

FG Jaarverslag 2024

Bescherming persoonsgegevens IB

Jan Peter Bergfeld, Functionaris Gegevensbescherming

Versie	1.0
Datum	14 april 2025
Auteur	Jan Peter Bergfeld

Inhoudsopgave

1.	Inleiding.....	3
2.	Privacybeleid.....	3
3.	AVG-rol	4
4.	Interne taken en verantwoordelijkheden	4
5.	PIA's, risico's en maatregelen	4
6.	Bewustwording en training van medewerkers.....	5
7.	Inzageverzoeken	5
8.	Gegevensbeveiliging.....	5
9.	Monitoring en handhaven	6
10.	Verantwoording en conclusie	6
	Bijlage 1: Overzicht privacyincidenten 2024.....	7

1. Inleiding

Onder de verantwoordelijkheid van bestuur en directie verwerkt Stichting Inlichtingenbureau persoonsgegevens. De AVG beschrijft het wettelijk kader voor het verwerken van persoonsgegevens. De organisatie dient transparant te zijn over de vraag welke persoonsgegevens worden verwerkt, voor welk doel en op basis van welke grondslag. Tijdens de levensduur van persoonsgegevens moeten ze goed worden beveiligd, mogen ze niet zomaar voor een ander doel worden verwerkt en moeten ze na afloop worden vernietigd of geanonimiseerd. Daarnaast gelden tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen bij het Inlichtingenbureau: het privacymanagement.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast heeft het Inlichtingenbureau een Functionaris Gegevensbescherming (FG) aangesteld als interne toezichthouder.

In dit jaarverslag bescherming persoonsgegevens rapporteert de FG aan bestuur en directie over zijn werkzaamheden en bevindingen aan de hand van de belangrijkste onderdelen van het Privacy Control Framework IB dat is gebaseerd op een modeldocument van de Nederlandse Orde van Register EDP-auditors (NOREA). Toepassing van dit framework borgt dat wordt voldaan aan de AVG.

2. Privacybeleid

Het Inlichtingenbureau is zich zeer bewust van de grote impact die het verwerken van persoonsgegevens in ketenverband heeft op de privacy van burgers. Er worden immers veel (gevoelige) gegevens van veel (kwetsbare) burgers in veel verschillende domeinen verwerkt. Een belangrijke doelstelling van het privacybeleid is daarom dat het Inlichtingenbureau bij de uitvoering van taken zorgdraagt dat aan alle vereisten wordt voldaan die voortvloeien uit privacykaders zoals vastgelegd in de AVG en in de overige relevante wettelijke voorschriften.

Het bestuur is eindverantwoordelijk voor de gegevensverwerkingen binnen het IB en heeft vanuit die verantwoordelijkheid het Algemeen Privacybeleid Stichting Inlichtingenbureau vastgesteld.

3. AVG-rol

Het Inlichtingenbureau besteedt in de PIA's (zie hierna onder 5) 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 op als verwerker.

4. Interne taken en verantwoordelijkheden

Binnen het privacybeleid zijn taken, verantwoordelijkheden en bevoegdheden toegewezen aan zogenoemde proces-verantwoordelijken. In het privacy control framework is dit nader uitgewerkt.

5. PIA's, risico's en maatregelen

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 voor alle informatiediensten van het Inlichtingenbureau Privacy Impact Assessments opgesteld, die ook periodiek worden geactualiseerd.

In 2024 is een succesvolle inhaalslag uitgevoerd met betrekking tot het uitvoeren van PIA's voor bestaande en nieuwe informatiediensten. De PIA's de interne bedrijfsvoering, zullen vanaf 2025 worden opgesteld.

In een aantal gevallen bevatten PIA's ook de beschrijving van risico's en maatregelen om deze risico's te mitigeren. De vlotte afhandeling van maatregelen bleek in het vorige verslagjaar onvoldoende geborgd. Helaas bleek ook over 2024 dat 20 maatregelen nog niet zijn uitgevoerd, terwijl dit volgens de planning wel had gemoeten. Sommige van de maatregelen dateren al uit eerdere jaren dan 2024. Een deel van de verklaring is de vertraagde vernieuwing/verservicing van informatiediensten (8 van de 20 per eind 2024 nog openstaande maatregelen zijn hieraan gerelateerd) en openstaande governance vraagstukken waarbij het IB wacht op reactie van o.a. SZW (4 van de 20). Zie verder hierover ook de tekst onder 9: Monitoring en handhaven.

6. Bewustwording en training van medewerkers

Alle nieuwe medewerkers hebben tijdig hun awareness gekregen bij binnenkomst op het gebied van Security & Privacy. In een plenaire sessie en middels een verplichte training is het gehele personeel gewezen op het belang van privacy en security en wat er van hen verwacht wordt.

7. Inzageverzoeken

De afhandeling van inzageverzoeken verloopt vooralsnog altijd via de aangesloten organisaties, hetzij omdat die de verwerkingsverantwoordelijke zijn (zie ook onder 3), hetzij omdat de wettelijke taakverdeling tussen gemeenten en IB de gemeente aanwijst als het contactpunt voor inzageverzoeken. In 2024 zijn geen formele inzageverzoeken ontvangen. In 2023 waren nog twaalf inzageverzoeken ontvangen en afgehandeld en in 2022 zeven. Het afgelopen jaar is wel regelmatig voorlichting aan burgers gegeven over het effectueren van hun inzagerecht.

8. 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 over 2024 bleek dat het IB in control is voor wat betreft de informatiebeveiliging, maar dat er wel aandachtspunten zijn. Korthedshalve verwijs ik hiervoor naar de betreffende audit-rapportages, de samenvatting van de bevindingen in het hoofdstuk over Informatiebeveiliging en privacybeleid in het jaarverslag 2024 van IB en de tekst hierover op de website van het IB.

De AVG verplicht verwerkingsverantwoordelijken om datalekken, waarbij persoonsgegevens betrokken zijn, te registreren en onder omstandigheden te melden bij de Autoriteit Persoonsgegevens (AP) en/of bij betrokkenen (de burgers die geraakt worden door een dergelijk datalek). Zoals onder 3 werd geconstateerd treedt het IB voor veel verwerkingen op als verwerker in opdracht van gemeenten en is dus niet (zelfstandig) verwerkingsverantwoordelijke. Het IB registreert datalekken conform de AVG en informeert de gemeenten waarop een datalek betrekking heeft daarover. Van een datalek wordt een privacyincident¹ geregistreerd. Een overzicht met privacy incidenten is opgenomen als bijlage 1.

¹ Een privacyincident betreft altijd een datalek met persoonsgegevens en vice versa. Er is sprake van een datalek als de beschikbaarheid, integriteit en/of vertrouwelijkheid is geschonden.

9. Monitoring en handhaven

De AVG legt de verantwoordelijkheid om aan te (kunnen) tonen dat het Inlichtingenbureau aan de privacyregels voldoet bij de organisatie zelf. Om hieraan invulling te kunnen geven is een proces 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.

Het Inlichtingenbureau was er in 2023 onvoldoende in geslaagd om tijdig (conform afgegeven planning) de risico's uit de PIA's te mitigeren. Als maatregel is toen afgesproken om maandelijks de voortgang van openstaande privacy acties en maatregelen te rapporteren in het directie-overleg. Dit heeft nog niet geleid tot het gewenste resultaat, zie ook 5.

10. Verantwoording en conclusie

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 (aantoonbaar) in control voor wat betreft het privacymanagement. Daarbij teken ik aan dat het tijdig mitigeren van de risico's die voortkomen uit de PIA's nog steeds aandacht van het management behoeft.

Voor het (ook) extern laten auditen van de beheersingsdoelstellingen uit het privacy control framework wordt een gefaseerde aanpak gehanteerd. Over kalenderjaar 2024 is een assurance-verklaring met betrekking tot het onderdeel Management en de daaronder vallende maatregelen afgegeven. Dit is een flinke uitbreiding ten opzichte van de verklaring met betrekking tot enkel het privacybeleid over 2023. Het beoogde eindresultaat is dat op basis van een volledige audit voor (een deel van) de dienstverlening van het Inlichtingenbureau het privacy-audit-proof certificaat kan worden toegekend.

Utrecht, 14 april 2025

Jan Peter Bergfeld, FG

Bijlage 1: Overzicht privacyincidenten 2024

Samenvatting Privacy-incidenten	2022	2023	2024
Totaal aantal incidenten	4	7	6
- Waarvan gemeld bij de verwerkingsverantwoordelijke (niet zijnde IB)	3	5	5
- Waarvan gemeld bij de Autoriteit Persoonsgegevens	0	1	0
Prioriteit	Laag: 0 Midden: 2 Hoog: 2	Laag: 5 Midden: 2 Hoog: 0	Laag: 6 Midden: 0 Hoog: 0
Overall oordeel: Het totaal aantal privacy-incidenten wordt door het IB als laag beschouwd gelet op de omvang van de dienstverlening van het Inlichtingenbureau.			