Jaarverslag privacy BSR 2024

Colofon

Titel	:	Jaarverslag privacy BSR 2024
Opdrachtgever	:	Directeur
Auteur	:	Functionaris Gegevensbescherming en Archief (FG)
Versie	:	1.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d. 13 maart 2025

W. van Wikselaar
Voorzitter

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

1 Voorwoord

In 2024 is de nieuwe Functionaris Gegevensbescherming (FG) en Archief op interim basis aangesteld. Het vinden van een juiste en volwaardige invulling van deze functie heeft de nodige tijd in beslag genomen nadat de vorige FG met pensioen is gegaan.

Gedurende 2024 zijn de werkzaamheden met de PDCA cyclus vanuit ons Information Security Management (ISMS) voortgezet. Dit systeem biedt ons inzicht op de status van de verschillende normen van de Baseline Informatiebeveiliging Overheid (BIO). Uit de PDCA cyclus zijn verder geen nieuwe onvolkomenheden naar voren gekomen.

In bijgevoegd jaarverslag vindt u op hoofdlijnen de weerslag van de verrichte werkzaamheden, de bevindingen over het afgelopen jaar en aanbevelingen voor het komende jaar.

Tiel, 3 maart 2025.

S. Sultani
Functionaris Gegevensbescherming en Archief

2 Samenvatting

Conform artikel 38 lid 3 van de Algemene verordening gegevensbescherming (AVG) brengt de Functionaris voor gegevensbescherming (FG) rechtstreeks verslag uit aan het hoogst leidinggevende niveau van de verwerkingsverantwoordelijke.

De Algemene Verordening Gegevensbescherming (AVG) wordt gehandhaafd vanaf 25 mei 2018. Deze verordening is twee jaren eerder ingegaan. Die twee jaren waren bedoeld om organisaties de gelegenheid te geven alle voorbereidingen te treffen om een juiste toepassing van de regelgeving te bewerkstelligen.

Het algemeen bestuur van BSR heeft op 16 mei 2018 het “Centrale Privacybeleid BSR” vastgesteld. In het vastgestelde beleid wordt uitgegaan van de “Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Per 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) gekomen. De BIO is het basis-normenkader voor informatiebeveiliging binnen alle overheidslagen (rijk, provincies, gemeenten en waterschappen), waarbij 2019 als overgangsjaar was ingesteld.

Met bovengenoemde toelichting heeft er een herziening van het “Centraal Privacybeleid BSR” plaatsgevonden. Hiertoe is het “Privacybeleid BSR 2022 - 2024” op 16 juni 2022 vastgesteld.

In 2024 zijn de werkzaamheden met het ISMS[1] en de controle op alle maatregelen voortgezet. Binnen de PDCA cyclus zijn hierin geen nieuwe onvolkomenheden naar voren gekomen. Om te voldoen aan de normen van de BIO, gebruikt het systeem enkele verplichte activiteiten waarmee op interval basis per norm een controle plaatsvindt. Hiermee wordt aantoonbaar dat BSR als organisatie op de juiste wijze aandacht en opvolging geeft aan de informatiebeveiliging en privacy.

In de voortgang van de ontwikkeling van procesbeschrijvingen via de Landelijke Lokale Belasting Processen (LLBP) zijn flinke stappen gemaakt. De activiteiten van de LLBP zijn ondergebracht in de stichting LLBP. Het aantal deelnemers aan de LLBP is gedurende 2024 wederom gegroeid.

In 2024 heeft BSR gewerkt met Virtual Private Network (VPN) en een uitgebreide controle voor Multi-factor Authenticatie (MFA) voor de beveiliging van haar eigen systemen. De systemen zijn hierdoor nog beter beveiligd buiten het eigen netwerk.

In 2024 is binnen BSR aandacht besteed aan het creëren van awareness omtrent AVG en privacy op de werkvloer. Ten behoeve hiervan is een sessie gecreëerd die medewerkers informeert over hun rechten met betrekking tot privacy en het belang van beschermen van persoonlijke informatie tegen misbruik, diefstal en ongeautoriseerde toegang.

Concluderend kan, terugkijkend op deze verslagperiode, worden gesteld dat er serieuze stappen zijn en worden gezet op het gebied van de BIO en aanscherping van de privacy- en informatiebeveiligings-processen en het creëren awareness omtrent AVG en privacy. Voor 2025 zal de aandacht vooral uitgaan naar nog meer awareness op deze onderdelen.

[1] ISMS: Information Security Management System. Een ISMS betreft alle zaken en de werkwijze voor het beveiligen van alle (vertrouwelijke) informatie binnen de organisatie.

3 Ontwikkelingen in 2024

3.1 Visie en ethiek

BSR is een vernieuwende en inclusieve organisatie. Dit kenmerkt ook onze kijk op privacy. De informatie die wij opvragen bij belastingplichtigen en samenwerkingspartners is enkel hetgeen dat echt nodig is om onze werkzaamheden naar behoren uit te kunnen voeren. Wij gaan dan ook met uiterste zorg om met deze informatie. Wij gaan uiteraard even zorgvuldig om met de persoonsgegevens van onze medewerkers binnen de daarvoor gestelde kaders.

3.2 Privacyontwikkelingen van binnenuit

In 2024 is binnen BSR gewerkt aan het actualiseren van het privacybeleid. Een cruciaal aspect hierbij is informatie en de beveiliging hiervan. Wij kunnen als heffende organisatie niet om informatiebeveiliging en informatiesystemen heen, de informatiesystemen vormen immers het zenuwstelsel van onze organisatie en van de (keten)partners waarmee wij zaken doen. De systemen die gebruikt worden kunnen alleen goed functioneren wanneer de beveiliging ervan op orde is. Dat wil zeggen: wanneer wij ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd blijft. Het doel hiervan is de informatie te beschermen tegen interne en externe bedreigingen.

In 2024 is binnen BSR ook gewerkt aan het creëren van privacy bewustwording. Ten behoeve hiervan is een sessie ontwikkeld die als doel heeft het vergroten van het bewustzijn van medewerkers over hoe persoonlijke gegevens worden verzameld, gebruikt, opgeslagen en gedeeld. De sessie omvat het informeren van medewerkers over hun rechten met betrekking tot privacy en het belang van het beschermen van persoonlijke informatie tegen misbruik, diefstal of ongeautoriseerde toegang.

3.3 BIO

Voor het uitvoeren van informatiebeveiliging maakt BSR gebruikt van de BIO-normen. De BIO geeft meer ruimte om op basis van een risicoafweging (risicomanagement) zelf te bepalen of bepaalde maatregelen nodig zijn om risico’s af te dekken. In dat kader is de insteek van risicomanagement dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging en privacy.

Met behulp van het ISMS is in 2024 wederom gewerkt met de PDCA. Hierbinnen zijn geen nieuwe onvolkomenheden naar voren gekomen.

3.4 Audit / assessment

Een privacy audit is een systematisch proces waarbij de privacypraktijken en -beleid van BSR worden geëvalueerd om te bepalen in hoeverre ze voldoen aan de wet- en regelgeving, evenals de effectiviteit van de genomen maatregelen ter bescherming van persoonlijke gegevens. Hiermee worden risico’s geïdentificeerd, naleving gewaarborgd en verbeterpunten te signaleren. Informatiebeveiliging en privacy maken onderdeel uit van de jaarlijkse te houden audits en assessment zoals:

- Verbijzonderde interne controle (VIC), intern en check door accountant;
- BAG audit, self-assessment in samenwerking met de gemeenten Montfoort en IJsselstein;
- ISO 9001 certificering door Dekra
- ICT-beveiligingsassessment DIGID, Logius; en
- Kantoorautomatisering 27001, certificering door leveranciers van BSR.

Deze verantwoordingen hebben in de loop van 2024 plaatsgevonden.

3.5 Verwerkers en verwerkersovereenkomsten

In 2024 is met een aantal bestaande en nieuwe verwerkers een (nieuwe of aangepaste) verwerkers-overeenkomst afgesloten. Een actueel overzicht hiervan is beschikbaar in de ISMS-tool. Door de verwerkers zijn geen incidenten gerapporteerd.

3.6 Rechten betrokken

In de privacyverklaring op de website van BSR (www.bsr.nl) is informatie opgenomen voor betrokkenen. BSR hecht veel waarde aan de privacy van gebruikers en zorgt voor een veilige en transparante manier van de behandeling van persoonsgegevens. In de verklaring wordt uitgelegd welke gegevens verzameld worden, hoe deze gebruikt worden en welke rechten je als bezoeker hebt met betrekking tot je persoons-gegevens.

Op de website zijn tevens de mogelijkheden tot het indienen van een verzoek of klacht op de website voorzien. Er zijn formats opgesteld voor de ontvangstbevestiging, afwijzing en toewijzing van een verzoek. Ook is een stroomschema opgesteld hoe een verzoek behandeld moet worden. In 2024 wordt er ook specifiek melding gemaakt op welke wijze BSR omgaat met zogenaamde cookies op onze website.

3.7 Beveiligingsincidenten, datalekken en verzoeken AVG

Met onderstaande tabel wordt inzicht gegeven op de inbreuk van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. Maar ook de inbreuk van een ongeoorloofde of onopzettelijke wijziging van persoonsgegevens. Daarnaast geeft het inzicht over de rechten van betrokkenen volgens artikel 13 t/m 22 van de AVG welke zijn toegepast in 2024.

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
Datalekken	1	Aanslag naar verkeerde persoon gestuurd	Afgehandeld
Datalek AP	1	Aanslag naar verkeerde persoon gestuurd	Afgehandeld
Incidenten			
Incidenten	1	Geklikt op phishing email	Hersteld
Incidenten	1	Privémap toegankelijk intern	Hersteld
Incidenten	1	Phishing email met QR code in omloop	
			Hersteld
Toegangsbeveiliging	0	Geen meldingen	-
AVG			
Rechtmatigheid	0	Privé adres op zakelijke aanslag	-
Inzageverzoek	0	Recht van inzage	-

Genoemde beveiligingsincidenten zijn onderzocht, waarbij bepaald is welke inbreuk van toepassing is en of er sprake is van een beveiligingsincident, sprake is van een datalek of dat het een niet geslaagde poging tot inbreuk betreft. Op basis van deze gegevens kan worden gesteld dat er geen ernstige datalek heeft plaatsgevonden. Bij 1 datalek is er een brief verstuurd naar een verkeerde klant. Herstelacties waren afdoende en medewerkers zijn hierop gewezen.

3.8 Governance

Er is een duidelijke structuur ten aanzien van de uitvoering van de AVG. Het dagelijks bestuur heeft een Chief Information Security Officer (CISO), een Privacy Officer (PO) en een Functionaris voor de gegevensbescherming (FG) aangewezen. Deze onderlinge relaties en verantwoordelijkheden blijken uit de vastgestelde beleidsdocumenten voor informatiebeveiliging en privacy. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient te kunnen aantonen ‘in control’ te zijn aangaande de uitvoering van de AVG.

Uitvoering informatiebeveiliging en privacy

- IB-team : bestaande uit CISO (voorzitter), FG en PO;
  (vergaderen 1 maal per maand tenzij er beveiligingsissues zijn)
- Escalatieteam : bestaande uit directeur (voorzitter), FG, CISO, PO en verantwoordelijke manager;
  (vergaderen alleen bij een datalek)
- Privacy team : bestaande uit directeur (voorzitter), managers, FG, CISO en PO.
  (vergaderen 2 maal per jaar bij voorkeur in mei en november)

3.9 Bewustwording

In 2024 is binnen BSR gewerkt aan het creëren van privacy bewustwording. Ten behoeve hiervan is een sessie ontwikkeld die als doel heeft het vergroten van het bewustzijn van medewerkers over hoe persoonlijke gegevens worden verzameld, gebruikt, opgeslagen en gedeeld. De sessie omvat het informeren van medewerkers over hun rechten met betrekking tot privacy en het belang van het beschermen van persoonlijke informatie tegen misbruik, diefstal of ongeautoriseerde toegang.

Ook wordt het belang benadrukt van veilige online gewoonten, zoals het gebruik van sterke wachtwoorden, het herkennen van nep e-mails en het kritisch nadenken over de gegevens die online gedeeld worden. Deze sessie zal in 2025 intern bij BSR verzorgd worden door de FG.

Daarnaast is door de FG in 2024 een e-learning module gevolgd over bewustwording omtrent AVG en privacy als experiment. Deze module heeft de FG als positief ervaren en zij is van mening dat dit van toegevoegde waarde zal zijn voor het creëren van bewustheid bij de medewerkers van BSR. Dit zal in 2025 mogelijk aangeboden worden aan de medewerkers van BSR.

Elke nieuwe medewerker doorloopt in de eerste werkweek een aantal modulen die aandacht besteden aan onder andere informatieveiligheid, integriteit en privacy. Dit draagt bij aan de bewustwording op deze thema's. We proberen hier middels awareness sessies opvolging aan te blijven geven.

3.10 Bewaring en vernietiging versus archiefwet en privacybeleid

De archiefwet en het privacybeleid omvatten de gehele 'data life cycle': van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

In 2024 heeft een nulmeting plaatsgevonden met behulp van de handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO). Deze nulmeting is uitgevoerd door het Regionaal Archief Rivierenland (RAR).

Het advies was hierbij om op basis van de resultaten van deze nulmeting een prioritering aan te brengen en de kwaliteitszorg in een jaarcyclus op te nemen. BSR heeft ervoor gekozen de verbeteracties op projectmatige werkwijze aan te pakken.

De volgende actiepunten zijn van belang:

- Er zal een kwaliteitssysteem voor informatiebeheer geïmplementeerd worden waarover de archiefinspecteur periodiek geïnformeerd wordt.
- De archiefbescheiden die onder beheer van BSR zijn moeten metagegevens toegekend krijgen.
- Er dient een vervangingsbesluit voor analoge archiefbescheiden genomen te worden.

Opslag en vernietiging van archief vinden tijdig en op wettelijke grondslag plaats. Zo is in 2024 de opdracht gegeven om bepaalde documenten uit het archief bij BSR volgens de geldende selectielijsten te laten vernietigen. Hetzelfde geldt voor de stukken die in beheer zijn bij het Regionaal Archief Rivierenland.

4 Conclusie en aanbeveling

Het is belangrijk om de bescherming van persoonsgegevens goed te borgen. Zowel vanuit privacy-overwegingen, als vanuit informatiebeveiliging.

4.1 Conclusie

Terugkijkend op deze verslagperiode kan gesteld worden dat er mooie stappen zijn gezet op het gebied van met name informatiebeveiliging. Met de inrichting van het Information Security Management System (ISMS) kan BSR de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO) continu bewaken. Op dit terrein loopt BSR voor op vergelijkbare organisaties.

Voorts kan terugkijkend gesteld worden dat er zeker stappen zijn gezet op het gebied van privacybeleid en het creëren van awareness binnen BSR. Met name de informatiebeveiliging is hierin aangescherpt door het nemen van maatregelen die ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd blijft. Ook zijn er mooie stappen gezet op het gebied van privacy bewustwording. Ten behoeve hiervan is een sessie ontwikkeld die als doel heeft het vergroten van het bewustzijn van medewerkers over hoe persoonlijke gegevens worden verzameld, gebruikt, opgeslagen en gedeeld. Ook wordt het belang benadrukt van veilige online gewoonten, zoals het gebruik van sterke wachtwoorden, het herkennen van neppe e-mails en het kritisch nadenken over de gegevens die online gedeeld worden.

Terugkijkend kan verder geconcludeerd worden dat de essentiële archiefwerkzaamheden binnen BSR conform de geldende wetten en regels zijn uitgevoerd.

Er hebben zich geen noemenswaardige incidenten voorgedaan op het terrein van privacy en informatie-beveiliging in 2024.

4.2 Aanbeveling

Informatiebeveiliging en Privacy zijn binnen BSR goed georganiseerd en er zijn voldoende aantoonbare beheersmaatregelen om dit te kunnen monitoren. De nodige handvaten zijn ontwikkeld voor het creëren van awareness op de werkvloer omtrent AVG en privacy.

In 2025 moet de aandacht vooral liggen op het verder vergroten van meer awareness bij de medewerkers. Ook de werkzaamheden, die gedaan moeten worden in het verlengde van de Archiefwet, vragen in 2025 de nodige focus en aandacht.

Bijlage 1 Organogram BSR 2024