Jaarverslag privacy BSR 2023

Colofon

Titel	:	Jaarverslag privacy BSR 2023
Opdrachtgever	:	Directeur
Auteur	:	Chief Information Security Officer (CISO)
Versie	:	1.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d. 14 maart 2024

G. van Bezooijen
Voorzitter

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

Colofon 2
1 Voorwoord 4
2 Samenvatting 5
3 Ontwikkelingen in 2023 6
3.1 Informatiebeveiliging (BIO) 6
3.2 Audit / assessment 6
3.3 Verwerkers en verwerkersovereenkomsten 6
3.4 Rechten betrokken 6
3.5 Beveiligingsincidenten, datalekken en verzoeken AVG 7
3.6 Governance 7
3.7 Bewustwording 7
3.8 Bewaring en vernietiging versus archiefwet en privacybeleid 8
4 Conclusie en aanbeveling 9
4.1 Conclusie 9
4.2 Aanbeveling 9
Bijlage 1 Organogram BSR 2023 10

1 Voorwoord

In 2023 is onze Functionaris Gegevensbescherming (FG) met pensioen gegaan. Het vinden van een juiste en volwaardige invulling van deze functie heeft de nodige tijd in beslag genomen. Goed om te melden is dat wij op het moment van schrijven een Functionaris Gegevensbescherming & Archief op interim basis hebben kunnen aanstellen.

Gedurende 2023 is voor het eerst met de PDCA cyclus vanuit ons Information Security Management System (ISMS) gewerkt. We zien dat dit nog wat verder aangescherpt kan worden, maar het biedt ons al wel inzicht op de status van de verschillende normen van de Baseline Informatiebeveiliging Overheid (BIO).

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, 21 februari 2024

Dustin van Berkum
Chief Information Security Officer

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. Bij BSR is de CISO plaatsvervangend FG.

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 2023 heeft de eerste PDCA cyclus van de Information Security Management System (ISMS) tool plaatsgevonden. 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. Goed om te melden is dat in 2023 het aantal deelnemers aan de LLBP flink gegroeid is en inmiddels ook de Vereniging Nederlandse Gemeenten (VNG) zich heeft aangesloten. Vanaf eind 2023 zijn de activiteiten van de LLBP ondergebracht in de stichting LLBP.

In 2023 heeft BSR een aanpassing doorgevoerd in de beveiliging van haar eigen systemen. Er werd voor 2023 al met een combinatie van wachtwoord, Virtual Private Network (VPN) & Multi-factor Authenticatie (MFA) gewerkt. Inmiddels is er overgestapt naar een uitgebreidere controle voor MFA waardoor systemen nog beter beveiligd zijn buiten het eigen netwerk.

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. Voor 2024 zal de aandacht vooral uitgaan naar nog meer awareness op deze onderdelen.

3 Ontwikkelingen in 2023

3.1 Informatiebeveiliging (BIO)

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 2023 de eerste PDCA cyclus gestart. Hierbij zijn we tot de conclusie gekomen dat de huidige PDCA cyclus nog wat verfijning vraagt. Nu komen alle acties die gecontroleerd dienen te worden op hetzelfde moment naar voren. Dit genereert een grote werkvoorraad die niet altijd binnen de gestelde periode kan worden verwerkt. Dit vraagt om betere fasering.

3.2 Audit / assessment

Een audit of assessment is een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van bewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de criteria is voldaan. 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 2023 plaatsgevonden.

3.3 Verwerkers en verwerkersovereenkomsten

In 2023 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.

3.4 Rechten betrokken

In de privacyverklaring op de website van BSR (www.bsr.nl) is informatie opgenomen voor betrokkenen. Tevens zijn 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 2023 wordt er ook specifiek melding gemaakt op welke wijze BSR omgaat met zogenaamde cookies op onze website.

3.5 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 2023.

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
Datalekken	1	Brief voor 1 klant naar verkeerde klant verstuurd	Afgehandeld
	1	Brief voor 1 klant naar verkeerde klant verstuurd	Afgehandeld
Datalek AP	2	2 meldingen doorgegeven aan de AP	Afgehandeld
Incidenten			
Incidenten	1	BSN vermeld op brief richting 1 klant	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 2 datalekken is er een brief verstuurd naar een verkeerde klant. Bij 1 datalek was er door menselijk handelen een BSN gecommuniceerd dat niet nodig is in communicatie met de klant. Herstelacties waren afdoende en medewerkers zijn hierop gewezen.

3.6 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)

3.7 Bewustwording

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. In 2023 is dit met het vertrek van onze FG slechts minimaal gelukt. We gaan hier in 2024 meer op inzetten.

3.8 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 2023 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. Op dit terrein zijn nog stappen te zetten. Onze functionaris Gegevensbescherming en Archief gaat hiermee in 2024, met de juiste prioritering, aan de slag.

Opslag en vernietiging vinden tijdig en op wettelijke grondslag plaats.

4 Conclusie en aanbeveling

Het is belangrijk om de bescherming van persoonsgegevens goed te borgen. Zowel vanuit privacyoverwegingen, 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.

Er hebben zich geen noemenswaardige incidenten voorgedaan op het terrein van privacy en informatie-beveiliging in 2023.

4.2 Aanbeveling

Informatiebeveiliging en Privacy zijn binnen BSR goed georganiseerd en er zijn voldoende aantoonbare beheersmaatregelen om dit te kunnen monitoren.

In 2024 moet de aandacht vooral liggen op nog meer awareness bij de medewerkers.
Ook de werkzaamheden, die gedaan moeten worden in het verlengde van de Archiefwet, vragen in 2024 de nodige focus en aandacht.

Bijlage 1 Organogram BSR 2023