Jaarverslag privacy BSR 2020

Colofon

Titel	:	Jaarverslag privacy BSR 2020
Opdrachtgever	:	Directeur
Auteur	:	Functionaris voor de gegevensbescherming (FG)
Versie	:	1.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d. 18 maart 2021

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

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

1 Voorwoord

Sinds 1 februari 2020 ben ik aangesteld als Functionaris voor de gegevensbescherming (FG) van BSR. De FG is door het dagelijks bestuur aangewezen als toezichthouder op de naleving van de AVG. De positie en taken van de FG zijn bij wet geregeld. Deze komen er op neer dat de FG in onafhankelijkheid vaststelt op welke punten de organisatie voldoet aan de AVG. Tevens signaleert de FG ook waar eventueel sprake is van terugval.

Om dit te kunnen doen, kan de FG:

- informatie verzamelen over gegevensverwerkingen binnen de organisatie;
- deze verwerkingen analyseren en beoordelen of ze aan de wet voldoen; en
- informatie, adviezen en aanbevelingen geven aan de organisatie.

In veel opzichten doet de rol van de FG denken aan die van de accountant. Echter, de FG combineert advies en toezicht, om op deze manier de organisatie houvast te bieden en te voorkomen dat er oplossingen achteraf moeten worden herzien. De naleving van de privacywet is geen verantwoordelijkheid van de FG, maar van de verwerkingsverantwoordelijke of de verwerker.

In het voorjaar van 2020 kregen wij te maken met de Corona restricties. Dit bemoeilijkte de uitvoering van de toezichthoudende taken. Het is een tijd van pionieren en samen ontdekken wat wel en niet mogelijk is. Echter, het reguliere proces blijft het vertrekpunt en dat is binnen onze organisatie bekend terrein.

Belangrijker is de constatering dat de aandacht voor gegevensbescherming binnen BSR het afgelopen jaar is gegroeid.

Tiel 25 februari 2021
Functionaris voor de gegevensbescherming

2 Samenvatting

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden.

Het Algemeen bestuur heeft op 16 mei 2018 het “Centrale Privacybeleid BSR” vastgesteld.
BSR geeft door de vaststelling van dit beleid duidelijk richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.
Het vastgestelde beleid was ook in 2020 nog actueel en voldeed aan de gestelde wet- en regelgeving.

BSR is op beleidsniveau in control en neemt momenteel vervolgstappen in de uitvoering.
Hiertoe zal in 2021 ter besluitvorming het “Uitvoeringsplan Informatie Security Management System (ISMS) 2021-2023 BSR” worden aangeboden.

Vervolgens zal dit uitvoeringsplan worden geïmplementeerd. Gelijktijdig zal het instrument “Data protection impact assessment” (zie paragraaf 3.2) worden ingevoerd.
Hiermee is rekening gehouden in de begroting van 2021.

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

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.

3 Ontwikkelingen in 2020

3.1 Covid-19

Het jaar 2020 was een interessant vervolg op de voorgaande twee jaren van de AVG. Als organisatie hebben wij in 2020, 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 2020.

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 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. Wel zal op voorhand begonnen worden met het identificeren en documenteren van processen met een verwacht hoog risico. Hiertoe zal een stappenplan en handleiding in het eerste met uitloop naar tweede kwartaal van 2021 worden uitgewerkt.

3.3 Informatieveiligheid BIG/BIO

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). Er is een grote mate van overlap tussen de BIG en de BIO, maar er zijn ook nieuwe maatregelen in opgenomen om risico's mee af te dekken. De BIO geeft meer ruimte om op basis van een risicoafweging als organisatie zelf te bepalen of bepaalde maatregelen nodig zijn om risico's af te dekken. De implementatie van de BIO zal binnen BSR projectmatig worden aangestuurd, waarbij op basis van de uitkomsten van een gap-analyse een verbeterplan opgesteld en uitgevoerd wordt. Bij het formuleren van verbeteracties zullen we ook nadrukkelijk telkens de afweging maken welk risico met de verbeteractie wordt afgedekt en in welke mate dat bijdraagt aan de betrouwbaarheid van onze dienstverlening.

Samenvattend heeft de organisatie in 2020 veel werk verzet op het gebied van informatieveiligheid. Zo zijn onder andere de volgende beleidsdocumenten herschreven dan wel uitgeschreven:

- "Informatiebeveiligingsbeleid BSR 2016-2020", vervangen door het "Strategisch informatie-beveiligingsbeleid BSR 2021-2023", welke is vastgesteld door het dagelijks bestuur van BSR op 14 september 2020.
- "Beveiligingsnota Suwinet IB 2016" vervangen door "Beveiligingsplan Suwinet-inkijk IB 2020" welke is vastgesteld door het dagelijks bestuur van BSR op 14 september 2020.

Momenteel wordt het Informatie Security Management System (ISMS) nader uitgewerkt voor vaststelling. De term ISMS staat niet voor een tool, maar voor een systematische aanpak van privacy en informatie-vraagstukken binnen een organisatie. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd.

Daarnaast beschikt BSR over een softwareoplossing in de vorm van ISMS-tooling. Deze tool is ondersteunend aan het procesgerichte informatiebeveiliging ISMS. Aan de inrichting van deze tool wordt hard gewerkt en zal naar verwachting in het derde kwartaal van 2021 beschikbaar zijn voor de organisatie.

3.4 Ensia / Dekra

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 2020 plaatsgevonden.

3.5 Verwerkers en verwerkersovereenkomsten

In 2019 zijn de meeste verwerkersovereenkomsten tot stand gekomen. In 2020 is met een aantal bestaande en nieuwe verwerkers een (nieuwe of aangepaste) verwerkersovereenkomst afgesloten. Een actueel overzicht hiervan is beschikbaar in de ISMS-tool. Een nieuwe, toegankelijke standaard verwerkersovereenkomst met de deelnemers wordt momenteel voorbereid. Bestaande verwerkers hebben niet gerapporteerd over incidenten.

3.6 Rechten betrokken

In 2019 is het proces rond de rechten van betrokkenen verbeterd. 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

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
datalekken intern en extern	1	mail onjuiste geadresseerde en.	hersteld
	1	hacking mailbox	hersteld
datalek naar AP	0	geen meldingen die voldeden aan de eisen.	-
Incidenten			
interne incidenten	8	waarvan 4 beveiligingsincidenten.	hersteld
toegangsbeveiliging	0	geen melding ontvangen.	-
AVG			
rechtmatigheid	1	gebruik BNS op aanslag.	afgehandeld
inzageverzoek	1	recht van inzage.	afgehandeld
rechtmatigheid	1	rechtmatig gebruik Suwinet.	afgehandeld
inzageverzoek	1	inzage “verwerkingsregister”.	afgehandeld
rechtmatigheid	1	aanvullende gegevens kwijtschelding.	afgehandeld

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 Functionaris informatiebeveiliging en archief en een Functionaris voor de gegevensbescherming (FG) aangewezen. Deze onderlinge relaties en verantwoordingen blijken uit het door het dagelijks bestuur vastgestelde “Centrale Privacybeleid BSR”. 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 de e-learning, met de vastgestelde 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.

Op de Actualiteitendag Privacy van 16 januari 2020 werd een presentatie gehouden over informatieveiligheid en AVG. Door de vragen die er werden gesteld is op te merken dat privacy en informatie beveiliging leeft bij de medewerkers.

Daarnaast zijn wij in oktober 2020 gestart met de vernieuwde modulen in de BSR academie te weten:

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

Op deze manier wordt de actualiteit van informatieveiligheid geborgd.

3.10 Kwaliteitssysteem bewaring en vernietiging

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 wordt in 2021 opgestart. 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

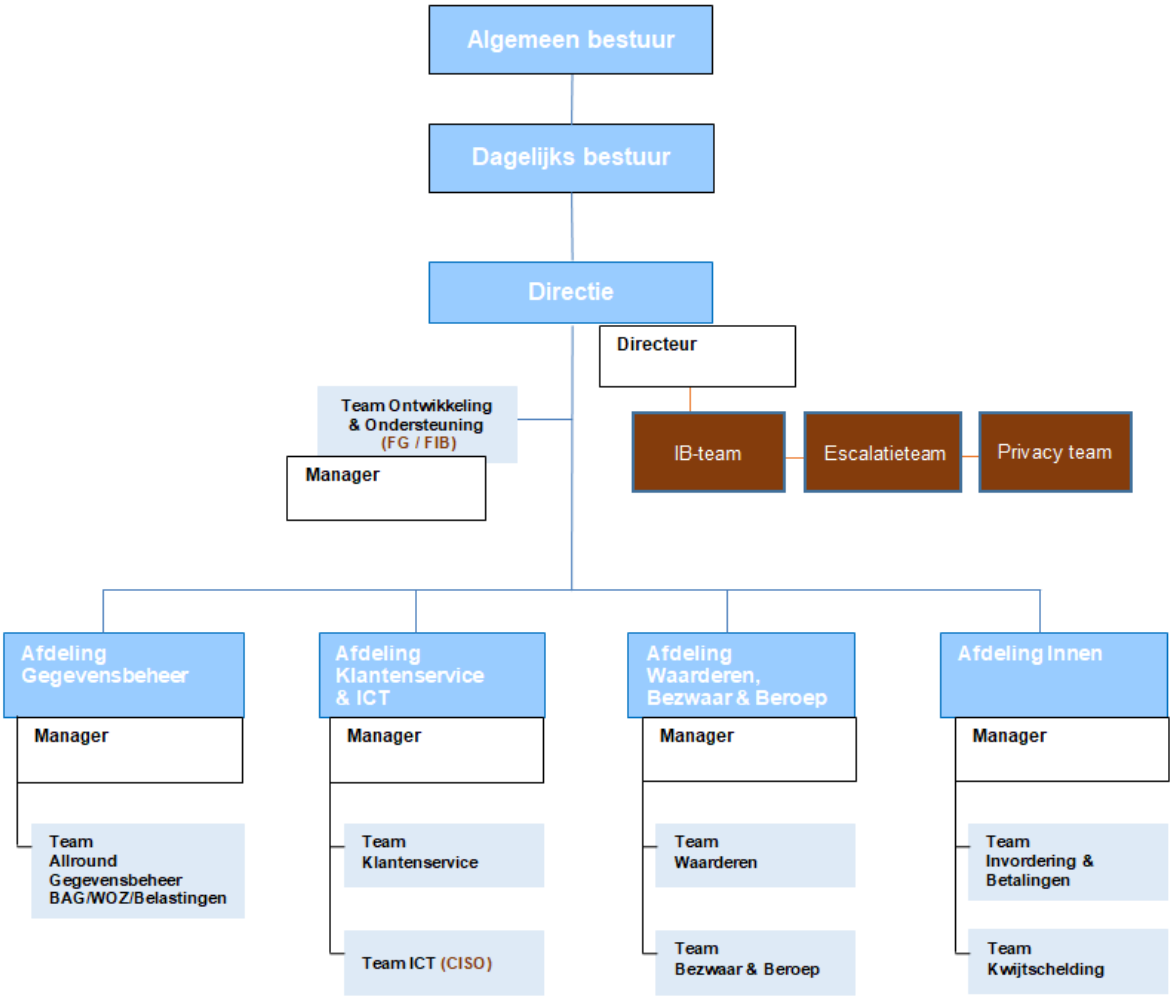
Privacy en dataprotectie (bescherming van persoonsgegevens) zijn grondrechten. En dat blijven het, ook nu in tijden van Covid-19. De privacywetgeving blijft hetzelfde, alleen zijn de omstandigheden nu even anders. Onder deze extreme omstandigheden maakt de privacywetgeving het uiteraard mogelijk om tijdelijk 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 heel moeilijke periode.

4.2 Aanbeveling

Het verdient 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.

Bijlage 1 Organogram BSR

Per 01-06-2020



Functies/rol

- Manager : sturen op resultaten (managen van processen & coachen medewerkers), MT-lid
- Senior medewerker : rol gericht op procesbegeleiding, signalering, aanspreekpunt inhoudelijke vraagstukken (aantal afhankelijk van grootte team/complexiteit/span of support)

- 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)