Belastingsamenwerking Oost-Brabant

Privacybeleid 2024

Belastingsamenwerking Oost-Brabant

Belastingsamenwerking Oost-Brabant

Inhoudsopgave

Inhoudsopgave 2

1. Inleiding 5

1.1 Kernwaarden en ambities 5

2. Wetgeving en definities 6

3. Scope 8

4. Raakvlakken en overlap met andere beleidsthema's 9

5. Verantwoordelijke 9

6. Privacybeginselen 10

7. Belangenafweging 11

8. Belang van de betrokkene 11

9. Publiek belang 11

10. Belangen van betrokkenen ten opzichte van elkaar 11

11. Privacy uitgangspunten 12

11.1 Rechtmatigheid 12

11.2 Behoorlijkheid 12

11.3 Transparantie 13

12. AVG 15

12.1 Het verwerkingsregister 15

12.2 Data Protection Impact Assessment (DPIA) 15

12.3 Privacy by Design & Privacy by Default 16

12.4 Datalekken 16

12.5 Rechten van betrokkenen 17

12.6 Gegevens delen met derden 17

12.7 Vragen of klachten 18

13. Governance 18

13.1 Het bestuur 19

13.2 Algemeen bestuur 19

13.3 Management team 20

13.4 Functionaris voor Gegevensbescherming (FG) 20

13.5 Privacy Officer (PO) 20

13.6 Chief Information Security Officer (CISO) 21
13.7 Privacy Team 21
13.8 Medewerkers BSOB 21
13.9 Proceseigenaren 21

Revisie

Dit beleidsdocument heeft een geldigheidsduur van 2 jaar. Jaarlijks dient dit beleidsdocument te worden herzien en waar nodig bijgewerkt te worden. Wijzigingen dienen bijgehouden te worden in onderstaande tabel.

Versiebeheer

Versie	Datum	Wijzigingen	Naam
V1	Oktober 2023	Concept versie 0.1	Esma Fierloos
V1	Oktober 2023	Aanvullingen en controle	Sevilay Tegmen
V2	Februari 2024	Concept voor MT en Bestuur	Sevilay Tegmen

1. Inleiding

Binnen Belastingsamenwerking Oost-Brabant (BSOB) wordt veel gewerkt met persoonsgegevens voor de goede uitvoering van haar publiekrechtelijke taken. Persoonsgegevens worden voornamelijk verzameld voor waarderen, heffen en innen van gemeentelijke-en waterschapsbelastingen. De burger moet erop kunnen vertrouwen dat BSOB zorgvuldig en veilig met de persoonsgegevens omgaat.

BSOB gaat ook mee met de nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, decentralisaties en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. BSOB is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. BSOB geeft middels dit beleid een duidelijke richting aan op welke manier zij dagelijks omgaat met persoonsgegevens en privacy en laat zien dat zij privacy waarborgt, beschermt en handhaaft.

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van BSOB.

1.1 Kernwaarden en ambities

BSOB hanteert de volgende kernwaarden:

Kwaliteit

Toegankelijkheid

Kostenbewust

BSOB handelt naar de kernwaarden. Hierdoor streeft BSOB ernaar om bij te dragen aan een betrouwbare en dienstverlenende overheid. Voor het realiseren van de kernwaarden is gegevensverzameling van groot belang. Het beschermen van persoonsgegevens en een rechtmatige gegevensverwerking is essentieel om op een kwalitatieve manier de publiekrechtelijke taken uit te voeren. Omdat bescherming van persoonsgegevens belangrijk is, heeft BSOB privacy hoog in het vaandel staan: BSOB verwerkt persoonsgegevens op een rechtmatige, behoorlijke en transparante manier, conform wet- en regelgeving.

2. Wetgeving en definities

Dit privacybeleid komt tot stand onder de Europese Verordening ten behoeve van de bescherming van persoonsgegevens; de Algemene Verordening Gegevensbescherming (AVG).

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

- Autoriteit Persoonsgegevens (AP): de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt;
- Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt;
- Chief Information Security Officer (CISO): informatiemanager met een adviserende, coördinerende en toezichthoudende rol op het gebied van informatiebeveiliging. Hij ziet toe dat de informatieveiligheid van de organisatie voldoet aan de hiervoor geldende normen;
- Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, verlies, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
- Data Protection Impact Assessment (DPIA) of in het Nederlands een gegevensbeschermingseffectbeoordeling (GEB): een GEB brengt in een vroeg stadium op een gestructureerde en heldere manier de privacyrisico's van een verwerking in beeld en geeft aan welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's. Een DPIA of GEB is verplicht bij een nieuwe verwerking of bij een bestaande verwerking als het risico of proces daarvan wijzigt;
- Functionaris voor Gegevensbescherming (FG): een onafhankelijke en deskundige toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de AVG;
- Management team (MT): medewerkers die verantwoordelijk zijn voor uitvoering van wettelijke taken die onder andere voortvloeien uit wet- en regelgeving op het gebied van het sociale domein, de belastingdienst, HRM en inburgering;
- Persoonsgegevens: alle informatie over een geïdentificeerde of indentificeerbare natuurlijke persoon. Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is. Denk hierbij aan naam, adres, geboortedatum. Naast deze algemene persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Denk hierbij aan financiële gegevens of gegevens over de gezondheid. Gegevens van organisaties of van overleden personen zijn geen persoonsgegevens volgens de AVG;

- Privacy Officer (PO): de PO zorgt voor naleving van de AVG binnen een organisatie. De PO geeft advies en biedt ondersteuning, geeft interne trainingen aan medewerkers en heeft een rol bij het melden van datalekken. Ook ondersteunt de PO de FG;
- Privacy audit: controle op de naleving van privacybeleid en privacywetgeving;
- Privacy by design/default: privacy by design houdt in dat de organisatie gegevensbescherming meeneemt in het ontwerp van een proces of systeem, zodat persoonsgegevens goed worden beschermd en de gegevens niet langer worden bewaard dan nodig is voor het doel van de verwerking. Privacy by default houdt in dat de standaardinstellingen voor een gebruiker zo privacy-vriendelijk mogelijk zijn;
- Procesdoel: een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens;
- Proceseigenaren: een proceseigenaar is de persoon die de bevoegdheid heeft om te bepalen hoe een proces verloopt, en de verantwoordelijkheid heeft ervoor te zorgen dat het proces aan de bedrijfsdoelstellingen blijft voldoen;
- Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt;
- Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een verwerkingsverantwoordelijke organisatie. Dit kan de gehele verwerking zijn, maar ook bepaalde onderdelen van de verwerking;
- Verwerkersovereenkomst: een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke;
- Verwerking: Een verwerking is volgens de AVG elke bewerking of elk geheel van bewerkingen met betrekking tot een persoonsgegeven, zoals: vastleggen, bewaren, verzamelen, met elkaar in verband brengen, beschikbaar stellen, verstrekken, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, wissen en vernietigen;
- Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

3. Scope

Het privacybeleid geldt voor de gehele datastroom van persoonsgegevens binnen BSOB. Van het genereren of verzamelen van persoonsgegevens, het dagelijks gebruik en de opslag ervan, tot en met de archivering en vernietiging van persoonsgegevens. Dit geldt voor zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag.
Dit privacybeleid is bindend voor de gehele organisatie van BSOB.

Het privacybeleid is of wordt nader uitgewerkt in operationeel beleid, werkinstructies en richtlijnen.
Wanneer BSOB samenwerkt met verwerkers of gegevens uitwisselt met derden gelden dezelfde uitgangspunten.
Diezelfde uitgangspunten vormen het kader bij de selectie van leveranciers c.q. verwerkers. Hiervoor maakt BSOB contractuele afspraken die BSOB kan toetsen bij de uitvoering van de werkzaamheden.
Het beleid is ook van toepassing in geval van uitwisseling van informatie met andere organisaties.

Het privacybeleid strekt zich uit over de verwerkingen van persoonsgegevens op grond van de Algemene Verordening Gegevensbescherming (hierna: AVG). Bij de toepassing van deze algemene wet moet ook de specifieke wet- en regelgeving in acht worden genomen.

4. Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van BSOB heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Zo is de uitvoering van het privacybeleid wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en daarmee ondersteunend aan het integriteitsbeleid. Ook richt het privacybeleid zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke wettelijke uitoefening van de taak en goed werkgeverschap.

Het privacybeleid biedt waarborging op het gebied van continuïteit en risicomanagement doordat het afbreuk- en aansprakelijkheidsrisico's tegengaat. Daarnaast wordt voorkomen dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerking(en) een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).

Daarnaast ondersteunt het privacybeleid het informatiebeveiligingsbeleid (en vice versa) door nadrukkelijk de aandacht te vestigen op het beschermen van de gegevens die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en de opgeslagen persoonsgegevens aantasten. De uitvoering van informatiebeveiliging wordt beschreven in het informatiebeveiligingsbeleid.

Het privacybeleid stuurt samen met het HR-beleid op een gekwalificeerde organisatie, cultuur, personeel en privacy-awareness van medewerkers.

5. Verantwoordelijke

De bestuursorganen van BSOB zijn verantwoordelijk voor de verwerkingen die door of namens BSOB worden uitgevoerd. De bestuursorganen van BSOB zijn het dagelijks bestuur (DB), algemeen bestuur (AB) en de directeur als gemandateerde namens het AB en DB. Daarnaast treedt BSOB op als verwerker voor de deelnemende gemeenten.

6. Privacybeginselen

Nu de AVG inmiddels enkele jaren van toepassing is, is een nieuwe fase aangebroken. De behoefte bestaat om de ruimte te nemen die de wet- en regelgeving biedt om de taken effectief en efficiënt te vervullen en tegelijkertijd betrokkenen met respect, eerlijk en begripvol te behandelen. Daarbij ontstaan (ethische) dilemma's. De (nationale) wet- en regelgeving is complex en biedt niet altijd voldoende houvast aan lokale beleidsmakers en –uitvoerders bij de uitvoering van hun taken. Verder heeft het recht op bescherming van persoonsgegevens geen absolute gelding en moet het worden beschouwd in relatie tot de functie ervan in de samenleving. Dat vraagt soms om afweging ten opzichte van andere (grond)rechten. Sommige opdrachten kunnen met elkaar botsen en soms voldoen bestaande (IT-)systemen en werkwijzen (nog) niet aan de privacy- en informatiebeveiligingseisen.

Privacy vraagt daarmee niet alleen om een heldere bestuurlijke visie maar ook om duidelijke beleidskaders. De privacywetgeving biedt niet voor ieder vraagstuk een pasklaar antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waaraan moet worden getoetst wanneer gegevens verwerkt worden. Deze regels kunnen verschillend worden ingevuld of toegepast. Een belangrijk onderdeel van het beleid is aandacht voor risico-oriëntatie en het moreel kompas: de wet is een belangrijk hulpmiddel, maar bij handelen conform de regels of gebruikmaken van de (wettelijke) ruimte, hoort een gewetensvraag: ook al houd ik me aan de regels, is deze oplossing ook in maatschappelijk opzicht wenselijk? De beoordeling of op de juiste wijze invulling is gegeven aan deze principes en voldoende borging is getroffen om de persoonlijke levenssfeer te beschermen, is aan de toezichthouder en aan de rechter.

BSOB wil met dit privacybeleid de ruimte benutten die er is om haar taken goed uit te kunnen voeren en de privacy van betrokkenen te beschermen. Verantwoording afleggen hoort bij een betrouwbare organisatie. Incorporatie van een goede privacybescherming hoort thuis in de werkzaamheden van de organisatie. Uit het voorgaande moge duidelijk zijn dat er onduidelijkheid kan zijn over de eisen die wet- en regelgeving stellen. Dit kan tot onzekerheid leiden en medewerkers kunnen zich gehinderd voelen in de uitvoering van hun taken en/of privacy ervaren als een vervelende extra check bij reguliere processen. Privacyregels worden, vaak ten onrechte, aangedragen als reden om informatie niet te delen. Iets om je achter te verschuilen. Iedereen is het er echter over eens dat van ons als regionale uitvoeringsorganisatie verwacht mag worden dat we ons werk met aandacht voor de bescherming van privacy uitvoeren.

Dit privacybeleid beoogt de professionals op de werkvloer in staat te stellen afwegingen te maken bij de uitvoering van het werk. We willen dat rechtmatige verwerking van gegevens geen extra belastende handeling vormt maar onderdeel is van de reguliere taken en processen. Binnen de organisatie zijn de bevoegdheden zo laag mogelijk in de organisatie

belegd, waarbij iedereen verantwoordelijkheid draagt voor zijn eigen taakveld op basis van vertrouwen. Dit betekent dat afwegingen rond privacy, zeker als deze meer en meer onderdeel worden van de reguliere taken en processen, ook gemaakt (zullen) worden op uitvoerend niveau. Om dit soort afwegingen te kunnen maken en uit te kunnen leggen (transparantie) is een afwegingskader nodig.

7. Belangenafweging

Bij verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Dat vraagt om een zorgvuldige afweging. Naast het belang van de individuele burger, zijn er het publieke (algemeen) belang, het zakelijk belang van BSOB en de belangen van betrokkenen ten opzichte van elkaar.

8. Belang van de betrokkene

Een betrokkene wil dat zijn persoonsgegevens veilig en betrouwbaar worden verwerkt. Daarnaast moet BSOB transparant zijn over wat zij met die informatie doet. Deze wensen kunnen van verschillend karakter zijn. Aan de ene kant heeft de betrokkene er belang bij dat zo min mogelijk gegevens worden opgeslagen en dat deze niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de betrokkene efficiënte dienstverlening, waarbij BSOB niet naar de bekende weg vraagt. BSOB doet haar best om systemen zo op elkaar af te stemmen dat er niet veelvuldig wordt uitgevraagd.

9. Publiek belang

BSOB voert op diverse gebieden wettelijke en bestuurlijke taken uit. Denk hierbij onder andere aan de taak met betrekking tot het innen van belastingen vanuit de Gemeentewet, de Wet Waardering Onroerende Zaken, en de Waterschapswet. Om deze taak goed te volbrengen is het noodzakelijk dat BSOB persoonsgegevens verwerkt.

10. Belangen van betrokkenen ten opzichte van elkaar

De bescherming van de rechten van de ene betrokkene kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander.

Voordat persoonsgegevens worden verwerkt vindt er een belangenafweging plaats. Daarbij worden de privacy uitgangspunten meegewogen. BSOB maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Aan de hand van een onderbouwde belangenafweging besluit BSOB of de gegevensverwerking kan plaatsvinden. Daarbij verkleint BSOB risico's zoveel mogelijk door het nemen van de juiste maatregelen.

11. Privacy uitgangspunten

De AVG omschrijft een aantal uitgangspunten die centraal staan in dit privacybeleid. BSOB hanteert hierbij de centrale uitgangspunten van Rechtmatigheid, Behoorlijkheid en Transparantie om invulling te geven aan alle uitgangspunten die de AVG stelt. Hieronder omschrijft BSOB deze uitganspunten en de wijze waarop BSOB deze concreet invulling geeft binnen haar organisatie.

11.1 Rechtmatigheid

- BSOB gaat uit van de geldende wet- en regelgeving voor gegevensverwerking en hanteert de AVG als basis. Voor verwerking van persoonsgegevens moet altijd een wettelijke grondslag bestaan.
- Het kan zijn dat BSOB persoonsgegevens vaker gebruikt. Dit kan alleen als dat doel verenigbaar is met de oorspronkelijke verzameldoeleinden. Mocht blijken dat het niet verenigbaar is, dan kijkt BSOB naar een rechtmatige grondslag. Dit wordt getoetst bij het Privacy Team.
- BSOB legt alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking. Het kan zijn dat de wet het BSOB verplicht of om de belangen van betrokkenen te beschermen. Dit wordt voor de verwerking concreet gemaakt en vastgelegd in het verwerkingsregister.
- Diverse taken vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. In het verwerkingsregister houdt BSOB per verwerking bij op welke grondslag deze gebaseerd is en welk doel deze rechtvaardigt.
- Bij de gegevensverwerking houdt BSOB rekening met de beginselen van ‘proportionaliteit’ en ‘subsidiariteit’. BSOB vraagt slechts die informatie die noodzakelijk is om het beoogde doel te bereiken. Daarbij gebruikt BSOB altijd de minst ingrijpende methode voor de betrokkenen.

11.2 Behoorlijkheid

- BSOB hanteert het principe van ‘minimale gegevensverwerking’. Dit wil zeggen dat er geen gegevens worden gevraagd die niet nodig zijn voor het vastgestelde doel. Hiermee geeft BSOB invulling aan het principe van ‘dataminimalisatie’. Zo richt BSOB haar systemen op een wijze in die waarborgt dat er niet te veel informatie wordt gevraagd. Er zijn werkinstructies en periodieke ‘data opschoonacties’ om het dataminimalisatie principe te waarborgen.
- BSOB hanteert het beginsel van ‘éénmalige vastlegging, meervoudig gebruik’: gegevens die al bekend zijn, worden niet nodeloos opnieuw gevraagd. Dit betekent ook dat BSOB zo veel mogelijk gebruik maakt van zogenoemde brongegevens zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is slechts mogelijk als hier een wettelijke grondslag en verenigbaar doel voor is. De grondslag en

verenigbaarheid worden niet op werknemersniveau bepaald. BSOB legt dit op afdelingsniveau vast middels werkinstructies en autorisaties om heldere kaders te schetsen voor haar medewerkers.

- BSOB bewaart persoonsgegevens niet langer dan noodzakelijk is. De noodzakelijkheid is altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen. Wanneer de wet hier niet in voorziet, staan de bewaartermijnen beschreven in ons verwerkingsregister. BSOB bewaart persoonsgegevens in ieder geval in overeenstemming met de "Selectielijst gemeenten en intergemeentelijke organen 2020". De interne organisatie heeft toegang tot het verwerkingsregister om de bewaartermijnen te raadplegen. Verder zijn er werkinstructies voor het gebruik van dit register.
- Alleen functionarissen (werknemers, externen, leveranciers, convenantpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Deze gegevens worden vertrouwelijk behandeld. BSOB heeft een autorisatiebeleid zodat enkel werknemers toegang hebben tot de gegevens die hier ook echt een doel voor hebben. BSOB gebruikt alleen de gegevens die voor de verwerking noodzakelijk zijn.
- BSOB werkt met geheimhoudingsverklaringen voor ingehuurde medewerkers, stagiaires en leveranciers. Met externe (keten)partners sluit BSOB overeenkomsten.
- BSOB slaat persoonsgegevens goed beveiligd op zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van 'privacy by design' schenkt BSOB tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacyverhogende maatregelen.
- Het is voor zowel BSOB als de betrokkene van belang dat persoonsgegevens actueel en correct zijn. BSOB voert periodiek controles uit om de basisregistratie personen actueel en juist te houden. Dit is tevens een wettelijke verantwoordelijkheid.

11.3 Transparantie

- Iedereen heeft het recht te vernemen welke persoonsgegevens BSOB over hem/haar heeft verzameld en waarvoor BSOB deze gebruikt. Dit gebeurt onder meer door een privacyverklaring op de website. BSOB bekijkt per afdeling hoe zij betrokkenen op een passende wijze informeert. BSOB legt dit vast in werkinstructies om te voldoen aan de informatieplicht onder de AVG.
- Betrokkenen hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens BSOB van hen verwerkt. In de basis verstrekt BSOB de gevraagde informatie tenzij de wet anders aangeeft. Verder kunnen betrokkenen om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald (bijvoorbeeld fiscale regelgeving).

- Om recht te doen aan verzoeken van betrokkenen heeft BSOB een Procedure rechten van betrokkenen vastgesteld. Hierin is beschreven op welke wijze BSOB verzoeken van betrokkenen afhandelt. Hier omschrijft BSOB ook wie daarbij welke taken en verantwoordelijkheden heeft.
- BSOB is transparant over het type persoonsgegevens dat zij voor een specifiek doel met derden deelt. Daarbij kan het zijn dat er een uitzondering geldt wanneer er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten. Typen persoonsgegevens worden bijgehouden in het verwerkingsregister en zijn opvraagbaar.
- BSOB is open en transparant over hoe zij met persoonsgegevens omgaat. Dit doet zij door de waarborg dat afwijkingen van dit beleidskader beargumenteerd worden voorgelegd aan het Privacy Team. Indien nodig zal de interne toezichthouder (FG) escaleren naar het MT en bestuur. Zo wordt maximaal invulling gegeven aan transparantie richting betrokkenen.

12. AVG

12.1 Het verwerkingsregister

BSOB werkt met zeer veel processen en dus ook diverse verwerkingen van persoonsgegevens. Middels een verwerkingsregister houdt BSOB precies bij waar welke verwerkingen plaats vindt.

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 behorende 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;
- Een algemene beschrijving van de beveiligingsmaatregelen.

De Privacy Officer (PO) beheert het verwerkingsregister. Proceseigenaren binnen de organisatie zijn verantwoordelijk voor het opnemen van nieuwe verwerkingen in het verwerkingsregister. Zij worden hierbij geadviseerd door de Privacy Officer. De Functionaris Gegevensbescherming (FG) controleert of het register volledig en up-to-date is. Middels een functiebeschrijving zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van het register van verwerkingsactiviteiten vastgelegd. Het verwerkingsregister valt onder de verantwoordelijkheid van het bestuur.

12.2 Data Protection Impact Assessment (DPIA)

BSOB staat niet stil en is altijd in ontwikkeling. Zo worden processen en systemen periodiek aangepast, waardoor er sprake kan zijn van een nieuwe verwerking of wijziging van een bestaande verwerking. Om de privacyrisico's in kaart te brengen voor een juiste belangenafweging voert BSOB vooraf een pre-DPIA uit. De uitvoering van de pre-DPIA valt onder de verantwoordelijkheid van de teamaanspreekpunten. Deze kan een DPIA-verantwoordelijke binnen het proces aanwijzen. Aan de hand van de uitgevoerde pre-DPIA wordt voor zowel informatiebeveiliging als privacy een risico-inventarisatie uitgevoerd.

Op basis van de uitgevoerde pre-DPIA wordt bepaald of voor een afzonderlijke verwerking een hoog risico bestaat. Is dit niet het geval dan kan een privacy-advies van het Privacy Team volstaan. Wanneer een verwerking wel een hoog privacyrisico voor betrokkenen met zich meebrengt, voert BSOB eerst een DPIA uit. Een DPIA geeft inzicht in welke maatregelen

getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau. Hiermee wordt invulling gegeven aan een juiste belangenafweging.

BSOB hanteert een standaard DPIA-model. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor verwerkingen met een hoog privacy risico. Het Privacy Team ondersteunt en adviseert hierbij. BSOB hanteert daarnaast een handreiking ter verduidelijking voor de DPIA-verantwoordelijke. De FG geeft advies over de uitgevoerde DPIA en ondertekent deze.

Het Privacy Team houdt een register bij van uitgevoerde DPIA´s en monitort de voortgang van het DPIA-proces. Er wordt gekeken naar de geïmplementeerde beheersmaatregelen en gerapporteerd aan de FG.

Processen kunnen regelmatig worden aangepast met mogelijke effecten op de verwerking. Als er een wijziging in het proces wordt doorgevoerd, is het noodzakelijk om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt. Kleine risico's kunnen groter worden, maar grote risico's kunnen ook kleiner worden. Dit wordt meegenomen bij de herijking van een DPIA.

12.3 Privacy by Design & Privacy by Default

BSOB hanteert de principes van 'Privacy by Design' en 'Privacy by Default' op haar verwerkingen.

Privacy by Design houdt in dat BSOB bij het ontwerpen van producten en diensten zorgt voor goede bescherming van persoonsgegevens. Bij de inrichting van het proces en/of de bouw van het systeem kijkt BSOB bijvoorbeeld naar de benodigde technische en organisatorische maatregelen. Privacy wordt vanaf het begin van de uitvoer van projecten meegenomen. Dit wordt gewaarborgd door de Privacy Officer mee te laten kijken in de voorfase van een project. De FG ziet erop toe dat dit ook daadwerkelijk gebeurt.

Privacy by Default houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacy vriendelijke manier. Zoals hiervoor genoemd, geldt voor BSOB dat voor een nieuwe verwerking of een wijziging in een bestaande verwerking BSOB een pre-DPIA uitvoert. Door deze pre-DPIA wordt aan de voorkant helder of een uitgebreidere DPIA noodzakelijk is. Bij het uitvoeren van een DPIA worden de voor Privacy by Design en Privacy by Default noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de voorgenomen verwerking. Zo worden in formulieren geen gegevens gevraagd die overbodig zijn. Op deze manier wordt geborgd dat nieuwe verwerkingen conform de normen van Privacy by Design en Privacy by Default worden ingericht.

12.4 Datalekken

Een datalek heeft potentieel een grote impact op betrokkenen en BSOB als organisatie. BSOB zet daarom meerdere processen, systemen en acties in om datalekken te voorkomen.

Volledig uitsluiten is onmogelijk, maar BSOB zet zich in om een cultuur te creëren waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Het kan namelijk zo zijn dat een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens en/of betrokkenen binnen 72 uur na ontdekking hiervan. Indien BSOB niet of niet tijdig melding maakt, loopt BSOB een risico op een boete van de AP. Deze kan oplopen tot een maximum van 20 miljoen euro of 4% van een jaaromzet. Los van een morele verplichting is er dus ook een financieel risico wanneer niet wordt voldaan aan de meldplicht.

Om te voldoen aan bovengenoemde verplichtingen is er een incidenten procedure opgesteld. Hierin staat beschreven op welke wijze BSOB incidenten afhandelt en wie daarbij welke taken en verantwoordelijkheden heeft. In deze procedure staat ook beschreven hoe en wanneer een datalek dient te worden gemeld bij de AP en/of betrokkenen. Alle datalekken kunnen gemeld worden via het incidentenformulier van BSOB.

Om te blijven anticiperen op mogelijke risico's, houdt BSOB een intern incidentenregister bij waarin alle geconstateerde beveiligingsincidenten worden geregistreerd. Hierin legt BSOB vast of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, of het datalek ook is gemeld bij de toezichthouder en/of de betrokkenen. Elk kwartaal evalueert het privacy team het incidentenregister om trends bij te houden en structurele verbeteringen intern door te voeren. Tevens worden gevoelige datalekken direct geëvalueerd om zo dringende aanpassingen gelijk door te voeren in de organisatie.

12.5 Rechten van betrokkenen

Betrokkenen zijn alle natuurlijke personen van wie BSOB de persoonsgegevens verwerkt. Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn naar een natuurlijk persoon; de betrokkene. Persoonsgegevens zijn dus veel meer gegevens dan alleen iemands persoonlijke gegevens zoals naam, adres en woonplaats. Betrokkenen hebben rechten die zij kunnen uitoefenen om te controleren of BSOB zich houdt aan de AVG. BSOB is verplicht goede en toegankelijke procedures te hebben voor de uitoefening van deze rechten van betrokkenen. De AVG-rechten van betrokkenen staan in hoofdstuk 3 van de AVG. Betrokkenen kunnen van hun rechten gebruikmaken door een verzoek te sturen naar privacy@bs-ob.nl en indien er een vraag is voor de FG het mailadres fg@bs-ob.nl.

12.6 Gegevens delen met derden

Wanneer sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, worden er afspraken gemaakt over de gegevensuitwisseling. Deze afspraken voldoen tenminste aan de AVG en worden vastgelegd in een onderlinge regeling, samenwerkingsovereenkomst, gegevensuitwisselings-overeenkomst of verwerkersovereenkomst.

Er is een model verwerkersovereenkomst aanwezig dat inhoudelijk voldoet aan de eisen die de AVG en Wpg daaraan stelt. In het verwerkingsregister van BSOB houdt de PO bij welke verwerkers er zijn. De ondertekende versies van de verwerkersovereenkomsten behoren bij

de proceseigenaren te zijn gearchiveerd. BSOB gebruikt zoveel mogelijk landelijke standaarden en richtlijnen om de contractuele verplichtingen met derden te regelen. Dit is uitgewerkt in werkinstructies en gewaarborgd in het inkooptraject.

Met betrekking tot doorgifte hanteert BSOB het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is. Rechtmatigheid wordt aangetoond in één van de volgende drie gevallen:

- Een adequaatheidsbesluit;
- Passende waarborgen middels een modelcontract (Standard Contractual Clauses);
- Specifieke uitzonderingen.

12.7 Vragen of klachten

Betrokkenen met een vraag, mededeling of klacht over het gebruik van hun persoonsgegevens door BSOB kunnen contact opnemen met BSOB via privacy@bs-ob.nl. Indien een vraag of klacht niet (voldoende) beantwoord is. dan kan men contact opnemen met de FG via fg@bs-ob.nl. Het is ook mogelijk dat een betrokkene direct contact opneemt met de FG. In gevallen waar het privacybeleid niets over zegt, beslist het dagelijks bestuur van BSOB. Tot slot kunnen betrokkenen een klacht indienen bij de AP.

Vragen worden zo snel mogelijk, maar uiterlijk binnen vier weken afgehandeld. Indien een vraag niet tot tevredenheid is afgehandeld, hebben betrokkenen het recht zich opnieuw te wenden tot het privacy team. Het privacy team registreert in dat geval de vraag als een klacht. Klachten worden zo snel mogelijk, maar uiterlijk binnen zes weken afgehandeld. Personen hebben het recht om na afhandeling van een klacht hiertegen verweer te voeren bij de FG voor zover het verweer gericht is op de naleving van privacywetgeving en/of het privacybeleid van BSOB.

13. Governance

Het privacybeleid staat niet op zichzelf en maakt onderdeel uit van een reeks aan maatregelen om de bescherming van c.q. de verwerking van persoonsgegevens binnen en door de organisatie te optimaliseren. Het is een inherent onderdeel van ieders functie en dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de corebusiness van de meeste medewerkers. Er zijn daarom medewerkers die advies geven over en toezicht houden op de bescherming van persoonsgegevens binnen de organisatie, namelijk team Gegevensbescherming.

13.1 Het bestuur

Het bestuur bestaat uit het algemeen bestuur, het dagelijks bestuur, het MT en directeur. Het bestuur stelt het privacybeleid vast en is verantwoordelijk voor het voorzien in passende privacy waarborging bij de uitvoering van wettelijke taken. Ook wijst zij uit haar midden een portefeuillehouder privacy aan. De verantwoordelijkheid voor de uitvoering van het privacybeleid ligt bij het algemeen bestuur. Binnen het bestuur valt de bescherming van persoonsgegevens onder de portefeuille privacy. Het bestuur informeert de verschillende Colleges en Raden van de deelnemende gemeenten en legt verantwoording af over de privacy beleidsvoering. Het bestuur betracht beleidstransparantie te bewerkstelligen met behulp van publieksvoorlichting. Er wordt zorggedragen voor documentatie van beleid en maatregelen zodat op ieder moment maatschappelijk en juridisch uitleg gegeven kan worden over de deugdelijkheid van de aanpak.

Het bestuur bevordert samen met het management een privacy bewuste organisatiecultuur door middel van voorbeeldgedrag en het voorzien in middelen voor bewustwording en training van medewerkers en leidinggevenden. Ook ziet het bestuur erop toe dat informatieveiligheid binnen BSOB in lijn is met de geldende norm en wordt vastgelegd in het informatiebeveiligingsbeleid.

13.2 Algemeen bestuur

Zoals eerder aangegeven valt de bescherming van persoonsgegevens onder de verantwoordelijkheid van het bestuur. Het algemeen bestuur zorgt ervoor dat:

- De organisatie in staat is om de gedelegeerde verantwoordelijkheden te dragen; en
- De controle op het privacybeleid binnen de organisatie is gewaarborgd.

13.3 Management team

Het management team is inhoudelijk verantwoordelijk voor de naleving van wet- en regelgeving bij processen die binnen een bepaald team vallen. Het gaat hier om wet- en regelgeving die specifiek voor een bepaald proces van toepassing is, zoals de Algemene wet bestuursrecht, de gemeentewet, de Wet gemeenschappelijke regelingen, de Wet Waardering Onroerende Zaken en de Waterschapswet. Daarnaast is de betreffende manager ook verantwoordelijk voor naleving van de AVG met betrekking tot de processen die binnen het team vallen. Managers dragen zorg dat de werkzaamheden die in het kader van hun afdelingstaken worden uitgevoerd binnen de grenzen van het privacybeleid vallen en rapporteren hierover aan de portefeuillehouder privacy van het bestuur.

13.4 Functionaris voor Gegevensbescherming (FG)

BSOB is een overheidsorgaan en heeft daarom de wettelijke plicht om een Functionaris Gegevensbescherming (FG) aan te stellen. 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, controleren, bewustwording creëren, en optreden als contactpersoon van het AP. Het is niet de bedoeling dat de FG de taken op het gebied van privacybescherming bij de teams wegneemt. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en richtlijnen op het gebied van privacy. De FG handelt privacy gerelateerde vragen van betrokkenen of medewerkers binnen 4 weken en klachten binnen zes weken af.

13.5 Privacy Officer (PO)

Voor medewerkers én bestuurders is/zijn de Privacy Officer het dagelijkse aanspreekpunt bij vragen over de bescherming van persoonsgegevens voor zover deze niet binnen het domein van de informatiebeveiliging vallen. Ook ondersteunt de PO teams bij het opstellen van verwerkersovereenkomsten, het waar nodig mede-implementeren van adviezen van de FG, en het opstellen van modellen, zoals een model-toestemmingsbrief. De PO vormt samen met de FG en de CISO het meldpunt datalekken.

Zoals aangegeven heeft de FG adviserende en toezichthoudende taken. Het gelijktijdig uitoefenen van beide taken kan spanningen geven. Wanneer dergelijke spanningen voorzienbaar en onwenselijk zijn, kan de PO de beantwoording van een concrete adviesvraag van de FG overnemen.

13.6 Chief Information Security Officer (CISO)

De CISO stelt het informatiebeveiligingsbeleid en de informatiebeveiligingsplanning op. Hij initieert en voert risicoanalyses uit en onderzoekt zelf kwetsbaarheden of laat dit doen. Hij handelt informatiebeveiligingsincidenten af en coördineert bij grote beveiligingsincidenten. Alle beveiligingsincidenten worden bijgehouden in het incidentenregister door de CISO. De CISO adviseert gevraagd en ongevraagd het bestuur, de directie en managers over risico's en te nemen maatregelen.

De CISO stimuleert de bewustwording binnen en het bewustzijn van de organisatie over informatieveiligheid en risico's. De CISO vormt samen met de FG en de PO het meldpunt datalekken.

13.7 Privacy Team

De FG, PO en CISO vormen samen het Privacy Team. De PO, CISO en FG kunnen elkaar vervangen indien noodzakelijk. Het Privacy Team valt onder de verantwoordelijkheid van de portefeuillehouder privacy.

13.8 Medewerkers BSOB

Medewerkers zijn verantwoordelijk voor een goede omgang met persoonsgegevens in hun werkzaamheden binnen BSOB. Medewerkers ondertekenen bij indiensttreding een geheimhoudingsverklaring waarin is opgenomen hoe wordt omgegaan met persoonsgegevens en/of leggen de Eed of Belofte af. Zo hebben medewerkers op basis van hun autorisatie alleen toegang tot de persoonsgegevens die nodig zijn ter uitvoering van hun werkzaamheden, is vertrouwelijke omgang met persoonsgegevens vereist, en is vereist dat medewerkers hun computer afsluiten en hun bureau opruimen als zij hun werkplek verlaten. Dit voorkomt dat persoonsgegevens onbeheerd worden achtergelaten. Bij vragen over privacy gerelateerde onderwerpen of bij een vermoedelijk datalek, richten zij zich tot de PO of FG.

13.9 Proceseigenaren

Een proceseigenaar voert, als onderdeel van zijn of haar verantwoordelijkheden binnen de afdelingen, regie en houdt toezicht op zijn of haar proces(sen) op basis van dit privacybeleid. Proceseigenaren zijn verantwoordelijk voor het (laten) opnemen van nieuwe verwerkingen in het verwerkingsregister en het laten uitvoeren van DPIA's. Ook archiveren zij ondertekende versies van verwerkingsovereenkomsten. Zij worden hierbij geadviseerd en ondersteund door de Privacy Officer. De Functionaris Gegevensbescherming adviseert en controleert hun werkzaamheden.

Bij processen waaraan privacyrisico's zijn verbonden, hanteert de proceseigenaar een procesplan waarin duidelijk en actueel beschreven is wat het procesdoel is. Het procesplan

stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd. Het procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering en omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden. De proceseigenaar spant zich in om geen onrechtmatig verkregen gegevens te (laten) verwerken en houdt zich bij uitvoering van zijn werkzaamheden aan het privacybeleid en in geval van incidenten aan de procedure beveiligingsincidenten en datalekken.

Dit privacy beleid treedt in werking met ingang van de eerste dag na die van bekendmaking. Dit privacy beleid kan worden aangehaald als "Privacybeleid 2024 Belastingsamenwerking Oost Brabant".

Aldus vastgesteld in de vergadering van het Dagelijks Bestuur van BSOB van 18 maart 2024.

De voorzitter	De secretaris
G.T. Buter	E. M. van der Heijden