

**AP**bescherming in een
digitale wereld

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

De Minister van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Datum

15 oktober 2026

Ons kenmerk

2026-032650

Uw brief van

27 augustus 2026

Contactpersoon**Uw kenmerk**

7757875

Onderwerp

Wetgevingstoets concept Regeling periodieke audit en toezicht op politiegegevens buitengewoon opsporingsambtenaren.

Geachte heer Van Weel,

Bij brief van 27 augustus 2026 is de Autoriteit Persoonsgegevens (AP) op grond van het bepaalde in artikel 35b, eerste lid, onder b, van de Wet politiegegevens (Wpg), geraadpleegd over het concept Regeling periodieke audit en toezicht op politiegegevens buitengewoon opsporingsambtenaren (hierna: het concept).

De AP heeft bezwaar omdat de bepaling met betrekking tot het uitvoeren door de functionaris gegevensbescherming (FG) van het risicogerichte toezicht - als onderdeel van de privacy audit - conflicteert met de taak van de FG uit de Wpg om toe te zien op de naleving van het bepaalde bij of krachtens de Wpg.

Strekking van het concept

De Wpg verplicht tot periodieke controle van de uitvoering van de Wpg door middel van privacy audits.¹ Deze privacy audits gelden als waarborg tegen ongerechtvaardigde inbreuken op de persoonlijke levenssfeer van personen van wie gegevens worden verwerkt. Hierbij wordt getoetst of de organisatie adequaat is ingericht om in voldoende mate tegemoet te komen aan de wettelijke bepalingen en daarmee een positieve bijdrage levert aan de naleving van de Wpg.

¹ Art. 33, eerste lid, Wpg. (vgl. Kamerstukken II, 2005/06, 30 327, nr. 3, p. 90).

Datum

15 oktober 2026

Ons kenmerk

2026-032650

De huidige ministeriële regeling periodieke audit politiegegevens sluit volgens het concept niet goed aan bij het werk van de werkgevers van buitengewoon opsporingsambtenaren (boa's). Deze werkgevers hebben weinig met verwerkingen van politiegegevens te maken. Dat leidt tot disproportionele lasten voor de boa-werkgevers. Daarom wordt voor hen in het concept een aparte regeling voorgesteld. Dit moet zorgen voor minder auditlasten (zowel financieel als qua frequentie) en tot meer gerichte audits.² Het concept maakt daarnaast onderscheid tussen normen die gecontroleerd moeten worden door een IT-auditor en normen die onder het toezicht van de FG vallen. De FG krijgt hierbij de taak om een deel van de privacy audit (het zogenoemde 'risicogerichte toezicht') uit te voeren³ en om daarvan verslag te doen in zijn jaarlijkse rapportage die hij moet opstellen op grond van de Wpg.⁴ Dit moet leiden tot meer rolzuiverheid en past volgens het concept beter bij de bestaande systematiek waarin de FG al de taak heeft om toezicht te houden op de naleving van de Wpg.⁵

Wetgevingstoets

Taak en onafhankelijke positie FG

De FG heeft (onder meer) als taak toe te zien op de naleving van het bepaalde bij of krachtens de Wpg, met inbegrip van de privacy audits.⁶ Hij zal dus ook moeten toezien of de verwerkingsverantwoordelijke voormelde auditverplichting uit de Wpg naleeft. Op grond van het concept wordt de verwerkingsverantwoordelijke verplicht om de FG een deel van de privacy audit te laten uitvoeren. Dat het blijkens de toelichting bij het concept niet bedoeld is als extra of aanvullende taak, maakt dat niet anders.⁷ Het concept noemt het deel van de privacy audit dat de FG zal gaan uitvoeren het 'risicogerichte toezicht'.⁸ Gedetailleerd wordt geregeld op welke specifieke bepalingen de FG dat risicogerichte toezicht ten minste moet uitvoeren. Het risicogerichte toezicht is daarmee ingebed in en onderdeel van de privacy audit(cyclus). Dat is bezwaarlijk, omdat de FG - zoals hiervoor opgemerkt - gehouden is toe te zien op de naleving van het bepaalde bij of krachtens de Wpg. Daarmee is de FG ook gehouden toe te zien of de verwerkingsverantwoordelijke diens plicht naleeft om privacy audits uit te voeren, inclusief de uitvoering van het risicogerichte toezicht. Door de FG te belasten met de uitvoering van een deel van de privacy audit, leidt dat tot een belangenconflict. Hij controleert dan immers zijn eigen werk en dat tast zijn onafhankelijke positie aan.⁹ De taak die nu in het concept wordt neergelegd bij de FG past naar zijn aard veel meer bij de rol en taak van een privacy functionaris.¹⁰ Deze kan de verwerkingsverantwoordelijke van advies dienen en namens hem toezien op de correcte verwerking van politiegegevens.

² Nota van Toelichting bij het concept, p. 2. Zie ook beleidscompas: [Overheid.nl | Consultatie Regeling periodieke audits en toezicht politiegegevens buitengewoon opsporingsambtenaren](#).

³ Art. 2, derde lid, van het concept.

⁴ Art. 2, vijfde lid, van het concept.

⁵ Nota van Toelichting bij het concept, p. 2.

⁶ Artikel 36, derde lid, aanhef en onder a, Wpg. Deze bepaling heeft een Unierechtelijke oorsprong en betreft de implementatie van art. 34, eerste lid, aanhef, onder b, Richtlijn (EU) 2016/680.

⁷ Artikelsgewijze toelichting van het concept bij art. 2, derde lid.

⁸ Art. 1, eerste lid, aanhef, onderdeel b, van het concept.

⁹ Zie voor de onafhankelijke positie van de FG's bij het uitvoeren van hun taken en verplichtingen overweging 63 van Richtlijn (EU) 2016/680 en Kamerstukken II, 2005/06, 30327, nr. 3, p. 5 en 92.

¹⁰ Art. 34 Wpg.



Datum
15 oktober 2026

Ons kenmerk
2026-032650

De AP concludeert dat het uitvoeren door de FG van het risicogerichte toezicht - als onderdeel van de privacy audit - conflicteert met de taak van de FG uit de Wpg om toe te zien op de naleving van het bepaalde bij of krachtens de Wpg. Deze taak tot het uitvoeren van het risicogerichte toezicht moet worden geschrapt evenals de daaraan gerelateerde taak daarvan verslag te doen.

Hiervoor is een fundamenteel punt gemaakt dat naar het oordeel van de AP noopt tot wijziging van het concept. Geheel los van dit fundamentele bezwaar lijkt het regelen van een taak van de FG in het concept ook om andere redenen bezwaarlijk. Daarvoor vraagt de AP uw aandacht. De AP heeft in de eerste plaats ernstige twijfels of de taak om een deel van de privacy audit uit te voeren door de FG¹¹ wel op het niveau van een ministeriële regeling kan worden geregeld. Delegatie aan de minister is beperkt tot voorschriften van administratieve aard, uitwerking van details van een regeling, voorschriften die dikwijls wijziging behoeven en voorschriften waarvan te voorzien is dat zij mogelijk met grote spoed moeten worden vastgesteld.¹² Het toebedelen van een nieuwe taak lijkt daar niet voor bedoeld. In de tweede plaats staat een dergelijke taaktoedeling ook op gespannen voet met het Besluit politiegegevens (Bpg) waarop het concept is gebaseerd. Het Bpg regelt expliciet dat een onafhankelijke auditor - die voldoet aan de bij ministeriële regeling te stellen eisen van werkwijze, deskundigheid en betrouwbaarheid - de privacy audit uitvoert.¹³ De toelichting bij de Wpg stelt dat dit een zogenoemde (externe) *Electronic Data Processing-auditor* moet zijn.¹⁴ De toelichting bij het Bpg sluit daarbij aan.¹⁵ Het is zeer twijfelachtig of de wetgever hiermee heeft beoogd dat dit ook een FG zou kunnen zijn. In het concept zelf wordt de FG overigens ook nadrukkelijk onderscheiden van de (IT-)auditor.¹⁶

Werklast AP

De AP merkt op dat het concept naar verwachting niet zal nopen tot extra inzet door de AP.

Openbaarmaking

Deze wetgevingstoets wordt binnen twee weken op de website van de AP gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens,

Monique Verdier
vicevoorzitter

¹¹ Art. 2, derde lid, van het concept.

¹² Aanwijzing 2.24 van de Aanwijzingen voor de regelgeving.

¹³ Art. 6:5, derde lid, Bpg.

¹⁴ Kamerstukken II, 2005/06, 30327, nr. 3, p. 90.

¹⁵ Staatsblad 2007 550, p. 109 en 110.

¹⁶ Art. 1, tweede en derde lid, van het concept.

Datum
15 oktober 2026

Ons kenmerk
2026-032650

-Bijlage

--*--

Toetsingskader AP

De AP beziet of het concept met betrekking tot de verwerking van persoonsgegevens strookt met het Handvest van de Grondrechten van de Europese Unie (EU), de AVG (Verordening 2016/679) of de Richtlijn politie en justitie (richtlijn 2016/680), de algemene rechtsbeginselen van de EU en het overige relevante recht, waarbij onder meer voldoende aannemelijk moet zijn gemaakt dat voldaan wordt aan het evenredigheidsbeginsel, doordat:

1. het concept geschikt is om de nagestreefde doelstelling van algemeen belang of de bescherming van de rechten en vrijheden van anderen te verwezenlijken (*geschiktheid*);
2. het doel niet redelijkerwijs even doeltreffend kan worden bereikt op een andere wijze, die de grondrechten van de betrokkenen minder aantast (*subsidiariteit*);
3. de inmenging niet onevenredig is aan dat doel, wat met name een afweging impliceert van het belang van het doel en de ernst van de inmenging (*proportionaliteit*);
4. het concept voldoende duidelijk en nauwkeurig is over de reikwijdte en in de toepassing voorspelbaar is (*rechtszekerheid*);
5. het concept voldoende aangeeft in welke omstandigheden en onder welke voorwaarden persoonsgegevens kunnen worden verwerkt, en aldus waarborgt dat de inmenging tot het strikt noodzakelijke wordt beperkt (*inhoudelijke en procedurele waarborgen*) en
6. het concept verbindend is naar nationaal recht (*verbindendheid naar nationaal recht*).

De AP slaat daarbij in het bijzonder acht op de rechten van betrokkenen en de overeenstemming van het concept met artikel 6, eerste en derde lid, en 9, van de AVG (Verordening 2016/679), dan wel 8 en 10 van de Richtlijn politie en justitie (richtlijn 2016/680) en met de in artikel 5 van de AVG dan wel artikel 4 van de Richtlijn vastgestelde beginselen. Hieruit volgt onder andere dat:

- (a) verwerkingen *rechtmatig, behoorlijk en transparant* moeten zijn ten aanzien van de betrokkene;
- (b) dat persoonsgegevens alleen mogen worden verzameld voor *welbepaalde, nadrukkelijk omschreven en gerechtvaardigde doeleinden*; en
- (c) verwerkingen *toereikend zijn, ter zake dienend en beperkt moeten zijn tot wat voor de doeleinden noodzakelijk is*.

--*--