Uitbestedings- en inkoopbeleid SBZ Pensioen

Inhoud

1. Inleiding

Het Uitbestedings- en inkoopbeleid beschrijft achtereenvolgens doelstelling, reikwijdte, uitbestedingsproces, formalisatie, monitoring en evaluatie van de uitbestede werkzaamheden. Het Uitbestedings- en inkoopbeleid van het fonds voldoet hiermee aan het bepaalde bij en krachtens artikel 34 van de Pensioenwet.

2. Doel van het Uitbestedings- en inkoopbeleid

Het Bestuur is verantwoordelijk voor de uitvoering van de pensioenregeling(en). Gezien de aard en omvang van de werkzaamheden heeft het Bestuur besloten dat het doelmatig is om werkzaamheden uit te besteden aan derden (leveranciers). De doelstelling van het Uitbestedings- en inkoopbeleid van het fonds is te waarborgen dat de uitbestede werkzaamheden bijdragen aan een deugdelijke, prudent en doeltreffend bestuur van het pensioenfonds en op een beheerste en integere wijze worden uitgevoerd.

Onderuitbesteding

Het Bestuur blijft eindverantwoordelijk voor de uitbestede werkzaamheden of processen. Dit geldt onverminderd wanneer de leverancier zelf ook uitbesteedt (onderuitbesteding). Omdat het Bestuur op de hoogte moet zijn van onderuitbesteding wordt contractueel vastgelegd dat de leverancier de werkzaamheden niet aan een derde partij mag uitbesteden zonder voorafgaande kennisgeving aan het fonds.

3. Reikwijdte

a. Werkzaamheden die niet worden uitbesteed

De volgende werkzaamheden worden niet uitbesteed:

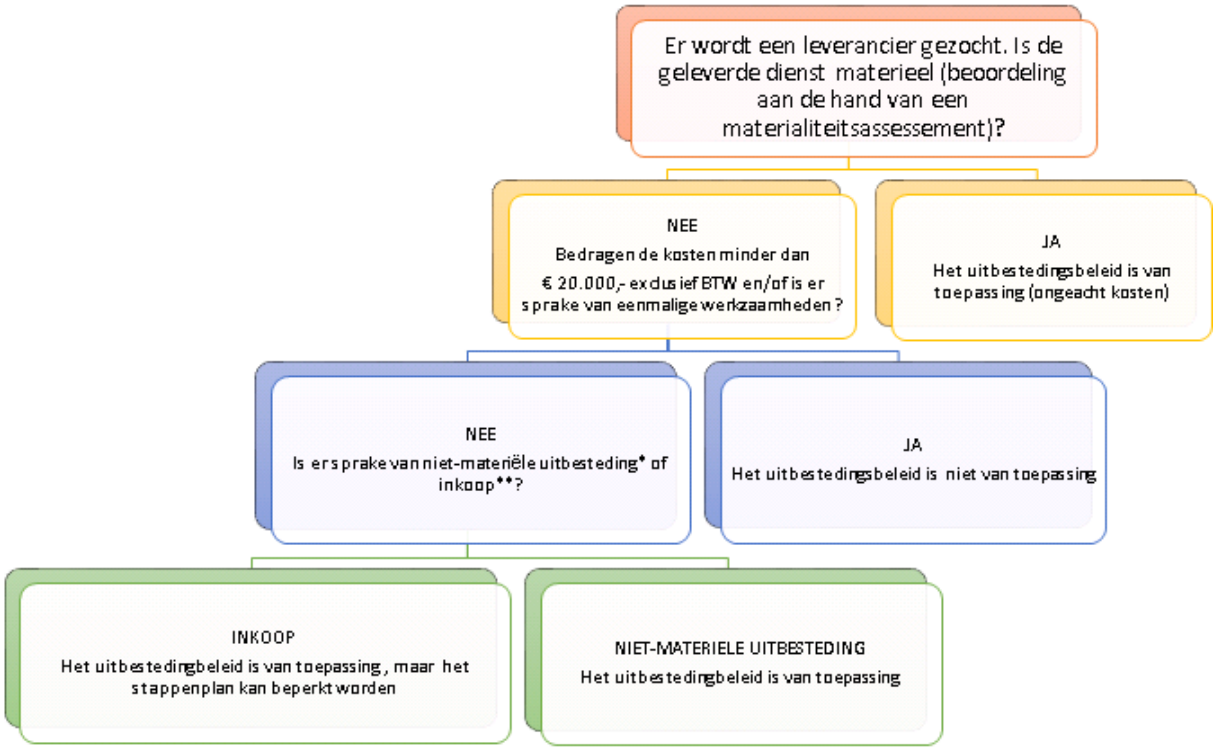
1. taken en werkzaamheden van personen die het dagelijks beleid bepalen, daaronder mede verstaan het vaststellen van beleid en het afleggen van verantwoording over het gevoerde beleid;
2. werkzaamheden waarvan uitbesteding de verantwoordelijkheid van de uitvoerder voor de organisatie en beheersing van bedrijfsprocessen en het toezicht daarop kan ondermijnen;
3. het opstellen van en toezien op het strategische beleid ten aanzien van vermogensbeheer;
4. werkzaamheden waarvan de uitbesteding een belemmering kan vormen voor een adequaat toezicht op de naleving van de wettelijke regels.
5. werkzaamheden waarbij - door de uitbesteding - het operationele (IT-)risico onnodig toeneemt; of
6. werkzaamheden waarbij - door de uitbesteding - de continuïteit en de toereikendheid van de dienstverlening aan (gewezen) deelnemers, andere aanspraakgerechtigden en pensioengerechtigden worden ondermijnd.

b. Toepasselijkheid Uitbestedings- en inkoopbeleid

Het Uitbestedings- en inkoopbeleid is van toepassing op alle selectietrajecten die gaan over:

- uitbesteding van werkzaamheden die materieel zijn;
- niet-materiële uitbesteding van werkzaamheden of inkoop van producten of diensten door het fonds tenzij:
    - het contractniveau naar schatting lager is dan een eenmalig bedrag van € 20.000,- exclusief BTW (per opdracht);
    - er sprake is van eenmalige niet terugkerende werkzaamheden;

Voor inkoop van producten of diensten kan voor het beperkt doorlopen van het selectieproces gekozen worden. Het Uitbestedings- en inkoopbeleid geldt voor alle bestaande en/of nieuwe uitbestedingen.



*Uitbesteding van niet-materiële of minder belangrijke operationele functies of activiteiten.

** Voorbeelden: Inkoop van producten, adviesdiensten, licenties, inhuur personeel

Alle uitbestedingen en inkopen staan met verleende dienst beschreven in het contractenregister (bijlage 2).

4. Uitbestedingsproces

4.1. Beoordeling materialiteit

Om te beoordelen of een dienst van een leverancier materieel (belangrijk, kritiek) is, voert het Bestuur een materialiteitsassessment uit. De materialiteit wordt beoordeeld aan de hand van de volgende criteria:

1. Het kritieke karakter en het profiel van inherente risico's van de uit te besteden activiteiten, dat wil zeggen de vraag of de activiteiten essentieel zijn voor de bedrijfsvoering / bedrijfscontinuïteit / levensvatbaarheid van het fonds en haar verplichtingen jegens haar belanghebbenden (in de zin dat het fonds zonder deze functie of activiteit niet in staat zou zijn om haar diensten op een beheerste ,integere en kwalitatief verantwoorde wijze te verlenen);
2. Het directe operationele effect van onderbrekingen van de dienstverlening en de daarmee gepaard gaande juridische risico's en reputatierisico's;
3. Het effect dat een verstoring van de activiteit kan hebben op de verwachte inkomsten van het fonds, en de gevolgen voor de deelnemers;
4. Het effect dat een schending van de vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens kan hebben op het fonds en haar belanghebbenden;
5. Indien het vermogensbeheer betreft, de uitbesteding van tenminste 30% van het beheerd vermogen;
6. Onder materiële activiteiten wordt ook het gebruik maken van fiduciair beheer en het gebruik maken van een custodian geschaard.

4.2. Risicoanalyse

Alvorens werkzaamheden worden uitbesteed voert het Bestuur van het fonds een risicoanalyse uit waarin is opgenomen:

1. De doelstelling of reden om tot uitbesteding over te gaan;
2. Een beschrijving van de uit te besteden werkzaamheden of processen;
3. Daar waar sprake is van verwerking van privacygevoelige informatie moet worden beoordeeld of een dataprivacy impactassessment (DPIA) moet worden uitgevoerd, en zo ja dan moet in het selectieproces een DPIA (door de leverancier) worden uitgevoerd;
4. Daar waar sprake is van materiële uitbestedingen waarbij IT-risico een rol speelt worden de relevante IT-principes van het fonds (bijlage 9) onderzocht.
5. Een kosten-baten analyse van de uitbesteding van die werkzaamheden of processen;
6. Een analyse van de risico's als gevolg van uitbesteding en de vereiste toezichtmaatregelen op basis van de checklist risico's (bijlage 3) en het format van DNB (bijlage 4);
7. De benodigde beheersmaatregelen.

Indien de risicoanalyse leidt tot het oordeel dat werkzaamheden uitbesteed gaan worden, doorloopt het Bestuur het volgende proces, Bij materiële uitbestedingen wordt een niet-uitvoerend bestuurslid aangehaakt als klankbord.

4.3. Selectieproces

Het Bestuur waarborgt een effectief proces voor leveranciersselectie.

a. De uitkomsten van de risicoanalyse worden gehanteerd als requirements die gesteld worden aan de leverancier. De gestelde requirements zien voor wat betreft IT-omgeving op Beschikbaarheid, Vertrouwelijkheid, Integriteit en Aanpasbaarheid (zie het Risicomanagement beleid voor een toelichting hierop).
b. Voorbereiden selectie uitbesteding, waaronder eventueel samenstellen van een selectiecommissie, inhuur van een adviseur (voor onafhankelijke externe toetsing van offertes, wanneer daarvoor onvoldoende expertise binnen SBZ Pensioen aanwezig is) en het opstellen van een lijst van mogelijke leveranciers. Deze leveranciers mogen niet op de uitsluitingenlijst (actuele versie zie website) staan.Vaststellen weging van de verschillende selectiecriteria. Een partij moet voldoen aan alle eisen in het Uitbestedings- en inkoopbeleid. SBZ Pensioen heeft haar processen voor het grootste deel uitbesteed dan wel als dienst ingekocht. Een leverancier die materiële processen uitvoert in opdracht van het Bestuur met privacy gevoelige persoonsdata zal een zwaarder beheersingskader gesteld krijgen dan een uitbestedingsrelatie die niet materieel is in de bedrijfsvoering en/of werkt met openbare data. Ten aanzien van de IT-omgeving van de uitbestedingsrelaties stuurt het fonds op de beheersmaatregelen van de diverse dienstverleners. De kwaliteitseisen met betrekking tot de organisaties, waaraan werkzaamheden zijn uitbesteed, vallen onder het uitbestedingsrisico.
c. Opvragen van informatie bij potentiële kandidaten aan de hand van het uitvraagformat (bijlage 5) en de op te vragen documenten (bijlage 6); Daar waar er sprake is van een onderuitbesteding dient de uitvoerder de benodigde informatie aan te leveren.
d. Opvragen offertes bij minimaal twee potentiële kandidaten;
e. Toets op selectiecriteria;
f. Beoordelen of de risicoanalyse aangevuld moet worden (bijvoorbeeld met informatie over onderuitbesteders; de uitvoerder dient hiervoor een analyse aan te leveren);
g. Indien relevant: site visits bij voorkeurskandidaten;
h. Opstellen rapport voorstel keuze;
i. Principebesluit;
j. Onderhandelen;
k. Besluit.

Na het selectieproces zal het risicomanagementraamwerk bijgewerkt worden.

4.4. Melding aan DNB

(Onder)uitbesteding van werkzaamheden moet bij DNB worden gemeld op voorgeschreven wijze. Indien de leverancier aan wie een fonds werk uitbesteedt, deze werkzaamheden zelf (deels) uitbesteedt is sprake van onderuitbesteding. Onderuitbesteding dient in beginsel aan het Uitbestedings- en inkoopbeleid van het fonds te voldoen. Op het moment dat het fonds een melding ontvangt van onderuitbesteding toetst het aan de hand van het materialiteitsassessment of de onderuitbesteding materieel is.

4.5. Formalisatie in overeenkomst en Service Level Agreement

Overeenkomst

Na het bestuursbesluit worden de uiteindelijke afspraken vastgelegd in een schriftelijke overeenkomst die voldoet aan de wettelijke eisen. In de overeenkomst die ziet op uitbesteding, worden tenminste de door het Bestuur in het document 'Bepalingen overeenkomst' (bijlage 7) vastgelegde zaken geregeld. Voor een overeenkomst die ziet op inkoop van diensten zal een beperktere en andere vorm van overeenkomst worden gesloten (overeenkomst van opdracht).

Indien de leverancier een verwerker voor het fonds is zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG) komt het fonds een verwerkersovereenkomst – zoals beschreven in artikel 28 van de AVG – overeen met de leverancier. De vertrouwelijke gegevens, waaronder persoonsgegevens, worden dan conform wettelijke voorschriften verwerkt. In de overeenkomst is beschreven wie verantwoordelijk is voor het melden van eventuele datalekken van persoonsgegevens bij de daartoe aangewezen autoriteiten, inclusief het in deze situaties te volgen proces.

Service Level Agreement

Eventuele detailwerkafspraken worden vastgelegd in een bijbehorende Service Level Agreement (SLA). Hierin zijn onder meer de prestatie-indicatoren opgenomen, waaronder de kwaliteit, tijdigheid, servicegraad, die als basis dienen voor de periodieke monitoring. Meer specifiek wordt in ieder geval opgenomen:

1. de specifieke werkzaamheden die de uitvoerder verricht voor het fonds met eisen t.a.v. de kwaliteit en de kwantiteit van de werkzaamheden;
2. wijze en periodiciteit van rapporteren van de uitvoerder over de door haar behaalde resultaatsnormafspraken en een aantal specifieke IT-controls en hieraan gekoppelde prestatienormen (SLA rapportages);
3. overige periodieke informatieverstrekking geïdentificeerd op basis van proportionaliteit en materialiteit, waaronder tenminste een SOC2- (waarin alle applicaties relevant voor SBZ Pensioen zijn opgenomen) en ISAE3402-verklaring (waarvan Changemanagement en verantwoording over onderuitbesteding onderdeel uitmaken), vergelijkbare of meer uitgebreide verklaring;
4. details over periodieke evaluatie (zie onder *e. Evaluatie*);
5. afspraken over het direct melden van incidenten en / of mandaatoverschrijdingen aan het fonds;
6. afspraken over het feit dat dat de leverancier bij de jaarlijkse evaluatie van de dienstverlening melding maakt van relevante wijzigingen in beleidsdocumenten die bij de selectie zijn gedeeld.

4.6. Monitoring

Het Bestuur toetst regelmatig of de manier waarop de uitbestede werkzaamheden of processen worden uitgevoerd in overeenstemming is met de gemaakte afspraken. Het Bestuur doet dit door middel van:

1. Het monitoren van jaarlijkse risico en control self-assessments van de uitvoerders;
2. Het monitoren van de uitvoerders via het laten uitvoeren van periodieke audits bij de uitvoerder en/of te laten rapporteren over de stand van zaken met betrekking tot de aanbevolen verbeteringen in de ISAE3402-verklaring of een daarmee vergelijkbare of meer uitgebreide verklaring;

3. Maandelijkse en kwartaalrapportages (financiële en niet- financiële) van de uitvoerders, waarin naast de gebruikelijke informatie ook wordt gerapporteerd over klachten, incidenten (waaronder integriteit, (cyber)security en datalekken) en uitzonderingen en over de uitkomsten van doorlopen testen (bijvoorbeeld penetratie, patch, uitwijk, en het business continuity plan);
4. Incidenten aangaande de verwerking van het fonds in de keten van uitvoerders die de integriteit van het fonds raken worden terstond aan het fonds gemeld, dit naast de bovengenoemde periodieke rapportages. Het fonds ontvangt een incidentenrapportage, aan de hand waarvan kan worden vastgesteld wat de impact is (geweest) op de IT-systemen en processen, hoe hier opvolging aan is gegeven en welke aanvullende beheersmaatregelen zijn getroffen. De integriteit van het fonds wordt ook geraakt als er sprake is van een datalek;
5. Tenminste jaarlijks leggen de (relevante) uitvoerders verantwoording af over de verwerking van persoonsgegevens;
6. Het actuarieel rapport van de certificerend actuaris;
7. Rapportages van de accountant;
8. Periodiek overleg en evaluatie met de uitvoerders over de uitvoering van de (bijgestelde) processen, dit met inbegrip van uitgevoerde of aangepaste relevante gegevensbeschermingseffectbeoordelingen die het fonds raken;
9. Rapportage door de Compliance Officer aan de Audit-, Risk- en Compliancecommissie over de uitvraag van de uitvoerders ten aanzien van:
    a. de governance van compliance bij de uitvoerders (waarbij de Compliance Officer desgewenst toegang heeft tot voor de toetsing relevante stukken van de uitvoerders);
    b. de voor het fonds relevante incidenten (wat onder een incident wordt verstaan staat in de ‘Regeling incidenten’) (waaronder tenminste integriteitsincidenten en datalekken); en
    c. het beloningsbeleid van de uitvoerder.

Het Uitvoerend Bestuur stelt een kwartaalrapportage op ten behoeve van het Bestuur, gehoord de Sleutelfunctiehouder Risicobeheer (SFH RB) en de Audit-, Risk- en Compliancecommissie (ARC), waarin een groot deel van rapportages voor alle uitbesteding en belangrijkste fondsrisico's bij elkaar verwerkt zijn tot een gecomprimeerd rapport. De SFH RB en de ARC hebben de mogelijkheid mondeling tijdens en/of schriftelijk voorafgaand aan de bestuursvergadering waarin deze kwartaalrapportage wordt besproken hun observaties bij de rapportage toe te lichten.
Indien de monitoring van de afspraken leidt tot de constatering dat de afgesproken niveaus van dienstverlening niet worden gerealiseerd zal onverwijld actie worden ondernomen. In samenwerking met de leverancier zullen de oorzaken worden achterhaald en zullen maatregelen worden getroffen om het gewenste niveau te kunnen realiseren. Indien geconstateerd wordt dat sprake is van structurele problemen die niet op korte termijn oplosbaar zijn, dient het Bestuur zich te beraden omtrent beëindiging van de uitbesteding.

4.7. Evaluatie

Ongeacht de specifieke afspraken met de leverancier voert het Bestuur een periodieke evaluatie uit van alle lopende uitbestedingen. Deze periodieke evaluatie vindt eenmaal per jaar plaats.
Deze periodieke evaluatie vormt een moment voor heroverweging van de uitbesteding en vindt plaats aan de hand van een evaluatieformulier (bijlage 8). Voor materiële uitbestedingen waarbij IT-risico een rol speelt worden de IT doelstellingen, – beheersdoelen en IT-principes van het fonds (bijlage 9) besproken.
Indien de evaluatie leidt tot de constatering dat de afgesproken niveaus van dienstverlening niet worden gerealiseerd zal onverwijld actie worden ondernomen. In samenwerking met de leverancier zullen de oorzaken worden achterhaald en zullen maatregelen worden getroffen om het gewenste niveau te kunnen realiseren. Indien geconstateerd wordt dat sprake is van structurele problemen die niet op korte termijn oplosbaar zijn besluit het Bestuur over beëindiging van de uitbesteding.
Los van de periodieke evaluatie kan het Bestuur op basis van verschillende gebeurtenissen besluiten tussentijds te evalueren dan wel een uitbesteding te heroverwegen.

Bij hercontractering, doch tenminste eens in de 3 jaar wordt in beginsel een meer uitgebreid marktonderzoek gedaan, tenzij het Bestuur om haar moverende redenen besluit tot een andere termijn.

5. Stakeholders

Partij:	Uitvoerende bestuur	Niet-uitvoerende bestuur	Bestuursonderondersteuning	VO
Taak:				
Beoordeling materialiteit	E	I	V	I
Risicoanalyse	V	E	I	I
Selectieproces tot definitieve keuze Materieel	V	E	R	I
Selectieproces tot definitieve keuze niet-materieel en inkoop	E	I	V	I
Besluit selectie Materieel	V	E	R	I
Besluit selectie niet-materieel en inkoop	E	I	R	I
Melding aan DNB	E	I	V	I
Formalisatie in overeenkomst en Service Level Agreement Materieel	V	E	I	I
Formalisatie in overeenkomst en Service Level Agreement niet-materieel en inkoop	E	I	V	I
Monitoring incl opstellen risicorapportage UB	V	E	R	I
Evaluatie contractspartijen Materieel	V	E	R	I
Evaluatie contractspartijen niet-materieel en inkoop	E	I	V	I
Jaarlijkse evaluatie van het beleid	V	E	R	I
Bewaken contractenregister	E	I	V	I

VERI-Matrix wat staat voor Verantwoordelijk / Eindverantwoordelijk / Raadplegen / Informeren.

6. Inwerkingtreding

Dit Uitbestedings- en inkoopbeleid treedt in werking na goedkeuring door het Bestuur op 7 september 2020. Het uitbestedings- en inkoopbeleid wordt intern bij wijziging vooraf en eenmaal in de drie jaar getoetst door de Compliance Officer van het fonds. Het uitbestedings- en inkoopbeleid wordt driejaarlijks door het Bestuur geëvalueerd.

Ijsselstein, 7 maart 2023

Namens het Bestuur van SBZ Pensioen

Ties Tiessen
Onafhankelijk Voorzitter

Edwin Schokker
Uitvoerend Bestuurder

Bij het Uitbestedings- en inkoopbeleid horen de volgende bijlagen:

1. Meldingsformulier DNB
2. Contractenregister
3. Checklist risico's
4. Format risicoanalyse van DNB
5. Uitvraagformat
6. Op te vragen documenten
7. Bepalingen overeenkomst

8. Evaluatieformulier
9. IT doelstellingen en – beheersdoelen
10. Selectiecriteria