BKBO

Bureau voor Kwaliteitsborging
bij de Overheid

Interne audit Wpg Heusden
versie 1.0 d.d. 2 december 2022 rapport BKBO/220623-2/IWPG

Agenda

1. **Introductie**
2. Doel van de audit
3. Object van onderzoek
4. Doorlooptijd van de interne audit
5. Onderzoeksinstrumenten
6. Resultaten
7. Verspreidingskring

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Introductie (1)

BKBO bv

www.bkbo.nl info@bkbo.nl 073 – 211 03 37

Productportfolio:

- ✓ DigiD en ENSIA assessments
- ✓ Wpg privacy audits
- ✓ IT audits
- ✓ TPM's leveranciers
- ✓ BIO audits
- ✓ ITIL®, BISL® en SSC audits
- ✓ VIPP audits
- ✓ ISAE 3402 Type I en Type II
- ✓ Privacy Assessments (keurmerk Privacy)

Marktsegment: overheid en zorg

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Introductie (2)

Betrokkenen BKBO bv

Felix IJpelaar
- Contactpersoon
- Bestuderen bewijsstukken
- Uitvoeren interviews
- Verslaglegging
- Opstellen rapportages
- Vbr oordeelsvorming en aanbevelingen
- Bespreking en presentatie

René IJpelaar (lead auditor, RE)
- Bestuderen bewijstukken
- Review concept rapportage

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie
2. **Doel van de audit**
3. Object van onderzoek
4. Doorlooptijd van de interne audit
5. Onderzoeksinstrumenten
6. Resultaten
7. Verspreidingskring

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Doel van de interne audit (1)

- Het beoordelen van de compliancy met de Wpg
- Daarmee uitvoering geven aan artikel 3 van de Regeling periodieke audit politie gegevens

- Deze interne audit is uitgevoerd als nulmeting (d.w.z. alle Wpg verwerkingen zijn meegenomen en de compliancy met de gehele wet)
- Let op! De interne audit moet jaarlijks worden uitgevoerd

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Doel van de interne audit (2)

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

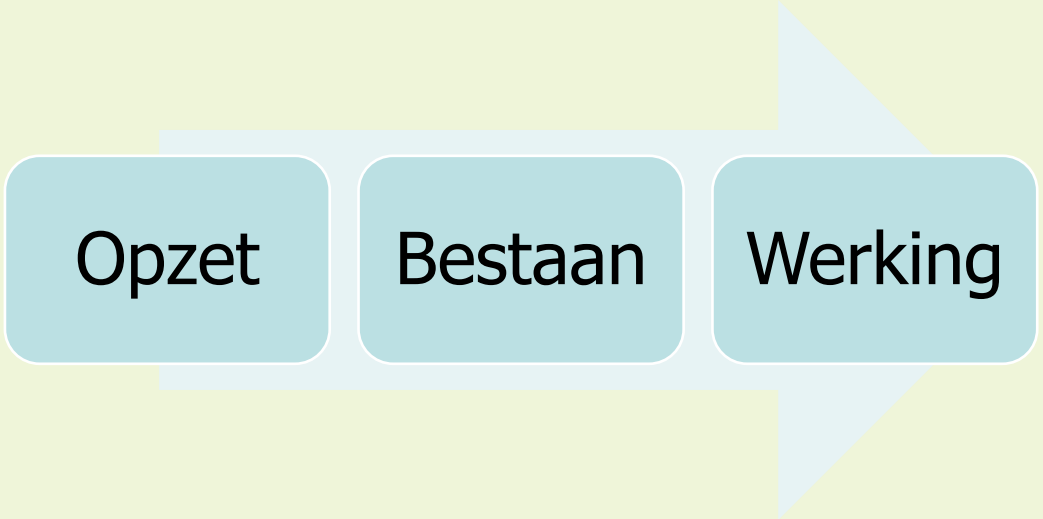
Agenda

1. Introductie
2. Doel van de audit
3. **Object van onderzoek**
4. Doorlooptijd van de interne audit
5. Onderzoeksinstrumenten
6. Beveiliging interne audit informatie
7. Resultaten
8. Verspreidingskring

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Object van onderzoek (1)

- De compliancy met de hele Wpg is beoordeeld → 0-meting
- Beoordeling vindt plaats op:



BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Object van onderzoek (2)

Domein	Van toepassing
I Openbare ruimte	Ja
II Milieu, welzijn en infrastructuur	Nee
III Onderwijs	Ja
IV Openbaar vervoer	Nee
V Werk, inkomen en zorg	Nee
VI Generieke opsporing	Nee

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Object van onderzoek (3)

Domein I:

- Sigmax met GITC TPM
- Office on premise zonder TPM
- Zaaksysteem zonder TPM

Domein III:

- Metaobjects met TPM
- Office on premise zonder TPM
- Zaaksysteem zonder TPM

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie
2. Doel van de audit
3. Object van onderzoek
4. **Onderzoeksperiode**
5. Onderzoeksinstrumenten
6. Beveiliging interne audit informatie
7. Resultaten
8. Verspreidingskring

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Onderzoeksperiode

Controle op de “werking” van de beheersmaatregelen:

- Onderzoeksperiode vanaf 1 januari t/m 31 december 2021
- Verslagperiode vanaf 9 maart 2019 t/m 31 december 2021 (alleen voor wat betreft de toezichtmaatregelen)

- De toezichtmaatregelen hebben betrekking op de volgende 6 normen:
  2. Doelbinding
  3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst
  4. Juistheid en volledigheid politiegegevens
  28. Logging
  29. Audit
  31. Functionaris voor Gegevensbescherming

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie
2. Doel van de audit
3. Object van onderzoek
4. Doorlooptijd van de interne audit
5. **Onderzoeksinstrumenten**
6. Resultaten
7. Verspreidingskring

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Onderzoeksinstrumenten

Toetsingsprocedure	Omschrijving
Documentatieonderzoek	Het inwinnen van inlichtingen bestaat uit het voorafgaand opvragen van gegevens door de auditor. De documentatie wordt verwerkt conform de Documentatierichtlijn van NOREA.
Houden van interviews	Het interviewen van medewerkers door de auditor die, naar het oordeel van de auditor relevante informatie kunnen geven, om inzicht in het systeem van de serviceorganisatie te verkrijgen, met inbegrip van de effectiviteit van de interne beheersmaatregelen, de risico's, de afbakening van de scope, de interne auditfunctie.
Inspectie	Het inspecteren van documenten, rapportages, uitgeprinte en elektronische vastleggingen ten behoeve van de verwerking van transacties.
Waarneming	Het observeren van activiteiten en het volgen van de handelingen van de betrokken medewerkers bij een proces of procedure. Veelal komt dit neer op het herhalen van de uitvoering van de interne beheersmaatregel dan wel het tonen van schermprints

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

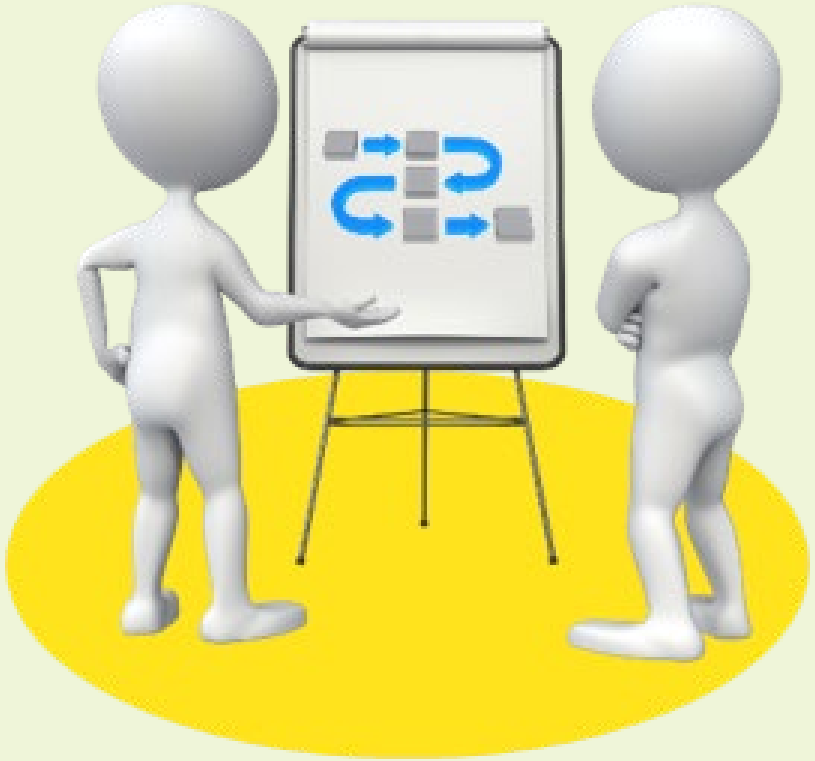
1. Introductie
2. Doel van de audit
3. Object van onderzoek
4. Doorlooptijd van de interne audit
5. Onderzoeksinstrumenten
6. **Resultaten**
7. Verspreidingskring

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Resultaten

- De rapportage bevat minimaal een beschrijving;
  - van de interne audit gevolgde werkwijze
  - van de resultaten van de interne audit
  - van het oordeel en de aanbevelingen

  Na afronding van de interne audit wordt de rapportage onverwijld aangeboden aan de verantwoordelijke



BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Legenda

normen	Conclusie		
	O	B	W
NORM 1 TOT MET 31			

Diepgang:

- O = opzet
- B = bestaan
- W = werking

Kleuren:

- Groen = de beheersmaatregelen zijn op afdoende wijze opgezet en hebben effectief gewerkt tijdens de onderzoeks/verslagperiode
- Oranje = de beheersmaatregelen zijn niet volledig op afdoende wijze opgezet, of hebben niet volledig effectief gewerkt
- Rood = de beheersmaatregelen zijn niet op afdoende wijze opgezet of hebben niet effectief gewerkt
- Grijs = de beheersmaatregelen zijn niet beoordeeld

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Samenvatting resultaten (1)

1e audit op de verwerking van politiegegevens. We hebben gekeken naar de opzet, bestaan en werking van de privacymaatregelen

Algemene bevindingen zijn:

- Werkprocessen en uitwerking in de praktijk sluiten onvoldoende aan bij de juridische vereisten vanuit de Wpg. I
- Medewerkers zijn betrokken en handelen zorgvuldig bij het verwerken van politiegegevens
- Op onderdelen wordt al wel conform de Wpg gewerkt
- Er is te weinig beschreven (opzet) waardoor niet kan worden gegarandeerd dat elke boa in dezelfde situatie hetzelfde zou handelen
- Vaak ontbreekt de vastlegging in beleid, procedures, richtlijnen en/of werkinstructies.
- Privacybeleid en verwerkingsregister nog af te stemmen op de Wpg
- Toezicht FG op de Wpg moet worden versterkt

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Samenvatting resultaten (1)

DOMEINSPECIFIEKE BEVINDINGEN

- Werkprocedures en instructies voor de Wpg verwerkingen ontbreken
- Er worden systemen gebruikt die niet zijn toegerust op de Wpg (scheiding Wpg en AVG gegevens, ander bewaarbeleid, logging etc)
- Autorisatieproces inrichten

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Samenvatting resultaten (2)

- Zie voor domein I bijlage 1a
- Zie voor domein III bijlage 1b
- De domeinen II, IV, V en VI zijn niet van toepassing
- Zie bijlage 2. Dit betreft de beoordeling van de “General IT Controls”:
  - GITC1: wijzigingsbeheer
  - GITC2: logische toegangsbeheer
  - GITC3: patchbeheer
  - GITC4: cryptografie
  - GITC5: pentesten

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Dwingende aanbevelingen

- Deze moeten worden opgevolgd om aan de norm te kunnen voldoen.
- We hebben geen verdere prioritering aangebracht aangezien ze allemaal moeten worden opgevolgd om aan de Wpg te voldoen.
- Zie ook separate bijlagen 1 en 2
- Tip! Onze “dwingende” aanbevelingen vormen samen met uw realisatieplanning, actiehouder en uw eigen prioritering uw wettelijk verplichte verbeterplan

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Dwingende aanbevelingen

- De Wpg vereist dat alle bestanden waarin politiegegevens opgeslagen worden, gescheiden zijn van andere gegevensbestanden. Draag zorg voor deze scheiding, identificeer en documenteer daarom voor alle Wpg-verwerkingen, waar u als verwerkingsverantwoordelijke verantwoordelijk voor bent, in alle bijbehorende informatiesystemen de bestanden met politiegegevens (opzet).
- Zorg dat politiegegevens alleen worden verwerkt in politiesystemen die van een Wpg keurmerk -dat wil zeggen een Wpg TPM van een RE- zijn voorzien. Bouw het gebruik van andere systemen zo snel mogelijk af.

Dwingende aanbevelingen

- Er is geen Wpg-privacybeleid waarin de doelbinding is vastgelegd. Neem in uw privacybeleid alsnog de Wpg voorschriften op (opzet).
- Draag ervoor zorg dat de werkinstructies/procedures ook daadwerkelijk aantoonbaar worden gevolgd (bestaan).
- **Uw FG is benoemd in het kader van het toezicht op de AVG verwerkingen. U zou ook het toezicht moeten gaan oppakken op Wpg verwerkingen. Dit betekent dat de verwerkingsverantwoordelijke beslissingen moet nemen over de gevolgen hiervan zoals capaciteitsbeslag, benodigde opleiding, ontslagbescherming, governance, achterstallig onderhoud van verwerkingsregister en dpia's evenals de wenselijkheid van implementatie van verbijzonderde interne controle en audits (bestaan).**
- **Er is geen aantoonbaar toezicht gehouden op de doelbinding tijdens de gehele verslagperiode (TZM). Zorg ervoor dat dit toezicht jaarlijks aantoonbaar wordt uitgevoerd (bestaan en werking).**

Dwingende aanbevelingen

- Zorg voor procedures waarbij als er onjuiste gegevens zijn verstrekt, de ontvanger daarvan meteen op de hoogte wordt gesteld en zodra bekend is wat de juiste gegevens zijn, de ontvanger de juiste gegevens krijgt verstrekt (opzet).

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Dwingende aanbevelingen

- Zorg ervoor dat u uw systeem periodiek test en evalueert om na te gaan in hoeverre de technische en organisatorische maatregelen doeltreffend zijn (bestaan en werking).
- Implementeer passende technische en organisatorische maatregelen om "privacy by default" zowel in de informatiesystemen als in de administratieve processen te bewerkstelligen.
- Stel vast voor alle Wpg-verwerkingen of er sprake is van een hoog privacy risico, en voer voor de hoog privacy risico-verwerkingen een DPIA uit (bestaan).
- Stel aan de hand van het Wpg-verwerkingenregister vast of voor alle relevante verwerkingen DPIA's zijn opgesteld (werking).

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Dwingende aanbevelingen

- Controleer periodiek of het verwerken van bijzondere persoonsgegevens wordt beperkt tot het onvermijdelijke (werking).
- Richt een adequaat toegangsbeheerproces voor alle systemen waar politiegegevens worden verwerkt, waarmee gewaarborgd wordt dat alleen geautoriseerde personen toegang krijgen tot de applicatie en dat toegekende autorisaties regelmatig worden geëvalueerd op rechtmatigheid. Deze procedure heeft een eigenaar, is voorzien van een datum en versienummer, is actueel en is tenslotte op het juiste niveau geaccordeerd.
- Draag zorg voor een aantoonbare jaarlijkse controle op de autorisaties (bestaan en werking).

Dwingende aanbevelingen

- Draag zorg voor een werkinstructie, waarin aandacht wordt gegeven aan verschillende categorieën van betrokkenen (verdachten, benadeelden en derden, zoals getuigen) bij het verwerken van politiegegevens (opzet).
- Controleer regelmatig of er onderscheid wordt gemaakt tussen verschillende categorieën van betrokken en wanneer zulks niet goed gebeurt, stuur dan meteen bij.

Dwingende aanbevelingen

Zorg ervoor dat er verwerkersovereenkomsten met uw verwerkers en/of subverwerkers worden overeengekomen, waarin het volgende is opgenomen:

- De verwerker moet inbreuken op de beveiliging melden aan de verwerkingsverantwoordelijke;
- Door de verwerker worden afdoende garanties verstrekt over toereikendheid van de geïmplementeerde technische en organisatorische maatregelen;
- Een andere partij wordt alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke;
- Indien dit het geval is, moeten de afspraken back-to-back worden doorgeleid;
- De verwerker en de verwerkingsverantwoordelijke moeten alle informatie ter beschikking stellen die nodig is om aantoonbaar te maken dat aan de verplichtingen in de verwerkersovereenkomst worden nageleefd.

Dwingende aanbevelingen

- Neem adequate maatregelen zodat artikel 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit/no hit).
- Bewaar- en vernietigingstermijnen worden niet gewaarborgd. Zorg ervoor dat de politiegegevens conform de wettelijke regels worden bewaard en vernietigd (bestaan).
- Er worden gegevens verwerkt op netwerkschijven. Van deze gegevens kunnen de bewaartermijnen niet worden gegarandeerd. Leg dus geen gegevens meer vast op netwerkschijven, maar alleen in het boa informatiesysteem.
- Registreer uw samenwerkingsverbanden waarmee een convenant is overeengekomen, op basis waarvan u politiegegevens verstrekt zorgvuldig en houdt dit ook steeds actueel
- Zorg dat de Bevoegd Functionaris aantoonbaar instemt met concrete verstrekkingen aan samenwerkingsverbanden (werking).

Dwingende aanbevelingen

- Zorg ervoor dat in het algemene inzage verzoek voor persoonsgegevens op de website ook de Wpg wordt opgenomen (opzet).
- Zorg voor een werkinstructie waarmee invulling wordt gegeven aan de informatieplicht aan de betrokkene en de uitzonderingen hierop c.q. vul de bestaande AVG instructies aan met de Wpg (opzet).
- Zorg voor een werkinstructie waarmee de rechten van de betrokkenen (behandelen van verzoeken, taken/verantwoordelijkheden, borgen en tijdigheid) worden geborgd (opzet).
- Zorg ervoor dat er aantoonbaar uitvoering wordt gegeven aan de informatieplicht aan de betrokkene en de uitzonderingen hierop (bestaan).
- Houdt structureel bij in een register, hoeveel inzageverzoeken, hoeveel correctieverzoeken, hoeveel geweigerde verzoeken et cetera er op jaarbasis zijn (werking).

Dwingende aanbevelingen

- Neem in het verwerkingsregister de Wpg-verwerkingen, die zijn geïnventariseerd in de nulmeting alsnog op (bestaan). Zie hiervoor tabel 1.
- Zorg dat kan worden aangetoond dat er wordt voldaan aan de documentatieplicht van de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid (inzage, rectificatie, verwijder verzoek) (bestaan en werking).
- Zorg dat logbestanden van alle gebruikte systemen afdoende zijn beschermd tegen (ongeautoriseerde) wijzigingen (bestaan en werking).
- Zorg dat het controleproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen (bestaan).
- Het datalekprotocol is toegesneden op de AVG, maar niet op de Wpg. Zorg dat het datalekprotocol wordt toegespitst op de Wpg (opzet).

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Aanbevelingen

- Deze aanbevelingen zijn vrijblijvend en hoeven niet te worden opgevolgd maar wij vinden het belangrijk dat we ze u melden in het licht van toekomstige ontwikkelingen.

- Deze aanbevelingen hebben we niet opgenomen in deze presentatie. Zie hiervoor de separate bijlagen

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Vervolg; het verbeterplan

- Onze dwingende aanbevelingen geordend per domein en verschil makend tussen algemene en sectorale maatregelen met een termijn, verantwoordelijk management, wie de acties gaat uitvoeren en evt het benodigde budget aan uren of externe kosten
- 3 maanden na de audit gereed.
- Moet naar verwerkingsverantwoordelijke
- Bij de externe audit rapportage maken we hier dan melding van en doen we een hercontrole

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie
2. Doel van de audit
3. Object van onderzoek
4. Doorlooptijd van de interne audit
5. Onderzoeksinstrumenten
6. Beveiliging interne audit informatie
7. Resultaten en vervolg
8. **Verspreidingskring**

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Verspreidingskring

Interne auditrapportage gaat naar:
- Management
- Respondenten
- Externe auditor
- NIET naar AP

Externe auditrapportage gaat naar:
- Management
- Respondenten
- WEL naar AP

Verbeterplan gaat naar:
- Management
- WEL naar BKBO bv
- NIET naar AP

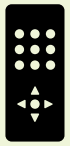
BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Vragen ?

BK
BO
Bureau voor Kwaliteitsborging
bij de Overheid

Meer informatie

Check onze website **www.bkbo.nl**



Bel 073 -211 03 37

Of stuur een mailtje met je vraag naar info@bkbo.nl

BK BO
Bureau voor Kwaliteitsborging bij de Overheid