BMC
YACHT GROUP

Auditplicht: waar moeten decentrale overheden met boa's in 2021 aan voldoen?

Partners in verbetering

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt gedeeltelijk onder de Algemene Verordening gegevensbescherming (AVG) en gedeeltelijk onder de Wet politiegegevens (Wpg). Maar wat betekent dit voor de werkgever van de boa's? In dit artikel gaan we in op de belangrijkste verplichtingen voor decentrale overheden en presenteren we een effectieve aanpak om hieraan te voldoen.

Sinds 25 mei 2018 valt de verwerking van persoonsgegevens in het kader van opsporing door boa's niet meer onder de AVG, maar onder de Wpg. Daarmee is er één wettelijk regime ontstaan voor de verwerking van persoonsgegevens in de strafrechtketen. Voor het toezicht door boa's valt de verwerking van persoonsgegevens nog steeds onder de AVG. In dit artikel gaan we in op de verwerking van persoonsgegevens door boa's in het kader van hun opsporingstaak; dit valt dus onder de Wpg.

Wie is de verwerkingsverantwoordelijke onder de Wpg?

De werkgever van de boa is en blijft verantwoordelijk voor de verwerking van persoonsgegevens. Voor gemeenten is dit het college van burgemeester en wethouders. Het college van B en W is dus verantwoordelijk voor de gegevensverwerking en het voldoen aan de verplichtingen uit de Wpg. Hieronder gaan we in op de belangrijkste verplichtingen uit de Wpg.

Wat zijn de belangrijkste verplichtingen uit de Wpg?

- De verwerking van persoonsgegevens in het kader van opsporing moet duidelijk gescheiden zijn van de verwerking van persoonsgegevens in het kader van toezicht. Als de scheiding binnen één systeem mogelijk is, mag dat ook.

- Scheiding van opsporings- en toezichtgegevens betekent ook dat er onderscheid moet worden gemaakt in autorisaties. Alleen als er een functionele noodzaak is om toegang te krijgen tot opsporingsgegevens, kan een autorisatie worden verleend. In dat geval kan zowel aan boa's of aan ondersteunde medewerkers een autorisatie worden toegekend (Wpg artikel 6 lid 4 jo. artikel 3 Besluit politiegegevens boa's).

- Voor de autorisatie van ondersteunende medewerkers geldt dat in de autorisatie het volgende moet worden verwerkt: het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van de betrokkenen (artikel 3 lid 3 Besluit politiegegevens boa's).

- Voor de persoonsgegevens die boa's verwerken in het kader van opsporing gelden duidelijke verwijderingstermijnen. In de meeste gevallen is deze termijn één jaar na de datum van de eerste verwerking. Dit betekent dus dat de gegevens na deze termijn moeten worden verwijderd en niet meer beschikbaar mogen zijn voor de dagelijkse politietaak.

- Verplichtingen uit de AVG, zoals de meldplicht datalekken, het uitvoeren van DPIA's, het opstellen van een verwerkingsregister, het opstellen van een verwerkersovereenkomst bij uitbestedingen en informatiebeveiliging, zijn ook in de Wpg opgenomen.

- Voor Wpg-verwerkingen geldt de verplichting om een Functionaris Gegevensbescherming (FG) aan te stellen. Dit kan dezelfde FG zijn als voor de AVG-verwerkingen, maar dat hoeft niet. Wel moet de werkgever de FG voor de Wpg-verwerkingen apart benoemen.

Hoe zit het met de verplichte IT-audits?

De Wpg verplicht de verwerkingsverantwoordelijke om elke vier jaar een externe IT-audit uit te laten voeren. Deze audit moet op systematische wijze toetsen of de bepalingen van de wet op een adequate manier zijn uitgevoerd. Het gaat kortom om een volledige toets op de Wpg. De uitkomsten van de externe IT-audit moeten worden gerapporteerd aan de toezichthouder, de Autoriteit Persoonsgegevens (AP). De eerste externe IT-audit moet in 2021 worden uitgevoerd (artikel 33 Wpg en artikel 6.5 Bpg).

Daarnaast moet er elk jaar – dus ook in 2021 – een interne IT-audit worden uitgevoerd. Het verschil met de externe audit is dat de interne audit zich richt op één dan wel een aantal onderdelen van de wet. De interne audit toetst of deze onderdelen op adequate wijze zijn uitgevoerd. De uitkomsten moeten worden meegenomen in de externe audit. Er moet dus eerst een interne audit plaatsvinden, gevolgd door de externe audit. Een ander verschil is dat de interne audit niet voorgelegd hoeft te worden aan de AP. De FG zal hier wel jaarlijks om vragen.

Het uitvoeren van de interne IT-audit vraagt om kennis en vaardigheden. Deze zijn te vinden in de Regeling periodieke audit politiegegevens. Het gaat onder meer om kennis van geautomatiseerde informatiesystemen en methoden en technieken rond IT auditing, de boa-organisatie, de informatievoorziening en processen van verwerking van politiegegevens en de wet- en regelgeving, in het bijzonder de Wet politiegegevens.

Waar moeten decentrale overheden rekening mee houden?

Voor de werkgevers van boa's – decentrale overheden – is er in 2021 werk aan de winkel! Niet alleen moeten ze een interne audit uitvoeren, voorafgaand aan de externe audit (doen zij dit niet, dan overtreden zij de Wpg). Ook moeten decentale overheden aan de slag met de implementatie van de Wpg, voor zover zij deze nog niet hebben afgerond.

Veel organisaties beschikken niet over de tijd of de kennis als het gaat om het implementeren van de Wpg. BMC kan u hierbij helpen. Zo hebben we een een instrument ontwikkeld, waarmee we eenvoudig in beeld kunnen brengen welke onderdelen van de Wpg u nog moet implementeren. Ook kunnen wij u helpen deze onderdelen te implementeren. BMC heeft ruime ervaring met de implementatie van de Wpg bij decentrale overheden. Daarmee kunt u de audits met vertrouwen tegemoetzien. Daarnaast kan BMC de verplichte audits ook voor u uitvoeren. Onze medewerkers zijn hiervoor gekwalificeerd.

Meer informatie & contact

Wilt u meer informatie over hoe BMC u kan helpen met de implementatie van de Wpg en de verplichtie IT-audits? Neem dan vrijblijvend contact op met onze adviseurs.

Alex Commandeur
managing consultant
alex.commandeur@bmc.nl
06 - 82 12 03 17

Julius Duijts
managing consultant
julius.duijts@bmc.nl
06 - 29 52 55 31

Willem de Vries
managing consultant
willem.de.vries@bmc.nl
06 - 51 62 97 80

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**