Stichting Inlichtingenbureau
Informatieknooppunt Gemeenten

# FG Jaarverslag 2023

Jan Peter Bergfeld, Functionaris Gegevensbescherming

| | |
|---|---|
| Versie | 1.0 |
| Datum | 15 mei 2024 |
| Auteur | Jan Peter Bergfeld |

Stichting Inlichtingenbureau
Informatieknooppunt Gemeenten

# Inhoudsopgave

## 1. Inleiding

In dit jaarverslag rapporteer ik als FG aan bestuur en directie over mijn werkzaamheden en bevindingen met betrekking tot de wijze waarop Stichting Inlichtingenbureau in 2023 invulling heeft gegeven aan privacy-management. Daarbij betrek ik de belangrijkste privacy-aandachtspunten, de in het jaarplan 2023 geformuleerde privacy-doelstellingen en ook de kaders voor legal design, die voor de dienstverlening van het Inlichtingenbureau van groot belang zijn.

## 2. Privacybeleid en privacydoelstellingen

Het bestuur is eindverantwoordelijk voor de gegevensverwerkingen binnen het IB en heeft vanuit die verantwoordelijkheid het *Algemeen Privacybeleid Stichting Inlichtingenbureau* 2023 met bijbehorende uitvoeringsregeling vastgesteld. Ter nadere uitwerking hiervan hanteert het Inlichtingenbureau het *Privacy Control Framework IB* (verder: PCF) dat is gebaseerd op een modeldocument van de Nederlandse Orde van Register EDP-auditors (NOREA).

In het Jaarplan 2023 heeft het Inlichtingenbureau de volgende privacy doelstellingen opgenomen:

1. De interne IB-norm uit het PCF wordt in 2023 geëvalueerd, aangescherpt en ook beschreven (bewijslast) hoe deze ook controleert of het IB ook op deze wijze zo werkt. In 2023 gaat het IB een interne audit uitvoeren op het gehele pcf.

Voor wat betreft de eerste doelstelling geldt dat wel een begin is gemaakt met het toetsbaar maken van het PCF, maar dat dit nog lang niet is afgerond. Ook een integrale interne audit op het gehele PCF heeft niet plaatsgevonden. Dat deze doelstelling te ambitieus was geformuleerd blijkt ook uit de hieronder integraal opgenomen tekst over dit onderwerp uit het IB jaarplan 2024:

“Het Inlichtingenbureau neemt in het privacy werkprogramma 2024 doelstellingen op om aantoonbaar (op basis van een externe audit) te gaan voldoen aan het Privacy Control Framework (PCF) op basis van een groeiscenario. In aanvulling op de toetsing van de beheersingsdoelstelling (vastgesteld en uitgedragen) IB-privacybeleid zal in 2024 worden gewerkt aan de aantoonbare invulling en uitwerking van de volgende beheersingsdoelstellingen:

- Benoemen van AVG-rollen (verwerker of verwerkingsverantwoordelijke) bij verwerkingen;
- Toekennen van verantwoordelijkheden aan medewerkers in kader privacybeleid;
- Identificatie en classificatie van (groepen) persoonsgegevens die worden verwerkt;
- Invulling geven aan privacy-risicomanagement;
- Opstellen en actueel houden van PIA’s;
- Beheren van (een overzicht van) beveiligings- en privacy-incidenten;
- Zorgdragen dat medewerkers met een privacyrol beschikken over de benodigde competenties;
- Bevorderen van privacy-awareness bij medewerkers;
- Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten.

Het onderdeel 'management' uit het Privacy Control Framework is hiermee volledig geïmplementeerd. Daarnaast wordt een implementatieplan opgesteld om ook aantoonbaar te voldoen aan de overige onderdelen uit het PCF.”

2. Vanuit privacy management zal met name aandacht worden besteed aan de onderwerpen doelbinding, transparantie en verantwoording (accountability) in ketenverband. Dit ook vanuit de apothekersrol van IB.

Deze doelstelling is naar mijn mening wel grotendeels gerealiseerd. Zie hiervoor de toelichting onder de paragrafen 4 PIA's, 6 Transparantie en 8 Monitoring en handhaving.

Het is belangrijk, mede in relatie tot het in de volgende paragraaf te benoemen aspect van legal design, om in te gaan op de apothekersrol die het IB voor zich ziet in relatie tot de rol die het IB bij vrijwel alle informatiediensten heeft als onderdeel van een keten. Het Inlichtingenbureau werkt in veel verschillende ketens die ieder op een eigen manier zijn ingericht voor wat betreft ketensturing. Het IB hanteert de term apothekersrol om aan te geven dat we niet alleen kritisch naar onze eigen rol kijken maar ook breder, dus naar de gehele keten. Onder instandhouding van ieders eigen verantwoordelijkheden in ketenverband wijzen we waar nodig andere ketenpartijen op aandachtspunten/verbeterpunten in het kader van het bevorderen van een transparante en zorgvuldige ketenbrede verwerking van persoonsgegevens op basis van een adequate (keten)governance. Ketengovernance in combinatie met duidelijke wettelijke grondslagen, waar nodig gebaseerd op wettelijke taken en met een passende invulling van AVG-rollen zorgt voor een passend legal design.

## 3. Legal design en AVG-rollen

Het Inlichtingenbureau besteedt in de PIA's (zie hierna onder 4) expliciet aandacht aan de AVG-rol waarin informatiediensten en bijbehorende informatieproducten worden aangeboden. Die rol kan zijn (al dan niet gezamenlijk-) verwerkingsverantwoordelijke of verwerker. In het geval dat sprake is van verwerkerschap dient duidelijk te zijn wie de verwerkingsverantwoordelijke is en ook dat die feitelijk invulling geeft aan diens verantwoordelijkheid. Voor veel verwerkingen treedt het Inlichtingenbureau nu nog op als verwerker. Er lopen diverse wetgevingstrajecten die beogen (wettelijke) taken toe te kennen aan het IB. Niet altijd wordt daarbij voldoende duidelijk gemaakt wie opdrachtgever is, hoe de betreffende keten is ingericht en hoe ieders verantwoordelijkheid in die keten moet worden gezien vanuit de AVG-rollen. Dit speelt met name met betrekking tot VWS-wetgeving.

Als FG adviseer en ondersteun ik het IB in dialogen met opdrachtgevers en derden met als doel om te komen tot een passend legal design en een goed werkende keten.

N.b.: Hoewel begrijpelijk vanuit het perspectief van verschillende opdrachtgevers die hierover eigen keuzes maken komen burgers nu en in de toekomst het Inlichtingenbureau tegen in allerlei verschillende AVG-rollen, afhankelijk van de al dan niet wettelijke taak die wordt uitgevoerd. Voor bijvoorbeeld de effectuering van het inzagerecht houdt dit in dat soms direct bij IB inzage kan worden gevraagd, soms naar een gemeente of waterschap moet worden verwezen of ook naar de minister van SZW (centrale verwerkingen BVV). Dit is niet altijd makkelijk uit te leggen.

## 4. PIA's

De werkprocessen waarin persoonsgegevens worden verwerkt moeten voldoen aan de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Ter toetsing en borging zijn inmiddels voor alle informatiediensten van het Inlichtingenbureau Privacy Impact Assessments opgesteld.

De termijn voor actualisering was initieel op twee jaar gesteld en is later verlengd tot drie jaar. Door een combinatie van factoren, waaronder een meer uitgebreid nieuw PIA-format en een verdiepingsslag ten opzichte van de bestaande PIA's, is het niet gelukt de actualisering van de achttien PIA's die voor 2023 op de rol stonden tijdig af te ronden. Dit is ook gerapporteerd in het IB jaarverslag.

Veel PIA's verkeerden wel in een min of meer afrondende fase en – wellicht nog belangrijker – in het kader van de herbeoordeling is wel een groot aantal aanpassingen in de dienstverlening aangebracht. Daarbij kan gedacht worden aan strikter invulling geven aan doelbinding, verkorten van bewaartermijnen, aanpassen (kleiner maken) van gegevensset en verkorten van bevragingsperioden. Dit alles komt de kwaliteit van de dienstverlening ten goede.

Desalniettemin verdient de bewaking van het PIA-proces en de tijdige afronding van openstaande maatregelen die voortvloeien uit het PIA-proces meer management aandacht. Aanvullend op deze constatering doe ik in paragraaf 9 de aanbeveling om het privacybeleid zodanig aan te passen dat niet eens per drie jaar maar jaarlijks, als regulier onderdeel van productmanagement, de PIA's worden geactualiseerd, op basis van een standaard checklist.

## 5. Bewustwording en training van medewerkers en gebruikers

Alle nieuwe medewerkers hebben in 2023 een verplichte security- & privacy-awareness training gekregen. Ook is het PIA proces (nogmaals) toegelicht in een medewerkersbijeenkomst. De privacymanager en de FG overleggen regelmatig met productmanagers en business analisten over privacy onderwerpen (veelal gekoppeld aan een onderhanden PIA), hetgeen bijdraagt aan de privacy-bewustwording.

Ook aan externe gebruikers geven de privacymanager en de FG regelmatig voorlichting. Bijvoorbeeld in de vorm van een presentatie op de relatie en bijdragen aan door de VNG/IBD georganiseerde FG-bespreekuren voor gemeentelijke collega FG's. Daarnaast zijn er regelmatig contacten met burgers naar aanleiding van vragen, inzageverzoeken en klachten.

## 6. Transparantie

Het Inlichtingenbureau besteedt veel aandacht aan transparantie. De combinatie van Diensten- en productencatalogus en de qua structuur en indeling daarop aansluitende en jaarlijks geactualiseerde Gegevensregisters van verwerkingsactiviteiten bieden een goed inzicht op hoofdlijnen van de verwerkingen die plaatsvinden en de keten-context waarin ze plaatsvinden. De PIA's bieden de mogelijkheid om desgewenst nog verder in te zoomen op de verschillende verwerkingen.

N.b.: In het kader van legal design is de organisatie voldoende scherp om in overleg met betrokken ministeries tijdig aandacht te vragen voor de noodzaak van een specifieke wettelijke taak en grondslag en een heldere duiding van de AVG-rollen in ketenverband. Echter de gekozen oplossing laat vaak lang op zich wachten en/of sluit niet goed aan in wat in andere ketens voor andere opdrachtgevers als oplossingsrichting is gekozen. Dit draagt niet bij aan de gewenste transparantie (zie ook paragraaf 3).

## 7. Gegevensbeveiliging

Het Inlichtingenbureau dient op grond van de AVG, passende technische en organisatorische maatregelen te nemen ter beveiliging van persoonsgegevens. Het informatiebeveiligingsbeleid van het IB is gebaseerd op de BIO. Jaarlijks wordt de externe dienstverlening van het IB getoetst door een EDP-auditor. Uit die audit bleek dat het IB in control is voor wat betreft de informatiebeveiliging, maar dat er wel aandachtspunten zijn. Kortheidshalve verwijs ik hiervoor naar de betreffende audit-rapportages en de samenvatting van de bevindingen in het hoofdstuk over Informatiebeveiliging en privacybeleid in het jaarverslag 2023 van IB.

## 8. Monitoring en handhaven

De AVG legt de verantwoordelijkheid om aan te (kunnen) tonen dat het Inlichtingenbureau aan de privacyregels voldoet bij de organisatie zelf. Dat betekent niet dat er nooit fouten mogen worden gemaakt of dat alles altijd optimaal ingeregeld moet zijn. Dat is een utopie. Wel mag van bestuur en directie worden verwacht dat een proces is ingericht om te waarborgen dat het uitvoeren en monitoren van de beheersingsdoelstellingen en maatregelen uit het privacy control framework op basis van een plan-do-check-act-cyclus resulteert in herstel van tekortkomingen en continue verbetering.

Als FG onderschrijf ik de door het bestuur uitgesproken ambitie om op basis van het PCF op termijn te komen tot een vorm van Privacy Proof certificering. De ervaring leert dat hiervoor een passend groeitraject moet worden vastgesteld. Het in jaarplan 2024 aangekondigde implementatieplan zal daarvoor de noodzakelijke stappen en tijdlijnen dienen te bevatten.

## 9. Conclusie en aanbevelingen

Door de combinatie van het algemeen privacybeleid van Stichting Inlichtingenbureau, de nadere uitwerking hiervan in een privacy control framework en de planmatige en gecoördineerde uitvoering daarvan op basis van het jaarplan en het werkprogramma privacy is - naar mijn mening als FG - het Inlichtingenbureau evenals in voorgaande jaren op hoofdlijnen in control voor wat betreft de hoofdlijnen van het privacymanagement.

Wel constateer ik dat op een aantal onderdelen van het privacy control framework achterstand optreedt ten opzichte van geformuleerde ambities. Een duidelijk voorbeeld hiervan vormt het proces van up to date houden van PIA's en treffen van maatregelen die voortvloeien uit bij PIA's gesignaleerde risico's alsmede het voortvarend verhelpen van bij de EDP-audit aangetroffen aandachtspunten. Hier is betere voortgangsbewaking noodzakelijk. In dit verband adviseer ik om het IB privacybeleid in die zin aan te passen dat PIA's niet iedere drie jaar maar jaarlijks zullen worden geactualiseerd als onderdeel van regulier productmanagement. Dit kan helpen om dit proces onderdeel te maken van de reguliere werkzaamheden in plaats van een periodieke (grote) klus.

Ook in algemene zin is de onverdeelde aandacht van bestuur en directie nodig voor de wijze waarop de organisatie invulling geeft aan de eigen privacydoelstellingen uit het *Privacy Control Framework IB.* Juiste en volledige toepassing van dit framework borgt dat wordt voldaan aan de AVG.

Utrecht, 15 mei 2024

Jan Peter Bergfeld, FG