Voorbereiding WPG Audit

Inleiding

De verwerking van persoonsgegevens door boa's viel tot 25 mei 2018 onder de Wet bescherming persoonsgegevens (Wbp). Door de komst van de AVG valt de verwerking van persoonsgegevens rondom strafbare feiten onder een andere Europese wet, namelijk EU-Richtlijn 2016/680. Deze richtlijn is omgezet in de Wet politiegegevens (Wpg), aangevuld met het Bpg (Besluit politiegegevens), en is sinds 1 januari 2019 van kracht.

De opsporing van strafbare feiten door boa's valt daarmee buiten het bereik van de AVG. Verwerking van persoonsgegevens op strafrechtelijke grond moet voldoen aan de vereisten van de Wpg. Alle andere verwerkingen – waaronder het toezicht – vallen nog wel onder de AVG. Gemeenten hebben daarmee bij de verwerking van persoonsgegevens bij handhavingstaken te maken met zowel de AVG als de Wpg. Dit betekent dat gemeenten binnen de bedrijfsvoering rekening moeten houden met voorschriften en verplichtingen uit beide wettelijke regimes.

Waarom een verplichte audit?

De verplichting tot het uitvoeren van een audit komt voort uit art 33 lid 5 van de Wet Politiegegevens welke verder is uitgewerkt in het Besluit Politiegegevens (art 6.5)

> Artikel 6:5. Audits
>
> Twee jaren na inwerkingtreding van de wet, en vervolgens eenmaal in de vier jaren, laat de verwerkingsverantwoordelijke de uitvoering van de bij of krachtens de wet gegeven regels door een privacy audit controleren, op bij ministeriële regeling te bepalen wijze.
>
> De controle heeft betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures.

Onderwerpen

De gemeente kan in een aantal gevallen gegevens verwerken die vallen onder WPG. Dit zijn de volgende zaken:

- Handhaving openbare ruimte
- Handhaving milieu, welzijn en infrastructuur (bouw en woningtoezicht, milieu inspecteurs) • Handhaving onderwijs (leerplichtambtenaar)
- Handhaving werk, zorg en inkomen. (sociale recherche)

Niet al deze onderwerpen worden altijd door de gemeente zelf uitgevoerd!

Stappenplan WPG audit

Stap 1: Inventarisatie

In de inventarisatie fase is het van belang om inzicht te krijgen in de verwerkingen die vallen onder de WPG en de systemen die hierbij gebruikt worden. De reeds genoemde onderwerpen zijn hierbij een leidraad.

Stap 2: Analyseren verwerking

In deze fase wordt geïnventariseerd welke gegevens worden verwerkt en of deze verwerkingen voldoen aan de eisen van de WPG.

Voldoet de verwerking aan de eisen van:

- Vaststellen van de grondslag
- Dataminimalisatie
- Scheiding in categorieën

Stap 3: Analyseren van de processen

In deze fase kijken we naar de procesbeschrijvingen.

Voldoen de procesbeschrijvingen aan de eisen van:

- Bestaan (is er een beschrijving)
- Actualiteit (zijn de procedures nog actueel en is er bewijs van de review)
- Volledigheid (zijn alle onderwerpen beschreven)

Stap 4: Analyseren van het systeem

Voldoet het systeem aan de gestelde eisen van:

- Toegankelijkheid
- Functiescheiding
- Invoervalidatie
- Logging (toekomstige eis)
- Zijn de maatregelen getroffen op grond van een risico-inschatting (DPIA)

Stap 5: Gegevensuitwisseling

Indien er sprake is van gegevensuitwisseling van partijen dient dit:

- Gedocumenteerd te zijn
- Een rechtmatige grondslag te hebben

Stap 6: Sturing

Besteed de organisatie aandacht aan:

- Geheimhoudingsplicht van de medewerker
- Geheimhoudingsafspraken met eventuele verwerkers (verwerkersovereenkomsten)
- Kennis en bewustzijn bij de medewerker

Stap 7: Interne controle

Heeft de organisatie de volgende zaken op orde ten aanzien van de interne controle.

- Beschikt de organisatie over een intern controleplan.
- Worden bevindingen gecommuniceerd naar de verantwoordelijke.

Verantwoordelijkheden

De eindverantwoordelijkheid van de veiligheidstaken vallen onder de portefeuille van de burgemeester en die in deze daarmee wettelijk gezien de eindverantwoordelijke.

In het kader van de delegatie van verantwoordelijkheden ligt de verantwoordelijkheid bij het management.

De applicatie beheerders zijn verantwoordelijk voor het uitvoeren van het informatiebeveiligingsbeleid. Dat houdt in deze in het uitvoeren van autorisatiebeheer, het instellen van de logging.

De proceseigenaar is verantwoordelijk voor het opstellen en actueel houden van de procedures en het inrichten van een systeem van interne controle op de naleving van de procedures.

De FG heeft een adviserende en controlerende taak. Middels deze nota geef ik advies over de voorbereiding en wanneer de werkzaamheden zijn uitgevoerd volgt een controle. De FG mag geen uitvoerende taken hebben omdat er anders geen sprake meer is van een objectieve interne audit.

De CISO heeft dezelfde rol als de FG. De CISO geeft advies over de te treffen beveiligingsmaatregelen.

Voor vragen en opmerkingen staan de FG en CISO uiteraard voor u klaar.

De planning

We moeten er in deze van uit gaan dat nog niet alles al op orde is en dat we nog niet auditgereed zijn. Daarom hebben we in deze planning ook rekening gehouden met extra stappen.

Stap 1, 2 en 5: In deze stappen stellen we feitelijk de scope van het onderzoek vast. Naar welke processen en systemen moeten we gaan kijken. De organisatie zou op grond van het verwerkingsregister deze stappen eenvoudig moeten kunnen zetten. Let specifiek even op de eventuele koppelingen tussen systemen.
Reken hier veiligheidshalve 2 weken doorlooptijd voor.

Stap 3 en 4: In deze stappen wordt gekeken naar de aanwezigheid van systeeminstellingen en procesbeschrijvingen. Wanneer de instellingen niet goed staan moet worden beoordeeld of het systeem de mogelijkheden heeft om te voldoen aan de eisen. Zo niet dan moet contact worden opgenomen met de leverancier van het systeem om te bekijken wat de mogelijkheden zijn om toch te gaan voldoen aan de eisen.

In de Wpg staan een aantal eisen over het op orde hebben van procesbeschrijvingen. De procedures dienen te worden beoordeeld op volledigheid, juistheid en actualiteit. Wanneer de procesbeschrijvingen niet bestaan of niet voldoen aan de kwaliteitseisen dan dient dit gerepareerd te worden.

Reken voor deze fase een maand doorlooptijd.

Stap 5: Kijk goed naar de structurele en incidentele gegevensuitwisseling. Het moet bij de beheerders van de informatie bekend zijn wat de rechtmatige grondslagen zijn om gegevens te mogen delen. Daarnaast moet er een grondslag zijn voor de eventuele automatische gegevensverstrekking.

De inventarisatie is al gedaan samen met stap 1 en 2 en de procesmatige kant kan in een week.

Stap 6: De mens is ondanks het feit dat de processen een hoge mate van automatisering plaatsvinden nog altijd de belangrijkste factor. De technische maatregelen voorkomen niet alles en recente incidenten hebben aangetoond dat kennis en bewustzijn erg belangrijk zijn. Kijk direct ook naar de logging en de logcontrole. Ondanks dat dit een toekomstige eis is kan je vanuit de logging wel bepaald gedraag waarnemen. Recente incidenten hebben aangetoond dat dit heel belangrijk is.

Reken hier een doorlooptijd van 2 weken.

Stap 7: Een interne audit is in feite een 2e lijns interne controle wat inhoud dat er een controle plaats gaat vinden op de reeds getroffen beheersingsmaatregelen. Vanuit de proceseigenaar dient er dan ook al aandacht besteed te zijn aan interne controlemaatregelen die betrekking hebben op:

- Correcte instellingen van het systeem.
    - Autorisaties;
    - Functiescheiding;
    - Invoercontrole;
    - Consistentie van de data;
    - Scheiding in categorieën conform de wettelijke bepalingen.
- Controle op de procesbeschrijving.
- Controle op de naleving van de procesbeschrijvingen.
- Controle op de gegevensverwerking.
- Controle op de logging.

Deze controles dienen periodiek te worden uitgevoerd.

De controles moeten betrekking hebben op een periode van 3 maanden voordat deze vanuit de interne audit bekeken kunnen worden.

Overzicht van maatregelen

Nr	Onderwerp	Maatregelen
1	Inventarisatie van gegevensverwerkingen.	De verantwoordelijke houdt een register van verwerkingen bij. Er is een procedure opgesteld inzake het bijhouden en periodiek controleren van het register.
2	Inventarisatie van gegevensverwerkingen.	Vastleggen en bewaken van bewaartermijnen. Bewijs van vernietiging. Controle op de tijdige vernietiging.
3	Inventarisatie van gegevensverwerkingen.	De organisatie dient een inventarisatie uit te voeren op de structurele gegevensuitwisseling. De organisatie dient te borgen dat informatie uitwisseling met andere partijen zowel intern als extern alleen maar worden toegestaan wanneer is een wettelijke grondslag voor is.
4	Governance	De organisatie heeft een privacy-officer aangewezen. De privacy-officer houdt bij wat de verbeterpunten zijn die nog aandacht behoeven.
4	Governance	Er is een FG aangewezen. De FG is aangemeld bij de AP.
5	Compliance	De procesbeschrijvingen dienen te borgen dat alleen noodzakelijke gegevens worden verwerkt (data-minimalisatie).
6	Risk	DPIA die inzicht geeft in de aard van de gegevens die verwerkt worden en de noodzakelijkheid daarvan.
6	Risk	Er dient een classificatie te worden uitgevoerd om het niveau van bescherming te bepalen. Er dient een risicoanalyse / DPIA te worden uitgevoerd welke inzicht geeft in getroffen en genomen maatregelen. Eventuele tekortkomingen worden in een verbeterplan uitgewerkt. Interne controles en audits worden gepland.
7	Verwerken van informatie	Er dienen werkinstructies te zijn voor de verwerking van bijzondere persoonsgegevens.
7	Verwerken van informatie	Er dienen werkinstructies te zijn voor het onderscheid in de verschillende categorieën van betrokkenen.
8	Gegevensverwerking	Er zijn werkinstructie opgesteld ten behoeve van de juiste en volledige verwerking van de politiegegevens. Maatregelen in het systeem die fouten in de verwerking van gegevens voorkomen (invoer validatie en koppelingen met andere systemen zoals de BRP/GBA-V). Er zijn werkinstructies inzake de tijdige vernietiging van politiegegevens. Er zijn instructies inzake het vastleggen van feiten en persoonlijke oordelen. Het onderscheid tussen beiden dient duidelijk te zijn. Procedure inzake het informeren van een betrokkene. Procedure rectificatie van gegevens.
9	Autorisatie	Er dient een autorisatiematrix te zijn opgesteld welke inzicht geeft in de rollen en bevoegdheden in het systeem.

Nr	Onderwerp	Maatregelen
		Er dienen procedures te zijn opgesteld inzake het beheren van autorisaties. Er dient een periodieke controle plaats te vinden op de autorisaties. Er dient een beschrijving te zijn van de toegangsbeveiliging (wachtwoordbeleid- 2-factor instellingen etc.)
11	Incidentmanagement	Er is een procedure opgesteld inzake het melden van datalekken. Datalekken worden geregistreerd en gemonitord op afhandeling. De procedure gaat in op het melden van een datalek bij de toezichthouder. De procedure gaat in op het informeren van de betrokkene. De oorzaak van een datalek wordt onderzocht en indien nodig worden aanvullende maatregelen getroffen.
10	Gegevensverwerking	Indien er sprake is van geautomatiseerd vergelijken van data dient dit vastgelegd te zijn in een werkinstructie. Indien gegevens in combinatie met elkaar worden gebruikt dient dit vastgelegd te zijn in een werkinstructie. Er dient vastgelegd te zijn wie inzicht heeft in deze specifieke verwerkingen van gegevens. Er dient logging plaats te vinden op deze activiteiten.
12	Rechten van de betrokkene	Procedure inzagerecht Procedure rectificatie Procedure gegevenswissing Verzoeken van de betrokkene worden geregistreerd en gemonitord op tijdige afhandeling.
13	Afspraken met derden	Er is een procedure voor het opstellen van verwerkersovereenkomsten. Er is een overzicht van verwerkers en verwerkingen. Er is met alle verwerkers een verwerkingsovereenkomst afgesloten. Er is een overzicht van incidenten bij verwerkers.
14	Logging en monitoring	Er is een proces ingericht ten aanzien van het inrichten van logging. De logging dient periodiek te worden geanalyseerd. Er wordt een rapportage opgesteld om de verantwoordelijke te informeren over de bevindingen.
15	Personeel	Er wordt een geheimhoudingsafspraak gemaakt met de medewerkers. Er is een werkinstructie inzake de geheimhouding. Er wordt intern aandacht besteed aan het uitdragen van informatiebeveiliging en privacybescherming. Er is een sanctiebeleid opgesteld.
16	Naleving	controleren van het register (zie 1) Controleren bewaartermijnen en tijdige vernietiging (zie 2). Controle op de dataminimalisatie (zie 5) Controle op de actualiteit van de werkinstructies en procedures (zie 7,8,11,12 en 13). Controle op het incidentenbeheer en datalekken (zie 11 en 13).