

Verslag Functionaris gegevensbescherming-WPG

Inleiding

Voor 31 december 2023 moest de gemeente Zutphen een (verplicht) verbeterplan met stappen aanleveren aan de autoriteit persoonsgegevens¹. Door interne oorzaken is dit niet gelukt. Een interne audit van de Wet politiegegevens (Wpg) is niet uitgevoerd in 2023. In een inventarisatie (zie externe audit 2023 Inergy²) blijkt dat er verbeterlagen gemaakt moeten worden om te voldoen aan de richtlijnen van de WPG. Een eerste aanzet voor de verbeterlagen is gemaakt in 2023 (middelen zijn beschikbaar gesteld om externe ondersteuning in te huren) en wordt vervolgd in 2024. Met als doel in 2024 volledig te voldoen aan de gestelde richtlijnen van de Wpg. De hoofdmoot voor deze verbeterlagen ligt bij de teams bestuursondersteuning, I&A, inkomen, jeugd (leerplicht) en het team Veiligheid.

Auditplicht bij de Wet politiegegevens

De gemeente heeft boa's in dienst. Dat betekent dat de Wet politiegegevens (WPG) en Besluit politiegegevens (BPG) van toepassing zijn. Voor het uitvoeren van de opsporingstaken van sommige boa's is toegankelijkheid van bevoegde medewerkers tot politiegegevens van belang.

Het betreft gevoelige informatie. Bij specifieke taken op het gebied van opsporing is voor de beveiliging van persoonsgegevens de Wetpolitiegegevens (Wpg) van toepassing en niet de Algemene verordening gegevensbescherming (AVG). Boa's combineren 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. De WPG komt in grote lijnen overeen met de AVG. Toch zijn er ook belangrijke verschillen. De WPG is een wet die de rechten en plichten van de politie en de burger regelt voor het verwerken van deze politiegegevens. Er zijn verschillen met de AVG. Deze verschillen zijn onder meer dat er specifieke verwerkingsgrondslagen met eigen voorwaarden en verwerkingstermijnen zijn voor politiegegevens. Daarnaast is de rol van de privacyfunctionaris anders ingericht. Het meest in het oog springende verschil tussen AVG en Wpg is de auditplicht op de gegevensverwerking bij opsporingstaken voor de Wpg. Jaarlijks moet een gemeente een interne audit uitvoeren. Eenmaal in de vier jaar moet er een externe audit uitgevoerd worden. Het eerste jaar waarin deze externe audit uitgevoerd diende te worden is 2021 (twee jaar na invoering van deze wet in 2019).

Om te kunnen voldoen aan de wettelijke eisen zijn de volgende stappen van belang:

Stel een normenkader op voor uw interne beheersing en om de interne en externe audits te kunnen voorbereiden en uitvoeren. Dit normenkader dient tenminste de verplichte elementen in het kader van de privacy audit te bevatten.

1. Verkrijg inzicht in de scope van de audit. Breng daarbij in beeld:
 - a. Welke gegevensverwerkingen in het kader van de Wpg worden gebruikt
 - b. Welke medewerkers en applicaties betrokken zijn
 - c. Welke type boa's worden gebruik
 - d. Of door de leverancier al een Wpg-audit op de applicatie is uitgevoerd.
 - e. Welke verantwoordelijkheden er over blijven voor de gemeentelijke organisatie.
2. Voer een periodieke (nul)meting uit. Hierna weet je waar je als organisatie staat en welke verbeterlagen je nog kunt maken.
3. Laat de interne en/of externe audit uitvoeren.

¹ De datum is verlengd door de autoriteit persoonsgegevens naar 1-3-2024

² Zie Memo d.d. 2022_BW_00592 van 20-12-2022; en rapport externe audit Inergy16-9-2022 zaaknummer 468535

Wet politiegegevens

De auditverplichting die organisaties als werkgever onder de Wet politiegegevens hebben (Wpg) is met ingang van 1 januari 2019 van kracht geworden. Deze wet verplicht de gemeente vanaf 2021 elke vier jaar een externe Wpg-audit te laten uitvoeren en de resultaten daarvan naar de toezichthouder, de AP, te sturen. De controle ziet toe op hoe het verwerken van politiegegevens door buitengewoon opsporingsambtenaren (boa's) is georganiseerd, de maatregelen die daarop van toepassing zijn en de werking van deze maatregelen. De organisatie heeft in 2022 een externe auditor ingeschakeld die een (pre) audit heeft uitgevoerd.

Uit de audit in 2022 bleek dat de gemeente Zutphen nog niet volledig voldeed aan de Wpg eisen. Het gevolg daarvan was dat er binnen één jaar een hercontrole moet worden uitgevoerd. Zorgvuldigheid is van groter belang dan snelheid. De extra tijd wijzigt de onderzoeksperiode echter niet. Dit blijft de periode tot en met het jaar 2021. Ontwikkelingen die zich daarna hebben voorgedaan kunnen in het auditrapport in een afzonderlijke paragraaf opgenomen worden, maar deze veranderen niets aan het wel of niet voldoen aan de Wpg. Het is aan te bevelen in 2024 als gemeente, (aan de hand van de auditrapportage 2022-2023) keuzes te maken over de inzet van de huidige privacyfunctionaris (-en) bij het verder implementeren van de Wpg en het wel of niet prioriteren van deze werkzaamheden ten opzichte van de werkzaamheden onder de AVG.

Toezichtsmaatregelen

De functionaris gegevensbescherming heeft onderzoek gedaan naar de werking van de beheersmaatregelen Wpg over het jaar 2023. Het betreft de beheersingsmaatregelen:

- a. Jaarlijks Toezicht van de FG op de doelbinding;
- b. Controles op de noodzakelijkheid en rechtmatigheid door de PO;
- c. Controles op het vernietigen en rectificeren van politiegegevens;
- d. Controles op uitvoering DPIA's;
- e. Beschikbaarheid logbestanden;
- f. Planning, uitvoering, en rapportage van de interne audits;
- g. Overige toezichttaken van de FG.

De te nemen maatregelen conform vorig verbeterplan zijn niet aantoonbaar uitgevoerd in 2022 en 2023. Er is wel een opdracht verstrekt in 2023 (met behulp van derden) om dit zo snel mogelijk op te pakken. Er is voor 2024 een verbetercyclus ingepland.

Er is geen specifiek beleid vastgesteld of goedgekeurd op het gebied van de uit te voeren taken in het kader van de Wpg en aanverwante regelgeving (waaronder het documenteren van autorisaties en het nemen van maatregelen onder andere logging);

Er zijn geen DPIA's uitgevoerd of aantoonbaar vastgelegd conform vastgestelde DPIA-procedure van de gemeente Zutphen om te bezien welke maatregelen wel of niet zijn genomen om te kunnen voldoen aan de eisen van de wet en regelgeving. (Onder andere Wpg en Bpg).

De controles door de privacyofficer op de noodzakelijkheid en rechtmatigheid van verwerkingen en op de te vernietigen of rectificerende activiteiten van politiegegevens zijn niet of niet aantoonbaar uitgevoerd. Gestructureerde documentatie ontbreekt. Er zijn geen aantoonbare interne audits uitgevoerd door gekwalificeerd personeel.

Er zijn geen aantoonbare bewijsstukken aangeleverd om de onder b tot en met g genoemde maatregelen te kunnen monitoren.

Conclusie

Er wordt ingezet op privacy als belangrijke randvoorwaarde om rechtmatige verwerking van persoonsgegevens te kunnen borgen en beheersen alleen is dit niet direct aantoonbaar. Er zijn ontwikkelingen die kunnen zorgen voor een succesvolle innovatie. Dit vergt tijd en prioriteit. Voldoen aan de Wpg vraagt om een verandering in het denken en handelen van iedereen die met persoonsgegevens werkt. Geen vinkjes cultuur maar een aanpassing van houding en gedrag naar een organisatie die in opzet, bestaan maar ook in de werkelijkheid en werking het zorgvuldig omgaan met gegevens als een waarde ziet die het vertrouwen in de gemeente versterkt. Dit is een ontwikkeltraject binnen de gemeentelijke organisatie dat nog niet is afgerond. Er liggen nog flinke uitdagingen voor de komende jaren.

Aanbevelingen

Draag uit dat de gemeente Zutphen kennis heeft genomen om te voldoen aan de Wet Politiegegevens (Wpg) waaronder het uitvoeren van interne en externe audits. Communiceer en registreer daarvoor al de acties die het heeft genomen om op termijn te voldoen aan de verplichtingen;

Stel specifiek beleid op met werkinstructies (aantoonbaar en gedocumenteerd en met de juiste mandaten);

Stel structurele middelen beschikbaar in 2024 en de jaren daarna voor de coördinatie, aansturing en omschrijving van werkprocessen aangaande de Wpg en dit te verantwoorden in een (bestuur)rapportage;

Zorg op tijd voor een jaarlijkse (verplichte) interne audit. Die audit uit laten voeren door gekwalificeerd personeel (in- of extern).