

Wat is een Wpg Privacy audit?

De Wet politiegegevens (Wpg) is sinds 2019 van kracht voor boa organisaties en vereist voor het eerst in 2021 een verplichte externe privacy audit. Deze controle is gericht op het verwerken van politiegegevens. De Wpg geldt al langer voor de politie zelf, maar sinds 2019 mogen buitengewoon opsporingsambtenaren (boa's) ook politiegegevens verwerken in het kader van opsporing van strafbare feiten. Het verwerken van dit type gegevens valt niet onder de Algemene Verordening Gegevensbescherming (AVG), maar onder de Wet politiegegevens (Wpg). De Wpg kent een apart privacyregime en jaarlijks moet er een interne audit worden uitgevoerd en vier jaarlijks een audit door een externe auditor. In deze flyer beschrijven we wat dit voor de boa's en hun werkgevers betekent en wat wij als BKBO b.v. u kunnen aanbieden om de verplichte externe audit efficiënt en effectief uit te voeren.



De boa's

Buitengewoon opsporingsambtenaren spelen een belangrijke rol in onze samenleving. Zij sporen bepaalde strafbare feiten op en staan zo de politie terzijde bij het handhaven van de openbare orde en veiligheid. Naarmate we de politie steeds minder op straat zien, wordt de rol van de boa steeds maar groter. Een boa heeft officiële opsporingsbevoegdheden die samenhangen met de functie. Deze bevoegdheden zijn altijd beperkt tot een bepaald werkterrein. Er zijn zes werkterreinen, ook wel domeinen genoemd, waarop boa's actief zijn. Een boa werkt voor een van de volgende domeinen:

- De openbare ruimte (o.a. handhavers, parkeerwachters, bouw en woningtoezicht, controleurs).
- Het milieu, welzijn en infrastructuur (o.a. groene Boa's, boswachters, jachtopzieners, milieu-inspecteurs, waterinspecteurs, weginspecteurs).
- Het onderwijs (leerplichtambtenaren).
- Het openbaar vervoer (conducteurs, BOA-OV).
- Werk, inkomen en zorg (o.a. sociaal rechercheurs, arbeidsinspectie, belastingcontroleurs en -inspecteurs).
- Generieke opsporing (boa's bij politie).

Landelijke bevoegdheid

Sinds 1 april 2010 zijn boa's landelijk opsporingsbevoegd. In overleg met de zogeheten lokale driehoek (officier van justitie, burgemeester en politiechef) mogen zij buiten het gebied van hun werkgever optreden. Wel moeten de partijen hun samenwerking schriftelijk vastleggen in een samenwerkingsconvenant.

De Wpg

De Algemene Verordening gegevensbescherming (AVG) staat volop in de publieke belangstelling. Veel minder bekend is dat er daarnaast nog een andere privacywet van kracht is geworden, de Wet politiegegevens (Wpg). Deze regelt, onder meer, de verwerking van persoonsgegevens in de strafrechtelijke keten.

Bij opsporing en tenuitvoerlegging van straffen worden per definitie uiterst gevoelige gegevens gebruikt. Boa's spelen hierin een belangrijke rol. Wat het extra ingewikkeld maakt, is dat de boa naast opsporingstaken vaak ook bestuursrechtelijke toezichts- en handhavingstaken heeft. De verwerking van persoonsgegevens voor de opsporingstak valt onder het regime van de Wpg en de verwerking van de overige taken valt weer onder de AVG. In het algemeen zijn boa's een groter deel van hun tijd bezig met toezicht en handhaving dan met de opsporing van strafbare feiten. Omdat opsporingstaken in het algemeen privacygevoeliger zijn, is het privacyregime van de Wpg dan ook een stuk zwaarder dan de AVG.

Specifiek noemen we dat de Wpg vereist dat:

- Steeds duidelijk is welke gegevens op feiten zijn gebaseerd en welke gegevens op een persoonlijk oordeel van de boa zijn gebaseerd.
- Er steeds een onderscheid wordt gemaakt tussen verschillende typen betrokkenen, zoals verdachten, slachtoffers, derden en getuigen.
- Logging geregeld is in de gebruikte informatiesystemen.
- Politiegegevens beschikbaar worden gesteld aan geautoriseerde politieambtenaren of boa's in andere organisaties voor zover nodig voor de uitvoering van hun taak. *Beschikbaar stellen* is zelfs een verplichting; iets dat de AVG helemaal niet kent.
- Politiegegevens kunnen ook worden verstrekt of zelfs beschikbaar worden gesteld aan buitenlandse opsporingsdiensten.
- Een periodieke externe privacy audit wordt uitgevoerd door een RE met een rapportage aan de Autoriteit Persoonsgegevens (AP).
- De FG een aantal specifieke Wpg taken toebedeeld heeft gekregen, zoals het (laten) uitvoeren van een jaarlijkse interne audit op o.a. de rechtmatigheid van de verwerking van politiegegevens.



Voor de verwerking van politiegegevens stelt de Wpg -net als de AVG- een aantal algemene eisen. Dit betreft criteria over noodzakelijkheid, rechtmatigheid, juistheid, proportionaliteit, subsidiariteit en volledigheid. Daarnaast moet de verwerkingsverantwoordelijke een aantal technische en organisatorische maatregelen nemen.

Specifieke eisen aan de werkgever van boa's

Een werkgever van boa's, zoals een gemeente, een sociale dienst, een ov-bedrijf, een waterschap of bijvoorbeeld een veiligheidsregio -kortom de verwerkingsverantwoordelijke- moet volgens de Wpg aan een aantal vereisten voldoen bij de verwerking van politiegegevens. De verwerking moet plaatsvinden in afzonderlijke systemen en Wpg gegevens mogen alleen worden verwerkt door aangewezen medewerkers. De reden voor deze strenge eisen ligt in de aard van de bevoegdheden. Bij het uitvoeren van een wettelijke opsporingstak zijn dit namelijk bevoegdheden uit het Wetboek van Strafvordering en de Wet op de economische delicten. Hiermee kan diep op de privacy van burgers worden ingegrepen – de burger weet niet dat hij of zij wordt onderzocht- en dit vraagt om strenge regels om de privacy van burgers te beschermen.

Inspanningsverplichting verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke moet zorgen voor een procesinrichting voor de verwerking van verschillende soorten gegevens waarmee opzet, bestaan en werking aangetoond wordt (artikel 4a Wpg).

Informatiebeveiliging

De verwerkingsverantwoordelijke moet technische en organisatorische beveiligingsmaatregelen voor onder andere het toegangsbeheer tot de politiegegevens implementeren. Deze toegang kan worden verleend aan personen die gelet op hun functie, de aard van de verwerking van politiegegevens en het doel ervan, noodzakelijkerwijs moeten werken met deze gegevens. Het gaat dan zowel om fysieke maatregelen zoals toegangszonering als digitale maatregelen als autorisatiebeheer, identiteitsmanagement, beheer van toegangs- en gebruikersrechten, logging, wijzigingsbeheer.



WPG-proof ICT-systeem

Als een ICT-systeem wordt gebruikt voor de verwerking van politiegegevens, moet dit systeem "Wpg-proof" zijn. Vereisten zijn een autorisatiestelsel, termijnbewaking van gegevens, onderscheid kunnen maken tussen soorten politiegegevens, soorten betrokkenen en een op komst zijnde loggingsverplichting. Voor sommige systemen zijn hier al TPM's afgegeven zodat we daarop kunnen steunen in onze audit.



Privacyrechten

Burgers hebben mogelijk recht op informatie over verwerking van politiegegevens. Dit kan een actieve informatieplicht zijn waarbij de verwerkingsverantwoordelijke het initiatief moet nemen om betrokken burgers te informeren, maar kan ook gaan om een passieve informatieplicht op verzoek van een burger. Anders dan in de AVG kunnen dergelijke verzoeken geheel of gedeeltelijk worden afgewezen als dit de opsporing en vervolging belemmert.

Gegevensbeschermingseffectbeoordeling (GEB)

Er zijn ook veel overeenkomsten tussen Wpg en AVG. De Wpg stelt net als de AVG een GEB of DPIA verplicht op verwerkingen van politiegegevens die een hoog risico inhouden voor de privacy van burgers. Dit geldt met name voor verwerkingen waarbij nieuwe technologieën worden ingezet.

Registerplicht

De registerplicht houdt in dat de verwerkingsverantwoordelijke – net als onder de AVG – voorziet in het beschrijven van alle verwerkingsactiviteiten in algemene zin, om dit vervolgens op te nemen in een register (artikel 31d Wpg).

Meldplicht datalekken

Er is – net als onder de AVG – een meldplicht voor datalekken bij de Autoriteit Persoonsgegevens. Anders dan in de AVG kan een dergelijke melding worden uitgesteld, beperkt of achterwege worden gelaten als dat bijvoorbeeld opsporing, vervolging of berechting belemmert.

Documentatieplicht

De documentatieplicht staat voor documenteren van belangrijke verwerkingen, zoals verstrekking van politiegegevens aan derden, redenen voor afwijzing inzage- of correctieverzoek en alle inbreuken op de beveiliging van persoonsgegevens.

Wat is de Wpg audit?

Bij de privacy audit beoordelen we kortweg de compliance met de Wpg. Het object van onderzoek van een privacy audit Wpg bestaat uit de verwerkingen van politiegegevens die onder verantwoordelijkheid van de verwerkingsverantwoordelijke worden verwerkt. De privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee:



- a) de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
- b) de werking van de getroffen maatregelen en procedures;
- c) de resultaten van de interne audits worden betrokken bij de privacy audit.

Wat is uw voordeel?



Bij BKBO b.v. ontzorgen wij u. Het voorbereiden en uitvoeren van de privacy audit vraagt de nodige expertise en capaciteit. Wij zijn daarvoor uw betrouwbare partner.

Uit de audit kan natuurlijk blijken dat de normen niet zijn behaald. Dan moet binnen drie maanden een hercontrole worden uitgevoerd. Afhankelijk van de ernst kan dat een intern of een extern uitgevoerde hercontrole zijn. Ingeval het een externe hercontrole zou moeten zijn, doen wij dat eveneens voor u. Zonder meerprijs. We kunnen u nóg meer zekerheid geven wanneer wij de interne audits voor uw organisatie uitvoeren. Voor uw gemak bieden wij daarvoor een abonnement aan.

Wij ondersteunen u met een aanpak die zowel tijd als kosten bespaart. Wij zijn zeker van onze zaak en bieden u een vaste prijs. Dat is voordelig en compleet, want het is inclusief eventuele hercontroles.

BKBO b.v. is vanaf de start vertegenwoordigd in de Wpg werkgroep van NOREA. We voeren de Wpg audit conform het protocol zoals beschreven in de Handreiking van NOREA. Zo bent u ervan verzekerd dat de door ons bureau uitgevoerde privacy audit voldoet aan de regels van de Autoriteit Persoonsgegevens. Wij zijn gespecialiseerd in het afnemen van audits bij de lokale overheid. Door onze bewezen ervaring voeren we audits uit bij meer dan 170 organisaties.

Hoe pakken wij dat aan?

Als u nog nooit een eigen interne audit heeft uitgevoerd op de Wpg, adviseren wij u om eerst een nulmeting te laten doen, zodat tekortkomingen vroegtijdig aan het licht komen. We geven u dan heldere en op maat toegesneden aanbevelingen om tekortkomingen snel op te heffen. U kunt dan gericht stappen zetten om de Wpg goed te implementeren.

Wij hebben een gestandaardiseerde en beproefde uitvoeringswijze ontwikkeld, waarbij we het aantal contactmomenten en daarmee de belasting van uw organisatie zoveel mogelijk beperken. De uitvoering begint met een documentatieverzoek inclusief een helder auditplan. Afhankelijk van uw opdracht zal onze auditor bij u eerst een complete nulmeting uitvoeren. Daarna bespreken wij de auditplanning met u. Hierbij gaan we na of uw boa systeem een TPM verklaring heeft. We bespreken welke interviews nodig zijn en met welke functionarissen en op welke termijn dat mogelijk is. Afhankelijk van een eventuele TPM, beoordelen wij zowel de infrastructuur en de general IT Controls. Gelijktijdig vindt een audit plaats op uw contracten, de procedures, de governance en de kwaliteit van de uitgevoerde interne audits. We voeren diepte-interviews pas uit nadat we uw bewijsstukken hebben ontvangen en bestudeerd om uw tijd zo efficiënt mogelijk te gebruiken en de belasting voor uw organisatie zoveel mogelijk te beperken. Interviews zullen veelal via Zoom of Teams plaatsvinden. Wij zorgen dat voor u alles compleet, geordend en begrijpelijk is.



We leggen onze bevindingen vast in een overzichtelijke conceptrapportage. We doen concrete aanbevelingen om de tekortkomingen efficiënt op te heffen. Het assessment wordt afgesloten met een persoonlijk gesprek waarin we de bevindingen en onze aanbevelingen helder toelichten. Daarna wordt de rapportage definitief gemaakt en kan deze worden verstuurd aan de AP.

Wat is uw investering?

Afhankelijk van wat u wilt dat onderzocht wordt, variëren de kosten tussen de € 3.500,- en € 10.000,-. De genoemde prijzen zijn exclusief BTW en inclusief reis- en verblijfskosten.

Dit assessment is ook voordelig te combineren met andere audits. Ook is een vijf jarig abonnement -waarbij we de interne audits uitvoeren in 2022, 2023 en 2024 en de 2^e externe privacy audit in 2025 uitvoeren- met korting mogelijk. Zo bent u verzekerd dat u aan alle eisen blijft voldoen: probleemloos, efficiënt en effectief!

Geen gekibbel garantie



graag met u in gesprek. U kunt direct bellen met BKBO b.v. via telefoonnummer: 073 – 211 03 37. Is het voor u meteen helemaal duidelijk? Dan kunt u ook meteen een offerte aanvragen via info@bkbo.nl

Onze garantie is uniek in de branche! Wij garanderen u een vaste prijs. De prijs is dus inclusief een eventuele hercontrole en verbeterrapport nadat u verbetermaatregelen heeft kunnen doorvoeren. Door onze bewezen aanpak durven wij hiervoor in te staan. Wij noemen dat onze "geen gekibbel garantie".

Wilt u meer weten?

Wij staan voor u klaar en gaan

