

Auditplicht bij de Wet politiegegevens

Zet uw organisatie opsporingsambtenaren in? Heeft u als gemeente boa's in dienst? In dat geval is de Wet politiegegevens (WPG) en Besluit politiegegevens (BPG) hoogstwaarschijnlijk voor u van toepassing.



Bij specifieke taken op het gebied van opsporing is voor de beveiliging van persoonsgegevens de Wet politiegegevens (WPG) van toepassing, niet de Algemene verordening gegevensbescherming (AVG). De WPG komt in grote lijnen overeen met de AVG. Toch zijn er ook belangrijke verschillen. Het meest in het oog springende verschil is de auditplicht op de gegevensverwerking bij opsporingstaken. Jaarlijks voert u een interne audit uit. Eenmaal in de vier jaar moet u een externe audit laten uitvoeren. Het eerste jaar waarin deze externe audit uitgevoerd dient te worden is 2021 (twee jaar na invoering van deze wet in 2019).

Wat is de WPG en wat is het verschil met de AVG?

Voor het uitvoeren van de opsporingstaken is toegankelijkheid van bevoegde medewerkers tot politiegegevens van belang. Dit betreft zeer gevoelige informatie. De WPG is een wet die de rechten en

plichten van de politie en de burger regelt voor het verwerken van deze politiegegevens.

Verschillen met de AVG zijn onder meer dat er specifieke verwerkingsgrondslagen met eigen voorwaarden en verwerkingstermijnen zijn voor politiegegevens. Daarnaast is de rol van de privacyfunctionaris anders ingericht. Ook worden er audits in opzet, bestaan en werking uitgevoerd.

Verder combineren boa's vaak opsporingstaken met toezichthoudende taken in hun werkzaamheden. Het verwerken van persoonsgegevens in verband met het uitoefenen van opsporingstaken voor strafbare feiten valt onder de WPG. Het verwerken van persoonsgegevens in verband met het uitoefenen van toezichthoudende taken valt onder de AVG. Dit betekent dat registratie en toezicht vanuit twee perspectieven plaats moeten vinden.

Wij helpen u voldoen aan de WPG-auditplicht

Wat houdt de auditplicht in?

- **Interne audit**

De jaarlijkse interne audit in opzet, bestaan en werking van de naleving van de WPG moet door een geregistreerde IT-auditor uitgevoerd worden. Deze interne audit mag op basis van een auditplan betrekking hebben op een deel van de uitvoering van de WPG.

- **Externe audit**

De externe audit vindt vanaf 2021 elke vier jaar plaats en heeft betrekking op de gehele uitvoering van de WPG. Om de werking vast te kunnen stellen, wordt in de externe audit over een onderzoeksperiode van tenminste zes maanden de maatregelen getest.

Neem contact met ons op!

Wij kunnen u op verschillende manieren helpen aan het tijdig voldoen aan uw auditverplichtingen in het kader van de WPG. Als u contact met een van ons opneemt, werken wij een op maat gemaakt plan voor u uit.

- **Gerke Roorda**

Senior consultant | g.roorda@bakertilly.nl
IT auditor bij Baker Tilly en gespecialiseerd in IT-audits en advies in de publieke sector (ENSIA, Suwi, BIO, DigiD, Privacy).

- **Lucinda Lunshof RE**

Senior consultant | l.lunshof@bakertilly.nl
IT auditor en consultant bij Baker Tilly en specialist op het gebied van privacywetgeving.

- **Roy Zwartjes RE**

Senior manager | r.zwartjes@bakertilly.nl
Heeft vanuit zijn ervaring een duidelijke visie op informatiebeveiliging en privacy in de publieke sector. Verantwoordelijk voor en gericht op voortdurende kwaliteitsverbetering.

Hoe kunnen wij u helpen?

De IT-auditors van Baker Tilly kunnen u op diverse manieren helpen om aan de WPG-auditplicht te voldoen:

1. **Maak gebruik van ons WPG-normenkader**

Voor uw interne beheersing en om de interne en externe audits te kunnen voorbereiden en uitvoeren, hebben wij een normenkader ontwikkeld. Dit normenkader bevat de verplichte elementen in het kader van de privacy audit.

2. **Krijg met onze scan inzicht in de scope van de audit**

Met onze WPG-scan krijgt u zicht op de verwerkingen in het kader van de WPG. Eveneens welke medewerkers en applicaties daarbij betrokken zijn. Van welke type bo's maakt u gebruik? Heeft u alle gegevensverwerkingen in het kader van de WPG in beeld? Welke applicaties worden daarbij gebruikt? Is er door de leverancier al een WPG audit op de applicatie uitgevoerd? Welke verantwoordelijkheden blijven er over voor uw organisatie? De scan helpt om de scope van de audit te bepalen.

3. **Voer een nulmeting of pre-audit**

Ter voorbereiding van de eigenlijke audit kunnen wij een nulmeting of pre-audit uitvoeren. Hierna weet u waar uw organisatie staat en welke verbeterlagen u nog kunt maken. Op uw verzoek stellen wij ook een verbeterplan met u op.

4. **Laat een van onze auditors de interne en/of externe audit uitvoeren:**

- Wanneer u zelf geen geregistreerde IT-auditor (RE) in dienst heeft, kunt u voor de interne audit gebruik maken van een externe auditor van Baker Tilly. Wij stellen met u een passend WPG-auditplan op. Zo worden door de jaren heen alle onderdelen van het normenkader getoetst en bent u goed voorbereid op de externe audit.

- Onze gecertificeerde IT-auditors hebben ruime ervaring en kunnen de vereiste externe audit bij u uitvoeren.