BMC
YACHT GROUP

Wat betekent de Wet politiegegevens voor organisaties met boa’s?

Partners in verbetering

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet onder de Algemene Verordening gegevensbescherming (AVG), maar in plaats daarvan onder de Wet politiegegevens (Wpg). De aangepaste wet is per 1 januari 2019 van kracht geworden. We gaan hier in op wat dit voor de boa's en hun werkgevers betekent en wat een effectieve aanpak kan zijn om aan de Wpg te voldoen.

Achtergrond van de Wpg

Tot 25 mei 2018 viel de verwerking van persoonsgegevens door boa's onder de Wet bescherming persoonsgegevens (Wbp). Met de komst van de AVG valt de verwerking van persoonsgegevens voor voorkoming van, onderzoek naar, opsporing van en vervolging van strafbare feiten onder een andere Europese wet, namelijk de EU-Richtlijn 2016/680. Deze richtlijn is omgezet in een nationale wet, namelijk de Wpg, aangevuld met het Bpg (Besluit politiegegevens). Daarmee ontstaat er één wettelijk regime voor de verwerking van persoonsgegevens in de strafrechtelijke keten, waar in het verleden voor delen van de keten de Wbp en voor andere delen de Wpg van kracht was.

Dit wetgevingsproces heeft in Nederland tot eind 2018 geduurd en de nieuwe Wpg is per 1 januari 2019 ingegaan. Per die datum is ook het bijbehorende Besluit politiegegevens aangepast. We richten ons in deze notitie op boa's in dienst van decentrale overheden.

Wat blijft gelijk?

De werkgever van de boa blijft verantwoordelijk voor de verwerking van persoonsgegevens volgens de Memorie van Toelichting bij de wetswijziging. Verder is in de EU-richtlijn 2018/680, waarop de Wpg is gebaseerd, aansluiting gezocht bij de AVG. Dat betekent dat organisaties die de AVG hebben geïmplementeerd voor een belangrijk deel ook voldoen aan de eisen die de Wpg stelt, bijvoorbeeld: de meldplicht datalekken, het uitvoeren van DPIA's en het aanstellen van een Functionaris Gegevensbescherming (FG).

Wat verandert er?

We beperken ons in onderstaand overzicht tot de afwijkingen van en aanvullingen op de AVG. Het gaat in hoofdlijnen om het volgende:

- De boa heeft bijna altijd ook bestuursrechtelijke toezichts- en handhavingstaken. Een boa krijgt daarom bij het verwerken van persoonsgegevens zowel met de AVG te maken als met de Wpg. In de verwerking van gegevens moet dus duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. In een aantal organisaties is deze scheiding al doorgevoerd door strafrechtelijke gegevens in het BRS (Boa Registratie Systeem) op te nemen en toezichts- en bestuursrechtelijke gegevens in andere systemen. Als de scheiding binnen één systeem mogelijk is, mag dat ook.

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd. (Wpg 4.3)

- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden. (Wpg 6b)

De Wpg vereist documentatie van (Wpg 32):
- doelen van onderzoeken;
- verstrekking of doorgifte;
- afwijzing van verzoeken om inzage;
- inbreuk op de beveiliging;
- doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens;
- melding van gemeenschappelijke verwerkingen aan de AP.

- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens. (Wpg 32a, Bpg 6:1a.3g)

- Er worden specifieke eisen gesteld aan de informatiebeveiliging die in het aangepaste Besluit politiegegevens zijn opgenomen.

Belangrijke aspecten die gehandhaafd blijven ten opzichte van de oude Wpg, maar die mogelijk nieuw zijn voor organisaties met boa's:

- Politiegegevens worden alleen aan geautoriseerde politieambtenaren in andere organisaties beschikbaar gesteld voor zover nodig voor de uitvoering van hun taak. (Wpg 6a.2 en 15.1)
- De mogelijkheid bestaat om in bijzondere gevallen personen die geen ambtenaar van politie zijn en onder beheer van de verantwoordelijke vallen te autoriseren voor het verwerken van politiegegevens. (Wpg 6.4)
- Toegang wordt verleend voor degenen die in opdracht van de werkgever technische werkzaamheden verrichten. (Wpg 6a.3)
- In de dagelijkse uitvoering van taken wordt alleen toegang verleend tot gegevens ouder dan 1 jaar op basis van een relatie met actuele gegevens. (Wpg 8.1, 8.2)
- Bij verstrekking van onjuiste of onrechtmatig verkregen gegevens moet de ontvanger worden geïnformeerd. (Wpg 4.4)
- Gegevens uit de dagelijkse uitvoering van taken moeten na 5 jaar worden vernietigd. (Wpg 8.6)
- Gegevens ten behoeve van een onderzoek moeten na maximaal een halfjaar worden verwijderd als ze niet langer nodig zijn voor het onderzoek (Wpg 9.4), maar ze mogen pas na 5 jaar worden vernietigd. (Wpg 14.1).
- Er bestaat een verplichting tot privacy-audits met rapportage aan de Autoriteit Persoonsgegevens (AP) (Wpg 33), twee jaar na inwerkingtreding en daarna elke 4 jaar. (Bpg 6:5)

Grotere veranderingen in lijn met de AVG zijn:

- inrichting van processen en systemen volgens de principes van gegevensbescherming door beveiliging en ontwerp, gegevensbescherming door standaardinstellingen (Wpg 4a,b);
- de uitvoering van DPIA's, deels in lijn met de AVG, deels met specifieke eisen (Wpg 4c);
- het uitbesteden aan een verwerker (Wpg 6c);
- versterkt recht van de betrokkene om op verzoek informatie over de verwerking van gegevens te krijgen (Wpg 24a, b);
- het recht op inzage (Wpg 25), rectificatie en vernietiging (Wpg 28), tenzij dit het onderzoek belemmert, et cetera (Wpg 27);
- het recht op het indienen van een klacht bij de AP (Wpg 31a);
- het recht op schadevergoeding (Wpg 31c);
- de plicht om een verwerkingsregister bij te houden (Wpg 31d) met voor de verantwoordelijke, aanvullend op de in de AVG gevraagde informatie:
  - het bestaan van profilering;
  - categorieën van gegevens die worden doorgegeven buiten de EU;
  - grondslag;
  - toekenning van autorisaties.
- melding van datalekken (Wpg 33a);
- voorafgaande raadpleging van de AP (Wpg 33b);
- benoeming van een FG (Wpg 36).

Meer informatie & contact

Wilt u weten hoe BMC uw organisatie kan ondersteunen?
Neem dan contact op met onze senior adviseurs. Zij helpen u graag verder.

ir. Julius Duijts
senior adviseur
julius.duijts@bmc.nl
06 – 29 52 55 31

mr. Alex Commandeur
senior adviseur
alex.commandeur@bmc.nl
06 – 82 12 03 17

drs. Willem de Vries
adviseur
willem.de.vries@bmc.nl
06 – 51 62 97 80

Wat moet er nu gebeuren?

Een en ander betekent dat er specifiek aandacht nodig is om de gegevensverwerking door boa's goed te regelen. Diverse vereisten van de wet zullen moeten worden ingevoerd. Afhankelijk van bijvoorbeeld de gebruikte systemen kan dat in de ene organisatie meer inspanningen vergen dan in de andere. Daarom adviseert BMC:

- een nulmeting te doen op basis van de verplichtingen in de nieuwe Wpg, zodat ook punten die mogelijk in het verleden niet helemaal goed waren geregeld in beeld komen. Het voordeel hiervan is dat er goed kan worden aangesloten bij de AVG-implementatie, dat het een overzicht biedt wat er te doen is en de mogelijkheid om daarin prioriteiten te onderscheiden;
- een traject te starten om de ontbrekende maatregelen in te voeren, waarbij zo veel mogelijk wordt aangesloten bij de werkwijze en procedures die rond de AVG al zijn ingericht.

BMC heeft een instrument ontwikkeld om de nulmeting uit te voeren en ontwikkelt sjablonen voor de benodigde werkwijze en procedures. BMC ondersteunt u graag in dit traject.

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