BSR

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 360

9 februari 2026

Officiële uitgave van de gemeenschappelijke regeling Belastingsamenwerking Rivierenland

Privacybeleid BSR 2022-2024

Leeswijzer
Indeling
*

Doel
Het doel van dit privacybeleid is, om te waarborgen dat BSR als organisatie aantoonbaar en zorg-vuldig omgaat met de verwerking van persoonsgegevens van burgers, en medewerkers in overeen-stemming met de privacywetgeving.
Doelgroep
Dit privacybeleid bevat afspraken tussen het dagelijks bestuur, directeur, management en de ambtelijk organisatie. Daarnaast vormt dit privacybeleid een kader waarbinnen medewerkers van BSR, die persoonsgegevens[1] verwerken dienen te opereren. Ook kunnen betrokkenen, personeel en burgers binnen het verzorgingsgebied, met behulp van dit document meer informatie krijgen over de manier waarop BSR als organisatie persoonsgegevens verwerkt.
Samenvatting
Door middel van het ondertekenen van de 'Gemeenschappelijke Regeling Belastingsamenwerking Rivierenland" hebben de deelnemers bevoegdheden overgedragen aan BSR. Hiertoe verwerkt BSR als organisatie, gegevens in het kader van het heffen en innen van gemeentelijke- en waterschapsbe-lasting. Deze gegevens vallen onder de geheimhoudingsplicht van artikel 67 van de Algemene wet inzake rijksbelastingen (AWR).
Daarnaast is het verzamelen, opslaan, verwerken en gebruiken van persoonsgegevens uitsluitend toegestaan op basis van één of meer in de Algemene verordening gegevensbescherming (AVG) genoemde grondslagen. Voor Nederland staan daarnaast aanvullingen in de 'Uitvoeringswet AVG'.
Onder verwerking van persoonsgegevens wordt in de AVG verstaan:

1. verzamelen, vastleggen en ordenen;
2. bewaren, bijwerken en wijzigen;
3. opvragen, raadplegen en gebruiken;
4. verstrekken door middel van doorzending;
5. verspreiding of enige andere vorm van ter beschikkingstellen;
6. samenbrengen, met elkaar in verband brengen; en
7. afschermen, uitwissen of vernietigen van gegevens.

Proceseigenaren hebben kennis van en zicht op de uitvoering van processen, sturen daarop en zijn betrokken.
[1] Zie artikel 4 lid 1 Algemene Verordening Gegevensbescherming (hierna: "AVG"): persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, voornamelijk aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Begrippenlijst *

*)

Hoofdstuk	Omschrijving
1	beschrijft de kernpunten van het privacybeleid, waaronder visie en uitgangspunten.
2	beschrijft aan welke voorwaarden processen en systemen moeten voldoen.
3	beschrijft de kaders en de verantwoordelijkheden van het privacybeleid.
4	beschrijft het toezicht op de naleving van privacyregels.
5	beschrijft de positie van de betrokkenen van wie persoonsgegevens worden verwerkt.
6	beschrijft de beleidsevaluatie.

*)

Afkorting	Toelichting
AP	*Autoriteit persoonsgegevens*
AVG	*Algemene verordening gegevensbescherming*
AWR	*Algemene wet inzake rijksbelastingen*
BIO	*Baseline Informatiebeveiliging Overheid*
BRP	*Basisregistratie personen*
BSR	*Gemeenschappelijk regeling Belastingsamenwerking Rivierenland*
CISO	*Chief Information Security Officer*

1 Kernpunten

Inleiding

Binnen de organisatie van BSR worden persoonsgegevens verwerkt van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verwerkt[1] voor het goed uitvoeren van wettelijke taken voor gemeentelijke- en waterschapsbelasting. Alle betrokkenen[2] moeten er op kunnen vertrouwen dat de organisatie zorgvuldig en veilig met persoonsgegevens omgaat.
In deze tijd van nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en ook een steeds meer digitale overheid stellen verdere eisen aan de bescherming van persoonsge-gevens. BSR is zich hiervan bewust en zorgt dat privacy en informatiebeveiliging gewaarborgd blijft, onder andere door maatregelen op het gebied van dataminimalisatie, transparantie en gebruikers-controle. Met deze beleidsnota beschrijft BSR het privacybeleid vanaf 2022 en vervangt hiermee het in 2018 vastgesteld 'Centraal privacybeleid BSR'. Deze beleidsnota is kaderstellend en richtinggevend en wordt waar nodig aangevuld met onderwerpspecifieke beleidsdocumenten en vastgelegde instructies op operationeel niveau. Dit privacybeleid geeft op bestuurlijk en organisatie niveau duidelijkheid en daarmee sturing aan de inrichting van privacy en de keuzes die daarbij gemaakt moeten worden. Dit is van belang om te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt conform de geldende wet- en regelgeving (compliance).

Visie

Privacy is een grondrecht (artikel 10) en vormt de basis van onze democratische rechtstaat. Middels het privacybeleid ondersteunt BSR dit en geeft aan dat zij respect heeft voor de rechten en vrijheden van betrokkenen. BSR als organisatie is transparant over de verwerking van persoonsgegevens en de manier waarop deze gegevens worden beschermd. Gegevens worden niet langer bewaard dan nodig is voor het doel waarvoor deze zijn verzameld en niet gebruikt voor doelen die hier niet mee verenigbaar zijn. Dit zal bijdragen aan een goede balans tussen adequate bescherming van privacy en de effectieve processen met als doel een efficiënte dienstverlening zowel in- als extern. Ook zal het een vernieuwende manier van samenwerking met de deelnemers en derde partijen ondersteunen, rekening houdend met de wettelijke vereisten.

Wettelijk kader

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit is de privacywet die binnen Europa geldt en die het algemene kader vormt voor de verwerking van persoonsgegevens. Voor Nederland zijn enkele onderwerpen uitgewerkt in de Uitvoeringswet AVG (UAVG). Privacy voorschriften zijn verder te vinden in (sector)specifieke wetgeving.

Uitgangspunten

Op grond van artikel 24 AVG moet het privacybeleid passend zijn voor de verwerkingen die onder verantwoordelijkheid van BSR als organisatie worden uitgevoerd. Hierbij rekening houdende met risico's voor de rechten en vrijheden van betrokkenen. Hiervoor zijn de beginselen uit artikel 5 AVG richtinggevend. Privacy maak ook onderdeel uit van het normenkader voor de overheid op het gebied van informatiebeveiliging (BIO). In het bijzonder wordt aangesloten bij de uitgangspunten voor de operationele borging van privacy binnen de organisatie. Dit is een doorlopend proces. Risicomanagement is daar een belangrijk onderdeel van (zie ook 'Strategisch- en Tactisch informatiebeveiligingsbeleid BSR'). Hieruit vloeien de volgende uitgangspunten voort, die in de volgende hoofdstukken uitgebreider worden toegelicht:

- zorg voor privacy is een verantwoordelijkheid van het dagelijks bestuur en directeur;

DPIA	*Data protection impact assessment*
ENSIA	*Eenduidige Normatiek Single Information Audit*
FG	*Functionaris voor de gegevensbescherming*
FIB	*Functionaris informatiebeveiliging en archief*
IB-team	*Informatiebeveiligingsteam*
IBD	*Informatiebeveiligingsdienst*
IBF	*Informatiebeveiligingsfunctionaris*
ICT	*Informatie- en communicatietechnologie*
ISMS	*Informatie Security Management System*
ISO	*Internationale Organisatie voor Standaardisatie*
IW	*Invorderingswet 1990*
NEN	*NEderlandse Norm, en voor Europese Norm*
NCSC	*National Cyber Security Center*
PO	*Privacy Officer*
UAVG	*Uitvoeringswet Algemene verordening gegevensbescherming*
VNG	*Vereniging van Nederlandse Gemeenten*

1. de formele eindverantwoordelijkheid voor privacy berust bij het dagelijks bestuur van BSR, daartoe stelt de directeur de kernpunten van het privacybeleid vast;
2. de directeur legt verantwoording af aan het dagelijks bestuur van BSR over het privacybeleid;
3. de lijnen van verantwoordelijkheden in de organisatie zijn vastgelegd in mandaatbesluiten.

- het borgen van privacy in de uitvoering van de processen vindt risicogestuurd plaats, daartoe maken de proceseigenaren afwegingen ter naleving van privacyregels op basis van een risico inschatting;
- de proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toe-zicht op zijn proces(sen) op basis van het privacybeleid;
- bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen tegen het privacy-beleid met een DPIA;
- binnen een proces worden alleen authentieke[1] gegevens verwerkt voor het realiseren van het procesdoel;
- bij privacyincidenten informeert de proceseigenaar het escalatieteam waar de datalek wordt vastgelegd, besproken en vervolgstappen worden opgenomen en uitgewerkt;
- er is een functionaris voor gegevensbescherming (FG) aangesteld als interne toezichthouder;
- er wordt voorzien in communicatie over het beleid en faciliteiten voor bewustwording en training, zodat iedere medewerker conform het privacybeleid kan handelen;
- naast een *escalatieteam* is er ook een *privacyteam*, om privacy minimaal 2 maal per jaar te bespreken en af te stemmen op directie- en uitvoerings niveau; en
- het privacyteam evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleid.

[1] Authentiek: oorsprong, echt, betrouwbaar, niet vervalst, geloofwaardig en waarachtig.
[1] Zie artikel 4 sub 2 AVG: verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Zie artikel 4 lid 1 AVG: een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”).
[2] Zie artikel 4 lid 1 AVG: een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”).
Scope
Het privacybeleid is van toepassing op de gehele bedrijfsvoering van BSR, voor zover in de bedrijfsprocessen gewerkt wordt met persoonsgegevens en de organisatie daar zeggenschap over heeft.
Het privacybeleid is het algemene deel van privacy binnen BSR als organisatie. Het privacybeleid is de kapstok voor privacy, waaraan aanvullende regelingen zijn opgehangen zoals regelingen voor het uitoefenen van rechten.
Het volgende is hierbij van belang:

1. het privacybeleid van BSR omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Dit betreft zowel analoge (papieren) als digitale gegevensverwerking;
2. het privacybeleid is ook van toepassing op processen die BSR uitbesteedt of op een andere manier organiseert. Voorbeeld hiervan is de inrichting van de informatie voorziening via Cloud computing (zie “Strategisch Informatiebeveiligingsbeleid BSR’). Het privacybeleid is tevens van toepassing op de inkoop van producten of diensten, zoals de aanschaf van informatie-systemen;
3. het privacybeleid is van toepassing op gegevensuitwisseling met derden, zoals de Belastingdienst, landelijke voorzieningen en deelnemende gemeenten. In 2021 is hiervoor het “Besluit ontheffing (fiscale) gegevensverstrekking aan derden BSR’ vastgesteld;
4. het privacybeleid omvat 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;
5. het privacybeleid is van toepassing op de verwerking van statistische en/of geanonimiseerde, dan wel gepseudonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd; en
6. het privacybeleid is van toepassing op informatiebeveiligingsvraagstukken, voor zover het de beveiliging van persoonsgegevens betreft.

Risico’s
Het niet naleven van de AVG, de Uitvoeringswet AVG en privacyvoorschriften in (sector)specifieke wetten (zoals: Wet BRP) kan verregaande (negatieve) consequenties voor de organisatie hebben.
De Autoriteit Persoonsgegevens (AP) heeft als landelijke toezichthouder enkele bevoegdheden zoals:

1. onderzoek naar mogelijke overtredingen;
2. handhavend optreden: bestuurlijke sanctie (inclusief betaling geldsom), last onder bestuursdwang); en

3. boete opleggen: hoogte van de boete is afhankelijk van de overtreding en de ernst daarvan, de AP heeft boetebandbreedtes vastgesteld in beleidsregels[1] . De hoogte van de boete kan variëren van minimaal € 120.000,- tot maximaal € 1.000.000,- (de maximale boete voor niet naleving van de wet bij een datalek is bijvoorbeeld € 525.000,-).

Betrokkenen van wie BSR als organisatie persoonsgegevens verwerkt, hebben de mogelijkheid de organisatie aansprakelijk te stellen en schadevergoeding te vragen als er sprake is van handelen in strijd met de AVG en de Uitvoeringswet AVG.
BSR als organisatie kan hierdoor reputatieschade oplopen en het vertrouwen van de burger deels of geheel verliezen, bijvoorbeeld als een datalek het nieuws haalt. Dit kan ertoe leiden dat BSR haar taken niet meer naar behoren kan uitvoeren en geen benodigde hulp, ondersteuning of diensten kan bieden, omdat burgers BSR onvoldoende als een betrouwbare partner zien.
Raakvlakken andere beleidsthema's
Het privacybeleid van BSR heeft raakvlakken met andere beleidsdocumenten of is hier onderdeel van, zoals:

1. *integriteitsbeleid*
   privacybewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te vol-doen aan de AVG, maar zorgvuldig omgaan met persoonsgegevens vereist een integere houding. In het kader van integriteit leggen (nieuwe) medewerkers de eed of belofte af en hebben zij een geheimhoudingsplicht. Privacybeleid is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het integriteitsbeleid van BSR;
2. *continuïteit- en risicomanagement*
   privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkproces-sen spaak lopen omdat de bijbehorende gegevensverwerking een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad);
3. *informatiebeveiliging*
   privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijk-heid aantasten van de informatievoorzieningen en opgeslagen persoonsgegevens. Informatie-beveiliging wordt uitgevoerd vanuit het strategisch- en tactisch informatiebeveiligingsbeleid en aanvullende operationele beleidsdocumenten;
4. *archiefbeleid*
   het archiefbeleid is vastgelegd in de archiefverordening en het besluit informatiebeheer van BSR. In deze beleidsstukken zijn bepalingen opgenomen omtrent gegevensvernietiging welke zijn gebaseerd op de Archiefwet. Privacywetgeving en de Archiefwet moeten in onderlinge samenhang bekeken en uitgevoerd worden.

Privacybeleid
Inleiding
BSR als organisatie is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden voert de organisatie proactief beleid op basis van dit privacybeleid en wordt de goede naleving van wet- en regelgeving op het gebied van privacybescherming bewaakt. Daarnaast faciliteert de organisatie de uitoefening van rechten van personen.
Begrippen
Allereerst volgt een korte beschrijving van de AVG-begrippen 'persoonsgegevens' en 'verwerken'.
Persoonsgegevens
Persoonsgegevens zijn alle gegevens waarmee een natuurlijk persoon te identificeren is of geïdentificeerd kan worden. Voorbeelden zijn: naam en geboortedatum, adres, e-mail en bankrekeningnummer. Artikel 5 geeft alle basisuitgangspunten en principes voor een legitieme *gegevensverwerking* en vereist een legitieme *verwerkingsgrondslag (*art. 6) voor het verwerken van 'gewone' persoons-gegevens.
Bijzondere categorieën persoonsgegevens.
Bepaalde persoonsgegevens zijn privacygevoeliger (art. 9 AVG), bijvoorbeeld gegevens over gezondheid, strafrecht (waaronder gegevens uit registers van politie en justitie), religie of etniciteit. Deze zogenaamde bijzondere gegevens mag de organisatie daarom alleen verwerken in die gevallen, dat dit wettelijk is toegestaan. Het burgerservicenummer (BSN) is eveneens een extra gevoelig persoonsgegeven waaraan extra bescherming toekomt en dat een wettelijke basis moet hebben.
In zekere zin is artikel 9 een lex specialis, een uitwerking van artikel 6. Het geeft aan wanneer de verwerking van 'bijzondere persoonsgegevens' legitiem is. Belangrijk is dat het verwerken van deze ge-gevens in principe niet is toegestaan (lid 1) tenzij er een uitzondering van toepassing is (lid 2). De achtergrond van dit uitgangspunt is dat de verwerking van bijzondere persoonsgegevens als potentieel gevaarlijk wordt gezien. Het verwerken van medische gegevens kan bijvoorbeeld grote gevolgen voor iemand hebben, niet alleen omdat bijvoorbeeld zeer intieme gegevens in de handen van vreemden kunnen komen, maar ook omdat een werkgever kan besluiten iemand niet aan te nemen vanwege een chronische ziekte.
Verwerken van persoonsgegevens

'Verwerken' omvat alle handelingen met persoonsgegevens, waaronder verzamelen, opslaan, verstrekken en vernietigen van gegevens. Verzamelen vindt vaak plaats bij een aanvraag of melding en soms ook doordat de organisatie navraag doet. De verzamelde gegevens worden opgeslagen in de daarvoor bestemde software systemen en indien nodig voor de taakuitvoering ook verstrekt. Als de gegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld, worden ze vernietigd.
Eisen aan gegevensverwerking
Verwerkingen van persoonsgegevens vinden plaats in overeenstemming met AVG-beginselen. Het gaat dan om eisen benoemd in artikel 5 AVG:

1. rechtmatigheid, behoorlijkheid en transparantie;

Persoonsgegevens die BSR nodig heeft voor de uitvoering van haar taak, worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
De verwerking van persoonsgegevens dient gebaseerd te zijn op een van de zes grondslagen als benoemd in artikel 6 AVG:
- toestemming van betrokkene;
- overeenkomst met betrokkene;
- nakomen wettelijke verplichting;
- bescherming vitale belangen betrokkene;
- uitoefening taken algemeen belang of uitoefening openbaar gezag; en
- gerechtvaardigd belang organisatie.

Wettelijk vastgelegde taak
Voor BSR als semi-overheidsorganisatie is de grondslag in de meeste gevallen gelegen in het nakomen van een wettelijke plicht (zie ook paragraaf *samenvatting* in hoofdstuk *leeswijzer* pagina 3), namelijk:
- de heffing en de invordering van de door de deelnemers aan BSR overgedragen belastingen;
- de uitvoering van de Wet waardering onroerende zaken (Wet WOZ) waaronder tevens wordt begrepen de administratie van vastgoedgegevens en het verstrekken van vast-goedgegevens aan de deelnemers en derden;
- de inrichting en het beheer van de door de deelnemers aan BSR overgedragen basis-registraties; en
- de verwerking van persoonsgegevens als werkgever.

Verwerking is noodzakelijk
Het verwerken van persoonsgegevens is noodzakelijk voor de taakuitoefening van BSR als semi-overheidsorganisatie. Zonder de verwerking van de persoonsgegevens kan de organisatie *niet* het gestelde doel bereiken (subsidiariteit). Het legitieme doel dat wordt nagestreefd staat in verhouding tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt. Het behalen van deze doelen kan niet op een andere, minder ingrijpende wijze worden bereikt.
Transparantie
BSR geeft duidelijkheid aan betrokkenen over de verwerking van persoonsgegevens. Het is daarbij van belang dat betrokkenen geïnformeerd worden over de wettelijke kaders en het beoogde doel van de verwerking. Maar ook welke persoonsgegevens nodig zijn en met wie gegevens noodzakelijkerwijze gedeeld gaan worden. Daartoe heeft BSR het privacybeleid en regelement opgesteld en beschikbaar gemaakt op de website van BSR. Dit document beschrijft in het kort en in begrijpelijke taal wat het beleid van BSR is.
De informatieplicht richting betrokkene is in de procesinrichting van de organisatie verwerkt.
Toestemming
BSR verwerkt op beperkte schaal persoonsgegevens op grond van (uitdrukkelijke) toestemming (artikel 9 AVG) van betrokkenen. Dit geldt alleen voor gegevens die niet uit basisregistraties gehaald kunnen worden. Hierbij kan gedacht worden aan e-mailadressen en telefoonnummers. Deze gegevens zijn ondersteunend aan betrokkenen en verbeteren de dienstverlening aan betrokkenen.
2. grondslag en doelbinding;

BSR als organisatie verzamelt persoonsgegevens alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en verstrekt deze gegevens alleen voor zover dat binnen het doel is toegestaan. Afwijkend gebruik voor andere doelen is slechts mogelijk na afweging van de wettelijke criteria. Deze afweging gebeurt in de vorm van een 'verenigbaar-heidstoets' conform artikel 6 lid 4 AVG (zie ook paragraaf *samenvatting* in hoofdstuk *leeswijzer* pagina 3).
3. minimaal noodzakelijke gegevensverwerking;

(incl. toepassing proportionaliteit/subsidiariteit)
- BSR als organisatie verwerkt alleen gegevens die strikt noodzakelijk zijn om het doel waarvoor ze nodig zijn te bereiken. De gegevensverwerking moet toereikend, ter zake dienend en niet bovenmatig zijn. De organisatie hanteert daarbij de regel 'need to know' in plaats van 'nice to know'.

- Bij de beoordeling van de noodzaak van de gegevensverwerking spelen de beginselen van proportionaliteit en subsidiariteit een belangrijke rol. Het beginsel van *proportionaliteit* verlangt een redelijke verhouding tussen het te dienen belang van het gegevensgebruik en de inbreuk op de privacy van betrokkenen. De inbreuk mag niet onevenredig zijn in verhouding tot het te bereiken doel.
- Het beginsel van *subsidiariteit* houdt in dat gekozen moet worden voor een manier die voor de betrokkenen het minst inbreuk maakt op de privacy. Als het doel ook te bereiken is op een minder privacyschendende manier moet daarvoor gekozen worden.

4. juistheid;
   Persoonsgegevens moeten altijd juist, volledig en actueel zijn, gelet op de doeleinde waarvoor zij worden verwerkt. In alle processen van BSR vinden controles plaats om te verifiëren dat de juiste persoonsgegevens gebruikt worden en onjuiste persoonsgegevens onverwijld te wissen of te rectificeren. Dit kan mede voorkomen dat datalekken ontstaan.

5. opslagbeperking en bewaartermijnen;
   BSR als organisatie bewaart gegevens volgens de wettelijk geldende termijnen in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Voor persoonsgegevens in archiefwaardige bescheiden geldt een bewaartermijn die is vastgelegd in de 'Selectielijst voor gemeenten en intergemeentelijke organen (VNG)', vastgesteld op grond van de archiefwet en archiefbesluit. Zie ook 'Archiefverordeningen BSR en het 'Besluitinformatiebeheer BSR'.
   Het opslaan van persoonsgegevens voor een langer periode louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1 van de AVG.
   Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan de directeur op voordracht van de *functionaris informatiebeveiliging en archief* een besluit over de bewaartermijn nemen.

6. integriteit en vertrouwelijkheid.

(inclusief organisatorische en technische beveiligingsmaatregelen).
BSR als organisatie neemt passende technische of organisatorische maatregelen zodat persoonsgegevens integer en vertrouwelijk worden verwerkt. Het kunnen borgen van de privacy kan niet gerealiseerd worden zonder adequate informatiebeveiliging. Daarbij horen ook maatregelen ter beveiliging van de persoonsgegevens zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO) gestructureerd volgens de NEN-ISO/IEC 27001/2. Hiertoe heeft BSR het 'Strategische- en Tactisch Informatiebeveiligingsbeleid BSR' vastgesteld en dit 'Privacybeleid BSR'.
Omgaan met persoonsgegevens
Persoonsgegevens worden alleen verwerkt voor het uitvoeren van bepaalde wettelijke taken en vastgestelde regelingen. Dit ter uitvoering van de in de AVG voorgeschreven doelbinding en proportionaliteit beginsel. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor het doel nodig is.
Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in de 'Basisregistratie Perso-nen' (BRP) of andere authentieke bronnen, worden daaruit opgevraagd. BSR is hiertoe geauthori-seerd door de Rijksdienst voor identiteitsgegevens. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid wordt gepropageerd. Wanneer voor het uitvoeren van bepaalde wettelijke taken en regelingen persoonsgegevens verwerkt moeten wor-den, dan worden deze gegevens opgevraagd uit de BRP. Specifieke eisen voor gegevensverwerking is vastgelegd in artikel 4.1 van de Wet BRP.
Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze worden verzamel. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor die medewerker die belast is met het uitvoeren van een bepaalde taak. Gegevens worden niet zonder toestemming van de betrokkene of wettelijke grondslag gedeeld. Informatiesystemen moeten voldoen aan de eisen van de BIO en NEN-ISO/IEC 27001/2. Bijzondere gegevens worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak of regeling.
Gegevensuitwisseling
BSR als organisatie beschikt in het kader van de in de GR BSR opgenomen taakuitoefening over veel gegevens die, naast deze taakuitoefening, ook relevant zijn voor de uitvoering van de publiekrechtelijke taken door de deelnemers van BSR. Bij de deelnemers van BSR is er sprake van een behoefte aan bepaalde gegevens, waarover BSR beschikt. De behoefte is ontstaan om de uitvoering en de wettelijke verplichtingen op een andere manier in te vullen. Hiertoe heeft BSR het "Besluit ontheffing (fiscale) gegevensverstrekking aan derden BSR' op 18 maart 2021 vastgesteld. Op grond van dit besluit is het de directeur van BSR toegestaan om, in bepaalde situaties, gegevens te verstrekken aan deelnemers van GR BSR.
Als uitgangspunt van haar handelen hanteert de BSR als organisatie de volgende werkwijze:

1. allereerst stelt de organisatie vast of het verwerken van gegevens, waaronder de uitwisseling van gegevens, binnen de kaders van de verschillende wetten kan plaatsvinden;
2. mochten de wetten niet in de uitwisseling van gegevens voorzien, dan valt de organisatie terug op de mogelijkheid van artikel 6 lid 4 AVG: het uitvoeren van een verenigbaarheidstoets. Bekeken wordt dan of gebruik van de gegevens mogelijk is voor ándere doelen dan de oorspronkelijke doelen waarvoor de gegevens verzameld zijn in de uitvoering van de taak. Gegevensuitwisseling met derden kan dan mogelijk worden; en
3. wanneer het gaat om verwerkingen die een hoog risico voor betrokkenen inhouden, wordt eerst een data protection impact assessement (DPIA) uitgevoerd. Een DPIA maakt inzichtelijk welke maatregelen er nodig zijn om op een rechtmatige en zorgvuldige manier met persoons-gegevens om te gaan, inclusief de uitwisseling met derden.

Deze uitgangspunten legt de organisatie vast in een privacyconvenant als het gaat om het delen van gegevens met externen alsmede in het privacyreglementen voor het delen van gegevens binnen de eigen organisatie. De afspraken in deze documenten integreert de organisatie in haar werkprocessen.
Risicogestuurde aanpak
*

Bij nieuw in te stellen processen, wordt privacy vanaf het begin van het ontwerpproces meegenomen, door na te denken over de benodigde technische en organisatorische maatregelen en die in te bouwen in processen en systemen ('privacy by design'). Aan nieuwe verwerkingen en risicovolle processen liggen data protection impact assessments (DPIA's) ten grondslag.
DPIA's zijn instrumenteel voor het inzichtelijk krijgen van het proces, de omgang met persoons-gegevens daarin met bijbehorende risico's en om passende beheersmaatregelen te bepalen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de DPIA.
DPIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG. Met behulp van de aanbevelingen in het DPIA-rapport wordt voorzien in passende organisatorische en technische privacybeschermende maatregelen. Voor processen met een laag privacyrisico volstaan algemene oplossingen. Zolang een proces als laag risico gekwalificeerd is, is daarvoor in mindere mate aandacht nodig.
Een risicogestuurde aanpak voorkomt dat in strijd met privacynormen en privacyprincipes wordt gehandeld, bijvoorbeeld bij:

1. *onrechtmatige gegevensverwerking*; zoals:
   wanneer er een verbod of beperking geldt voor gebruik, opslag of uitwisseling van persoons-gegevens.
2. *disproportionele gegevensverwerking*; zoals:
   (a) ontoereikende of bovenmatige gegevensverwerking of (b) gegevensverwerking waarbij het organisatiebelang onevenredig klein is in verhouding tot de impact van de verwerking op personen.
3. *irrelevante gegevensverwerking*; zoals:
   gegevensverwerking voor niet ter zake dienende of verouderde doeleinden;
4. *onnauwkeurige gegevensverwerking*; zoals:
   wanneer de gebruikte, opgeslagen of uitgewisselde gegevens geen juiste weergave van de werkelijkheid bieden.
5. *onveilige gegevensverwerking*; zoals:
   wanneer gegevens toegankelijk zijn of dreigen te worden voor onbevoegden waardoor misbruik mogelijk is).
6 *niet-inachtneming van bijzondere wettelijke voorschriften*; zoals:
   niet-nakoming van meldplichten, wettelijke termijnen, toestemmingsverplichtingen).
7 *onbewaakte gegevensverwerking*. zoals:
   wanneer niet gecontroleerd wordt of privacywaarborgende maatregelen geëffectueerd zijn.

Verantwoordelijkheid voor privacy
Governance
De wijze van verankering van het privacybeleid binnen BSR als organisatie vormt als het ware de fundamentele grondslag en borging ervan. Op grond van de AVG is het hoogst leidinggevende niveau in de organisatie eindverantwoordelijk voor de rechtmatige en verantwoordelijke verwerking van persoonsgegevens. Het privacybeleid is van toepassing op het algemeen- en dagelijks bestuur, directeur, managementteam en de ambtelijke organisatie van BSR en zal uitgangspunt van handelen zijn. De

*) Het privacybeleid van BSR is erop gericht aantoonbaar te voorzien in passende maatregelen voor doeltreffende bescherming van persoonsgegevens en de bescherming van rechten van personen. Wat 'passend' is, hangt af van de concrete risico's die de verwerking van persoonsgegevens voor burgers en medewerkers met zich meebrengt wanneer er geen doeltreffende beschermingsmaatregelen genomen zouden zijn. Inzichtelijk moet zijn of een gegevensverwerking te classificeren is als laag, midden of hoog risico, en of het mitigeren van deze risico's een inspanning vergt die laag, midden of hoog is. Door het uitvoeren van risicoanalyses wordt de risicoclassificatie bepaald. Afhankelijk van de risico-classificatie geldt een ander toetsingsregime.

uitvoering van het privacybeleid is onderdeel van de bedrijfsvoering van BSR als organisatie en volgt de verantwoordelijkheidslijnen van de mandaatbesluiten.
Verantwoordelijkheid voor verwerking
De AVG kent het begrip 'verwerkingsverantwoordelijke'. De verwerkingsverantwoordelijke (directeur) is verantwoordelijk voor de verwerking van persoonsgegevens in overeenstemming met wetgeving, regelingen en beleid op het gebied van privacy. De verwerkingsverantwoordelijke stelt doel en middelen vast voor de verwerkingen van persoonsgegevens.
Bestuurlijk verantwoordelijkheid
De bestuurlijke en strategische verantwoordelijkheid voor privacy berust bij het dagelijks bestuur en de directeur. Zij dragen zorg voor een passend privacybeleid. De directeur en dagelijks bestuur leggen over de uitvoering van het privacybeleid verantwoording af aan het algemeen bestuur. Om dit te borgen heeft privacy zelfstandige aandacht in de planning- en controlcyclus van de organisatie (zie ook paragraaf *uitgangspunten* in hoofd-stuk 1. *kernpunten* pagina 6 en 7).
Verantwoordelijkheid organisatie
De verantwoordelijkheid van het dagelijks bestuur en directeur wordt praktisch vertaald naar de organisatie volgens de lijnen van het mandaatbesluit. De directeur zal binnen de jaarlijkse planning & control cyclus het dagelijks bestuur informeren over de risico's en over de getroffen beheersmaat-regelen op het gebied van privacy.
Daarnaast is er voor de operationele ondersteuning en aansturing op het gebied van privacy een informatiebeveiligingsfunctionaris benoemd. Privacy is verweven met informatiebeveiliging, waarmee afstemming wordt gezocht. Voor informatiebeveiliging is een Chief Information Security Officer (CISO) aangesteld. Ook is de wettelijk verplichte interne toezichthouder aangesteld: de Functionaris voor de gegevensbescherming (FG) artikel 37-39 AVG.
Op grond van de AVG wordt de uitvoering van het privacybeleid door de FG geauditeerd (jaarverslag). De FG rapporteert rechtstreeks aan de directeur en managementteam. De directeur meldt bijzonderheden ten aanzien van gegevensverwerkingen, te denken valt aan ernstige datalekken, proactief aan de dagelijks bestuur. De directeur als verwerkingsverantwoordelijke is ambtelijk verantwoordelijke voor de borging van het privacybeleid.
Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen en documenteren die maatregelen in de werkinstructies. Ook zorgen zij voor de volledigheid en actualiteit van het 'register van verwerkingen'.
Alle verwerkingen van persoonsgegevens worden bijgehouden in een register van verwerkingen, conform artikel 30 AVG. Het register is een digitaal overzicht van alle actieve processen die de organisatie uitvoert. Aan de hand van dit register is vast te stellen welke gegevens in welke processen verwerkt worden en wat ermee gebeurt. Per verwerkingsproces worden verschillende componenten geregistreerd, zoals de grondslag, doelen, categorieën van persoonsgegevens, categorieën betrokkenen, ontvangers, verwerker en bewaartermijnen.
Datalek
In geval van een datalek voldoet BSR als organisatie aan de meldplicht, conform artikelen 33 en 34 AVG. Alle datalekken worden bijgehouden in een register van het ISMS. Er is een vaste procedure ingesteld voor het melden van datalekken welke is verankerd in het incidentmanagersysteem. De procedure maakt deel uit van het proces ter afhandeling van incidenten op het gebied van informatie-beveiliging.
Toezicht
Landelijk toezicht wordt uitgevoerd door de Autoriteit Persoonsgegevens (AP). Toezicht binnen de organisatie van BSR, wordt uitgevoerd door de FG, de wettelijk verplichte interne toezichthouder. Daarnaast zijn er interne controles op toepassing van de privacynormen.
Controle op werking en naleving
Beleid, procedures en maatregelen worden steekproefsgewijs en periodiek getoetst op opzet, bestaan en werking in de praktijk. Een periodieke toets op het onderdeel privacy vindt plaats aan de hand van het kwaliteitssysteem (ISMS). Proceseigenaren (verantwoordelijken) in de organisatie dienen ook zelf periodiek te (laten) controleren in hoeverre de feitelijke situatie in overeenstemming is met toepassing van het privacybeleid. De toetsing aan de hand van het kwaliteitssysteem helpt hen hierbij. Daarnaast zijn vragen, klachten, incidentmanagement, verenigbaarheidstoetsen en DPIA's steekproefsgewijze toetsing van naleving van het privacybeleid.
Functionaris voor gegevensbescherming
Om aan de vereisten van de AVG te kunnen voldoen is het aanstellen van een FG niet alleen verplicht maar draagt het ook bij aan een effectieve beheersing ervan. De FG heeft een onafhankelijke positie in de organisatie en ziet toe op de naleving van privacywet- en regelgeving en dit privacybeleid. De directeur informeert interne en externe doelgroepen over de FG en communiceert zijn contactgegevens aan de landelijke toezichthouder, de AP.
De FG voert zijn rol en taken uit conform artikelen 37 - 39 AVG. Conform artikel 37 lid 5 AVG is de FG aangewezen op grond van:

1. zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacymanagement-praktijk;
2. zijn vermogen om de functie gebonden taken te vervullen; en
3. zijn onafhankelijkheid, met name de afwezigheid van een belangen conflict.

De taken van de FG zijn, kort samengevat: informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens.
Vanwege zijn expertise van wetgeving en de praktijk, geldt een advies van de FG als zwaarwegend en de geëigende wijze voor naleving van privacywetgeving door BSR. De FG doet jaarlijks verslag van zijn werkzaamheden en bevindingen aan de directeur. Dit verslag wordt vastgesteld door het dagelijks bestuur van BSR en is onderwerp van gesprek in het privacyteam.

Privacy voor betrokkenen

Een fundamenteel uitgangspunt, dat opgenomen is in de considerans van de AVG, is dat de verwerking van persoonsgegevens 'ten dienste van de mens' staat. Mede hierom moeten personen controle over hun eigen persoonsgegevens hebben. Dit hoofdstuk beschrijft de manieren waarop betrokkenen dit kunnen doen.

Rechten

Personen van wie BSR als organisatie gegevens verwerkt mogen ervan uitgaan dat dit in overeenstemming met privacyregels gebeurt. Tevens zijn in de AVG specifieke privacyrechten voor personen opgenomen. Betrokkenen hebben recht op het volgende:

1. dat BSR handelt conform privacywetgeving en dit privacybeleid;
2. dat BSR transparant is over doelen van gegevensverwerking en toepassing van het privacy-beleid;
3. dat betrokkenen inzage in hun eigen gegevens hebben (recht van inzage);
4. dat betrokkenen (in geval van fouten) hun gegevens kunnen (laten) verbeteren of verwijderen (recht op rectificatie en recht op gegevenswissing);
5. dat de verwerking van hun persoonsgegevens beperkt wordt of tijdelijk niet toegestaan is (recht van beperking van de verwerking en recht van bezwaar); dit verplicht BSR tot het maken van een afweging; en
6. dat betrokkenen BSR bij niet-naleving van de wet of het privacybeleid van de organisatie hierop mogen aanspreken.

(Nadere uitwerking zie bijlage 1)

Vragen en klachten

Betrokkenen hebben altijd de mogelijkheid om vragen te stellen over de verwerkingen van persoonsgegevens. Bij beantwoording van de vragen kan het advies gevraagd worden aan de FG.
Met klachten over de verwerking van persoonsgegevens door BSR moeten personen altijd terecht kunnen bij BSR als organisatie, of direct bij de FG.
Een niet tot tevredenheid afgehandelde vraag of klacht over gegevensverwerking door BSR wordt voorgelegd aan de FG. Betrokkenen hebben altijd het recht een klacht in te dienen bij de landelijke toezichthouder, de AP.
Bij klachten over de bejegening door medewerkers van BSR is de 'Klachtenregeling' van toepassing.

Beleidsevaluatie

Er bestaat niet alleen een wettelijke verplichting om een passend gegevensbeschermingsbeleid te hebben en uit te voeren, maar ook om dit beleid te evalueren en waar nodig te actualiseren.
Het privacybeleid wordt eens per twee jaren geëvalueerd en besproken in het privacyteam, waarbij in ieder geval de volgende aspecten beoordeeld zullen worden: wet en regelgeving, borging, inhoud, uitvoerbaarheid en werking. Indien daartoe aanleiding bestaat wordt het privacybeleid geactualiseerd.
(zie ook paragraaf *uitgangspunten* in hoofdstuk 1.K*ernpunten* pagina 6 en 7)
De FG heeft zitting in het privacyteam en wordt geïnformeerd op basis van deze evaluatie.