# JAARRAPPORTAGE AVG/Wpg
# GEMEENTE KOGGENLAND 2023

*"De basis op orde."*

Functionaris gegevensbescherming

MAART 2024

# Inleiding

*Disclaimer: deze rapportage is geschreven vanuit het perspectief van de FG, onafhankelijk toezichthouder privacy van Koggenland. Hoewel deze beoordeling plaatsvindt op basis van objectieve data, het in deze rapportage geschetste beeld kan op onderdelen verschillen met dat van het college van B&W, dan wel Gemeenteraad.*

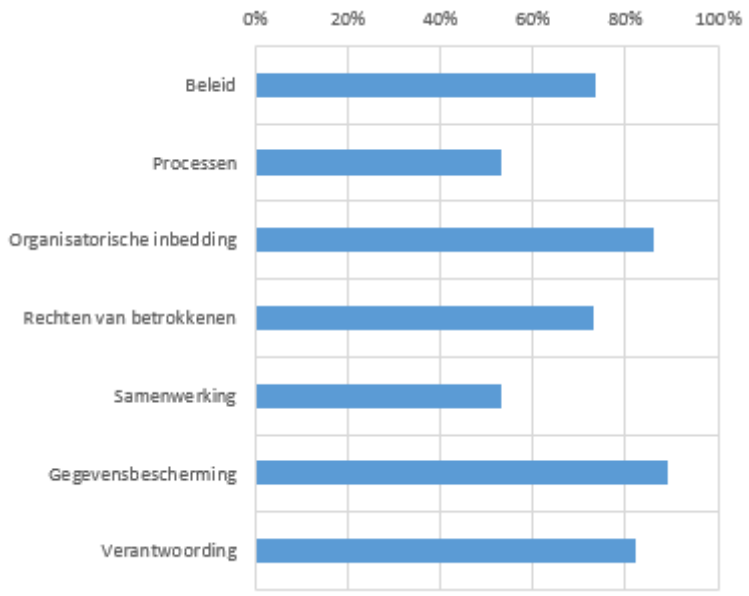
Het is goed om te constateren dat Koggenland in 2023 de basis nagenoeg op orde heeft gekregen. Na een periode van beperkte capaciteit heeft de gemeente in 2023 de (privacy-)rollen op een adequate wijze in de organisatie georganiseerd. Ook is nieuwe wetgeving zoals de Wet politiegegevens (Wpg) gesignaleerd en zijn meerdere beheersmaatregelen geïmplementeerd. Het tijdig uitvoeren, en aanleveren bij de Autoriteit Persoonsgegevens (AP), van de externe audit Wpg is hierbij een noemenswaardig gegeven. Hoewel uit het auditrapport nog meerdere actiepunten openstaan, Koggenland toont aan een plan te hebben om deze onvolkomenheden onder controle te krijgen.  Naar mening van de FG doet Koggenland hiermee recht aan het structurele werk dat het naleven van de Wpg, en AVG, inhoudt.

En dat is belangrijk. Want, onder verantwoordelijkheid van Koggenland (college van B&W en gemeenteraad) blijven namelijk een groot aantal gegevensverwerkingen plaats vinden. In een tijd waarin burgers zich, bijvoorbeeld door de toeslagenaffaire, meer bewust zijn geworden van een juiste omgang met persoonsgegevens, rust op Koggenland de verantwoordelijkheid om goed met persoonlijke gegevens om te blijven gaan. Een verantwoordelijkheid waar de gemeente doorlopend op gecontroleerd zal blijven worden. Door haar inwoners, haar medewerkers, maar ook door de Autoriteit Persoonsgegevens en de FG. Naar mening van de FG blijkt uit deze rapportage dat de gemeente goed op weg is, maar ook nog veel stappen te zetten heeft. Met name in het transparant maken van de gemeentelijke beleidskeuzes merkt de FG een belangrijk aandachtpunt op.

### Verantwoording

Qua objectiviteit steunt deze rapportage op het 'Borgingsproduct privacy 3.0' van de VNG/IBD. Conform deze leidraad is het gevoerde AVG-privacybeleid van de gemeente aan de hand van  196 beheersmaatregelen getoetst, zie bijlage 1 voor de managementsamenvatting. Voor wat betreft de Wpg wordt qua objectiviteit aangesloten op de meest recente resultaten van de externe en interne audits.

**Resultaat borgingsproduct 2023** ***(percentage van 196 beheersingsmaatregelen)***



INHOUDSOPGAVE

## Koggenland 2023

Naar mening van de FG voert een organisatie goed AVG-privacybeleid wanneer jaarlijks aandacht uitgaat naar een vijftal onderwerpen, te weten beleidvorming, bewustwording, monitoring, privacy-instrumenten en beveiligen. Een soortgelijke systematiek geldt voor de Wpg.

Hieronder licht de FG iedere privacy pijler toe met een korte beschrijving van het onderwerp, de resultaten uit het borgingsdocument AVG en een beschrijving van de werkzaamheden die in 2023 hebben plaatsgevonden. Iedere paragraaf wordt afgesloten met een advies van de FG.

## Beleidsvorming

Het privacybeleid is een kader waarin Koggenland aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Privacybeleid valt onder te verdelen in algemeen privacy beleid en sector- c.q. domein specifiek privacybeleid.

| Score borgingsproduct: | |
|---|---|
| 1. Beleid | 74% |
| 2. Processen | 53% |

Koggenland kent verschillende regeling die – in enige vorm - ingaan op de omgang met persoons- en politiegegevens. Meest in het oog springende, er is een algemeen privacybeleid dat kaders stelt aan de algehele omgang met persoonsgegevens. In positieve zin merkt de FG op het privacybeleid in 2023 opnieuw is vastgesteld. Ook is Wpg beleid vastgesteld.

Naar mening van de FG is het privacybeleid van Koggenland inhoudelijk juist en beschrijft het op een duidelijke wijze de kaders van gegevensverwerking binnen Koggenland. Daarbij dient wel te worden opgemerkt dat het privacybeleid ' *beleidsarm* 'is opgesteld. Bepalingen uit wetgeving zijn in beleid overgenomen, maar nog niet altijd uitgewerkt in concrete maatregelen. Wanneer het beleid stelt dat Koggenland '*transparant is over de omgang met persoonsgegevens*' dan wordt hiermee voldaan aan wet- en regelgeving. Voorgenoemde laat echter onbenoemd hoe Koggenland transparant is in de omgang met persoonsgegevens. Koggenland heeft namelijk wel degelijk keuzes gemaakt over hoe zij communiceert met haar inwoners over de omgang met persoonsgegevens. Zo communiceert Koggenland bijvoorbeeld richting haar inwoners via de privacyverklaring op de website. De privacyverklaring is laagdrempelig geschreven en voldoet daarmee aan de daaraan gestelde normen. Via de privacyverklaring worden burgers in de gelegenheid gesteld om - via verschillende wijzen - gebruik te maken van de beschikbare privacy rechten. Hierover merkt de FG op dat dit een – voor de inwoner – prettig leesbaar stuk is.

Gelet op bovenstaande wordt geadviseerd om bij de actualisatie van beleid de wettelijke bepalingen, zoals transparantie, doelbinding, bewaar- en vernietigingstermijnen, vertrouwelijkheid, meer concreet uit te werken. Hierbij stelt de FG als uitgangspunt dat inwoners minimaal eens in een procedure worden gewezen op de omgang met persoonsgegevens.

### Governance

Tevens wordt geadviseerd om het privacybeleid volledig in te richten op basis van het 'three lines of defence' model. Dit model gaat ervan uit dat eenieder verantwoordelijk is voor de juiste omgang met persoonsgegevens. In een gemeentelijke organisatie dient dit geïnterpreteerd te worden dat teams en afdelingen zelfstandig verantwoordelijk zijn voor de naleving van de privacy regels. Hierin worden zij

ondersteunt door de tweede lijn, de privacy officer(s) en informatiebeveiliger(s). Vanuit de derde lijn wordt vervolgens toezicht gehouden door de FG.

Naast organisatie brede uitgangspunten merkt de FG op dat het voor bepaalde domeinen en gegevensverwerkingen wenselijk is om aanvullende privacy regels te stellen. Als voorbeeld noemt de FG alle gegevensverwerkingen die samenhangen met de openbare orde en veiligheid, het sociaal domein en de omgang met personeelsgegevens. De FG adviseert om voor deze specifieke domeinen aanvullende privacy protocollen op te stellen. Tot slot wordt geadviseerd om de werkprocessen waarin persoonsgegevens worden verwerkt te beschrijven, met daarin aandacht voor de juiste omgang met persoonsgegevens. Juist op deze wijze worden de Koggenlandse keuzes op het gebied van privacy inzichtelijke en daardoor toetsbaar.

### Advies FG

Samenvattend wordt geadviseerd om:

- Bij toekomstige actualisatie van het privacybeleid de wettelijke bepalingen zoals transparantie, doelbinding, bewaar- en vernietigingstermijnen en vertrouwelijkheid meer concreet uit te werken;
- Het privacybeleid volledig in te rechten op basis van het ‘three lines of defence’ model;
- Te bepalen voor welke teams/domeinen het noodzakelijk is om aanvullende privacyregels op te stellen.

## Bewustwording

Om de privacy van inwoners te kunnen waarborgen is het van belang dat medewerkers zich goed bewust zijn van de kaders op het gebied van gegevensbescherming. Doordat eenieder een datalek kan veroorzaken is privacybeleid zo sterk als de zwakste schakel. In die hoedanigheid ondersteunt Koggenland haar medewerkers in het 'veilig werken' door in te zetten op bewustwording.

| Score borgingsproduct: | |
|---|---|
| 3. Organisatorische inbedding | 86% |

Voor een goede naleving en juiste uitvoering van de AVG, met andere woorden, voor een goede waarborging van de privacy van inwoners en medewerkers, dient aan een aantal voorwaarden te worden voldaan:

- Eenieder binnen de organisatie is op de hoogte van de beginselen van de AVG en het belang van privacy en voor zover nodig voor de functie strekt de kennis verder.
- De medewerkers beschikken over de vaardigheid én tijd om deze kennis ook bij hun werkzaamheden toe te passen.
- Medewerkers worden daarbij geholpen door privacybeleid en protocollen e.d.
- Werkprocessen en procedures zijn zodanig ingericht dat privacy daar een integraal onderdeel van uitmaakt.
- Door middel van een effectieve governancestructuur, het toewijzen van taken, verantwoordelijkheden en bevoegdheden wordt geborgd dan aan de voorgaande voorwaarden wordt voldaan.

Het rekening houden met privacy van de Koggenlandse inwoners is één van de belangrijkste randvoorwaarden waar Koggenland als gemeentelijke organisatie mee te maken heeft. Zeker omdat in nagenoeg ieder gemeentelijk proces persoonlijke gegevens van burgers worden gebruikt. In die hoedanigheid is het belangrijk dat medewerkers weten hoe zij op een juiste manier omgaan met persoonsgegevens.

Koggenland heeft in 2023 op meerdere momenten aandacht besteed aan bewustwording. Met berichten op het intranet is stilgestaan bij ontwikkelingen op het gebied van privacy- en informatiebeveiliging.
Ten aanzien van nieuw personeel geldt dat zij gedurende 2023 worden uitgenodigd voor een introductieprogramma. Onderdeel van het introductieprogramma is uitleg over privacy en informatiebeveiliging. Daarnaast wordt opmerkt dat de gemeente eind 2022 gestart is met een structurele e-learning privacy en informatiebeveiliging, ARDA. Deze e-learning is verplicht voor zowel nieuw als zittend personeel. Iedere maand wordt van (nagenoeg alle) medewerkers verwacht dat zij deelnemen met als doel de kans op datalekken zo klein mogelijk te houden en aandacht te houden voor een correcte omgang met persoonsgegevens. Tot slot helpt de gemeente haar medewerkers om veilig te werken door een veilig e-mailvoorziening aan te bieden. Hierdoor kan iedere medewerker, afhankelijk van de gevoeligheid van het bericht, op een simpele wijze extra aanvullende beveiligingsmaatregelen koppelen. Koggenland organiseert cursussen over het juiste en veilige gebruik van de veilig e-mailvoorziening.

De FG merkt – in het algemeen - op dat lering in herhaling zit. Het structureel, en in de gehele organisatie, aandacht hebben voor de juiste omgang met persoonsgegevens is essentieel om aan de privacy regels te voldoen. Maar ook om datalekken tijdig te herkennen en op te lossen.

<u>Bewustwordingsplan</u>
Hoewel Koggenland in 2023 wel degelijk aandacht heeft gehad oor de bewustwording op het gebied van privacy en informatiebeveiliging, Koggenland heeft niet uitgesproken wat haar ambities op dit punt zijn. Aangezien lering in herhaling zit is het bij uitstek belangrijk dat Koggenland aangeeft hoe '*hoog de lat moet liggen*'.

De FG adviseert dan ook om voor 2024 een bewustwordingsplan op stellen, met daarin concrete uitganspunten over de wijze waarop veilig werken wordt gestimuleerd. Specifiek voor Koggenland wordt geadviseerd om in ieder geval de volgende bewustwordingselementen uit te voeren in 2024:

- Gesprekscyclus privacy en informatiebeveiliging

Om als organisatie tijdig te kunnen sturen op risico's (en kansen) op het gebied van privacy en informatiebeveiliging wordt opgemerkt dat de organisatie op verschillende niveaus in gesprek moet zijn. Naar mening van de FG dient Koggenland dan ook strategische, tactische en operationele gesprekken in te richten met diverse stakeholders. Op strategisch niveau dient met de bestuurder te worden gesproken over de grote lijnen van het privacybeleid. Op tactisch niveau dient integraal met het lijnmanagement te worden gesproken over de organisatiebrede uitvoering van het privacybeleid. Tot slot dient op operationeel niveau te worden gesproken over de feitelijke ontwikkelingen in de (privacy-)organisatie.

Naar mening van de FG heeft Koggenland haar gesprekscyclus op een goede wijze ingericht. Geadviseerd wordt dan ook om deze in 2024 in stand te houden.

- Managementbewustwording privacy en informatiebeveiliging

De toon aan de top is bepalend in het realiseren van een organisatie die serieus omgaat met privacy en informatiebeveiliging. Kortom, het bestuur en management moeten uitstralen dat privacy en informatiebeveiliging belangrijk is, willen medewerkers het belangrijk vinden. Geadviseerd wordt om dit binnen het management te stimuleren.

### Advies FG

Samenvattend wordt geadviseerd om:

- Voor 2024 een bewustwordingsplan privacy en informatiebeveiliging op te stellen met daarin ruimte voor de gesprekscyclus en managementbewustwording.

## Monitoring

Aantoonbaar blijven voldoen aan privacy wet- en regelgeving brengt verschillende fases met zich mee. Na inventarisatie en implementatie is het van belang dat alles ook goed geregeld blijft. Om dit te waarborgen is sturing, FG-toezicht en evaluatie van belang.

| Score borgingsproduct: | |
|---|---|
| 7. Verantwoording | 68% |
| 4.5 websites en applicaties | 33% |
| 4.6 technische ondersteuning | 100% |
| 6.5 privacy incidenten en datalekken | 92% |

### Onderzoek FG

Naast deze jaarrapportage 2023 heeft de FG in 2023 een voortgangsrapportage opgesteld. Ook zijn naar aanleiding van actualiteiten onderzoeken uitvoert naar de werking van het privacybeleid binnen Koggenland. In 2024 voert de FG weer een volledig toezichts- en adviesplan uit.

### Privacy als standaard en bij ontwikkeling

De AVG verplicht organisatie tot de toepassing van het beginsel van ‘privacy by design’. Een definitie die tot doel heeft te duiden dat privacy in iedere ontwikkeling van een proces of (digitaal) systeem dient te worden meegenomen. Daarnaast verplicht het beginsel van ‘privacy by default’ tot het inrichten van processen en (digitale) systemen op zo’n wijze dat hij de privacy van betrokkenen maximaal beschermt.

Naar mening van de FG wordt met wisselend succes invulling gegeven aan ‘privacy by design’ en ‘privacy by design’. De FG merkt op dat de gemeente softwarematig nog te maken heeft met keuzes uit het verleden, waarbij na-inrichting lastig is of erg kostbaar. Daarentegen staat dat gemeente wel degelijk maatregelen dient te treffen om persoonsgegevens te beschermen. Denk hierbij aan het inrichten van autorisaties, op een need-to-know basis, maar ook het bijhouden van logging en het uitvoeren van loggingscontroles.

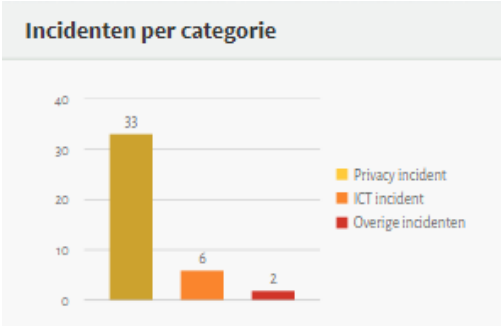
Het valt de FG op dat wanneer nieuwe diensten/software wordt aangekocht inkoopeisen op het gebied van privacy- en informatiebeveiliging worden meegegeven. Oftewel, de FG verwacht dat voorgenoemde principes de komende jaren duidelijk zichtbaar worden in de digitale systemen van Koggenland.

Daarbij merkt de FG op dat privacy één van de belangrijkste randvoorwaarden is in een gemeentelijke organisatie. Maar wel, een randvoorwaarde. Oftewel, privacy dient niet te worden gezien als struikelblok, maar als één van de lijnen om een sportveld heen. De FG adviseert dan ook om vraagstukken integraal te benaderen. Heel concreet, organiseer dat de disciplines informatiebeveiliging, informatiemanagement, archivering, data-analyse en IT integraal adviseren over de organisatie brede vraagstukken waar Koggenland mee te maken krijgt.

### Datalekken

Op basis van artikel 33 en 34 AVG en artikel 33a Wpg heeft Koggenland verschillende verplichtingen op het moment dat er zich een datalek of beveiligingsincident voordoet. Afhankelijk van het risico (verkeerd verstuurde brief of gehackt systeem) moet bijvoorbeeld de AP worden ingelicht of de betrokkene (inwoner) op de hoogte worden gesteld.

Koggenland heeft – net zoals iedere ander denkbare organisatie - datalekken en beveiligingsincidenten, zo ook in 2023. In de behandeling van datalekken wordt – in positieve zin – opgemerkt dat de gemeente een goed proces volgt in de afhandeling van incidenten. Conform vastgestelde procedures zijn bevoegde organen (Gemeenteraad, Burgemeester, College van B&W) geïnformeerd over de context en oplossingen van voorgedane datalekken.




### Advies FG

Samenvattend wordt geadviseerd om:

- Veranderingen in proces, en of ICT, integraal te benaderen. Heel concreet, organiseer dat de disciplines informatiebeveiliging, informatiemanagement, archivering, data-analyse en IT integraal adviseren over de organisatie brede vraagstukken waar Koggenland mee te maken krijgt.

## Privacy instrumenten

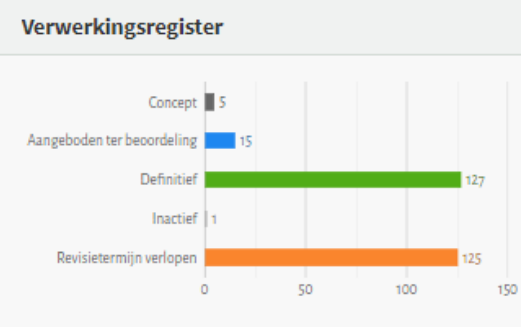
Privacywetgeving verplicht tot het toepassen van zogenoemde privacy instrumenten. Dit betreft het uitvoeren van specifieke privacy onderzoeken (DPIA's), het bijhouden van een actueel overzicht van gegevensverwerkingen en het maken van specifieke privacy afspraken met externe partijen. Daarnaast biedt privacy wetgeving aan betrokken personen de mogelijkheid om gebruik te maken van privacy rechten, zoals inzage, correctie en verwijdering.

| Score borgingsproduct: | |
|---|---|
| 2.2 Verwerkingsregsiter | 63% |
| 2.4 DPIA's | 30% |
| 4. Rechten van betrokkenen | 73% |
| 5. Samenwerkgin | 53% |

### Verwerkingsregister

Koggenland heeft veel verwerkingen van persoonsgegevens opgenomen in het verwerkingsregister. Voor Koggenland zou dit register één van de belangrijkste (wettelijke) controlemiddelen kunnen, en moeten, zijn ten aanzien van het gevoerde privacybeleid. Het verwerkingsregister maakt het mogelijk om zicht te houden op de omgang met persoonsgegevens per specifiek werkproces. Daarbij is Koggenland, op basis van de AVG en Wpg, verplicht om – te allen tijde - een volledig en actueel verwerkingsregister te hebben.

Gedurende 2023 is tijd gestoken om het register te actualiseren. Ook is een start gemaakt met het opzetten van een verwerkingsregister voor de Wpg. Dit is grotendeels gelukt. Aan het verwerkingsregister valt echter op dat de verantwoordelijkheden voor het beheer nog niet zijn belegd. Hierdoor is nog geen proces ingericht voor het daadwerkelijke beheer van het register. Hierdoor worden nieuwe/veranderende gegevensverwerkingen vaak niet tijdig in het verwerkingsregister opgenomen.




Geadviseerd wordt om de verantwoordelijkheid voor het beheer van het verwerkingsregister in de organisatie te beleggen (1), het register structureel te behoren (2) en een gedeelte van het verwerkingsregister – omwille van transparantie – in enige vorm openbaar te maken.

### DPIA (lees: verplicht privacy onderzoek)

In het privacybeleid geeft de gemeente aan dat risicoanalyses op het gebied van privacy (DPIA's) voor bepaalde processen uitgevoerd moeten worden. Echter, in 2023 zijn er geen DPIA's uitgevoerd. In die hoedanigheid heeft Koggenland zeer beperkt zicht op de privacy-risico's die zij mogelijk in haar risicovolle gegevensverwerkingen loopt. De FG overweegt hierover dat het uitvoeren van DPIA's geen keuze is, maar een wettelijke plicht op basis van de AVG en Wpg. Wél heeft Koggenland om de beleidsvrijheid om, binnen de kaders van de AP[1], aan te geven wélke gegevensverwerkingen als risicovol worden aangemerkt. Alleen op de risicovolle gegevensverwerkingen hoeft een DPIA te worden uitgevoerd.

De FG adviseert om zo snel als mogelijk te starten met het uitvoeren van DPIA's.

### Rechten van betrokkenen

Koggenland heeft in 2022 een goede verbetering doorgevoerd wat betreft het faciliteren van de privacy rechten van haar inwoners. Met de implementatie van DigiD formulieren is het voor inwoners mogelijk om op

[1] Autoriteit Persoonsgegevens, besluit lijst verplichte DPIA, 27 november 2019.

een laagdrempelige wijze inzage te krijgen in de eigen gegevens. In 2023 is Koggenland op een goede wijze omgegaan met de privacy vragen van haar inwoners.

### Privacy afspraken met externen (verwerkersovereenkomsten en privacy convenanten)

Koggenland werkt veel samen met externe partijen. Van de GGD, Politie tot commerciële partijen die de organisatie diensten of goederen leveren. In de uitvoering van deze samenwerkingen worden vaak persoonlijke gegevens van burgers en ambtenaren gebruikt. De AVG/Wpg stellen eisen aan de dergelijke samenwerkingen om een veilige omgang met persoonsgegevens te realiseren.

Zo mag alleen samengewerkt worden met partijen die aantoonbaar goed en veilig met persoonsgegevens kunnen omgaan. Op gemeentelijke niveau wordt hier bijvoorbeeld mee om gegaan door een ISO27001 informatiebeveiligingscertificaat verplicht te stellen in IT-aanbestedingen. Daarbij dient de gemeente privacy afspraken vast te leggen in de vorm van een verwerkersovereenkomst of een privacy convenant.

Over 2023 valt op dat er meer verwerkersovereenkomsten zijn gesloten dan in 2022. Dit getuigt dat de organisatie de collega's op het gebied van privacy beter beginnen te vinden bij het sluiten van contracten. In steeds meer aanbestedingen worden ook inkoopeisen op het gebied van privacy en informatiebeveiliging meegegeven.

### Advies FG

Samenvattend wordt geadviseerd om:

- het register van verwerkingsactiviteiten te actualiseren en in beheer te nemen;
- Phanmatig DPIA's uit te voeren op de risicovolle gegevensverwerking.

## Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de Koggenland passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.

| Score borgingsproduct: | | Opmerking |
|---|---|---|
| 6. Gegevensbescherming | 89% | Goed beveiligingbeleid<br>Logging is een uitdaging, maar in de maak<br>Goede risico-analyse gedaan. |

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de Koggenland passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Hierbij is naast de AVG, de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft alle technische- en organisatorische maatregelen die Koggenland te treffen heeft om te komen tot een veilige organisatie. Naleving van de BIO draagt dan ook direct bij aan naleving van de AVG.

In dit licht wordt er veel samengewerkt tussen de FG, de CISO en de privacy officer. Volledigheidshalve wordt verwezen naar de 'Jaarrapportage informatiebeveiliging 2023', opgesteld door de CISO. De FG steunt in zijn beoordeling op het gebied van privacy op de resultaten van het borgingsproduct, alsmede hetgeen beschreven in het verslag van de CISO, waarvan onderstaande infographic de managementsamenvatting is. Qua adviezen voor 2024 steunt de FG de adviezen van de CISO.

"*Op het gebied van de ENSIA heeft de gemeente een zelfevaluatie uitgevoerd, dan wel is geaudit door een externe auditor Duijnborgh Audit BV. Uit de audit komt naar voren dat de gemeente Koggenland in 2023 een goed resultaat heeft behaald betreffende het voldoen aan de verplicht gestelde onderstaande normen.*

*De resultaten ten aanzien van de Ensia verantwoording 2023 zijn: Compliant (voldoen aan wet- en regelgeving/ aanbevelingen):*

- *Basisregistratie Adressen en Gebouwen (BAG);*
- *Basisregistratie Grootschalige Topografie (BGT);*
- *Basisregistratie Ondergrond (BRO);*
- *De Basisregistratie Personen (BRP) en Reisdocumenten;*
- *Digitale persoonsidentificatie (DigiD);*
- *Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).*

*Uit de audit komt naar voren dat de gemeente Koggenland in 2023 een negatief resultaat heeft behaald betreffende het voldoen aan de verplicht gestelde onderstaand normen.*
*Niet compliant (niet voldoen aan wet- en regelgeving/ verbetermaatregelen):*

- *Baseline Informatiebeveiliging Overheid (BIO).*

*In de gemeente Koggenland is momenteel een uitvoeringsplan voor informatiebeveiliging van kracht, en er zijn financiële middelen beschikbaar gesteld om dit plan te ondersteunen. Ondanks deze positieve ontwikkelingen staat de gemeente voor de uitdaging om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO), zoals blijkt uit de huidige 'niet-compliant'-status.*
*Het bewustzijn van de samenhang tussen verschillende beveiligingsmaatregelen en het belang van een holistische benadering wordt benadrukt. Hoewel de BIO-vragenlijst in de ENSIA-verantwoording als leidraad dient, wordt erkend dat 'afvinken' geen garantie biedt voor absolute veiligheid.*

*Met een huidige implementatie van de BIO op 57%, staat Koggenland openlijk voor ruimte tot verbetering. De ambitieuze doelstelling om dit percentage in 2024 te verhogen tot meer dan 70% is niet alleen in lijn met strategische gemeentelijke informatiebeveiligingsdoelen, maar toont ook vastberadenheid in het streven naar digitale veerkracht. Diverse geplande acties, waaronder het versterken van bewustwording en deskundigheid onder medewerkers, verbetering van processen en procedures, verhoogde controle en monitoring, en intensivering van samenwerking met SSC DeSom, illustreren de vastbeslotenheid van Koggenland om informatiebeveiliging op hoog niveau te handhaven."*

## Wet politiegegevens (Wpg)

Vanaf 2019 geldt Wpg ook voor boa-werkgevers. Koggenland verricht boa werkzaamheden in twee domeinen, te weten:

- Domein 1: Openbare ruimte – zegge: alle opsporingstaken die raken aan de openbare orde en veiligheid
- Domein 3: Onderwijs: zegge: alle meldingen die horen bij verzuim op de Leerplichtwet
    - In dit domein werkt Koggenland samen met de gemeente Hoorn.

Ten aanzien van deze domeinen valt Koggenland onder de Wpg. De Wpg stelt regels aan hoe Koggenland om dient te gaan met persoonsgegevens die gebruikt worden voor de opsporing van strafbare feiten, de verwerking van politiegegevens. In afwijking van de AVG kent de Wpg een strenger auditregime. Conform de Regeling periodieke audit politiegegevens dient Koggenland zichzelf jaarlijks intern te auditen en eens per vier jaar dient Koggenland zich extern te laten auditen. De eerste externe audit diende Koggenland in 2021 uit te voeren. Daarnaast dient Koggenland, parallel aan de audits, de Wpg volledig in haar bedrijfsvoering te implementeren.

In 2023 constateerde de Autoriteit Persoonsgegevens dat de naleving van de Wpg bij veel boa-werkgevers nog niet op orde is[2]. De FG is van mening dat dit beeld voor Koggenland niet volledig van toepassing is. De Koggenland voldoet in afdoende mate (in opzet en bestaan) aan de normatiek van de politiegegevens. De FG merkt hierbij op dat Koggenland bij die enkele gemeenten zit dit in 2023 de Wpg voldoende op orde had. Een geweldige prestatie.

### Audits

Koggenland heeft een meerjaren auditplanning waardoor uitvoering wordt gegeven aan de verschillende Wpg-audits. Koggenland heeft ervoor gekozen om de uitvoering van alle wpg-audits extern te organiseren. De FG overweegt hierover dat hierdoor de onafhankelijkheid van de auditresultaten is gewaarborgd. Vanaf 2019 had Koggenland verschillende audits moeten uitvoeren. Koggenland heeft **niet** alle verplichte audits uitgevoerd, namelijk:

- Interne audit 2019: deze audit is **niet** uitgevoerd;
- Interne audit 2020: deze audit is **niet** uitgevoerd;
- Externe audit 2021: deze audit is **wel** uitgevoerd;
    - Hercontrole audit: deze audit wordt in februari 2024 **wel** uitgevoerd. *Ten tijde van oplevering van deze rapportage zal de hercontrole audit hoogstwaarschijnlijk zijn afgerond.*
- Interne audit 2022: deze audit is **wel** uitgevoerd;
- Interne audit 2023: deze audit wordt in 2024 **wel** uitgevoerd.

### Naleving

Tegenover het wettelijke auditregime staat de uitvoeringspraktijk, de dagelijkse gang van zaken. De FG steunt de opvattingen van het verbeterplan Wpg. Aan de boa's in Koggenland wordt opgemerkt dat zij zich, in de regel, goed bewust zijn van hun taken als toezichthouder en bijzonder opsporingsambtenaar. Het naleven van de Wpg, en wetgeving in zijn algemeen, is geen eenmalige exercitie, maar een continue proces. Daarbij merkt de FG op dat er sprake is van een beheersmatige situatie. Het Wpg project is in 2023 afgerond waarna de Wpg onderdeel is geworden van het reguliere werk De belangrijkste uitdaging zit, naar mening van de FG, in het doorlopend blijven voldoen aan de eigen processen en werkinstructies. De FG adviseert dan ook om de output van de jaarlijks audits als input voor het jaarplan, van het opvolgend jaar, te nemen.

### Advies

- Voer de hercontrole audit uit en lever deze aan bij de Autoriteit Persoonsgegevens.
- Voer de interne audit 2023 uit en zet eventuele bevindingen om in actiepunten

[2] Autoriteit Persoonsgegevens, veel boa-werkgevers voldoen niet aan verplichte Wpg-audit, 12 juni 2023.

## Bijlage 1: Managementsamenvatting borgingsproduct VNG/IBD

| | | |
|---|---|---|
| **Naam organisatie** | Gemeente Koggenland | |
| **Datum ingevuld** | 13 februari 2024 | |
| **Aantal beantwoord** | 149 van de 155 | |
| **Score** | 71% | |

| Par | Titel | Leeg | N.v.t | Beantwoord | Percentage |
|---|---|---|---|---|---|
| 1. | Beleid | 0 | 0 | 17 | 74% |
| 1.1 | Beleid vaststellen | 0 | 0 | 2 | 100% |
| 1.2 | Privacybeleid | 0 | 0 | 9 | 92% |
| 1.3 | Verantwoordelijkheden | 0 | 0 | 6 | 38% |
| 2. | Processen | 0 | 0 | 38 | 53% |
| 2.1 | Werkprocessen | 0 | 0 | 7 | 57% |
| 2.2 | Verwerkingsregister | 0 | 0 | 10 | 63% |
| 2.3 | Pre-DPIA's | 0 | 0 | 3 | 17% |
| 2.4 | DPIA's | 0 | 0 | 10 | 30% |
| 2.5 | Bewaar- en vernietigingsbeleid | 0 | 0 | 8 | 81% |
| 3. | Organisatorische inbedding | 0 | 0 | 20 | 86% |
| 3.1 | Privacyteam | 0 | 0 | 2 | 38% |
| 3.2 | Aanstelling, positie en taken FG | 0 | 0 | 11 | 98% |
| 3.3 | Informeren OR | 0 | 0 | 2 | 63% |
| 3.4 | Bewustwording | 0 | 0 | 5 | 90% |
| 4. | Rechten van betrokkenen | 0 | 6 | 24 | 73% |
| 4.1 | Recht op informatie | 0 | 0 | 5 | 50% |
| 4.2 | Processen rechten van betrokkenen | 0 | 1 | 8 | 97% |
| 4.3 | Toestemming | 0 | 0 | 4 | 56% |
| 4.4 | Geautomatiseerde individuele besluitvorming | 0 | 5 | 0 | 0% |
| 4.5 | Websites en applicaties | 0 | 0 | 3 | 33% |
| 4.6 | Technische ondersteuning | 0 | 0 | 4 | 100% |
| 5. | Samenwerking | 0 | 0 | 15 | 53% |
| 5.1 | AVG rollen | 0 | 0 | 8 | 72% |
| 5.2 | Gegevensverstrekking | 0 | 0 | 7 | 32% |
| 6. | Gegevensbescherming | 0 | 0 | 28 | 89% |
| 6.1 | Risico's | 0 | 0 | 2 | 100% |
| 6.2 | Gegevensbescherming door ontwerp | 0 | 0 | 2 | 88% |
| 6.3 | Gegevensbescherming door standaardinstellingen | 0 | 0 | 1 | 75% |
| 6.4 | Informatiebeveiliging | 0 | 0 | 10 | 85% |
| 6.5 | Privacyincidenten en datalekken | 0 | 0 | 13 | 92% |
| 7. | Verantwoording | 0 | 0 | 7 | 82% |
| 7.1 | Evaluatie naleving AVG | 0 | 0 | 4 | 94% |
| 7.2 | Evaluatie informatiebeveiliging | 0 | 0 | 2 | 50% |
| 7.3 | Rapportage | 0 | 0 | 1 | 100% |

# Bijlage 2: FG-controle (medio september 23)

**FG controle – formele verplichtingen AVG/Wpg 2023**
**Controle:** Register van verwerkingsactiviteiten (e.v. verwerkingsregister)
**Datum beoordeling:** 9 augustus 2023

| Beoordelingscriteria register van verwerkingsactiviteiten<br>Wettelijk kader: art. 30 AVG en artikel 31 D Wpg | | Kritische afwijking | Onvoldoende | Voldoende | Goed |
|---|---|---|---|---|---|
| | Beoordelingspunten | | | | |
| **Formele vereisten** | | | | | |
| 1.1 | Naam en contactgegevens verwerker en verwerkingsverantwoordelijken | | | | X |
| 1.2 | Naam en contactgegevens FG verwerker en verwerkingsverantwoordelijken | | | | X |
| 1.3 | (Sub-)verwerkingsdoeleinden | | | | X |
| 1.4 | Categorieën van betrokkenen | | | | X |
| 1.5 | Ontvangers en derde partijen | | | | X |
| 1.6 | Beschrijving beveiligingsmaatregelen | | | | X |
| 1.7 | Bewaar- en vernietigingstermijnen | | | | X |
| 1.8 | Doorgifte aan een derde land of internationale organisatie | | | | X |
| **Inhoudelijke vereisten** | | | | | |
| 1.9 | Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld | | | X | |
| 1.10 | Het register is volledig | | X | | |
| 1.11 | Het register is actueel | X | | | |
| 1.12 | Het register is intern toegankelijk | | | X | |
| 1.13 | Het register is voor de betrokkene toegankelijk | X | | | |

Opmerkingen FG
Het verwerkingsregister is voor het eerst opgesteld in 2018. Sindsdien is er veel tijd gestoken in het vullen en onderhouden van het verwerkingsregister. Echter, uit controle blijkt dat er sinds december 2023 geen mutaties meer op het verwerkingsregister hebben plaatsgevonden. Hieruit dient geconcludeerd te worden dat het verwerkingsregister in huidige vorm niet actueel is.

**Advies**
Naar mening van de FG wijkt het verwerkingsregister af van de wettelijke norm. Door deze afwijking heeft de gemeente onvoldoende inzicht (en daarmee grip) op de gegevensverwerkingen die in de organisatie plaatsvinden.

De gemeente wordt dan ook geadviseerd om:

- het verwerkingsregister te actualiseren.

- Het actualiseren van het gehele verwerkingsregister is – gelet op de hoeveelheid gemeentelijke gegevensverwerkingen - een groot project. Een project dat veel onderzoek en afstemming vraagt met meerdere stakeholders. In dit licht wordt geadviseerd om de actualisatie van het verwerkingsregister procesmatig aan te vliegen en voldoende middelen beschikbaar te stellen.

- een procesbeschrijving op te stellen voor het onderhouden van het verwerkingsregister.
  **Tip**: Neem in het proces een bepaalde periodiek op waarmee het verwerkingsregister door, een verantwoordelijk manager, dient te worden gecontroleerd en geaccordeerd.

Inhoudelijk over het verwerkingsregister in huidige vorm:

- Maak een overzicht van de externe partijen met wie, in welke gegevensverwerking, wordt samengewerkt. Inventariseer op basis van dit overzicht met welke partijen al privacy afspraken gemaakt (en welke niet).
- Maak in het verwerkingsregister, op eenduidige wijze, inzichtelijk wanneer er wel/niet sprake is van internationale doorgifte (en op welk adequaatheidsbesluit dit indien van toepassing berust).
- Beschrijf op eenduidige wijze, conform de Archiefwet, de bewaar- en vernietigingstermijnen

**Controle:** Procedure datalekken
**Datum beoordeling**: 11 september 2023

| Beoordelingscriteria procedure datalekken Wettelijk kader: art. 33 juncto 34 AVG, artikel 33a Wpg | | Ontbreekt | Onvoldoende | Voldoende | Goed |
|---|---|---|---|---|---|
| | Beoordelingspunten | | | | |
| **Formele vereisten** | | | | | |
| 1.1 | Feiten over de inbreuk in verband met persoonsgegevens | | | | X |
| 1.2 | De gevolgen van het datalek | | | | X |
| 1.3 | Genomen corrigerende en preventieve maatregelen | | | | X |
| 1.4 | Melding aan de betrokkene | | | | X |
| 1.5 | Melding aan de AP | | | | X |
| 1.6 | Betrokkenheid FG | | | | X |
| 1.7 | Procesbeschrijving beveiligingsincidenten en datalekken | | | | X |
| **Inhoudelijke vereisten** | | | | | |
| 1.7 | Het register van datalekken is volledig | | | | X |
| 1.8 | Het register van datalekken is actueel | | | | X |

Opmerkingen FG
De gemeente voldoet in opzet, bestaan en werking aan de eisen die de AVG stelt aan een datalekkenprocedure stelt. Echter, deze dient nog van toepassing te worden verklaard op de Wet politiegegevens. Hoewel deze datalekken daar al wel in worden bijhouden, formeel is het nog het datalekkenregister op basis van de AVG.

**Controle:** Beoordeling externe gegevensdeling
**Datum:** 11 september 2023

| Beoordelingscriteria externe gegevensdeling Wettelijk kader: art. 26 jo. 28 jo. 29 AVG en artikel 6c Wpg | | Ontbreekt | Onvoldoende | Voldoende | Goed |
|---|---|---|---|---|---|
| | Beoordelingspunten | | | | |
| **Formele vereisten** | | | | | |
| 1.1 | De verwerkingen door verwerkers worden geregeld in een overeenkomst of andere rechtshandeling | | | X | |
| 1.2 | De gezamenlijke verwerkingsverantwoordelijken stellen op transparante wijze hun respectieve verantwoordelijkheden vast | | | X | |
| 1.3 | Met iedere externe partij die persoonsgegevens voor het College verwerkt zijn privacy afspraken gemaakt | | X | | |
| **Inhoudelijke vereisten** | | | | | |
| 1.4 | Onderwerp | | | X | |
| 1.5 | Duur | | | X | |
| 1.6 | Aard en het doel van de verwerking | | | X | |
| 1.7 | Soort persoonsgegevens | | | X | |
| 1.8 | Categorieën van betrokkenen | | | X | |
| 1.9 | Rechten en verplichtingen verwerkingsverantwoordelijke | | | X | |

Opmerkingen FG:
De gemeente dient met iedere partijen, waarmee persoonsgegevens worden uitgewisseld, privacy afspraken te maken/hebben. De gemeente heeft sinds 2018 – ten tijde van de komst van de AVG – gedeeltelijk inzichtelijk gemaakt met welke partijen zij wel/niet privacy afspraken heeft gemaakt of moet maken. Echter, dit overzicht was niet volledig. Hoewel er anno 2023 ad hoc verwerkersovereenkomsten worden gesloten, de gemeente heeft nog niet volledig inzichtelijk in hoeverre zij aan haar wettelijke verplichting op dit punt voldoet.

Geadviseerd wordt om:
- te inventariseren met welke externe partijen al wel verwerkersovereenkomsten en/of privacy convenanten zijn gesloten;
- te inventariseren met welke externe partijen nog geen privacy afspraken zijn gemaakt met als doel deze alsnog te maken;
- het register van verwerkingsactiviteiten hierop aan te passen;
- een actieve rol te nemen in het inkoopproces en het IT-wijzigingsproces. Door privacy in een eerder stadium een rol te geven bij nieuwe/veranderende ontwikkelingen wordt het beter mogelijk om privacy by design/default te borgen en privacy afspraken tijdig te maken

**Controle**: Uitvoeren privacy-onderzoeken
**Datum:** 30 augustus 2023

| Beoordelingscriteria DPIA<br>Wettelijk kader: artikel 35 AVG en artikel 4c Wpg | | Ontbreekt | Onvoldoende | Voldoende | Goed |
|---|---|---|---|---|---|
| | Beoordelingspunten | | | | |
| **Formele vereisten** | | | | | |
| 1.1 | Er is een proces om de (hoge) risico's op het gebied van privacy te beoordelen middels het wettelijke DPIA-instrument | X | | | |
| 1.2 | In de uitgevoerde DPIA's wordt vastgesteld:<br>**a.** wat de aard van de geplande verwerkingen inhoudt;<br>**b**. wat de doelstelling, noodzaak, en proportionaliteit is;<br>**c.** wat de privacyrisico's zijn die de beoogde verwerkingen met zich meebrengt voor betrokkenen;<br>**d.** welke maatregelen moeten worden genomen om deze risico's te beperken. | | X | | |
| 1.3 | Er is een proces om ervoor zorg te dragen dat de in de DPIA goedgekeurde privacy maatregelen zijn geïmplementeerd voordat de wijziging wordt doorgevoerd. | X | | | |
| 1.4 | Alle relevante belanghebbenden zijn bij de DPIA betrokken en de specifieke richtlijnen van de toezichthoudende autoriteit ten aanzien van beoordelingscriteria worden nageleefd. | | X | | |
| 1.5 | De FG wordt bij DPIA's om advies gevraagd | X | | | |

Opmerkingen FG:
De gemeente is verplicht om DPIA's (privacy onderzoeken) uit te voeren op alle gegevensverwerkingen die een (potentieel) hoog risico inhouden voor de privacy van betrokkenen. Dit is bijvoorbeeld aan de orde op het moment dat bijzondere persoonsgegevens (medische-, strafrechtelijke persoonsgegevens en gegevens van jeugdigen) worden verwerkt. In 2022 zijn er geen DPIA's uitgevoerd. In 2023 zijn er nog geen volledige DPIA's uitgevoerd.

De gemeente voert geen actief beleid op het uitvoeren van DPIA's. Zodoende voert de gemeente DPIA's ook niet structureel uit. Daarbij wordt opgemerkt dat de gemeente niet inzichtelijk heeft op welke gegevensverwerkingen, veranderende ontwikkelingen zij wel/niet een DPIA moet uitvoeren. Geadviseerd wordt om kaders te stellen aan het uitvoeren van DPIA's. Aansluitend wordt geadviseerd om planmatig, conform deze kaders, vanaf heden DPIA's uit te voeren.