Jaarverslag privacy BSR 2021

Colofon

Titel	:	Jaarverslag privacy BSR 2021
Opdrachtgever	:	Directeur
Auteur	:	Functionaris voor de gegevensbescherming (FG)
Versie	:	2.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d. 17 maart 2022

Ir. J.H.L.M. de Vreede
Voorzitter

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

1 Voorwoord

Ook in 2021 was COVID-19 van invloed op ons werken, met het dringende verzoek om zoveel mogelijk thuis te werken. Uitzonderingen vormden onder andere de functies waarvoor het werken op kantoor noodzakelijk was. Daarnaast was ons kantoorgebouw langere tijd beperkt geopend. Onze medewerkers werkten dus veel vanaf de thuiswerkplek.

Bij de uitvoering van informatieveiligheid en privacy blijkt dat de onderlinge sociale relaties belangrijk zijn. Dit aspect hebben we in dit kader minder kunnen uitwerken. De geschetste bijzondere COVID-19 omstandigheden zorgden ervoor dat de plannen tot het verder investeren in de ontwikkeling en vergroting van de bewustwording van medewerkers op privacy, voornamelijk via intranet konden plaatsvinden.

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, 15 februari 2022
Functionaris voor de gegevensbescherming

2 Samenvatting

De Algemene Verordening Gegevensbescherming (AVG) wordt gehandhaafd vanaf 25 mei 2018. De verordening is al 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 basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (rijk, gemeenten, provincies en waterschappen), waarbij 2019 als overgangsjaar is ingesteld. Had voorheen iedere overheidslaag zijn eigen baseline, nu is er één BIO voor de gehele overheid. Mede hierdoor wordt er momenteel een nieuw ‘Privacybeleid BSR’ voorbereid. Dit nieuwe Privacybeleid zal naar verwachting in het eerste kwartaal van 2022 ter besluitvorming in het dagelijks bestuur worden ingebracht.

BSR is op beleidsniveau in control en neemt momenteel vervolgstappen in de uitvoering. Hiertoe zijn de noodzakelijke beleidsdocumenten geschreven en vastgesteld zoals:

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

Als aanbeveling wordt aangemerkt het inzetten van een data protection impact assessment (DPIA) als instrument, om vooraf de privacyrisico’s van gegevensverwerking in kaart te brengen. Dit om preventief maatregelen te kunnen nemen en risico’s te verkleinen (zie paragraaf 3.2). Momenteel wordt procesmatig gekeken naar de invoering van het instrument “Data protection impact assessment”. Hiermee is rekening gehouden in de begroting van 2021 - 2022.

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

3 Ontwikkelingen in 2021

3.1 Covid-19

Het jaar 2021 was een interessant vervolg op de voorgaande drie jaren van de AVG. Als organisatie hebben wij in 2020 en 2021 als gevolg van Covid-19, heel andere prioriteiten moeten stellen. Bijvoorbeeld bij het opstellen van spelregels voor het thuiswerken, bij het inrichten van digitaal vergaderen. Steeds zijn de aspecten van privacy meegenomen in de afwegingen en de inrichting. Dat laat zien dat de bescherming van persoonsgegevens stevig verankerd is in het beleid van BSR. De verhoogde aandacht voor het beschermen van de privacy van burgers stond mede door het digitaal werken centraal in 2021.

3.2 Data Protection Impact Assessment (DPIA)

BSR heeft ervoor gekozen om in het laatste kwartaal van 2019 over te stappen naar de SaaS oplossing van Centric. Centric zorgt dat de 'achterkant' betrouwbaar is en de belastingoplossingen meegaan met de actuele ontwikkelingen, zoals wijzigingen in wet- en regelgeving.
Dit kan gevolgen hebben voor de routing van een aantal processen binnen BSR. Momenteel wordt dit nog geïnventariseerd en vastgelegd. Nadat de processen opnieuw zijn beoordeeld en vastgelegd zal het "Verwerkingsregister" worden bijgewerkt en kunnen we starten met de uitvoering van een DPIA.

3.3 Informatieveiligheid 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. De implementatie van de BIO wordt binnen BSR projectmatig aangestuurd, waarbij op basis van de uitkomsten een verbeterplan wordt opgesteld en uitgevoerd. Bij het formuleren van verbeteracties zal nadrukkelijk telkens de afweging worden gemaakt welke risico's met de verbeteractie worden afgedekt en in welke mate dat bijdraagt aan de betrouwbaarheid van de dienstverlening.
De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging.

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 overheidsmaatregelen vanuit de ISO/IEC 27002.
De BBN's met de controls en overheidsmaatregelen zijn nader uitgewerkt in het tactisch informatiebeveiligingsbeleid van BSR.

3.4 Audits

Een audit is een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan. Privacy is en maakt onderdeel uit van onderstaande gehouden audits.

Jaarlijks vinden o.a. de volgende audits plaats:

- Suwinet audit, door externe auditor;
- Dekra audit ten behoeve van ISO 9001, door externe auditor;
- Verbijzonderde interne controle (VIC), intern en check door accountant; en
- BAG audit, zelfcontrole in samenwerking met de gemeenten Montfoort en IJsselstein.

De verantwoording heeft in de loop van 2021 plaatsgevonden.

3.5 Verwerkers en verwerkersovereenkomsten

In 2019 zijn de meeste verwerkersovereenkomsten tot stand gekomen. In 2021 is met een aantal bestaande en nieuwe verwerkers een (nieuwe of aangepaste) verwerkersovereenkomst afgesloten.
Een actueel overzicht hiervan is beschikbaar in de ISMS-tool. Bestaande verwerkers hebben niet gerapporteerd over incidenten.

3.6 Rechten betrokken

In de privacyverklaring op de website van BSR 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.

3.7 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 2021.

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
datalekken intern en extern	1	presentatie verkeerde klantgegevens in de digitalebalie.	hersteld
	1	brief van ander burger aan geadresseerde.	afgehandeld
datalek AP	1	valt niet onder de categorie datalek voor AP.	hersteld
Incidenten			
interne incidenten	5	waarvan 2 beveiligingsincidenten.	hersteld
toegangsbeveiliging	0	geen melding ontvangen.	-
AVG			
rechtmatigheid	4	gebruik BSN op aanslag.	afgehandeld
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 ernstig datalek heeft plaatsgevonden. Herstelacties waren afdoende.

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 Informatiebeveiligingsfunctionaris (IBF) en een Functionaris voor de gegevensbescherming (FG) aangewezen. Deze onderlinge relaties en verantwoordingen blijken uit de vastgestelde beleidsdocumenten voor beveiliging. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen ‘in control’ te zijn aangaande de uitvoering van de AVG (zie ook bijlage 1).

3.9 Bewustwording

Elke nieuwe medewerker doorloopt in de eerste werkweek een aantal modulen over informatieveiligheid en die aandacht besteden aan 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.
Sinds najaar 2020 maken wij gebruik van de modulen:

- i-bewustzijn;
- integriteit;
- meldplicht datalekken;
- omgaan met social media;
- privacy; en
- veilig thuiswerken.

Op deze manier wordt de actualiteit van informatieveiligheid geborgd.

3.10 Bewaring en vernietiging versus archiefwet / 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 is 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 er voor gekozen de verbeteracties op projectmatige werkwijze aan te pakken. Dit is uitgezet in de organisatie en is in 2021 opgestart en heeft een vervolg in 2022.
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 de beveiliging van informatie en het (be)veilig(d) omgaan met informatie, gegevens en documenten.

4.1 Conclusie

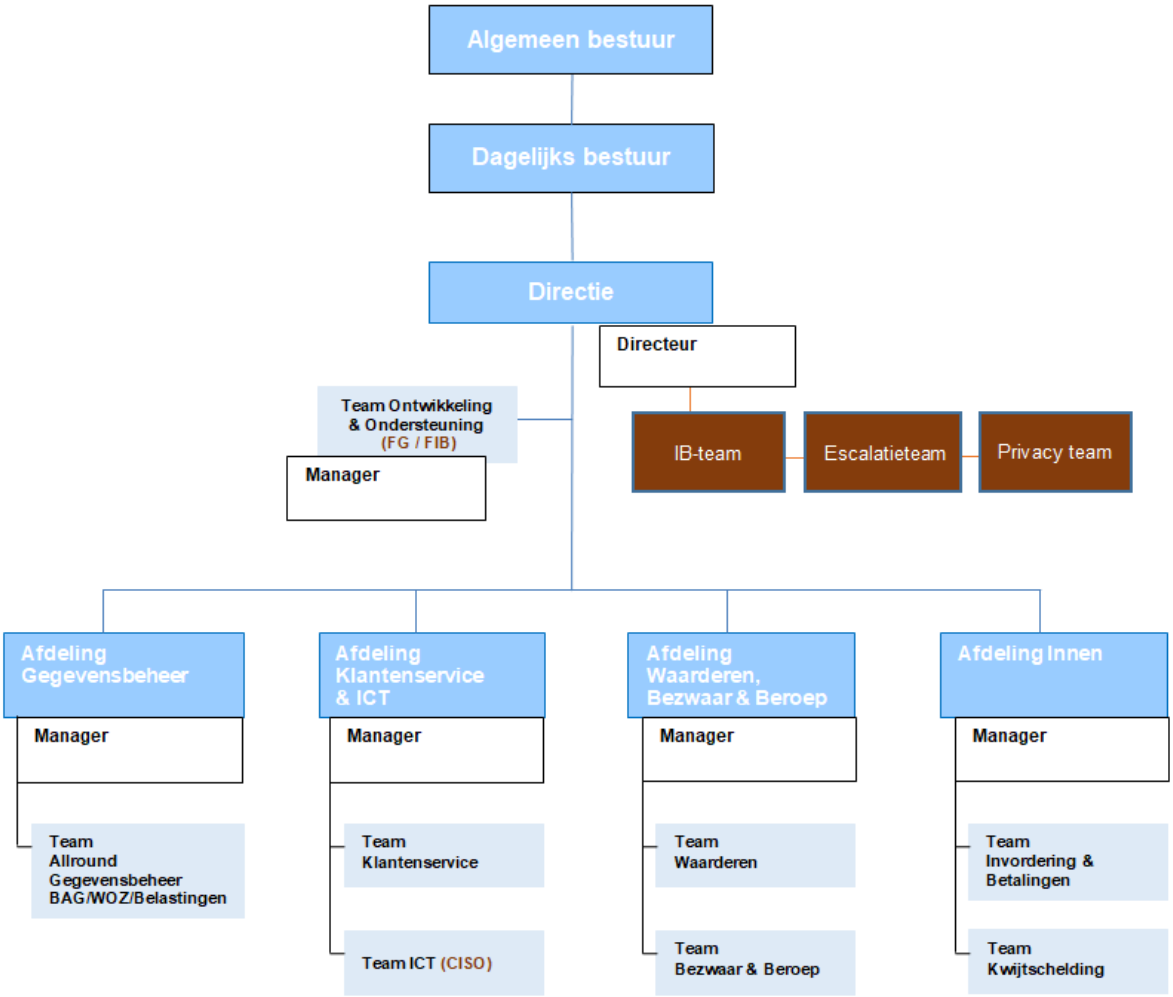
Privacy en dataprotectie (bescherming van persoonsgegevens) zijn grondrechten. En dat blijven het, ook nu in tijden van COVID-19. De privacywetgeving blijft hetzelfde, alleen zijn de omstandigheden nu even anders. Onder deze extreme omstandigheden maakt de privacywetgeving het uiteraard mogelijk om tijdelijk andere afwegingen te maken.
Terugkijkend op deze verslagperiode kan gesteld worden dat er serieuze stappen zijn gezet op het gebied van awareness en verfijning van de privacy processen in een moeilijke periode.

4.2 Aanbeveling

Het verdient extra aanbeveling om het houden van een data protection impact assessment (DPIA) als instrument in te zetten, om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen. Dit om preventief maatregelen te kunnen nemen en risico's te verkleinen.

Inmiddels is vastgesteld dat BSR hiertoe rekening heeft gehouden, ook in haar begroting. BSR heeft haar primaire processen en bedrijfsvoeringsprocessen grotendeels geactualiseerd. In de loopt van 2022 wordt dit traject afgerond. Nadat de processen opnieuw zijn beoordeeld op privacygevoeligheid zal het "Verwerkingsregister" worden bijgewerkt en starten wij met de uitvoering van een DPIA.

Bijlage 1 Organogram BSR 2021



Functies inzake privacy

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