Privacybeleid BSR
2022 - 2024

Colofon

Titel : Privacybeleid BSR 2022 - 2024

Opdrachtgever : Directeur BSR

Auteur : Functionaris informatiebeveiliging en archief (FG)

Versie : 2.1

Vastgesteld in de vergadering van het dagelijks bestuur BSR d.d.16 juni 2022

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

G.M. Scholtus MBA
Directeur

Versiebeheer

Versienummer	Wijziging	Auteur	Datum
1.0	Concept	Directeur, manager ICT	21 januari 2022
1.1	Definitief concept	Directeur, manager ICT en CISO	18 februari 2022
2.0	Definitief	Directeur	24 maart 2022
1.2	Definitief	Managementteam (besluitvorming)	11 mei 2022
1.2	Definitief	Dagelijks bestuur (besluitvorming)	16 juni 2022

Leeswijzer

Indeling

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.

Doel

Het doel van dit privacybeleid is, om te waarborgen dat BSR als organisatie aantoonbaar en zorgvuldig omgaat met de verwerking van persoonsgegevens van burgers, en medewerkers in overeenstemming 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 waterschapsbelasting.
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:

- verzamelen, vastleggen en ordenen;
- bewaren, bijwerken en wijzigen;
- opvragen, raadplegen en gebruiken;
- verstrekken door middel van doorzending;
- verspreiding of enige andere vorm van ter beschikkingstellen;
- samenbrengen, met elkaar in verband brengen; en
- 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.

Inhoudsopgave

Colofon 2
Leeswijzer 3
Begrippenlijst 5
1 Kernpunten 6
2 Privacybeleid 9
3 Verantwoordelijkheid voor privacy 14
4 Toezicht 15
5 Privacy voor betrokkenen 16
6 Beleidsevaluatie 17
Bijlage 1 Rechten van betrokkenen 18
Bijlage 2 Privacybeleid BSR 20
Bijlage 3 Privacyreglement BSR 22

Begrippenlijst

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*
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 Kernpunten

Inleiding

Binnen de organisatie van BSR worden persoonsgegevens verwerkt van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verwerkt[2] voor het goed uitvoeren van wettelijke taken voor gemeentelijke- en waterschapsbelasting. Alle betrokkenen[3] 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 persoonsgegevens. BSR is zich hiervan bewust en zorgt dat privacy en informatiebeveiliging gewaarborgd blijft, onder andere door maatregelen op het gebied van dataminimalisatie, transparantie en gebruikerscontrole.

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').

[2] 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").
[3] Zie artikel 4 lid 1 AVG: een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene").

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;
    - de formele eindverantwoordelijkheid voor privacy berust bij het dagelijks bestuur van BSR, daartoe stelt de directeur de kernpunten van het privacybeleid vast;
    - de directeur legt verantwoording af aan het dagelijks bestuur van BSR over het privacybeleid;
    - 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 toezicht op zijn proces(sen) op basis van het privacybeleid;
- bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen tegen het privacybeleid met een DPIA;
- binnen een proces worden alleen authentieke[4] 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.

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:

- het privacybeleid van BSR omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Dit betreft zowel analoge (papieren) als digitale gegevensverwerking;
- 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 informatiesystemen;
- 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;
- 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;
- 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
- het privacybeleid is van toepassing op informatiebeveiligingsvraagstukken, voor zover het de beveiliging van persoonsgegevens betreft.

[4] Authentiek: oorsprong, echt, betrouwbaar, niet vervalst, geloofwaardig en waarachtig.

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:

- onderzoek naar mogelijke overtredingen;
- handhavend optreden: bestuurlijke sanctie (inclusief betaling geldsom), last onder bestuursdwang); en
- boete opleggen: hoogte van de boete is afhankelijk van de overtreding en de ernst daarvan, de AP heeft boetebandbreedtes vastgesteld in beleidsregels[5] . 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:

- *integriteitsbeleid*
  privacybewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te voldoen 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;
- *continuïteit- en risicomanagement*
  privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerking een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad);
- *informatiebeveiliging*
  privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de informatievoorzieningen en opgeslagen persoonsgegevens. Informatiebeveiliging wordt uitgevoerd vanuit het strategisch- en tactisch informatiebeveiligingsbeleid en aanvullende operationele beleidsdocumenten;
- *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.

[5] Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Stcrt. 2019, nr. 14586)

2 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' persoonsgegevens.

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 persoonsge-geven 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:

- 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 vastgoedgegevens aan de deelnemers en derden;
- de inrichting en het beheer van de door de deelnemers aan BSR overgedragen basisregistraties; 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.

- 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 ‘verenigbaarheidstoets’ conform artikel 6 lid 4 AVG (zie ook paragraaf *samenvatting* in hoofdstuk *leeswijzer* pagina 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.

- 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.

- 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.

- 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 Personen' (BRP) of andere authentieke bronnen, worden daaruit opgevraagd. BSR is hiertoe geauthoriseerd 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 worden, 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.

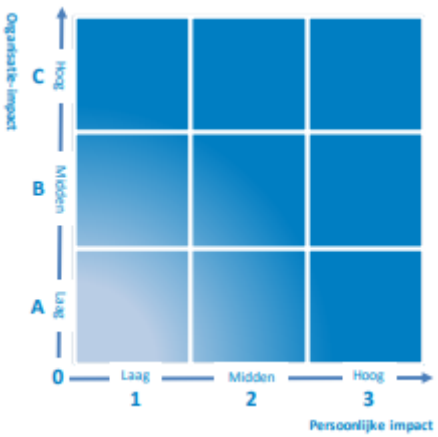
Als uitgangspunt van haar handelen hanteert de BSR als organisatie de volgende werkwijze:

- allereerst stelt de organisatie vast of het verwerken van gegevens, waaronder de uitwisseling van gegevens, binnen de kaders van de verschillende wetten kan plaatsvinden;
- 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
- 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 persoonsgegevens 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

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 risicoclassificatie geldt een ander toetsingsregime.



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 persoonsgegevens 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:

- *onrechtmatige gegevensverwerking*; zoals:
  wanneer er een verbod of beperking geldt voor gebruik, opslag of uitwisseling van persoonsgegevens.
- *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.
- *irrelevante gegevensverwerking*; zoals:
  gegevensverwerking voor niet ter zake dienende of verouderde doeleinden;
- *onnauwkeurige gegevensverwerking*; zoals:
  wanneer de gebruikte, opgeslagen of uitgewisselde gegevens geen juiste weergave van de werkelijkheid bieden.

- *onveilige gegevensverwerking*; zoals:
  wanneer gegevens toegankelijk zijn of dreigen te worden voor onbevoegden waardoor misbruik mogelijk is).
- *niet-inachtneming van bijzondere wettelijke voorschriften*; zoals:
  niet-nakoming van meldplichten, wettelijke termijnen, toestemmingsverplichtingen).
- *onbewaakte gegevensverwerking*. zoals:
  wanneer niet gecontroleerd wordt of privacywaarborgende maatregelen geëffectueerd zijn.

3 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 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 bijzonder-heden 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 rechtmatig-heid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen en documenteren die maatregelen in de werkinstructies. Ook zorgen zij voor de volledigheid en actualiteit van het 'regi-ster van verwerkingen'.
Alle verwerkingen van persoonsgegevens worden bijgehouden in een register van verwerkingen, con-form 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 geregi-streerd, 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.

4 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:

a. zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacymanagement-praktijk;
b. zijn vermogen om de functie gebonden taken te vervullen; en
c. 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.

5 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:

- dat BSR handelt conform privacywetgeving en dit privacybeleid;
- dat BSR transparant is over doelen van gegevensverwerking en toepassing van het privacybeleid;
- dat betrokkenen inzage in hun eigen gegevens hebben (recht van inzage);
- dat betrokkenen (in geval van fouten) hun gegevens kunnen (laten) verbeteren of verwijderen (recht op rectificatie en recht op gegevenswissing);
- 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
- 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.

6 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.*Kernpunten* pagina 6 en 7)

De FG heeft zitting in het privacyteam en wordt geïnformeerd op basis van deze evaluatie.

Bijlage 1 Rechten van betrokkenen

Rechten van betrokkenen (artikel 13 t/m 22 AVG)

Om een rechtmatige verwerking van persoonsgegevens te waarborgen geeft de AVG diverse rechten aan betrokkene. De betrokkene kan deze rechten uitoefenen tegen BSR als deze optreedt als verwerkingsverantwoordelijke. In de AVG zijn de volgende rechten van betrokkenen opgenomen:

- informatieplicht (artikel 13 en 14 AVG);
  BSR informeert betrokkenen over het verwerken van persoonsgegevens. Dit kan bijvoorbeeld via een vermelding op een aanvraagformulier gebeuren, of op andere algemeen gangbare wijze (informatiefolder e.d.). De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de organisatie persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.
  Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, dan dient betrokkene daarover geïnformeerd te worden op het moment dat deze persoonsgegevens voor de eerste keer worden verwerkt.

- recht van inzagerecht (artikel 15 AVG);
  De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt, heeft hij recht op uitleg welke persoonsgegevens het betreft en op welke manier deze gegevens worden verwerkt. Ook heeft hij recht op inzage en een kopie van zijn persoonsgegevens (zie nader artikel 20 AVG). De organisatie kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het recht van inzage is mede bedoeld om uitoefening van het recht op rectificatie, het recht op gegevens wissen en beperking van de ver-werking mogelijk te maken. Een verzoek om dit recht uit te oefenen kan bijvoorbeeld via het invullen van een formulier gebeuren. Hierna zal de CISO inzage verstrekken in de persoons-gegevens welke over de betrokkene verwerkt worden.

- recht op rectificatie (artikel 16 AVG);
  Als verwerkte persoonsgegevens onjuist of onvolledig zijn kan de betrokkene aan BSR als organisatie verzoeken deze te laten corrigeren of aanvullen. De organisatie en eventuele externe partijen die in opdracht van BSR persoonsgegevens verwerken moeten onverwijld alle redelijke maatregelen nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd.

- recht op vergetelheid (gegevenswissing) (artikel 17 AVG);
  Betrokkenen hebben het recht om BSR te verzoeken bovenmatige persoonsgegevens te wissen. Er is sprake van bovenmatige persoonsgegevens in de volgende gevallen:
  - als persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij verwerkt worden;
  - als de betrokkene zijn toestemming voor de verwerking op valide gronden intrekt;
  - in geval van een gegrond bezwaar en er is geen zwaarwichtig belang voor de verwerking;
  - als de persoonsgegevens onrechtmatig verwerkt zijn; en
  - als de wet dwingt tot verwijdering.

  BSR is in een dergelijk geval verplicht om zo snel mogelijk aan het verzoek om gegevenswissing gehoor te geven, tenzij er sprake is van een uitzondering zoals opgenomen in artikel 17 lid 3 AVG.

- recht op beperking van de verwerking (artikel 18 AVG);
  Betrokkene mag vragen om beperking van de verwerking in de volgende gevallen:
  - de juistheid van de gegevens wordt door betrokkene betwist;
  - de gegevens worden onrechtmatig verwerkt maar betrokkene wil niet dat de gegevens worden verwijderd, maar verzoekt om beperking van het gebruik ervan;
  - de doeleinden zijn vervallen, maar betrokkene heeft de gegevens nog nodig voor de uitoefening / verdediging van enig recht in rechte; en
  - in geval van een lopende bezwaarprocedure.

Als hier sprake van is, mag tijdelijk geen andere verwerkingshandeling plaatsvinden dan opslag, tenzij:

- de betrokkene daar toestemming voor geeft;
- dit nodig is voor de uitoefening/ verdediging van enig recht in rechte; en
- dit nodig is om gewichtige redenen van algemeen belang.

De betrokkene dient vervolgens geïnformeerd te worden voordat de blokkade opgeheven wordt.

- recht op dataportabiliteit (overdraagbaarheid van gegevens) (artikel 20 AVG);
  De betrokkene heeft het recht om zijn persoonsgegevens desgevraagd te verkrijgen in een gestructureerd, gangbaar en machine leesbaar format. Hij mag deze gegevens overdragen aan een andere verantwoordelijke zonder daarbij te worden gehinderd door de eerste verantwoordelijke. Waar mogelijk heeft de betrokkene er recht op dat een verantwoordelijke rechtstreeks zijn persoonsgegevens doorstuurt naar de nieuwe verantwoordelijke, mits de verwer-king berust op toestemming of geschiedt in het kader van de uitvoering van een overeenkomst én de verwerking geautomatiseerd plaatsvindt.

- recht van bezwaar tegen verwerking (artikel 21 AVG); en
  Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens onder de volgende voorwaarden:
  - er is sprake van verwerking op basis van een publiekrechtelijke taak van een bestuursorgaan; of
  - er is sprake van een verwerking op basis van een gerechtvaardigd belang (inclusief profilering) en betrokkene kan aantonen dat er sprake is van specifieke persoonlijke omstandigheden die het maken dat de belangenafweging van de verwerking in zijn geval anders zou moeten uitpakken.

  Als aan deze voorwaarden voldaan is dient de organisatie te stoppen met verwerken tenzij:
  - BSR “dwingende wettige redenen” heeft die prevaleren boven de belangen van de betrokkene; en
  - de persoonsgegevens nodig zijn voor uitoefening/ verdediging van enig recht in rechte.

  Als de verwerking plaatsvindt in het kader van wetenschappelijk of historisch onderzoek en statistiek geldt het recht van bezwaar niet als de verwerking geschiedt in het kader van algemeen belang.

- recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling (artikel 22 AVG).
  Betrokkenen hebben het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (waaronder profilering), gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, behalve als er sprake is van de in artikel 22 AVG genoemde gevallen.

Uitoefening rechten betrokkenen

Om gebruik te maken van voornoemde rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via het contactformulier op de website worden ingediend. BSR heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal BSR beslissen wat er met het verzoek gaat gebeuren.

Hoewel het in principe de bedoeling is dat aan de rechten van betrokkenen gehoor wordt gegeven, kan het zijn dat de organisatie een uitzondering moet maken op grond van wet- of regelgeving. Indien het verzoek wordt afgewezen is er de mogelijkheid om bezwaar te maken bij BSR, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Hierover zal betrokkene geïnformeerd worden.

Bijlage 2 Privacybeleid BSR

Privacybeleid BSR
Binnen BSR wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld door middel van basisregistraties, daarnaast wordt eventuele aanvullende informatie bij de burgers opgevraagd voor het goed uitvoeren van privaatrechtelijke taken. De burger moet erop kunnen vertrouwen dat BSR zorgvuldig en veilig met deze persoonsgegevens omgaat. In deze tijd gaat ook BSR mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en in toenemende mate digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. BSR is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. BSR geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van BSR. Dit privacybeleid van BSR is in lijn met het algemene beleid van BSR en de relevante lokale, regionale, nationale en Europese wet- en regelgeving op het gebied van de privacy.

Wettelijke kaders voor de omgang met gegevens
BSR is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming;
- Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Algemene wet rijksbelastingen; en
- Invorderingswet 1990.

Uitgangspunten
BSR gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. BSR houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie;
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding;
BSR zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie;
BSR verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. BSR streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

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.

Bewaartermijn;
Persoonsgegevens worden, met inachtneming van de Archiefwet, niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om privaatrechtelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid;
BSR gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt BSR voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Delen met derden;
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt BSR in een verwerkingsovereenkomst afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. BSR ziet jaarlijks toe op naleving van deze afspraken.

Subsidiariteit;
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit; en
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Rechten van betrokkenen.
BSR honoreert, waar mogelijk, alle rechten van betrokkenen.

Dit privacybeleid treedt in werking op 11 mei 2022 en vervangt het privacybeleid dat is vastgesteld op 25 mei 2018. Het beleid wordt jaarlijks geëvalueerd en indien nodig bijgesteld en bekendgemaakt via www.bsr.nl.

Bijlage 3 Privacyreglement BSR

Privacyreglement BSR
In dit reglement laat BSR zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. BSR heeft de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Overheden waaronder belastingsamenwerkingen zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, uitvoering Wet WOZ en belastingheffing en inning voor de deelnemers van BSR. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van BSR. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vindt BSR het belangrijk om transparant te zijn over de manier waarop BSR met persoons-gegevens omgaan, en de privacy waarborgen.

1. Wetgeving en definities
Met ingang van 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG), welke op 25 mei 2016 in werking trad, samen met de uitvoeringswet gehandhaafd. De AVG bouwt voort op de Wet bescherming persoonsgegevens (Wbp), (welke voorheen van kracht was) en zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (artikel 4, AVG):

- *Betrokkene:*
  De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt;
- *Verwerker:*
  De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie;
- *Persoonsgegevens:*
  Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld: naam, adres en geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN);
- *Gegevensbeschermingseffectbeoordeling:*
  Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Data Privacy Impact Assessment (DPIA);
- *Verwerkingsverantwoordelijke:*
  Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt; en
- *Verwerking:*
  Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

2. Reikwijdte
Dit reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van BSR, oftewel: voor alle verwerkingen die binnen BSR plaatsvinden.

3. Verantwoordelijke
De directeur van BSR is eindverantwoordelijk voor de verwerkingen die door of namens BSR worden uitgevoerd.

4. Verwerkingen (artikel 4, AVG)
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:

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

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden (artikel 5, AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden.

Rechtmatige grondslag (artikel 6, AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- om een verplichting na te komen die in de wet staat;
- voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was;
- om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden;
- voor de goede vervulling van wettelijke taak; en
- wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

BSR verwerkt de meeste persoonsgegevens op grond van een wettelijke verplichting. BSR gebruikt bij de verwerking gegevens die beschikbaar zijn gesteld via de landelijke basisregistraties. Op grond van de wet is er een vermoeden dat deze registraties juist zijn. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligt BSR alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe BSR dit doet staat in het informatiebeveiligingsbeleid van BSR en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (artikel 44 t/m 50, AVG)
BSR geeft geen persoonsgegevens door met een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

5. Transparantie en communicatie
Wet open overheid (Woo)
Op grond van de Woo kan een verzoek om informatie worden ingediend bij BSR. Er dient per geval een afweging te worden gemaakt tussen het belang bij de openbaarmaking van de betreffende informatie en de eerbieding van de persoonlijke levenssfeer. Indien de eerbiediging van de persoonlijke levenssfeer zwaarder weegt, dan blijft openbaarmaking achterwege.

Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt BSR altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht (artikel 13,14, AVG)
BSR informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan BSR geven, worden zij op de hoogte gesteld van de manier waarop BSR met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren.
Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat BSR persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Verwijdering
BSR bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van privaatrechtelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Rechten van betrokkenen (artikel 13 t/m 20, AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie:
  Betrokkenen hebben het recht om aan BSR te vragen of zijn/haar persoonsgegevens worden verwerkt;
- Inzagerecht:
  Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- Correctierecht:
  Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen de instanties die de basisregistratie beheren om dit te corrigeren;
- Recht van verzet:
  Betrokkenen hebben het recht aan BSR te vragen om hun persoonsgegevens niet meer te gebruiken;
- Recht om vergeten te worden:
  In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen; en
- Recht op bezwaar:
  Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. BSR zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking, in de vorm van het uitvoeren van wettelijke taken.

Indienen van verzoek
Om gebruik te maken van voornoemde rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via het contactformulier op de website worden ingediend. BSR heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal BSR beslissen wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij BSR, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan BSR aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

6. Geautomatiseerde verwerkingen
Profilering (artikel 22, AVG)
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een per-soon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen

voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn: financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de website van BSR naar een bepaalde dienst kijkt, mag BSR geen actie ondernemen om de dienst aan te bieden. BSR mag wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.
BSR maakt geen gebruik van profilering, met uitzondering van het verwerken van verhuizingen en kwijtschelding. Wanneer een betrokkene verhuist krijgt diegene automatisch een verminderingsbesluit. Dit proces wordt door middel van steekproeven gecontroleerd.
Daarnaast wordt er bij de verwerking van kwijtschelding gebruik gemaakt van profilering. Een betrokkene moet toestemming geven om jaarlijks automatisch te toetsen of diegene in aanmerking komt voor kwijtschelding. Deze toestemming wordt aan betrokkene gevraagd nadat zij de eerste keer in aanmerking gekomen zijn voor kwijtschelding.

Big data en tracking
Door middel van big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, BSR of haar deelnemers wordt uitgevoerd. De verzamelde gegevens door big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden, zodat zij niet herleidbaar zijn tot een persoon.

BSR maakt op dit moment geen gebruik van big data en tracking, maar sluit niet uit dit in de toekomst wel te gaan doen. Wanneer er wel sprake is van big data en tracking zal dit regelement aangepast worden. Wel verstrekt BSR gegevens aan haar deelnemers ten behoeve van big data tracking op de punten zoals genoemd in het “Besluit ontheffing (fiscale) gegevensverstrekking aan derden BSR”.

7. Plichten van BSR
Register van verwerkingen (artikel 30, AVG)
BSR is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan BSR de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- de naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- de doelen van de verwerking;
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist; en
- een algemene beschrijving van de beveiligingsmaatregelen.

Data Protection Impact Assessment (DPIA) (artikel 35, AVG)
Met een DPIA worden de effecten en risico’s van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. BSR voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, er sprake is van nieuwe technologieën of wanneer er een nieuwe verwerking plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (artikel 37 t/m 39, AVG)
BSR heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de organisatie overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en geldende richtlijnen op het gebied van privacy.
Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de FG van BSR via het contactformulier op de website of via telefoonnummer: 0344 - 704 704

Datalekken (artikel 33,34, AVG)
Van een datalek is sprake indien persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt BSR dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt BSR dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaan de datalekken geëvalueerd. Alle datalekken worden vastgelegd in een register.

8. Afsluiting
indien BSR een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van BSR worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van BSR.

Disclaimer:
Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.