeren, maar dit moet dan

vallen onder een van de afwijzingsgronden genoemd in artikel 27 Wpg (zie 2.7). Die afwijzingsgrond moet dan worden afgewogen tegen het belang van verzoeker door degene die het besluit neemt namens de Korpschef.

Tip: vraag als behandelaar wel om een nadere uitleg aan de Bevoegd Functionaris, want een (gedeeltelijke) weigering moet je - met redenen omkleed - kunnen motiveren en kan leiden tot een beroepsprocedure bij de rechtbank. Ook een gerichte persoonsverwerking onder artikel 10 Wpg moet worden medegedeeld en zeker als in BVH is verwerkt dat iemand (DRIO)subject is, kun je dat niet standaard afwijzen[21]. Wel zal een artikel 10 Wpg verwerking nagenoeg altijd tot een gedeeltelijke weigering leiden, omdat er (mogelijk) informatie wordt verwerkt afkomstig van informanten, die volledig afgeschermd moeten blijven.

Anonimiseren. Bij Rechten van betrokkene gaat het over de hem betreffende politiegegevens en dus niet die van derde(n). De persoonsgegevens van andere(n) dan de betrokkene zelf vallen dus niet onder een inzageverzoek en moeten derhalve geanonimiseerd worden. Het gaat hierbij om direct naar personen herleidbare informatie (bijv. personalia) en indirect naar personen herleidbare informatie (bijv. adres, telefoonnummer, of de buren van melder). De gegevens van verbalisanten of rapporteurs (waaronder stam-/dienstnummer) zijn ook aan te merken als politiegegevens van derde(n)[22] en moeten derhalve ook worden weggelaten of geanonimiseerd. Dit zijn dus géén weigeringen op grond van artikel 27 Wpg, maar vallen buiten het initiële verzoek ex artikel 25 Wpg. De verklaring of melding door een ander over de betrokkene, valt weer wel onder het inzagerecht van die betrokkene, waarbij wel de afwijzingsgrond voor rechten en vrijheden van derde(n) moet worden afgewogen.

Tip: bij een inzage wordt informatie van derde(n) en ook politietactieken of -inzet onleesbaar gemaakt bij het inzien van politiegegevens[23]. Dit is geen weigering, maar vat niet onder het inzagerecht. Leg dit wel uit en wil je hiervan wegblijven kun je ook alle informatie waar je kennis van laat nemen in één document opnemen.

Tot slot ziet de Wpg toe op de verwerking van politiegegevens en stelt niets over documenten[24], waarin die gegevens eventueel zijn opgenomen[25]. Mocht de betrokkene het niet eens zijn met de verwerking wijs hem/haar dan op het recht tot wijziging.

2.6 Beoordelen besluit

Een inzage kan alleen toegewezen en feitelijk uitgevoerd worden als er ook daadwerkelijk gegevens van betrokkene zijn verwerkt. De 1e toets is dus artikel 25 Wpg zelf en als dat wordt toegewezen, dan is de 2e toets of er een beperking ex artikel 27 Wpg moet worden meegegeven. Als er géén gegevens worden verwerkt, wordt het verzoek om inzage afgewezen en daarvan schriftelijk mededeling gedaan aan de betrokkene of verzoeker. Dit wordt opgenomen in een besluit.

[21] Uitspraak d.d. 25 mei 2022 zaaknummerUTR21/3817AVG V169
[22] Uitspraak ECLI:NL:RvS:2018:3350
[23] ECLI:NL:RVS:2025:3976 uitspraak waarbij inzage in processen-verbaal zijn geweigerd en voldoende is gemotiveerd dat inzage in de verwerkte gegevens het onderzoek zou schaden, omdat de betrokkene daarmee inzicht zou krijgen in de omvang van het onderzoek en de onderzoeksstrategieën naar hem. Hierop zou betrokkenen vervolgens kunnen anticiperen en eventuele af te leggen verklaringen hierop kunnen aanpassen.
[24] ECLI:NL:RVS:2025 uitspraak dat de Wpg geen grond biedt om kopieën te verkrijgen van documenten waarin politiegegevens zijn opgenomen, het recht op inzage alleen ziet op inzage in persoonsgegevens van de betrokkene en niet van anderen (namen en dienstnummers van politieagenten) en te lang bewaarde gegevens definitief zijn verwijderd en daarmee handhavend optreden van de AP dus niet meer nodig was.
[25] Uitspraak: ECLI:NL:RvS:2013:CA0634

Toewijzen verzoek. Als er gegevens worden verwerkt kan schriftelijk of mondeling op een verzoek worden gereageerd[26]. Uit praktische overwegingen zullen de meeste verzoeken schriftelijk worden afgehandeld door het opstellen van een besluit en een overzicht van specifieke informatie over de verwerkingen van betrokkene. Dit is een besluit. Wanneer de verwerking informatie betreft over de oorsprong van de persoonsgegevens, mag die informatie de identiteit van natuurlijke personen, in het bijzonder van vertrouwelijke bronnen, niet onthullen[27].

Als geen overzicht wordt verstuurd, of na een eerder verstuurd overzicht om inzien van politiegegevens wordt gevraagd, wordt een inzage aan een bureau georganiseerd. De verzoeker wordt uitgenodigd voor een feitelijk kennisnemen van politiegegevens en daartoe wordt een concrete afspraak gemaakt. Dit wordt opgenomen in het besluit.
Indien nog geen concrete afspraak kan worden gemaakt, wordt het besluit om inzage formeel genomen en daarin aan de verzoeker gevraagd om contact op te nemen en een afspraak te maken.

De bovengenoemde afhandelingen zijn een formele beslissing en geen deelbesluit op het verzoek om inzage en dienen schriftelijk aan de verzoeker kenbaar te worden gemaakt[28]. Er mag in beginsel niet te veel tijd zitten tussen het besluit en de inzage zelf. Dit vanwege de beroepstermijn die geldt vanaf de datum van het besluit.

Afwijzen verzoek. Er kunnen na de toetsing op artikel 25 Wpg ook redenen zijn om het verzoek om inzage geheel of gedeeltelijk af te wijzen (artikel 27 Wpg). Dat mag alleen wanneer dat noodzakelijk is in geval van één van de volgende situaties (= limitatieve opsomming):

a) vermijden van belemmeren van gerechtelijke onderzoeken of procedures
b) vermijden van nadelige gevolgen voor voorkoming, de opsporing, het onderzoek en vervolging van strafbare feiten of tenuitvoerlegging van straffen
c) beschermen van openbare veiligheid
d) beschermen van de rechten en vrijheden van derden
e) beschermen van de nationale veiligheid
f) kennelijk ongegrond of buitensporig verzoek (zie 2.5) en
g) gegevens betreffende verwerking op basis van artikel 12 Wpg (informantenbeheer)[29]

Doet een situatie onder a t/m f zich voor, dan wordt de inzage geweigerd voor zover dit een noodzakelijke (1) en evenredige (2) maatregel is. Daarbij dient het belang van de betrokkene op inzage te worden afgewogen tegen het belang van de verantwoordelijke om inzage te weigeren. Met de criteria van noodzakelijkheid en evenredigheid wordt dit tot uitdrukking gebracht. Er is dus, anders dan onder de ‘oude Wpg’, sprake van een belangenafweging. Van een gehele of gedeeltelijke afwijzing van de inzage krijgt de betrokkene of verzoeker een schriftelijk besluit. In dat besluit zijn de feiten en juridische grond(en) met de motivering welke belangen zijn afgewogen opgenomen.

Tip: neem de afweging die is gemaakt op in het genomen besluit. Er zijn al uitspraken waarbij hier vragen over zijn gesteld en de rechtbank heeft geoordeeld dat er bij een (gedeeltelijke) afwijzing eerst nog een zienswijze moet worden gevraagd. H*et advies is om bij gebruik van bovenstaande weigeringsgronden de privacyfunctionaris en/of jurist te raadplegen voor het (aanvullend) formuleren van de belangenafweging en motivering. Let er ook op als eerdere verzoeken voor inzage bekend zijn en daarbij inzage (deels) is geweigerd, of die noodzakelijkheid daarvoor nu nog geldend is. Zo kan*

[26] Zie memorie van toelichting op artikel 25 Wpg en prejudiciële vraag bij het Europese Hof voor de Rechten van de Mens (HvJ EU 17-07-2014, ECLI:EU:C:2014:2081, AB 2014/365).
[27] Overweging 43 van de Europese Richtlijn 2016/680
[28] Zie ECLI:NL: RVS:2018:1982.
[29] Bij een artikel 12 Wpg verwerking worden gegevens verwerkt over informanten subjecten, contacten van beiden en politieambtenaren.

een strafzaak zijn beëindigd, waardoor de weigeringsgrond 'opsporings- en vervolgingsbelang' komt te vervallen.

De uitzondering op bovenstaande is de situatie onder g, waarbij geen belangenafweging plaatsvindt en het verzoek altijd wordt afgewezen met een schriftelijk besluit. Stem dit altijd af met de TCI in verband met de grote belangen die meespelen bij een dergelijke verwerking.

2.7 Uitvoeren inzage

Er zijn twee opties voor het uitvoeren van de inzage van politiegegevens, te weten:

a) het toesturen van een overzicht van de verwerkingen van politiegegevens (soms is dit vanuit efficiency en praktisch oogpunt effectiever), of
b) het inzien van de verwerking van politiegegevens op het politiebureau (of mogelijk andere locatie).

Het is een beleidsmatige keuze, gesteund door vaste jurisprudentie, dat de Korpschef bepaalt op welke wijze inzage wordt gegeven. Inzage van politiegegevens ziet toe op kennisnemen van verwerkingen en verplicht niet tot het geven van een kopie van de feitelijke politiegegevens.[30]

Tip: neem vooraf contact op met verzoeker en vertel wat inzage inhoudt en wat onze mogelijkheden zijn. Hierdoor voorkom je dubbel werk met eerst versturen van een overzicht en later een feitelijke inzage. Leg gemaakte afspraken wel vast in de brief en/of het dossier.

Toesturen overzicht. Met het toesturen van een overzicht van de verwerkingen als bijlage van een toegewezen besluit wordt ook (grotendeels) tegemoetgekomen aan het verzoek tot inzage. Echter uit de wettelijke verplichting en jurisprudentie volgt niet alleen dat betrokkene informatie kan verkrijgen over al zijn verwerkingen, maar ook over de context daarvan. Om hieraan tegemoet te komen kan het nodig zijn dat je in het overzicht de relevante inhoudelijke tekst van de verwerking opneemt. Hiermee wordt echter ook de mogelijkheid vergroot, dat het overzicht voor andere doeleinden dan de toetsing op doelmatigheid, noodzakelijkheid en rechtmatigheid wordt gebruikt. Uitgangspunt is dan ook om alleen alle verwerkingen waarvan kennisnemen wordt toegestaan, in het overzicht op te nemen, zonder de concrete inhoud. Wil de verzoeker de verwerkingen inhoudelijk toetsen, dan kan dat worden ingezien aan het politiebureau. Daarnaast geldt ook dat als je in het overzicht van de verwerkingen over betrokkene een deel weglaat, dit dan wel een formele weigering is, die je in het besluit moet opnemen en motiveren.

Tot slot wordt inzage van politiegegevens niet gezien als een verstrekking van politiegegevens aan derde(n) voor een ander doel dan de politietaak (zie paragraaf 3 Wpg). Alleen al niet omdat de inzage ex artikel 25 Wpg is opgenomen in paragraaf 4 van de Wpg.

Inzage aan bureau. Met het kennisnemen van politiegegevens op het politiebureau (= inzien), wordt volledig tegemoetgekomen aan het recht op inzage van de betrokkene. Een politiebureau is ingericht om veilig te kunnen werken en de politiegegevens blijven in een afgeschermde omgeving. Als iemand fysiek niet in staat is om inzage aan het politiebureau uit te voeren, is het bij uitzondering mogelijk dat op een andere locatie te doen. Denk bijvoorbeeld aan mensen met fysieke beperkingen of die verblijven in een Penitentiaire Inrichting. Dit blijft maatwerk, waarbij veiligheid en afscherming van politiegegevens en dienstbaarheid voorop staan en altijd achteraf de toets door de rechter wordt uitgevoerd of wij voldoende tegemoet zijn gekomen aan verzoeker met betrekking tot zijn recht op inzage.

[30] Zie memorie van toelichting op artikel 25 Wpg

Het recht op inzage is wel een persoonlijk recht en betekent dat een ander dan de betrokkene (of diens wettelijke vertegenwoordiger) het niet kan uitoefenen. Indien betrokkene zich niettemin wil laten vergezellen, of zijn recht door een ander dan zijn advocaat of wettelijk vertegenwoordiger wil laten uitvoeren, is dit in beginsel uitgesloten en wordt inzage **niet** toegestaan. Het zou tegen de bescherming van de privacy van de betrokkene indruisen als anderen de verwerkte gegevens zouden mogen inzien[31] en er is ook geen titel om aanwezigheid bij de inzage te rechtvaardigen. In bijzondere gevallen kan hierop een uitzondering worden gemaakt, maar dit is maatwerk en zonder de (schriftelijke) toestemming van de betrokkene niet toegestaan. Leg een uitzindering goed vast om geen precedentwerking te krijgen.

Voor de inzage dient de identiteit van de verzoeker (betrokkene, advocaat of wettelijk vertegenwoordiger) en bij uitzonderring degene die hem/haar vergezelt deugdelijk te worden vastgesteld. Leg daarvoor het soort ID bewijs en bijbehorend nummer vast in het dossier. En voor alle duidelijkheid: de verzoeker zelf voert het recht van inzage uit (zie ook 1.4). Krijg je de indruk dat dit niet het geval is, overweeg dan om de inzage te stoppen. Leg de reden en omstandigheden vast in het dossier.

Bij de inzage mogen aantekeningen worden gemaakt, die uiteraard moeten passen bij het uitvoeren van het recht op inzage en/of rectificatie door de betrokkene. Dit betekent dus geen kopieën maken van documenten, niet alles letterlijk gaan overschrijven of inspreken, en geen foto's maken. Het gebruik van een laptop past daarin, mits geen foto's of opnames worden gemaakt. In de besluiten is opgenomen dat er huisregels gelden.

De betrokkene kan alleen inzage krijgen over wat van hem/haar wordt verwerkt in de politiesystemen. Dus niet van anderen! Dit betekent dat je in sommige documenten delen moet weglaten of anonimiseren. In die gevallen is er sprake van verwerking politiegegevens over anderen. Denk aan namen van verbalisanten of rapporteurs, verklaringen van derden, etc. Die vallen niet binnen het bereik van artikel 25 Wpg.

Tip: bepaal vooraf of je documenten wilt laten lezen of zelf voorleest. Voorlezen betekent dat je minder werk hebt aan het anonimiseren van informatie over derde(n). Van belang is dat de betrokkene zijn recht kan halen en weet wat er over hem wordt verwerkt. Dus als je bij het voorlezen politiegegevens over betrokkene weglaat, dan moet er gemotiveerd een afwijzingsgrond in het besluit zijn terug te vinden.

De Nationale Ombudsman heeft de uitspraak gedaan dat het een burger moet worden toegestaan om in zijn contact met het bestuursorgaan het gesprek op te kunnen nemen. Dit heeft betrekking op de interactie tussen politie en betrokkene en betekent wel spraak, maar geen beelden. Dit initiatief kan ook vanuit de politie komen. Belangrijk daarbij is dat dit voorafgaande aan de inzage wordt gemeld. De betrokkene mag zelf de tekst van zijn gegevensverwerking lezen en daarvan aantekeningen maken, maar geen kopieën. Dit houdt tevens in dat het gebruik van audiovisuele en/of technische middelen (bijvoorbeeld mobiele telefoon) om documenten weer te kunnen geven die onderdeel zijn van de inzage wordt geweigerd. Er is dan sprake van een inhoudelijke verstrekking, die voor andere doeleinden kan worden gebruikt en dit past niet binnen de doelstelling van inzage (= rechtsbescherming burger).

[31] Zie ook: ECLI:NL:RVS:2019:801.

Tip: geef bij de inzage uitleg over het doel van deze vorm van rechtsbescherming. Neem de tijd voor een feitelijke inzage en doe dat bij voorkeur met twee personen. Dit kun je in de schriftelijke uitnodiging opnemen. Leg kort vast hoe de inzage is verlopen en maak een kort verslag van de inzage als er 'gedoe' is geweest en een beroepsprocedure of klacht valt te verwachten.

Als de uitgenodigde perso(o)n(en) niet verschijnt op de afspraak voor inzage en binnen de gestelde termijn (standaard: vier weken) geen contact opneemt voor een afspraak, wordt ervan uitgegaan dat verzoeker geen verder belang meer heeft bij het door hem/haar ingediende verzoek om inzage. Hiermee wordt het ingediende verzoek als afgehandeld beschouwd.

Samenloop van toesturen overzicht en feitelijk inzage. Bij het toesturen van het overzicht als bijlage van het besluit, wordt tegelijk de mogelijkheid aangeboden om een nadere afspraak te maken voor het inzien van de verwerkingen. Als de betrokkene of diens advocaat of wettelijk vertegenwoordiger daarvan gebruik maakt wordt geen tweede, afzonderlijk besluit genomen. Mocht er onduidelijkheid ontstaan bij het inzien (bijvoorbeeld over gebruik van uitzonderingsgronden) kan er een (nieuw) besluit worden genomen. Jurisprudentie geeft aan dat hier dan geen sprake is van deelbesluiten, maar twee afzonderlijke besluiten.

2.8 Afsluiten en archiveren

Als het verzoek om inzage geheel is afgehandeld wordt het fysieke en/of digitale dossier afgesloten en op termijn gearchiveerd. Het verdient aanbeveling om goed vast te leggen waar het concrete verzoek uit bestond en hoe dit is uitgevoerd. Zo kan later een (her)nieuw(d) verzoek of bij een vervolgprocedure (bemiddeling – bezwaar –beroep) juist worden beoordeeld. En daarmee wordt aangesloten op een eerder genomen besluit en kan dus nu een nieuw (deugdelijk) besluit worden genomen.

Tip: belangrijk is het vastleggen welke tijdsperiode en welke politiegegevens het verzoek tot inzage betreft. Dit kan de uitvoering van een nieuw of herhaald verzoek ondersteunen en is cruciaal voor het nemen van een zorgvuldig besluit.

Het dossier met de betreffende politiegegevens die bij het verzoek om inzage zijn betrokken blijft in ieder geval zes maanden bewaard op de afdeling en/of digitaal bewerkbaar vanaf de datum van afsluiten van het verzoek. Het gaat om zowel de on-geanonimiseerde als geanonimiseerde gegevens en het liefst met gelijke paginanummering. Dit is een redelijke termijn om af te wachten of er een beroep is ingesteld bij de rechtbank of advies voor bemiddeling is gevraagd bij de Autoriteit Persoonsgegevens en je nog beschikt over de van belang zijnde gegevens.

Hierna wordt het dossier bestaande uit alle correspondentie, besluiten, overzichten van – en de betreffende - politiegegevens onder een kenmerk gearchiveerd. Ook de machtiging hoort daarbij en blijft in het dossier.

Tip: het inscannen van dossierstukken (vooral grote dossiers) ten behoeve van archivering kan ook intern worden uitbesteed (bijv. drukkerij).

Het dossier wordt maximaal vijf (5) jaar bewaard vanaf de beëindigingsdatum van de afhandeling van het verzoek. De Archiefwet vereist dat overheidsorganen een selectielijst opstellen waarin ze beschrijven welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven. Bij de bepaling van de vernietigingstermijn in de selectielijst is rekening gehouden met de Wpg. De termijn van vijf jaar is opgenomen in de selectie van de uitvoeringslijst Nationale Politie onder code 3.01.07.

Tip: voor een goede informatiepositie binnen de operatie is het van toegevoegde waarde dat de inzage is vastgelegd in BVH met de maatschappelijke klasse i90.

2.9 Specifiek: verzoek nabestaande(n)

Voor het beoordelen van een verzoek om inzage door nabestaanden van een overleden betrokkene is geen grondslag in de Wpg. Iedereen heeft alleen recht op inzage van 'de hem betreffende' politiegegevens en de Raad van State heeft zich hierover in een casus gebogen en uitgesproken dat het inzagerecht niet overgaat naar wettige erfgenamen[32].

In wetgeving (zowel Wpg als AVG) wordt gesproken over natuurlijke personen en daar is na overlijden geen sprake meer van. Wel blijft op de politiegegevens van een overleden persoon het ambtsgeheim gelden en in het verlengde daarvan dat zorgvuldig met gegevens moet worden omgegaan. De verwerkingsverantwoordelijke blijft eigenaar van die politiegegevens en het recht van inzage gaat niet over op de nabestaanden. Dit betekent dat:

a. het informeren van nabestaanden, uitsluitend met als doel rouwverwerking, alleen plaats kan vinden als vorm van hulpverlening. Dit valt onder de uitvoering van de politietaak (artikel 3 Politiewet) en mag in dat kader noodzakelijk worden genoemd (artikel 7 Wpg). Er wordt dan ook zoveel mogelijk tegemoet gekomen aan de informatiebehoefte van de nabestaanden, maar houdt ook rekening met de 'veronderstelde wil' van de overledene. Denk hierbij bijvoorbeeld aan een zogenaamd 'dubbel' leven.

   Verder is er een Landelijke richtlijn voor familieagenten, die vanaf het moment kort na een incident bij de slachtoffers/nabestaanden betrokken zijn om hen te informeren en behoeften bij hen te inventariseren. Zij kunnen ook wijzen op de mogelijkheid van rouwinzage of als de slachtoffers/nabestaanden daar zelf al om vragen, dit begeleiden. Indien er familieagenten bij een verwerking betrokken zijn volgt altijd afstemming en voeren zij in beginsel de feitelijke inzage uit.

   Tip: wees zeer terughoudend met kennisnemen en eventueel verstrekken van kopieën van documenten of foto's. Je weet nooit zeker of die gebruikt worden in civiele zaken tegen hulpverleners, in verzekerings- of erfeniskwesties, etc. Zorg ook dat gegevens van derde(n) zijn geanonimiseerd en vraag nabestaanden vooraf welke vragen of wensen er zijn. Betrek de betrokken politiemedewerkers (bijv. van FO) of familieagenten hierbij.

b. als nabestaanden twijfels hebben over de doodsoorzaak en/of het uitgevoerde politieonderzoek en mogelijk een artikel 12 Sv procedure bij het gerechtshof overwegen, altijd afstemmen met het OM. De OvJ heeft immers het opsporingsonderzoek afgesloten en beslist dat er geen sprake is van een misdrijf en het lichaam ter beschikking van de nabestaanden gesteld. Er is dus altijd een verwerking bij het OM met als grondslag de Wjsg en na afstemming met het OM[33] kan het verzoek doorgezonden worden aan hen. Een dergelijk verzoek om inzage wordt schriftelijk overgedragen aan het OM en de verzoeker wordt hiervan schriftelijk in kennis gesteld.

   Tip: als het OM aangeeft geen stukken (meer) te hebben, verstrek het OM dan alsnog een kopie van het dossier, zodat het verzoek door hen kan worden beoordeeld en/of afgehandeld.

Een dergelijk verzoek van nabestaanden wordt binnen het proces Rechten van betrokkene in behandeling genomen onder 'Overige verzoeken'. In het geval van een verzoek om inzage door

[32] Uitspraak Raad van State ECLI:NL:RVS:2017:3223 en uitspraak Rechtbank Den Haag onder SGR 18/806 op 16 oktober 2018.
[33] Zie 'Aanwijzing Wpg' en doorzend plicht in kader van artikel 2:3 Awb

nabestaanden wordt op grond van de Awb een redelijke termijn van acht (8) weken gehanteerd om te reageren. In tegenstelling tot normale inzageverzoeken is hierbij het uitgangspunt dat de eenheid waar betrokken is overleden leidend is bij de afhandeling van een dergelijk verzoek en dus niet de woonplaats van verzoeker. In overleg kan om moverende redenen hiervan worden afgeweken.

2.10 Specifiek: verzoek loggingsgegeven(s)

Voor alle handelingen met betrekking tot de verwerking van politiegegevens geldt bij inwerkingtreden van artikel 32a Wpg een loggingsverplichting. Dit maakt onderdeel uit van de informatiebeveiliging en worden logbestanden bijgehouden met persoonsgegevens. Daarmee worden ook persoonsgegevens verwerkt die ook binnen een verzoek om kennisneming vallen. In de praktijk blijkt dat betrokkene incidenteel inzage vragen bij de politie, nadat ze van de gemeente informatie hebben gekregen over de bevraging binnen -en dus verstrekking vanuit- het BRP van hun persoonsgegevens.

Ook de Raad van State heeft in een specifieke casus het inzagerecht ruim uitgelegd[34]. Daarbij oordeelt de Raad dat het inzagerecht zich volgens hen niet alleen uitstrekt tot een overzicht van de persoonsgegevens die worden verwerkt, maar ook tot de personen die daar toegang toe hebben gehad. In onderhavige casus ging het om externe partners, die toegang hadden tot die gegevens bij de verwerkingsverantwoordelijke. Het gaat hier dus feitelijk om het ter beschikking stellen of verstrekken van persoonsgegevens van de betrokkene.

Als uitgangspunt geldt om loggingsbestanden buiten de behandeling van een verzoek om inzage te laten. Op basis van die jurisprudentie is het uitgangspunt dat log-bestanden niet binnen de reikwijdte van een verzoek om inzage vallen[35]. Echter, als er specifiek naar wordt gevraagd dan is het zaak te achterhalen wat er aan de hand is en bijvoorbeeld het hoge aantal bevragingen vanuit de politie naar het BRP te verklaren. In het bijzonder de automatische verstrekking van politiegegevens voor het up-to-date houden van de Personenserver levert namelijk een groot aantal hits op.

Tip: neem bij een verzoek waarin specifiek gevraagd wordt om loggegevens contact op met de privacyfunctionaris of jurist.

2.11 Specifiek: verzoek foto- en camerabeelden

AVR. Voor het kennisnemen van auditieve of audiovisuele registraties van verhoren van aangevers, getuigen en verdachten is een aanwijzing door het college van Procureurs-Generaal afgegeven en altijd afstemming met de zaaks-OvJ vereist[36]. Het doel daarvan is het scheppen van waarborgen om het verspreiden, vernietigen, het wijzigen, het kopiëren en ander oneigenlijk gebruik van de tijdens de verhoren geregistreerde beelden of geluid te voorkomen.

MONO-cam. Het opvragen van een foto die is gemaakt door een camera van een overtreding (zogenaamde MONO-cam) kan ook door de Privacydesk worden afgehandeld, in afwachting van de ontwikkeling van een koppeling naar het landelijk CJIB-portaal, waar de tenaamgestelde van een voertuig zelf toegang krijgt tot fotobestanden. Deze werkwijze is afgesproken met het Team

[34] Zie ECLI:NL:RVS:2011:BU6383

1 [35] Zie ECLI:NL:RBDHA:2021:3697, R.O. 3.2

[36] Aanwijzing auditief en audiovisueel registreren van het College van Procureurs-Generaal, d.d. 1 november 2018, registratienummer 2018A008, onderdeel 5

Buitengerechtelijke Afhandelingen (TBA) om de aanvrager niet de dupe te laten zijn van een nog niet werkend burgerportaal en onnodige belasting met bezwaarprocedures te voorkomen.



Om voor een foto een inzageverzoek aan het bureau te organiseren kost te veel voor beide kanten, waarbij is afgesproken dat na zorgvuldige verificatie de foto wordt opgestuurd, eventueel via de mail. Het verzoek kan enkel en alleen worden gedaan door de tenaamgestelde van het voertuig en de communicatie verloopt in eerste instantie via het Regionaal Service Center (RSC), de balie van ene bureau of van een contactformulier. De aanvrager moet kunnen aantonen dat hij ook die persoon is die als tenaamgestelde staat geregistreerd. Is dit geverifieerd en voldoende aangetoond, kan de foto worden verzonden.

Camerabeelden. Ook camerabeelden ex artikel 151c Gemeentewet vallen onder een inzageverzoek ex artikel 25 Wpg. Immers de verwerkte camerabeelden voor de handhaving van de openbare zijn gelijkgesteld aan politiegegevens en de burgemeester bedient zich van de politie voor die handhaving en ook het verwerken van die gegevens daarvoor[37]. In het algemeen wordt contact gezocht met het Team Technisch Toezicht (TTT) van een eenheid, als het aanspreekpunt voor deze vorm cameratoezicht.

De verwerking van deze politiegegevens is een verwerking als bedoeld in artikel 8 van de Wpg, maar in afwijking van het bepaalde in dat artikel worden de vastgelegde beelden na ten hoogste vier weken (= 28 dagen) vernietigd. Alleen indien er concrete aanleiding bestaat te vermoeden dat die gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit, kunnen die camerabeelden ten behoeve van de opsporing van dat strafbare feit verder worden verwerkt, waarmee de termijnen van artikel 8 en/of 9 Wpg gelden.

Let op: de termijn van maximaal 4 weken (=28 dagen) is soms korter en daarmee niet voor elke gemeente hetzelfde. Vanwege uitkijk- en/of opslagcapaciteit is die termijn soms teruggebracht tot bijvoorbeeld 14 dagen. Na de verwerkingstermijn geldt dat de camerabeelden direct worden vernietigd[38] en dus niet eerst worden verwijderd en bewaard.

[37] Zie artikel 151c lid 4 en 9 Gemeentewet
[38] Zie artikel 151c lid 9 Gemeentewet

2.12 Specifiek: internationale signaleringen

Buitenlandse informatie. Tegenwoordig wordt er veel internationale informatie verwerkt. Zowel bij strafrechtzaken als in de grensstreken worden internationaal gegevens uitgewisseld. Indien bij de afhandeling van het inzageverzoek duidelijk is dat er buitenlandse informatie is verwerkt, dan mag de informatie die afkomstig is van het buitenland nooit ter inzage worden gelegd **zonder toestemming** van het buitenland! De Bevoegd Functionaris van het strafrechtelijk onderzoek kan daarin duidelijkheid verschaffen en in andere gevallen kan het (L)IRC daarin een rol spelen.

(Inter)Nationale signaleringen. Bij de afhandeling van een inzageverzoek dient ook de politiegegevens te worden gecontroleerd welke de politie verwerkt in het kader van (inter)nationale signaleringen. Een nationale signalering is bijvoorbeeld de aandachtsvestiging in het systeem OPP en Executie & Signaleringen (E&S). Voorbeelden van internationale signaleringen zijn die van een signalering in het Schengen Informatiesysteem (SIS-signalering) en de zogenaamde Interpol- signalering afkomstig uit Nederland zelf. Interpol-signaleringen die door het buitenland zijn opgelegd dient een betrokkene bij Interpol zelf op te vragen en komen dus niet in aanmerking voor Rechten van Betrokkene, tenzij die signalering van een buitenlandse Interpol in het nationaal systeem (E&S) is opgenomen en onder de Wpg valt. Wel moet toestemming worden gevraagd aan LIRC/LP of de signalering kenbaar mag worden gemaakt.

Signaleringen zijn op te vragen via BVI-IB. Bij een daadwerkelijke signalering moet altijd Bureau Sirene benaderd worden (email: 5.1.2.i @politie.nl), of de signalering kenbaar gemaakt mag worden. Bureau Sirene zal vervolgens contact leggen met de signalerende autoriteit om te vragen of de signalering kenbaar gemaakt mag worden of niet. Dit geldt alleen voor de SIS signaleringen. Voor het overige contact leggen met het (L)IRC. Indien de signalering niet bekend mag worden dan zal ook een van de afwijzingsgronden van toepassing zijn (artikel 27 Wpg).

Internationale signaleringen met een CTER-indicatie. De afgelopen jaren is duidelijk geworden dat er veel mensen zijn die hinder ondervinden bij het reizen naar het buitenland. Deze mensen worden bij de grens van andere landen staande gehouden en vaak de toegang tot het land geweigerd. Gebleken is dat dit veelal mensen betreffen die gesignaleerd hebben gestaan in relatie tot mogelijke uitreizen naar Syrië ten tijde van IS of dat mensen gesignaleerd hebben gestaan in relatie tot CTER. Diverse belangenorganisaties hebben hier nationaal de aandacht van de politiek en de media gevraagd. De LO/LX levert in deze situaties een extra inspanning om te achterhalen wat er speelt en als het nodig en mogelijk is een oplossing.

Bij een dergelijk inzageverzoek moeten dan ook de volgende stappen worden doorlopen:

1. meldt een dergelijk verzoek altijd bij de Privacydesk van de LX, zodat zij overzicht houden op de omvang van het aantal en soort vragen;
2. handel het betreffende verzoek in de eigen eenheid af en houdt rekening met de volgende punten:
   - vraag via de Privacydesk van de LO/LX of er SIS- of Interpol signaleringen zijn;
   - stem af met jullie eigen CTER-cluster;
   - weet dat er in deze gevallen een LOP- J-lijst en een afstemmingslijst bestaat;
   - de LOP- J lijst bevat alleen subjecten met betrekking tot het uitreizen naar het toenmalige strijdgebied en werd tot 2018 gebruikt;
   - de afstemmingslijst omvat alle subjecten waarvan een signaal is binnengekomen welke door de intelcel als CTER-waardig is bestempeld (eventueel op basis van eerdere signalen) en waarvan vervolgens door de intelcel besloten is deze perso(n)on(en) actief of passief te monitoren gezien hun zorgelijke activiteiten of uitingen;
   - in de media is al bekend geworden dat deze LOP- J-lijst met de VS en Turkije is gedeeld, dus houdt daar in de besluitvorming rekening mee;
3. stem het besluit met de Privacydesk van de Landelijke eenheden LO/LX af, zodat een check kan worden uitgevoerd op consistentie in de besluitvorming;

4. het is mogelijk dat door een belangenorganisatie er centraal bij de LO/LX diverse inzageverzoeken zal worden ingediend, waarbij de LO/LX de mogelijke Schengen (SIS) en Interpol signaleringen zal opvragen en vervolgens de inzageverzoeken zal doorzenden voor afhandeling naar de eenheid waar betrokkene woont.

3 Wijzigen van politiegegevens (Wpg)

3.1 Algemeen

Artikel 28 Wpg geeft de betrokkene of diens wettelijk vertegenwoordiger de mogelijkheid om een verzoek tot wijziging (rectificatie of vernietiging) van politiegegevens te doen. Rectificatie indien de verwerkte politiegegevens onjuist, of onvolledig zijn; vernietiging indien de verwerkte gegevens in strijd met een wettelijk voorschrift worden verwerkt, of niet voldoen aan een wettelijke verplichting. En afschermen in plaats van vernietiging indien de juistheid van de gegevens wordt betwist en niet kan worden geverifieerd, of gegevens moeten worden bewaard als bewijsmateriaal.

In de praktijk blijkt dat betrokkenen een verzoek tot wijziging ook doen om verwerkingen over hen, die door anderen zijn gemeld of waarover is verklaard, en waar zij het niet mee eens zijn, te laten wijzigen. Een dergelijk verzoek kan vaak worden afgewezen, omdat de informatie op zichzelf feitelijk niet onjuist hoeft te zijn: de verklaring is weergegeven zoals de getuige deze heeft gemeld en betrokkene was daar doorgaans niet bij aanwezig.

Tip: de Raad van State heeft uitgesproken dat artikel 28 Wpg alleen toeziet op de feiten en niet toeziet op meningen en opvattingen van anderen waarin men (de betrokkene) zich niet kan vinden[39]. Uiteraard moet de verwerking wel passen binnen onze taakstelling en daarvoor noodzakelijk zijn.

Ook geldt voor de verwerking het zogenaamde ABC principe. De verwerkte gegevens moeten Actueel, Betrouwbaar en Correct zijn. Bij een verzoek tot wijziging of vernietiging van politiegegevens zal dit uitgangsprincipe meegenomen moeten worden in de beslissing op een dergelijk verzoek.

Tip: wordt bij een inzage duidelijk dat politiegegevens niet voldoen aan het ABC principe, dan moten deze ambtshalve al gecorrigeerd worden (artikel 4 Wpg).

3.2 Indienen verzoek

In de wet staat: *'De betrokkene heeft het recht op diens schriftelijk verzoek ….'* (artikel 28 Wpg). Dit impliceert dat het verzoek tot wijziging schriftelijk moet worden ingediend. Er is een modelbrief beschikbaar die hiervoor kan worden gebruikt. De brief vraagt tevens om specifieke informatie, waarmee aan bepaalde formaliteiten wordt voldaan. Het gebruik hiervan door de verzoeker is géén wettelijke verplichting, maar stroomlijnt en bespoedigt het proces van afhandelen.

Tip: let ook op de dienstbaarheid naar de verzoeker toe. Een handgeschreven briefje is ook een formeel verzoek. Op politie.nl is het nieuwe privacy statement gepubliceerd, waar bij Rechten van betrokkenen opgenomen is dat voor een dergelijk verzoek een kopie van een identiteitsbewijs meegestuurd moet worden. Daarbij is ook aangeven om de foto en BSN – in lijn met AVG en Wpg – af te schermen.

3.3 Registreren verzoek

Een dergelijk verzoek wordt geregistreerd en krijgt een uniek dossierkenmerk, zodat dit bij correspondentie steeds kan worden aangehaald. De wettelijke termijn voor afhandeling start met de datum van ontvangst van het betreffende verzoek. In beginsel is dat de dag nadat het door verzoeker is verzonden.

[39] Zie uitspraak RvS op 5 oktober 2010 (ECLI:NL:RvS:201012713/1/H3)

Het ontvangen verzoek met bescheiden wordt ingeboekt door DIV, waarna het verdere proces van afhandeling en termijnbewaking wordt bijgehouden in het (post)verwerkingssysteem. In het (post)verwerkingssysteem wordt over het verzoek vastgelegd:

- ✓ de datum ontvangst bij de politie
- ✓ de naam, adres en woonplaats van de verzoeker en de betrokkene (indien dit verschillende personen betreffen)
- ✓ alle correspondentie over het verzoek

Vervolgens wordt vanuit de behandelaar een ontvangstbevestiging verstuurd op het binnengekomen verzoek, waarin de termijn voor uitsluitsel, mogelijkheid van een klacht bij de AP, het kosteloos afhandelen en verwijzing naar het privacy statement van de politie zijn opgenomen.

3.4 Beoordelen formaliteiten

Het is niet (meer) noodzakelijk dat verzoeker voorafgaand aan een verzoek tot wijziging eerst een verzoek tot inzage heeft gedaan. In de praktijk blijkt dat soms direct een verzoek tot wijziging gedaan als een onjuiste verwerking door verzoeker wordt vermoed. Voorbeelden hiervan zijn: na een politiecontrole, waarbij iets wordt gezegd over antecedenten of een onjuist opgemaakte aangifte.

Identiteit vaststellen. Ook bij behandeling van een verzoek tot wijziging moet de politie zorgen voor deugdelijke vaststelling van de identiteit van de betrokkene en eventueel de verzoeker als dat iemand anders is (artikel 26 Wpg). Dit is een wettelijk voorschrift. Daarom wordt standaard gevraagd bij een schriftelijk verzoek tot wijziging om een kopie van een formeel geldig identiteitsbewijs bij te voegen van betrokkene en (indien van toepassing) diens wettelijk vertegenwoordiger, waar het BSN en foto onleesbaar van zijn gemaakt.

Als een advocaat als gemachtigde optreedt, zal een machtiging van de betrokkene overlegd moeten worden. Het deugdelijk vaststellen van de identiteit van de advocaat zelf kan ook op andere wijze plaatsvinden (zie 1.3). Ontbreekt een kopie van een identiteitsbewijs en/of machtiging, dan wordt de verzoeker in de gelegenheid gesteld, onder gelijktijdige opschorting, om dat verzuim herstellen.

Verzoeker Een verzoek tot wijziging van politiegegevens kan niet worden ingediend door iemand anders, of door een minderjarige onder de 16 jaar, of door iemand die onder curatele is gesteld. Een dergelijk verzoek kan formeel/juridisch worden geweigerd, maar vanuit dienstbaarheid en behoorlijkheid wordt de mogelijkheid tot verzuimherstel geboden. Indien het verzuim niet wordt hersteld is het verzoek daarmee niet-ontvankelijk en wordt alsdan afgewezen, waarmee je niet toekomt aan de inhoudelijke behandeling.

Het gaat voor de betrokkene ‘om de hem betreffende politiegegevens’ en niet die van een ander (artikel 28 Wpg), tenzij de verzoeker als advocaat is gemachtigd, of als wettelijk vertegenwoordiger optreedt. Een verzoek tot wijziging kan dus niet worden ingediend over iemand anders. Verzoekt iemand om wijziging van politiegegevens over een ander, dan wordt de verzoeker in de gelegenheid gesteld, onder gelijktijdige opschorting, om dat verzuim te herstellen.

Het verzoek voor een minderjarige, die de leeftijd van 16 jaar nog niet heeft bereikt, moet worden gedaan door diens wettelijk vertegenwoordiger (artikel 26 Wpg). Als hier niet aan wordt voldaan, wordt verzoeker alsnog de mogelijkheid geboden, onder gelijktijdige opschorting, om dit te herstellen. Wordt hier wel aan voldaan dat wordt de wettelijk vertegenwoordiger tijdens de procedure verder geïnformeerd en niet de betrokkene. Een eventuele machtiging wordt in het dossier opgenomen.

Tip: wees voorzichtig bij minderjarigen tot 16 jaar en check of de verzoeker ook daadwerkelijk als wettelijk vertegenwoordiger kan optreden. Er kunnen belangen spelen zoals scheiding, voogdijschap,

zedenverhaal, ouderlijk gezag, etc. Een verzoek kan worden ingediend door één van de vertegenwoordigers en hoeft niet ondertekend te zijn door alle vertegenwoordiger(s).

Ook ten aanzien van een onder curatele gesteld persoon, kan het verzoek tot wijziging alleen worden gedaan door diens wettelijk vertegenwoordiger (artikel 26 Wpg). Dit is een wettelijk voorschrift. Als hier niet aan wordt voldaan, wordt betrokkene alsnog de mogelijkheid geboden, onder gelijktijdige opschorting, om dit te herstellen. Wordt hier wel aan voldaan dat wordt de wettelijk vertegenwoordiger tijdens de procedure verder geïnformeerd en niet de betrokkene. Een eventuele machtiging wordt in het dossier opgenomen.

Tip: check bij een vermoeden of de betrokkene onder curatele is gesteld in het landelijk register, dat is te vinden onder: https://curateleenbewindregister.rechtspraak.nl. Leg dit in het dossier vast.

Zodra alle (gevraagde) benodigde bescheiden zijn aangeleverd wordt het verzoek verder in behandeling genomen en gaat de afhandelingstermijn weer (verder) lopen. Voldoet de verzoeker niet of onvoldoende aan het herstellen van het verzuim, dan wordt de behandeling beëindigd en in een besluit ex artikel 4:5 Awb opgenomen. Het voornemen van een dergelijk besluit is al opgenomen in de opschortingsbrief en tegen dit besluit staat bezwaar open. Hierdoor kom je niet meer toe aan een inhoudelijk besluit zoals onder stap 5 is genoemd. Dit besluit moet binnen vier (4) weken na ontvangst van onvoldoende (aanvullende) informatie, of het verstrijken van de gestelde termijn, worden verstuurd.

Verzoekschrift. Een verzoek om wijziging van politiegegevens kan alleen als zodanig worden afgehandeld als duidelijk is dat dit ook de bedoeling van het verzoekschrift is. Het interpreteren van een verzoekschrift is niet aan de behandelaar van de politie voorbehouden. De verwerkingsverantwoordelijke mag een redelijke vergoeding vragen of weigeren aan een verzoek gevolg te geven wanneer dat kennelijk ongegrond of buitensporig is, zoals wanneer de betrokkene zonder goede reden herhaaldelijk verzoekt tot wijziging, of wanneer de betrokkene zijn recht tot wijziging misbruikt, bijvoorbeeld door bij het verzoek valse of misleidende informatie te verstrekken[40]. Ook een (te) algemeen en (te) uitgebreid verzoek tot wijziging kan worden afgewezen. Het verzoek moet immers ook de aan te brengen wijzigingen bevatten. Bij een kennelijk ongegrond, of buitensporig verzoek, in het bijzonder vanwege de geringe tussenpozen[41] tussen opeenvolgende verzoeken, kan het verzoek worden geweigerd (zie 4.5). In beginsel wordt voor een herhalingsverzoek een termijn van 6 maanden gehanteerd.

Tip: vraag bij een algemeen verzoek tot wijziging aan de verzoeker om zijn verzoek te specificeren en concreet aan te geven wat hij gewijzigd wil hebben. Hiermee wordt een onevenredige inspanning van beide kanten voorkomen. Leg dit wel vast in het dossier.

Beslistermijn. Het verzoek tot rectificatie, vernietiging en/of aanvulling moet binnen vier (4) weken afgehandeld worden. Deze termijn start vanaf het moment dat het verzoek is ontvangen. Indien blijkt dat niet aan alle vereisten wordt voldaan (=verzuim), dan wordt de behandeling opgeschort. De termijn van afhandeling gaat weer lopen als het verzuim is hersteld (zie 3.5).

Anders dan bij een verzoek om inzage kan deze beslistermijn niet worden verlengd op basis van een verdaging. In artikel 4:14 Awb is de verplichting opgenomen om de verzoeker schriftelijk te informeren als de gestelde termijn niet wordt gehaald met de mededeling op welke - zo kort mogelijke - termijn alsnog aan het verzoek wordt voldaan.

[40] Overweging 40 van de Europese Richtlijn 2016/680
[41] Overweging 43 van de Europese Richtlijn 2016/680 zegt dat een natuurlijke persoon het recht op inzage van de gegevens die over hem zijn verzameld met redelijke tussenpozen moet kunnen uitoefenen, zodat hij kennis kan nemen van de verwerking en de rechtmatigheid daarvan kan nagaan.

Doorsturen verzoek. Het verzoek tot wijziging wordt in principe in behandeling genomen door de eenheid waar dat is ingediend, tenzij blijkt dat de betrokkene in een andere eenheid woonachtig is of de te wijzigen gegevens bij een andere eenheid zijn verwerkt. Dan wordt contact opgenomen met die andere eenheid en afgestemd door wie en/of op welke wijze het verzoek verder wordt afgehandeld. Van een eventuele interne doorverwijzing wordt de verzoeker schriftelijk in kennis gesteld.

Tip: vraag bij andere eenheden na of (eerder) een identiek verzoek is ingediend. En laat een verzoek tot wijziging in beginsel afhandelen door de eenheid waar de verwerking plaatsvindt, omdat dit soms om lokale informatie of nadere toelichting van de rapporteur(s) vraagt.

3.5 Verzamelen persoonsgegevens

Verzamelen gegevens. Op basis van het ingediende verzoek, waarin de aan te brengen wijziging(en) is/zijn opgenomen, worden de relevante politiegegevens opgevraagd door de behandelaar bij de afdeling DRIO/DLIO. De aard van het verzoek is leidend voor de vraag hoe uitgebreid de zoektocht naar gegevens moet zijn.

Toestemming Bevoegd Functionaris. Voor zover blijkt van artikel 9 en 10 Wpg verwerkingen vraagt de behandelaar toestemming van de Bevoegd Functionaris om de gevraagde wijziging van die verwerking door te voeren. Er is een standaardbrief met uitleg, waarmee de gegevens bij een Bevoegd Functionaris kunnen worden opgevraagd. De Bevoegd Functionaris kan dit weigeren, maar dit moet dan vallen onder een van de redenen genoemd in artikel 27 Wpg (zie 3.7) en (mogelijk) worden afgewogen tegen het belang van verzoeker.

Tip: vraag als behandelaar wel om een nadere uitleg aan de Bevoegd Functionaris, want een (gedeeltelijke) weigering moet je - met redenen omkleed - kunnen motiveren en kan leiden tot een beroepsprocedure bij de rechtbank.

3.6 Beoordelen besluit

Een wijziging van politiegegevens kan alleen toegewezen en feitelijk uitgevoerd worden als de genoemde gegevens over betrokkene ook daadwerkelijk worden verwerkt. De eerste toets is dus artikel 28 Wpg zelf en als dat wordt toegewezen, dan is de tweede toets of er een beperking ex artikel 27 Wpg moet worden meegegeven.

Toewijzen verzoek. In het geval dat wel politiegegevens worden verwerkt moet voor het verzoek tot wijziging in algemene zin worden getoetst of de gegevens nog Actueel, Betrouwbaar en Correct zijn. Daarnaast moeten vragen worden beantwoord voor:

- het wijzigen van politiegegevens:
  - is de informatie (on)juist en moet dat gerectificeerd worden?
  - is de informatie voor het doel van de verwerking (on)volledig en moet dat aangevuld worden?
- het vernietigen van politiegegevens[42]:
  - worden de gegevens in strijd met wettelijk voorschrift verwerkt?
  - wordt niet voldaan aan een wettelijke verplichting?
- het afschermen van politiegegevens:
  - wordt de juistheid van gegevens betwist en kan die niet worden geverifieerd?
  - moeten de gegevens worden bewaard als bewijsmateriaal?

[42] Uitspraak ECLI:NL:RBOVE:2025:4126 geeft aan dat de korpschef geen beslissingsruimte heeft en politiegegevens niet op grond van een belangenafweging kunnen of moeten worden vernietigd.

Hierdoor wordt duidelijk of de verwerkte informatie juist is, noodzakelijk is voor de politietaak[43], past binnen doel van de verwerking, juist en volledig is en/of er (nog) een verwerkingsgrondslag is.

Tip: laat het aanvullen of rectificeren van politiegegevens in beginsel door een verbalisant of rapporteur zelf uitvoeren, waardoor zij actief betrokken worden bij een genomen besluit en mogelijk het lerend vermogen wordt vergroot.

Artikel 14 van de Wpg bepaalt dat verwijderde artikel 8, 9 en 10 gegevens nog vijf jaar moeten worden bewaard en daarna pas worden vernietigd. Deze bewaartermijn van verwijderde gegevens volgt rechtstreeks uit de wet[44]. De korpschef kan daarom naar aanleiding van een rectificatieverzoek wel eerder dan de genoemde verwerkingstermijn, tot verwijdering van politiegegevens overgaan, maar binnen de bewaartermijn niet eerder tot vernietiging.[45] Ook bij een sepotcode 01 (onterecht verdachte) of 09 (geen strafbaar feit) geldt dat de betreffende politiegegevens direct moeten worden aangepast (rol verdachte weg) en moeten worden verwijderd (geen doel en noodzaak meer), maar nog wel vijf jaar moeten worden bewaard voor onder andere klachtafhandeling of verantwoording van verrichtingen. Dit sluit volledig aan bij de genoemde sepotcodes waarbij iemand is aangehouden en vervolgens procedures tegen de politie voert.

Tip: als voorbeeld de verwerking van een aanrijding met eventuele getuige(n), die na één jaar volledig is afgehandeld door politie en de verzekeringsmaatschappij. Dit is een artikel 8 Wpg verwerking waaruit mogelijk na dat jaar geen noodzaak meer is, voor de verwerking van de persoonsgegevens van de getuige. De aanrijding op zichzelf kan nog een doel dienen voor het adviseren op verkeersveiligheid (hot spot) over een bepaalde periode. Kortom je zult de noodzakelijkheid binnen de politietaak moeten kunnen benoemen en anders - na een daartoe ingediend verzoek - de gegevens eerder moeten verwijderen (zie ook artikel 14 Wpg).

Verder is het beleid dat reeds verwijderde politiegegevens niet structureel of geautomatiseerd na vijf (5) jaar bewaren, vernietigd worden en daardoor nog steeds verwerkt worden. Dit komt voort uit het kunnen oplossen van zogenaamde ‘cold cases’ met oudere politiegegevens. Op individuele verzoeken moet na afweging van belangen wel een besluit worden genomen om te lang bewaarde politiegegevens (dus langer dan 5 jaar verwijderd) aslnog te vernietigen en dit ook feitelijk door Functioneel Beheer te laten uitvoeren[46].

Indien de gevraagde wijziging wordt toegekend wordt dit schriftelijk gemotiveerd kenbaar gemaakt aan de verzoeker en opgenomen in een besluit.

Afwijzen verzoek. Er kunnen ook redenen zijn om het verzoek tot wijziging geheel of gedeeltelijk af te wijzen (artikel 27 Wpg). Dit mag alleen wanneer dat een noodzakelijke en evenredige maatregel is voor een van de volgende situaties (= limitatieve opsomming):

a. vermijden van belemmeren van gerechtelijke onderzoeken of procedures
b. vermijden van nadelige gevolgen voor voorkoming, de opsporing, het onderzoek en vervolging van strafbare feiten of tenuitvoerlegging van straffen
c. beschermen van openbare veiligheid
d. beschermen van de rechten en vrijheden van derden
e. beschermen van de nationale veiligheid
f. kennelijk ongegrond of buitensporig verzoek (zie 3.4) en
g. gegevens betreffende verwerking op basis van artikel 12 (informantenbeheer)

Doet de situatie van a t/m f zich voor, dan wordt het verzoek tot wijziging afgewezen voor zover dit een noodzakelijke en evenredige maatregel is. Daarbij dient het belang van de betrokkene tot wijziging te

[43] Uitspraak ECLI:NL:RVS:2009:BJ8264 geeft aan dat niet per registratie een motivatie tot noodzakelijkheid voor de verwerking hoeft te worden gegeven, omdat dit zou leiden tot herhalingen die geen redelijk doel dienen.
[44] Uitspraak ECLI:NL: RvS:2017:583
[45] Uitspraak ECLI:NL:RVS:2017:583, r.o. 5.
[46] Zie brief GA d.d. 31 maart 2021

worden afgewogen tegen het belang van de politie om rectificatie te weigeren. Met de criteria van noodzakelijkheid en evenredigheid wordt dit tot uitdrukking gebracht. Er is dus, anders dan onder de ‘oude Wpg’, sprake van een belangenafweging. Van een geheel of gedeeltelijke afwijzing van de wijziging krijgt de betrokkene of verzoeker een (gemotiveerd) schriftelijk besluit, met vermelding van de feitelijke en juridische gronden.

De uitzondering hierop is de situatie onder g, waarbij geen belangenafweging plaatsvindt en het verzoek altijd wordt afgewezen. Stem dit altijd af met de TCI en de privacyfunctionaris in verband met de grote belangen die meespelen bij een dergelijke verwerking.

In artikel 32 Wpg (= documentatieplicht) is vastgelegd dat de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing zoals in artikel 27 Wpg genoemd, schriftelijk moeten worden vastgelegd en bewaard tot de laatste auditcontrole (= 4 jaar).

Tot slot. Als geen gegevens worden verwerkt, wordt daarvan schriftelijk mededeling gedaan aan de betrokkene of verzoeker en opgenomen in een besluit.

3.7 Uitvoeren verzoek

Indien het verzoek tot wijziging heeft geleid tot een besluit om politiegegevens te verbeteren, aan te vullen, te vernietigen of af te schermen moet dit zo spoedig mogelijk worden uitgevoerd.
Voor het verwijderen van gegevens uit BVH moet contact worden gelegd met Functioneel Beheer die een beleidsdocument hiervoor heeft ontwikkeld[47]. Hierbij hoort een formulier voor het verwijderen of vernietigen van politiegegevens uit BVH, waarbij als voorwaarde een akkoord door de privacyfunctionaris is opgenomen.

Daarnaast geldt de verplichting op grond van artikel 28 Wpg om:

1. bij rectificatie van onjuiste politiegegevens dit aan de bevoegde autoriteiten van wie die onjuiste gegevens afkomstig zijn (= bron) door te geven en
2. bij rectificatie, vernietiging of afscherming van politiegegevens dit aan de ontvangers van die gegevens door te geven

3.8 Afsluiten en archiveren

Als het verzoek tot wijziging geheel is afgehandeld wordt het dossier afgesloten en op termijn gearchiveerd. Het verdient aanbeveling om goed vast te leggen waar het concrete verzoek uit bestond en hoe dit is uitgevoerd. Zo kan later aansluitend een (her)nieuw(d) verzoek of bij een vervolgprocedure (bemiddeling – bezwaar - beroep) juist worden beoordeeld en een deugdelijk besluit worden genomen.

Het fysieke/ en/of digitale dossier met de betreffende politiegegevens die bij het verzoek tot wijziging zijn betrokkenen blijven in ieder geval zes maanden bewaard op en/of bewerkbaar door de afdeling vanaf de datum van afsluiten van het verzoek. Dit is een redelijke termijn om af te wachten of er een beroep is ingesteld bij de rechtbank of advies voor bemiddeling is gevraagd bij de Autoriteit Persoonsgegevens.

Hierna wordt het fysieke en/of digitale dossier bestaande uit alle correspondentie, besluiten, overzicht van - en de betreffende - politiegegevens onder een kenmerk gearchiveerd bij DIV. Vervolgens wordt dit dossier maximaal vijf jaar bewaard vanaf de beëindigingsdatum van de afhandeling van het onderzoek. De Archiefwet vereist dat overheidsorganen een selectielijst opstellen

[47] Verwijderen-, vernietigen-, en samenvoegen van gegevens in de BVH, versie 2.7 d.d. 9 maart 2023.

waarin ze beschrijven welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven. Bij de bepaling van de vernietigingstermijn in de selectielijst is rekening gehouden met de Wpg. De termijn van vijf jaar is opgenomen in de selectie van de uitvoeringslijst Nationale Politie onder code 3.0107.

3.9 Specifiek: verwijderen identiteitsgegevens

In aanvulling op het beoordelen en uitvoeren van een specifiek verzoek tot rectificatie van identiteitsgegevens, zoals biometrische gegevens en SKDB-nummer, volgt hier een nadere uitleg.

Het is allereerst van belang om vast te stellen dat er identiteitsgegevens worden opgemaakt en vastgelegd op grond van het Besluit Identiteitsvaststelling Verdachten en Veroordeelden (Bivv) met als doel de juiste persoon aan het juiste dossier. De politie stelt de identiteit van de aangehouden verdachte vast op de wijze, bedoeld in artikel 27a, Sv.
Wanneer iemand als verdachte voor de BIVD-zuil komt en de vingerafdrukken worden afgenomen, dan gaat er een set vingerafdrukken naar de biometrievoorziening van de Matchingsautoriteit en er wordt een set verstrekt aan de politie, die worden opgenomen in een applicatie (HAVANK). Ook een afgenomen (aangezicht)foto wordt verstrekt aan de politie en weergegeven in een applicatie (Catch).

Een persoon kan niet langer als verdachte worden aangemerkt indien er een onherroepelijke beslissing is in een zaak doordat:

- in een zaak is besloten tot een sepot;
- in een zaak een transactie is opgelegd;
- een zaak is geëindigd in een vrijspraak;
- een zaak is geëindigd in een niet-ontvankelijkheid inzake de vervolging,
- of er is een Halt traject afgerond.

Indien bovenstaande van toepassing is, wordt door de afdeling Persoonsinformatie bij de Matchingsautoriteit op basis van de Bivv besloten of de Identiteitsvaststelling moet worden verwijderd of behouden moet blijven.

De basis voor afdeling persoonsinformatie om biometrie te verwijderen is verankerd in de Bivv. (Besluit Identiteitsvaststelling verdachten en veroordeelden). De grondslag en verdere verwerking van die biometrische gegevens is gelegitimeerd in het Bivv en daarin zijn ook de gronden voor verwijdering en de uitzonderingen daarop opgenomen (artikel 5 Bivv).
De verwerkingsverantwoordelijke voor deze verwerking is de Minister van Justitie en Veiligheid en derhalve kan het verzoek na vaststelling dat het om dit soort gegevensverwerking gaat, worden doorgestuurd naar de Justitiële Informatiedienst (Just ID) afdeling Matchingsautoriteit. Concreet kan het verzoek worden doorgemaild naar het frontoffice via info@justid.nl. De Matchingsautoriteit is in eerste instantie verantwoordelijk voor de verdere afhandeling en eventueel beantwoorden van het verzoek. Aan verzoeker wordt schriftelijk geïnformeerd over de doorzending vanuit de politie. Vanuit de afdeling Persoonsinformatie vindt er alleen correspondentie plaats met de betrokkene, indien de betrokkene zelf een verzoek tot verwijderen heeft ingediend. De afdeling privacy neemt een beslissing op basis van dezelfde beoordelingscriteria uit de Bivv en er wordt een besluit genomen als bedoeld in artikel 22, tweede lid van de Wet justitiële en strafvorderlijke gegevens (Wjsg).

Voor de politie geldt dan nog wel dat wij moeten toetsen of gegevens nog juist en daarmee rechtmatig worden verwerkt. Bijvoorbeeld of de rol van ‘verdachte’ nog aan betrokkene in de hoofdgebeurtenis

gekoppeld kan blijven. Zo niet, dan moet dit worden aangepast (vervolgregistratie i24 in BVH) en een formeel besluit worden genomen en aan verzoeker worden verstuurd.

*Tip: als bij een verwijderverzoek van één betrokkene blijkt dat ook verwerkingen van andere betrokkenen onjuist blijken te zijn, dan **moeten** die ook worden aangepast en gerectificeerd. Er rust een wettelijke verantwoordelijkheid op de Korpschef dat de verwerkte politiegegevens juist en nauwkeurig zijn (artikel 4 Wpg). Hier hoeft dus niet eerst een separaat verzoek voor te worden gedaan en dus ook **géén** apart besluit op te worden genomen en verstuurd.*

Bijlage A: bevragingen inzage Wpg

	Systeem/applicatie/verwerking	J/N	Toelichting
1	Opsporingsregister (OPS)	Ja	Signalering van personen en goederen voor de politietaak ogv artikel 13 lid 1 Wpg
2	Schengen Informatie Systeem (ook SIS II)	Ja	idem
3	Gripbestanden	Ja	Gerichte verwerking van politiegegevens van gedetineerden ogv artikel 13 lid 2 Wpg
4	(N)CID registers, waaronder tip/toonregeling, informantenjournaals, o.t-rapportages, gespreksverslagen met de CID officier van justitie	Nee	Artikel 12 Wpg is uitgesloten (artikel 27 lid 3 Wpg)
6	CIE of TCI register	Ja	zit in jouw bevraging (art. 10 lid 1a Wpg)
8	BFO registers	Ja	zit in jouw bevraging en is Summ IT (art. 9 Wpg)
9	Journaals van onderzoeken	Ja	zit in jouw bevraging van Summ IT (art. 9 Wpg)
10	HKS systeem	Ja	zit in jouw bevraging (art. 13 Wpg)
11	MOT registers	Nee	verwerking door FIU (Wwft)
12	Registers Zwacri	Ja	is art 10 lid 1a verwerking (zie 6)
13	RID registers	Ja	is art 10 lid 1c verwerking
14	PIT registers	Nee	is uitgesloten (art 12 Wpg)
15	KLPD registers	Ja	vallen gewoon onder zoekslag NP
16	FIOD registers	Nee	Verwerking door FIOD (Wpg)
17	BVD registers	Nee	verwerking door AIVD (WIV)
18	AIVD registers	Nee	idem
19	MIVD registers	Nee	verwerking door MIVD (WIV)
20	CTC registers	Nee	Verwerking door OM
21	Registers Nationale recherche	Ja	opsporing zit in jouw bevraging
22	Registers rechter-commissaris	nee.	Verwerking door Rechtbank
23	Registers Landelijk Parket	Nee	Verwerking door OM
24	Registers Arrondissementsparket	Nee	Idem
25	Registers College Procureurs-Generaal	Nee	idem
26	Bedrijfsprocessensysteem	Ja	zit in jouw bevraging
27	AID registers	Nee	Verwerking door NVWA (AVG of Wpg)
28	Audio, video en fotobestanden	Ja	zit in jouw bevraging
	KA omgeving	Ja	Met name de O:schijf waarop opersationele informatie staat

BVI-IB		**Blueview**	
BEST-MTRGL		HKS	(KMAR – niet)

BLUESPOT		RBS	(KMAR – niet)
GBA	niet	FIU	Niet
NDS		BPS	(KMAR – niet)
OPP-EnS		BVH	
PSHV		LURIS	Niet
RDW	Niet	LSM	
SKDB	Niet	SUMMIT POLITIE	(KMAR, FIOD, NVWA - niet)
VERONA		NDS	
EUCARIS			
NL-SIS II			
SLTD			
SMV			

Zie voor een uitleg van de afkortingen o.a.:

5.1.2.i

PSHV en VERONA zijn vanaf 1-1-2019 geen politiebestanden meer, dus niet bevragen

|EUCARIS is van RDW, ook niet bevragen