

Jaarverslag privacy 2024

Zorgvuldig omgaan met persoonsgegevens

Datum

30 december 2024

Van

interim FG

Telefoon

Email

Jaarverslag 2024 Functionaris Gegevensbescherming (FG)

Dit jaarverslag biedt een overzicht van de belangrijkste werkzaamheden, bevindingen en aanbevelingen van de Functionaris Gegevensbescherming (FG) binnen de Provincie Noord-Brabant (PNB) gedurende 2024. Het verslag is opgesteld om de status van gegevensbescherming binnen zowel het college van Gedeputeerde Staten (GS) als Provinciale Staten (PS) afzonderlijk te belichten. Hiermee wordt inzicht geboden in de voortgang, uitdagingen en verbeterpunten met betrekking tot de naleving van de Algemene Verordening Gegevensbescherming (AVG).

- Dit verslag behandelt GS en PS in aparte secties;
- Het biedt concrete aanbevelingen voor verbetering;
- Het doel is transparantie te bieden over de status van gegevensbescherming.

Samenvatting

Het jaar 2024 kenmerkte zich door aanzienlijke uitdagingen voor het privacy team. Tijdelijke onderbezetting beïnvloedde de uitvoering van kernactiviteiten, zoals het opstellen van DPIA's, de monitoring van verwerkingsregisters en het opvolgen van datalekken. Een nulmeting - uitgevoerd in oktober 2024 - toonde aan dat er nog aanzienlijke stappen nodig zijn om de gewenste privacy volwassenheid te bereiken. Een datalek binnen Corsa werd gemeld bij de Autoriteit Persoonsgegevens, wat leidde tot een intensief verbetertraject.

De werkzaamheden binnen PS richtten zich vooral op privacy beheer rondom bestaande projecten en interne/externe contacten.

Hoofdstuk 1: Uitgevoerde werkzaamheden

1.1 Gedeputeerde Staten (GS)

Binnen GS zijn audits en controles uitgevoerd die wezen op aandachtspunten in de naleving van AVG-voorschriften. Een van de redenen daarvoor was dat het privacy team door onderbezetting¹ meerdere taken moest combineren, wat de opvolging van belangrijke dossiers soms bemoeilijkte. Het jaar werd afgesloten met een herstel in bezetting, wat mogelijkheden biedt voor de implementatie van verbeteringen in 2025.

Datum

30 december 2024

Documentnummer

De belangrijkste werkzaamheden binnen GS:

- **Nulmeting AVG-compliance:** Deze meting wees op serieuze aandachtspunten in privacy beheer. De resultaten zijn verwerkt in een plan van aanpak voor 2025 en opgenomen in het activiteitenplan van het privacy team.
- **Datalekken:** In totaal zijn vijf datalekken geregistreerd, waarvan één grootschalig incident binnen Corsa werd gemeld bij de Autoriteit Persoonsgegevens. De overige meldingen betroffen voornamelijk veelvoorkomende risico's, zoals het onjuist gebruik van cc/bcc in e-mails.
- **DPIA's:**
 - **Ondersteuning en begeleiding:** DPIA's werden uitgevoerd en begeleid, onder meer op arbodienstverlening, track & trace-systemen, en servermigraties naar KPN.
 - **Uitdagingen:** Veel DPIA's zijn oorspronkelijk gestart door voorgangers of waren in principe taken voor een Privacy Officer (PO). Door de onderbezetting kreeg de FG ook een taak in de begeleiding van DPIA's. Dit bracht extra belasting met zich mee en zorgde soms voor vertraging.
 - **Corsa:** Een kritische DPIA voor de migratie van Corsa bleef onafgerond door onvolledige informatie en een gebrek aan technische ondersteuning vanuit andere teams. Dit dossier vraagt blijvende aandacht in 2025.
 - **Lessen:** Structurele samenwerking met Informatieveiligheid en een beter planmatig DPIA-proces zijn essentieel om herhaling van dergelijke situaties te voorkomen.
- **Verwerkingsregister:** De implementatie en ontwikkeling van Juriblox, een applicatie voor het bijhouden van het verwerkingsregister, werd hervat na een tijdelijke vertraging door onderbezetting.

Maatregelen en herstel:

- Eind 2024 is er 1 PO in dienst getreden en is er 1 PO ingehuurd, waardoor werkzaamheden opnieuw konden worden opgepakt.
- Het opgestelde plan van aanpak en de activiteitenkalender voor 2025 bieden een duidelijke routekaart voor verdere verbeteringen.

¹ De onderbezetting was een gevolg van langdurige uitval van een medewerker, het vertrek van een medewerker en de krappe arbeidsmarkt waardoor het moeilijk was om snel goede vervanging te regelen.

1.2 Provinciale Staten (PS)

De werkzaamheden binnen PS richtten zich op doorlopende aandacht voor het waarborgen van privacy rondom nieuwe projecten en met externe contacten. Hierbij werd aandacht besteed aan het aanvullen van het verwerkingsregister en het voorkomen van datalekken. Ook heeft overleg plaatsgehad met de medewerker van de griffie die PO-taken vervult. Dit overleg zal in 2025 periodiek plaatsvinden.

Datum

30 december 2024

Documentnummer

De belangrijkste werkzaamheden binnen PS:

- **Privacy beheer:** doorlopende aandacht voor gegevensbescherming in projecten en met externen, opvolging datalekken en incidenten.
- Verwerkingsregister is actueel en gecontroleerd.
- **Samenwerking:** Er vindt op reguliere basis overleg plaats tussen de FG en de medewerker van de griffie die PO-taken vervult.

Maatregelen en herstel:

- Werkafspraken met de medewerker van de griffie die PO-taken vervult, zodat een structurele samenwerking met de FG vorm krijgt.
- Voortdurende aandacht voor het beheer van het verwerkingsregister en voor borging van privacy in processen in 2025.

Hoofdstuk 2: Stand van zaken AVG-compliance

2.1 Gedeputeerde Staten (GS)

De AVG-compliance binnen GS vertoonde in 2024 duidelijke aandachtspunten, met name door de eerdergenoemde tijdelijke onderbezetting. Belangrijke verbeteringen werden geïdentificeerd in de nulmeting, die leidde tot een actiegericht plan voor 2025.

Datum

30 december 2024

Documentnummer

Status en verbeterpunten:

- **Compliance-niveau:** Niet alle processen voldoen momenteel volledig aan de AVG-normen, met name op het gebied van toegangsbeheer in grootschalige systemen zoals Corsa.
- **Uitdagingen:** Het ontbreken van een systematische integratie van privacy by design binnen projecten en een inconsistente samenwerking met betrokken disciplines, zoals Informatieveiligheid.
- **Positieve ontwikkelingen:** De uitbreiding in de bezetting eind 2024 maakte het mogelijk om de uitvoering van verbeteracties te herstarten, waaronder DPIA's en het bevorderen van ingebruikname van tools zoals Juriblox.

Risico's:

- De toegankelijkheid van gevoelige informatie zonder afdoende beveiligingsmaatregelen (technisch en organisatorisch).
- Onvoldoende kennisdeling tussen betrokken afdelingen, wat leidt tot een fragmentarische aanpak.

2.2 Provinciale Staten (PS)

Binnen PS was de AVG-compliance in 2024 operationeel van aard en richtte zich op het verbeteren van enkele basisprocessen.

Status en verbeterpunten:

- De meeste basisprocessen zijn beschreven en gedocumenteerd.
- Er is afstemming geweest tussen de FG en de privacy contactpersoon, gericht op een meer structurele samenwerking.

Risico's:

- Door het operationele karakter en beperkte scope ontstaat het risico dat privacy-risico's buiten die scope niet worden opgemerkt. Door bredere inzet van de privacy-contactpersoon wordt dit risico gemitigeerd.

Hoofdstuk 3: Bewustwording en trainingen

3.1 Gedeputeerde Staten (GS)

In 2024 werden binnen de organisatie verschillende activiteiten ondernomen om de bewustwording rondom gegevensbescherming te vergroten. De trainingen rondom Juriblox zijn succesvol afgerond.

Datum

30 december 2024

Documentnummer

Initiatieven en resultaten:

- **Juriblox-trainingen:** Begin 2024 werden trainingen georganiseerd om medewerkers bekend te maken met de werking en toepassing van Juriblox, het nieuwe systeem voor het verwerkingsregister. Deze trainingen zijn afgerond en ontvingen positieve feedback van deelnemers.
- **Advies op verzoek:** Medewerkers en projectteams hebben gebruikgemaakt van ad-hoc advies voor AVG-gerelateerde vraagstukken, vooral gericht op specifieke projecten en processen.

Uitdagingen:

- Door beperkte bezetting verliep de implementatie van Juriblox traag, wat zorgde voor vertragingen in het gebruik van het systeem.
- De promotie en steun van bewustwordingsinitiatieven was beperkt, wat leidde tot beperkte betrokkenheid van medewerkers.

3.2 Provinciale Staten (PS)

Binnen PS waren bewustwordingsactiviteiten in 2024 zeer kleinschalig en gericht op specifieke situaties waar AVG-naleving vereist was.

Initiatieven:

- Incidenteel advies over AVG-vraagstukken in externe samenwerkingen.

Uitdagingen:

- Door beperkte behoefte en middelen is er gekozen voor een smaller en beperkter trainingsprogramma .

Hoofdstuk 4: Aanbevelingen

4.1 Gedeputeerde Staten (GS)

Om de AVG-compliance binnen de organisatie structureel te verbeteren, zijn de volgende aanbevelingen opgesteld:

Datum

30 december 2024

Documentnummer

Bezetting en samenwerking:

- Behoud de huidige bezettingsniveaus binnen het privacy team en zorg voor een efficiënte verdeling van de werklast en capaciteiten binnen het team om de hoge inzet optimaal te benutten.
- Versterk de samenwerking tussen het privacy team en andere disciplines om een efficiëntere aanpak van beveiligings- en privacyvraagstukken te realiseren.

Procesoptimalisatie:

- Integreer privacy by design structureel in de projectmethodologie. Zorg ervoor dat dit niet alleen op papier staat, maar ook aansluit op de wensen en behoeften van medewerkers, zodat zij er effectief mee kunnen werken in de praktijk.
- Versnel de implementatie van Juriblox en zorg voor meer training en ondersteuning vanuit het management, zodat medewerkers het systeem optimaal kunnen benutten.

Bewustwording en monitoring:

- Start een breed bewustwordingsprogramma dat alle medewerkers betreft bij gegevensbescherming en AVG-naleving.
- Verbeter de monitoring en rapportage van gevoelige gegevens om risico's beter in kaart te brengen en te mitigeren.

4.2 Provinciale Staten (PS)

De aanbevelingen voor PS zijn meer gericht op het ondersteunen van specifieke processen en externe samenwerkingen:

Ondersteuning en advies:

- Verhoog de frequentie van structurele adviesmomenten om ervoor te zorgen dat externe samenwerkingen AVG-compliant blijven.

Procesoptimalisatie:

- Maak duidelijke afspraken over het verkrijgen van privacy-advies bij kleine projecten, zodat AVG-naleving beter gewaarborgd wordt zonder grote administratieve lasten.

Bewustwording:

- Besteed met regelmaat aandacht aan het onderwerp privacy, om het bewustzijn te vergroten. Dit geldt zowel voor Statenleden, als griffiemedewerkers.

Datum

30 december 2024

Documentnummer

Hoofdstuk 5: Monitoring en Evaluatie

5.1 Gedeputeerde Staten (GS)

Monitoring en evaluatie zijn cruciale onderdelen van het nalevingsproces van de AVG binnen de organisatie. Het afgelopen jaar heeft aangetoond dat er ruimte is voor verbetering, zowel in het verzamelen van gegevens als in de opvolging ervan.

Datum

30 december 2024

Documentnummer

Huidige situatie:

- Er is een basisproces voor monitoring aanwezig, maar dit is sterk afhankelijk van handmatige inspanningen van het privacy team.
- Gegevensstromen en toegangsrechten werden in het verleden slechts sporadisch gecontroleerd. Het is nu essentieel om veel intensiever te monitoren, zodat incidenten zoals het datalek binnen Corsa niet meer kunnen ontstaan. Dit vereist een proactieve aanpak waarbij zowel de technische als organisatorische aspecten regelmatig worden beoordeeld.

Aanpak voor monitoring en evaluatie:

- **Geautomatiseerde monitoringtools:** Introduceer geavanceerde monitoringtools die automatisch signaleren wanneer toegang tot gevoelige gegevens onregelmatigheden vertoont. Dit verkleint de kans op menselijke fouten en biedt een continue bewaking van cruciale processen.
- **Risico-evaluaties:** Voer periodieke risico-evaluaties uit, waarbij nadruk wordt gelegd op systemen die gevoelige informatie verwerken. Deze evaluaties moeten minimaal elk kwartaal plaatsvinden.
- **Rapportage en opvolging:** Implementeer halfjaarrapportages die inzicht geven in trends, risico's en verbeterpunten. De rapportages moeten standaard (tijdig) worden besproken in relevante vergaderingen en direct leiden tot actiepunten.
- **Bewustwording:** Train medewerkers in het herkennen en rapporteren van mogelijke onregelmatigheden in gegevensstromen. Dit vergroot de interne waakzaamheid en zorgt voor snellere reacties op incidenten.

5.2 Provinciale Staten (PS)

Binnen PS zijn monitoringactiviteiten beperkt van aard en gericht op incidentele situaties. Er is geen structureel proces voor evaluatie en monitoring.

Huidige situatie:

- AVG-compliance wordt op ad-hoc basis gemonitord bij specifieke projecten of externe samenwerkingen.

Aanbevelingen:

- Introduceer een eenvoudige checklijst voor projectleiders om basisaspecten van AVG-naleving te waarborgen.

Conclusie

Het jaar 2024 stond voor de Functionaris Gegevensbescherming (FG) binnen de Provincie Noord-Brabant in het teken van het herstellen en verbeteren van AVG-compliance na een periode van beperkte bezetting. Ondanks deze uitdagingen heeft de provincie belangrijke stappen gezet om gegevensbescherming te versterken en risico's beter te beheersen.

Datum

30 december 2024

Documentnummer

Een van de belangrijkste aandachtspunten was het verbeteren van de monitoring van gegevensstromen en toegangsrechten. In het verleden werden deze aspecten slechts sporadisch gecontroleerd, wat heeft bijgedragen aan incidenten zoals het datalek binnen Corsa. Geautomatiseerde tools en regelmatige proactieve risico-evaluaties zijn cruciale maatregelen om de gegevensbescherming te waarborgen en incidenten te voorkomen.

Daarnaast werden in 2024 belangrijke inspanningen geleverd om bewustwording rondom de AVG te vergroten. Trainingen, zoals die voor de implementatie van Juriblox, werden succesvol afgerond, hoewel de implementatie zelf nog uitdagingen kent. Het is essentieel dat deze bewustwordingsinitiatieven verder worden uitgebouwd, zodat medewerkers niet alleen voldoen aan wettelijke verplichtingen, maar ook actief bijdragen aan een cultuur van gegevensbescherming. Bewustwording blijft een sleutelement in het voorkomen van risico's en het versterken van interne processen.

De nulmeting die in oktober 2024 werd uitgevoerd, bracht aandachtspunten aan het licht. Het opgestelde plan van aanpak voor 2025 biedt een stevige basis om deze tekortkomingen aan te pakken.

Voor het bestuursorgaan Provinciale Staten (PS) waren de activiteiten in 2024 beperkter van aard. Hoewel de behoefte aan uitgebreide maatregelen hier minder groot is, blijven incidentele evaluaties en praktische richtlijnen belangrijk om AVG-naleving te waarborgen. Het maken van duidelijke werkafspraken over het gebruik van persoonsgegevens kan de consistentie en efficiëntie binnen PS verbeteren zonder grote administratieve belasting.

Samenvattend is de bezetting binnen het privacy team weer op peil, wat een stevige basis biedt voor verdere professionalisering in 2025. Het succes hiervan hangt af van het consistent toepassen van verbetermaatregelen, het verbeteren van de samenwerking binnen het privacy team en aanverwante disciplines, het behouden van aandacht voor monitoring en het bevorderen van een organisatie brede betrokkenheid bij gegevensbescherming. Door deze lijn voort te zetten, kan de provincie haar doel bereiken: een volwassen niveau van gegevensbescherming dat voldoet aan de eisen van de AVG en voorbereid is op toekomstige uitdagingen.