Stichting Inlichtingenbureau

Assurance-rapportage (richtlijn 3000A)

1 januari 2022 – 31 december 2022

Datum:	2 maart 2023
Van:	drs. M.M.H. van Ernst RE
Kenmerk:	2302-06596/NH
Richtlijn:	3000(A) NOREA

1 Inleiding, doelstelling en opbouw van het rapport

1.1 Inleiding en doelstelling van het rapport

Stichting Inlichtingenbureau (hierna: het Inlichtingenbureau) is in opdracht van het ministerie van Sociale Zaken en Werkgelegenheid (SZW), de Vereniging van Nederlandse Gemeenten (VNG) en het ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) actief in informatiedistributie op de gebieden Werk & Inkomen, Onderwijs, Belastingen en Wmo & Jeugdzorg. Het Inlichtingenbureau verzamelt gegevens bij verschillende bronnen zoals het UWV, de Belastingdienst of de RDW. Door het slim combineren van de verzamelde gegevens ontstaan signalen die het Inlichtingenbureau vervolgens geautomatiseerd aanlevert bij gemeenten. De betrokken gemeenteambtenaren kunnen hiermee gemakkelijk vaststellen of deze signalen onderzoekwaardig zijn. Daarnaast structureert en vergemakkelijkt het Inlichtingenbureau, via het beveiligde gegevensknooppunt, de digitale gegevensuitwisseling tussen gemeenten en zorgaanbieders op het gebied van de WMO en Jeugdwet.

Beschikbaarheid, integriteit en vertrouwelijkheid van data is een belangrijk aspect voor het Inlichtingenbureau. Om dit te bewerkstelligen maakt het Inlichtingenbureau gebruik van het normenkader BIO (Baseline Informatiebeveiliging Overheid). Het Inlichtingenbureau heeft in 2020 een op de BIO gebaseerd informatiebeveiligingsbeleid vastgesteld en heeft, op basis van een risico analyse, een selectie van de in haar ogen belangrijkste BIO normen geïmplementeerd.

Omdat het Inlichtingenbureau persoonsgegevens verwerkt is vanaf 2022 aanvullend uit het PCF (Privacy Control Framework 2.0) door het Inlichtingenbureau het onderwerp Privacybeleid (PPO) met de onderliggende normen geselecteerd om over te rapporteren.

Om aan de geselecteerde BIO en Privacy normen en bijbehorende beheersdoelstellingen te voldoen heeft het Inlichtingenbureau beheersingsmaatregelen geformuleerd en geïmplementeerd. Op basis hiervan stelt het management een attest op over de mate waarin het Inlichtingenbureau gedurende de controleperiode procedures en maatregelen heeft geïmplementeerd en deze hebben gewerkt.

Het Inlichtingenbureau heeft aan Baker Tilly verzocht een assurance-rapportage op te stellen over de periode vanaf 1 januari 2022 tot en met 31 december 2022.

1.2 Inhoud van het rapport

Het rapport bestaat uit de volgende onderdelen:

- Hoofdstuk 2: Verklaring van het management van het Inlichtingenbureau omtrent de mate waarin aan de geselecteerde BIO- en PCF-normen wordt voldaan.
- Hoofdstuk 3: Assurance-rapport van de onafhankelijke auditor waarin een uitspraak wordt gedaan of en in hoeverre het attest een getrouw beeld weergeeft.
- Bijlages waarin zijn opgenomen
    A. Een nadere beschrijving van de scope van het attest
    B. Een toelichting op de uitgevoerde werkzaamheden
    C. Een opsomming door het Inlichtingenbureau van de geselecteerde BIO- en PCF-normen, met per norm de conclusie

2 Verklaring door het management van het Inlichtingenbureau

Het Inlichtingenbureau rapporteert aan haar opdrachtgevers en afnemers over de mate waarin het Inlichtingenbureau een stelsel van beheersmaatregelen heeft geïmplementeerd om aan eisen ten aanzien van informatiebeveiliging en privacy te voldoen. Het Inlichtingenbureau heeft, om te kunnen voldoen aan de gestelde eisen een informatiebeveiligingsmanagementsysteem (ISMS) en privacymanagementsysteem (PMS) geïmplementeerd. Door middel van een operationele planning van controle taken (interne audit), maandelijkse rapportage hierover en een tweetal directiebeoordelingen conform hoofdstuk 9.3 Directiebeoordeling van de ISO27001 (2017) blijft het Inlichtingenbureau in 'control'. Op deze wijze voldoet het Inlichtingenbureau aan de plan-do-check-act cyclus voor de genoemde management systemen.

De scope betreft alle informatiediensten zoals vermeld in de Dienstencatalogus, die in 2022 draaiden op de bestaande infrastructuur. Er is een nieuwe infrastructuur voor het Inlichtingenbureau in ontwikkeling. De infrastructuur in ontwikkeling behoort echter niet tot de scope van het attest en de uit te voeren EDP-audit.

Gedurende het jaar heeft het Inlichtingenbureau een wijziging doorgevoerd in de organisatiestructuur met personele wisselingen en herbeleggen van verantwoordelijkheden tot gevolg. Risico's ten aanzien van de interne beheersing met betrekking tot informatiebeveiliging zijn door het Inlichtingenbureau ondervangen. De interne auditor die normaliter de derde lijn vormt, heeft waar nodig tijdelijke de tweedelijns controles uitgevoerd.

Het Inlichtingenbureau heeft aan Baker Tilly de opdracht gegeven een assurance-rapportage op te stellen over de periode vanaf 1 januari 2022 tot en met 31 december 2022 of het Inlichtingenbureau voldoet aan onderstaand geformuleerde attest.

Het Inlichtingenbureau verklaart dat:

1. Het Inlichtingenbureau een op de BIO gebaseerd informatiebeveiligingsbeleid heeft. Het Inlichtingenbureau op basis van een risico-analyse een selectie van de belangrijkste BIO normen heeft gemaakt. Dit om in voldoende mate de risico's ten aanzien van informatiebeveiliging te ondervangen. Op basis van de geïmplementeerde beheersmaatregelen heeft het Inlichtingenbureau zelf periodieke controles uitgevoerd om vast te stellen in hoeverre aan de geselecteerde BIO normen wordt voldaan. In de controleperiode van 1 januari 2022 tot en met 31 december 2022 het Inlichtingenbureau aan de geselecteerde BIO-normen voldoet in opzet, bestaan en werking. Dit met uitzondering van een aantal bevindingen (die hieronder zijn opgenomen). Dit betreft met name bevindingen die in de voorgaande jaren ook opgetreden zijn.
2. Het Inlichtingenbureau een privacybeleid heeft vastgesteld. Dit is op basis van het Privacy Control Framework (PCF) voor het onderdeel PPO (privacybeleid) uitgewerkt in een toetsbare interne norm. Het Inlichtingenbureau heeft periodieke controles uitgevoerd om vast te stellen in hoeverre aan de PPO normen wordt voldaan. In de controleperiode van 1 januari 2022 tot en met 31 december 2022 voldoet het Inlichtingenbureau volledig in opzet, bestaan en werking aan de PPO normen.
3. Het Inlichtingenbureau haar Directiebeoordeling uitvoert conform hoofdstuk 9.3 Directiebeoordeling van de ISO27001 (2017).

Bevindingen

Deze paragraaf bevat de bevindingen die in de interne audit van het Inlichtingenbureau zijn geconstateerd. Deze bevindingen zijn gegroepeerd per BIO hoofdstuk met daarbij vermeld de doelstelling zoals opgenomen in de BIO.

1. H6.1 Interne organisatie. Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen. Uitzonderingen:
    - De door HR uitgegeven functies komen niet overeen met de rollen genoemd in de RBAC (voor toegang tot OTAP omgevingen) en in de uitgedeelde rechten waardoor de controle niet zonder afwijkingen kan plaatsvinden. Tevens zijn enkele accounts niet tijdig gesloten en/of voor de juiste periode toebedeeld. Het netwerk account is in alle gevallen tijdig afgesloten waardoor het risico van onbevoegde toegang is gemitigeerd.
2. H7.1 Voorafgaand aan het dienstverband. Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. Uitzonderingen:
    - Niet alle VOG's zijn tijdig aanwezig. De uitzondering betrof nieuwe medewerkers die al wel meeliepen maar nog geen bedrijfsmiddelen hadden ontvangen, dit is echter niet aantoonbaar vastgelegd.
3. H8.1 Verantwoordelijkheid voor bedrijfsmiddelen. Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren. Uitzonderingen:
    - Geen eenduidig overzicht van toegangstags uitgegeven aan medewerkers (en leveranciers).
    - Laptops op voorraad en in de CMDB komen niet overeen.
4. H9.2 Beheer van toegangsrechten van gebruikers. Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. Uitzonderingen:
    - Er is een medewerker aangemaakt in de systemen en hardware uitgereikt zonder een indiensttredingsmelding.
5. H12.1 Bedieningsprocedures en verantwoordelijkheden. Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen. Uitzonderingen:
    - De wijzigingsprocedure voor het Inlichtingenbureau (bepalen impact analyse) functioneert niet in alle gevallen naar behoren. Vrijgave van releases vinden niet altijd eenduidig plaats. Niet altijd duidelijk of bevindingen nu opgelost zijn. Status beveiligingstest niet altijd duidelijk.
6. H12.3 Back-up. Doelstelling: Beschermen tegen het verlies van gegevens. Uitzonderingen:
    - De uitwijktest heeft niet plaatsgevonden in 2022 als gevolg van een vertraagde verhuizing van het uitwijkdatacenter door de leverancier.
7. H17.1 Informatiebeveiligingscontinuïteit. Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie. Uitzonderingen:
    - Huidige infrastructuur is onvoldoende benoemd in het bedrijfscontinuïteitsplan.

Utrecht, 2 maart 2023

Stichting Inlichtingenbureau

Peter Jansz
Directeur Stichting Inlichtingenbureau

3 Assurance-rapport van de onafhankelijke auditor

Aan: de directie van het Inlichtingenbureau

3.1 Scope

Ingevolge uw opdracht hebben wij de in hoofdstuk 2 opgenomen verklaring door het management van het Inlichtingenbureau inzake informatiebeveiliging van uw dienstverlening onderzocht.

3.2 Ons oordeel

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel, zijn de criteria die in de verklaring van het Inlichtingenbureau in hoofdstuk 2 staan beschreven.

Naar ons oordeel is de verklaring van het Inlichtingenbureau ten aanzien van het voldoen aan de geselecteerd BIO- en PCF-normen, in alle van materieel belang zijnde opzichten, getrouw weergegeven.

Wij wijzen de lezer op paragraaf *3.3. Benadrukking aangelegenheden* waarin wij aanvullende informatie hebben opgenomen aangaande de resultaten van onze werkzaamheden.

3.3 Benadrukking aangelegenheden

Wij benoemen hierbij de volgende aangelegenheden:

1. Het Inlichtingenbureau heeft op basis van een risico analyse een selectie van de belangrijkste normen van de BIO gemaakt. Op basis van deze selectie is een ISMS ingericht om daarmee aantoonbaar aan de maatregelen te voldoen. Wij hebben de toereikendheid van het normenkader beoordeeld door een analyse uit te voeren op de niet geselecteerde normen in hoeverre deze terecht als “niet van toepassing” of als “normen met een laag risico” werden beoordeeld. Hierbij hebben wij geconstateerd dat de normen aangaande een SIEM/SOC niet geselecteerd zijn en derhalve als zodanig geen onderdeel uitmaken van het ISMS en de interne audit. Wij achten echter deze normen gezien aard van de dienstverlening van het Inlichtingenbureau wel van toepassing. Wij hebben van het Inlichtingenbureau vernomen dat de normen aangaande SIEM/SOC niet zijn geselecteerd omdat meldingen van het SIEM/SOC die als informatie beveiligingsincident worden beoordeeld in het incidentmanagementproces worden afgehandeld. Wij hebben aanvullend vastgesteld dat door het Inlichtingenbureau een SIEM/SOC dienst is afgenomen.
2. Het ISMS is zodanig ingericht dat de uitvoering van kwartaalcontroles over Q4 2022 ingepland zijn om in Q1 2023 uit te voeren.
3. Naar aanleiding van onze werkzaamheden hebben wij beoordeeld in hoeverre onze bevindingen overeenkwamen met de bevindingen van de interne audit van het Inlichtingenbureau. Hierbij hebben wij geen verschillen tussen de bevindingen geconstateerd die zouden leiden tot een ander oordeel. Wel betreft het de volgende aanvullende constatering ten aanzien van de normen 6.1.2 en 9.2.1:
    - Er zijn door het Inlichtingenbureau op basis van een deelwaarneming uitzonderingen geconstateerd ten aanzien van het aanmelden en afmelden van gebruikers. De bevindingen zijn opgevolgd echter is geen aanvullende controle uitgevoerd om vast te stellen of dit een eenmalig incident betreft of een structureel probleem.

3.4 De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de verklaring van het management van het Inlichtingenbureau verricht in overeenstemming met de NOREA Richtlijn 3000A 'Assuranceopdrachten door IT-auditors in de Attestvorm'. Deze richtlijn vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen voor ons oordeel. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht '.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij hebben het Reglement Kwaliteitsbeheersing NOREA (RKBN) toegepast. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

3.5 Beperkingen

De procedures en maatregelen van het Inlichtingenbureau kunnen vanwege hun aard, niet alle fouten of omissies voorkomen of ontdekken. Tevens is de projectie van een eventuele evaluatie van de effectiviteit naar toekomstige verslagperiodes onderhevig aan het risico dat procedures en maatregelen inadequaat kunnen worden of falen.

3.6 Beoogde gebruikers en doel

Dit assurance-rapport is bestemd voor het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het ministerie van Onderwijs, Cultuur en Wetenschappen (OCW), de Waterschappen en de Vereniging van Nederlandse Gemeenten (VNG) en haar leden. Doel van de verklaring van het management van het Inlichtingenbureau is om gebruiker van de rapportage te informeren over de mate waarin (opzet, bestaan en werking) beheersingsmaatregelen borgen dat het Inlichtingenbureau voldoet aan de geselecteerde BIO- en PCF-normen.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de eerder genoemde gebruikers en dient niet te worden verspreid aan of te worden gebruikt door anderen.

3.7 Verantwoordelijkheden van het Inlichtingenbureau

Het Inlichtingenbureau is verantwoordelijk voor:

- Het opstellen van de verklaring zoals in hoofdstuk 2 is opgenomen;
- Het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om aan de geselecteerde BIO- en PCF-normen te voldoen.

3.8 Onze verantwoordelijkheden voor de assurance-opdracht

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de verklaring van het management nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de NOREA Richtlijn 3000A ‘Assuranceopdrachten door IT-auditors in de Attestvorm’.

Onze werkzaamheden bevatten het toetsen van de werking van de interne beheersingsmaatregelen die wij noodzakelijk achten bij het verschaffen van een redelijke mate van zekerheid dat dat de geselecteerde BIO maatregelen die in de verklaring staan vermeld gedurende de verslagperiode zijn opgezet en effectief zijn.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.

Amsterdam, 2 maart 2023

Baker Tilly (Netherlands) N.V.

drs. M.M.H. van Ernst RE
Partner IT Advisory