Jaarverslag privacy BSR 2022

Colofon

Titel	:	Jaarverslag privacy BSR 2022
Opdrachtgever	:	Directeur
Auteur	:	Functionaris voor de gegevensbescherming (FG)
Versie	:	1.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d. 7 maart 2023

G. van Bezooijen
Voorzitter

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

1 Voorwoord

Ook in 2022 had COVID-19 nog invloed op ons werken. Ons kantoorgebouw was begin 2022 nog beperkt geopend maar in de loop van 2022 waren er geen beperkingen meer.

De geschetste omstandigheden zorgden er ook in 2022 nog voor dat de plannen tot het verder investeren in de ontwikkeling en vergroting van de bewustwording van medewerkers op informatiebeveiliging en privacy, nog voornamelijk via intranet plaatsvond.

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 januari 2023
Functionaris voor de gegevensbescherming

2 Samenvatting

Conform artikel 38 lid 5 van de Algemene verordening gegevensbescherming (AVG) brengt de Functionaris voor gegevensbescherming (FG) rechtstreeks verslag uit aan het hoogst leidinggevende niveau van de verwerkingsverantwoordelijke.
Dit jaarverslag is het verslag van de FG van BSR over het jaar 2022.

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.

Bovengenoemde toelichting en de 3 jaarlijkse verplichte actualisatie van het beleid is waardoor er een herziening van het “Centraal Privacybeleid BSR” heeft plaatsgevonden. Hiertoe is het “Privacybeleid BSR 2022 - 2024” op 16 juni 2022 vastgesteld.

BSR is op beleidsniveau in control en neemt momenteel vervolgstappen in de uitvoering. Hiertoe zijn de volgende beleidsdocumenten geschreven en vastgesteld door het dagelijks bestuur:

- Strategisch Informatiebeveiligingsbeleid BSR 2021-2023;
- Tactische Informatiebeveiligingsbeleid BSR 2022-2024;
- Uitvoeringsplan Informatie Security Management System (ISMS) BSR 2021-2023; en
- Privacybeleid BSR 2022–2024.

Voor de uitvoering van informatiebeveiliging is het “Operationeel Informatiebeveiligingsbeleid 2022-2024” geschreven. Dit wordt momenteel voorbereid voor besluitvorming in het MT.
Daarnaast heeft in 2022 de inrichting van de ISMS tool (systeem) plaatsgevonden, zodat het continu verbeterproces van informatiebeveiliging en privacy kan plaatsvinden (managementinstrument).
Om te voldoen aan een norm zoals de ISO 27001/27002, zal het systeem enkele verplichte activiteiten zoals een interne en externe audit omvatten. Hiermee wordt aantoonbaar dat BSR als organisatie op de juiste wijze aandacht en opvolging geeft aan de informatiebeveiliging en privacy.

De voortgang van de ontwikkeling van procesbeschrijvingen via de Landelijke Lokale Belasting Processen (LLBP) loopt op schema en er wordt hard gewerkt aan voltooiing. Van hieruit wordt het verwerkingsregister bij gewerkt en kan ook de inzet voor het houden van een Data protection impact assessment (DPIA) gestalte krijgen.

Concluderend kan, terugkijkend op deze verslagperiode, worden gesteld dat er serieuze stappen zijn en worden gezet op het gebied van awareness (bewustzijn) en verfijning van de privacy- en informatie-beveiligingsprocessen.

3 Ontwikkelingen in 2022

3.1 Covid-19

BSR heeft, mede door Covid-19, ingestoken op hybride werken als passende werkvorm. Bij het opstellen van de regels voor het thuiswerken en digitaal vergaderen zijn de aspecten van informatiebeveiliging en privacy meegenomen in de afwegingen en de inrichting ervan. Dat laat zien dat de bescherming van persoonsgegevens stevig verankerd is in het beleid van BSR. De aandacht voor het beschermen van de privacy van burgers stond mede door het digitaal werken ook centraal in 2022!

3.2 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.
Ter ondersteuning van dit proces beschikt BSR over een softwareoplossing in de vorm van ISMS-tooling. Deze tool is ondersteunend aan de bedrijfsprocessen en geeft die ondersteuning die nodig is om het juiste basisbeveiligingsniveau (BBN) te bepalen met de daaraan gekoppelde controls en overheids-maatregelen vanuit de ISO/IEC 27001/2.
Deze BBN's met de controls en overheidsmaatregelen zijn ook nader uitgewerkt in het tactisch informatiebeveiligingsbeleid van BSR.

3.3 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 criteriums is voldaan.
Informatiebeveiliging en privacy maken onderdeel uit van de jaarlijkse te houden audits en assessement zoals:

- Dekra audit ten behoeve van ISO 9001, door externe auditor;
- Verbijzonderde interne controle (VIC), intern en check door accountant;
- BAG audit, zelf assessment in samenwerking met de gemeenten Montfoort en IJsselstein;
- WOZ audit, zelf assessment vanuit de Ensia vragenlijst WOZ deelnemende gemeenten;
- ICT-beveiligingsassessment DIGID, Logius; en
- Kantoorautomatisering 27001, certificering door leveranciers van BSR.

Deze verantwoordingen hebben in de loop van 2022 plaatsgevonden.

3.4 Verwerkers en verwerkersovereenkomsten

In 2019 zijn de meeste verwerkersovereenkomsten tot stand gekomen. In 2022 is met een aantal bestaande en nieuwe verwerkers een (nieuwe of aangepaste) verwerkersovereenkomst afgesloten.
Een actueel overzicht hiervan is beschikbaar in de ISMS-tool. Door de verwerkers zijn geen incidenten gerapporteerd.

3.5 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.

3.6 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 2022.

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
datalekken intern en extern	1	geldigheid cookie	afgehandeld
	1	koppeling subject/object niet juist (KvK)	hersteld
datalek AP	0	geen meldingen	-
Incidenten			
interne incidenten	1	beveiligingsalarm inloggen	afgehandeld
	1	werking duo app	afgehandeld
toegangsbeveiliging	0	geen meldingen	-
AVG			
rechtmatigheid	2	privé adres op zakelijke aanslag	in behandeling
inzageverzoek	1	recht van inzage	afgehandeld

Genoemde beveiligingsincidenten zijn onderzocht, waarbij bepaald is welke inbreuk van toepassing is en of er sprake is van een beveiligingsincident, sprake 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. Herstel acties waren afdoende.

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

3.8 Bewustwording

Elke nieuwe medewerker doorloopt in de eerste werkweek een aantal modulen die aandacht besteden aan informatieveiligheid, ons werk als BSR, onze positie in het bestuurlijke veld, onze missie, integriteit en nog veel meer. De modules geven ook praktische informatie, wat het werken de eerste periode makkelijker maakt.
Op deze manier wordt de actualiteit van informatieveiligheid geborgd.

3.9 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.

Er heeft in 2020 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. Dit is in 2021 uitgezet in de organisatie en heeft een vervolg gehad in 2022 en zal ook in 2023 doorlopen.

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 privacy-overwegingen, als vanuit informatiebeveiliging.

4.1 Conclusie

Privacy en dataprotectie (bescherming van persoonsgegevens) zijn grondrechten. De privacywetgeving blijft hetzelfde, ook als de omstandigheden veranderen.
Terugkijkend op deze verslagperiode kan gesteld worden dat er serieuze stappen zijn gezet op het gebied van beleid, awareness en verfijning van de privacy processen. Hierbij moet niet worden vergeten dat de uitvoering ook extra inzet vraagt!.

4.2 Aanbeveling

BSR heeft de beschrijvingen van haar primaire processen en bedrijfsvoeringsprocessen grotendeels geactualiseerd (LLBP).
Het verdient aanbeveling nadat de beschrijvingen van deze processen zijn voltooid, ook het “Verwerkingsregister” bij te werken zodat er een start kan worden gemaakt met de uitvoering van een DPIA. Hiermee is rekening gehouden in de begroting.

Bijlage 1 Organogram BSR 2022