

Beleid uitbesteding en inkoop

Stichting Pensioenfonds Ecolab

13 maart 2025

# Inhoudsopgave

## Inleiding

|   |                                                                           |   |
|---|---------------------------------------------------------------------------|---|
| 1 | Uitgangspunten bij uitbesteding .....                                     | 1 |
| 2 | Doel van het beleid uitbesteding en inkoop .....                          | 2 |
| 3 | Risicoanalyse.....                                                        | 2 |
| 4 | Belangenverstrengeling .....                                              | 3 |
| 5 | Selectieproces .....                                                      | 3 |
| 6 | Criteria voor de selectie van een uitbestedingsrelatie .....              | 3 |
| 7 | Waarborgen en normen voor de kwaliteit van uitbestede werkzaamheden ..... | 4 |
| 8 | Monitoring en evaluatie .....                                             | 5 |
| 9 | Inwerkingtreding.....                                                     | 6 |

## Inleiding

Stichting Pensioenfonds Ecolab B.V. (verder: het pensioenfonds) heeft bedrijfsprocessen en -activiteiten uitbesteed aan derden (verder: uitbestedingsrelaties). Deze processen en activiteiten hebben betrekking op de pensioenadministratie, het vermogensbeheer en alle overige processen en activiteiten waarvan het bestuur van het pensioenfonds het in verband met de bedrijfsvoering zinvol acht om deze uit te besteden.

Aan uitbesteding is voor het pensioenfonds een aantal risico's verbonden. Het bestuur van het pensioenfonds heeft daarom beleid vastgesteld met betrekking tot de beheersing van risico's die samenhangen met de uitbesteding.

Het bestuur van het pensioenfonds is en blijft te allen tijde verantwoordelijk voor de uitvoering van het te voeren beleid, ook voor het gedeelte van de werkzaamheden dat is uitbesteed.

Het beleid uitbesteding en inkoop van het pensioenfonds is in overeenstemming met de relevante artikelen van de Pensioenwet, Digital Operational Resilience Act (DORA), het Besluit uitvoering Pensioenwet en het Besluit financieel toetsingskader pensioenfonds.

# 1 Uitgangspunten bij uitbesteding

De uitgangspunten bij uitbesteding zijn als volgt:

- Het pensioenfonds gaat over tot uitbesteding van bedrijfsprocessen en/of bedrijfsactiviteiten indien en voor zover daardoor:
  - de bedrijfsvoering van het pensioenfonds effectiever en efficiënter wordt;
  - de continuïteit van de bedrijfsvoering van het pensioenfonds kan worden gewaarborgd;
  - de kwaliteit van de bedrijfsvoering van het pensioenfonds op constant niveau kan worden gehouden;
  - de risico's adequaat kunnen worden beheerst; en
  - door het pensioenfonds continu kan worden voldaan aan wet- en regelgeving.
- Het pensioenfonds zorgt ervoor dat door de uitbesteding het bereiken van de statutaire doelstelling en de belangen van de bij het pensioenfonds betrokken deelnemers, gewezen deelnemers, pensioengerechtigden en werkgevers niet in gevaar komen.
- Het bestuur van het pensioenfonds selecteert een uitbestedingsrelatie op basis van objectief vast te stellen criteria zoals kwaliteit, prijs en marktconformiteit. De uitbestedingsrelatie voldoet aan de in dit document geformuleerde criteria. Het bestuur laat zich bij de selectie zo nodig bijstaan door een onafhankelijke adviseur.
- Het bestuur blijft eindverantwoordelijk voor en behoudt volledige zeggenschap over de uitbestede bedrijfsprocessen en bedrijfsactiviteiten.
- Het pensioenfonds houdt zich bij de uitbesteding aan de daarvoor geldende wet- en regelgeving en ziet erop toe dat ook de uitbestedingsrelatie zich houdt aan de wet- en regelgeving die voor de uitvoering van de uitbestede werkzaamheden geldt. Ook geeft het pensioenfonds opvolging aan de normen uit de Code Pensioenfonds.
- Het pensioenfonds heeft de mogelijkheid om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de uitbestedingsrelatie geschiedt.
- Structurele aandacht en goede afspraken met de uitbestedingsrelatie, periodieke monitoring en evaluatie en tijdig optreden zijn belangrijke voorwaarden voor de uitbesteding van werkzaamheden.
- Het bestuur van het pensioenfonds selecteert een uitbestedingsrelatie ook op het criterium dat de uitbestedingsrelatie voldoet aan de korte- en lange termijn beleidsdoelstellingen die het pensioenfonds zich gesteld heeft. Tevens wordt bij deze selectie de toekomstbestendigheid van het fonds in aanmerking genomen.
- Het kan voorkomen dat een uitbestedingsrelatie van het pensioenfonds gebruik maakt van diensten van derden. We spreken dan van onderuitbestedingen. Voor deze onderuitbestedingen geldt dat dit beleid onverkort van toepassing is op de "onder uitbestede" werkzaamheden.
- Het bestuur draagt zorg voor zijn eigen deskundigheid en geschiktheid, zodat het voldoende "countervailing power" heeft ten opzichte van de uitbestedingspartner.
- Het bestuur van het pensioenfonds zorgt onder andere voor voldoende countervailing power door ondersteuning/ advisering op de diverse beleidsterreinen zoals beleggingen, financieel, actuair, governance en juridisch.

## 2 Doel van het beleid uitbesteding en inkoop

Doelstelling van het beleid uitbesteding en inkoop is het vastleggen van procedures en maatregelen met betrekking tot de uitbesteding van werkzaamheden, als onderdeel van een beheerste en integere bedrijfsvoering. Daarnaast heeft het beleid als doel het waarborgen van de continuïteit van de uitbestede werkzaamheden.

Het beleid uitbesteding en inkoop is van toepassing op alle kernactiviteiten en -processen van het pensioenfonds die zijn uitbesteed. Het beleid uitbesteding en inkoop is van toepassing op alle bestaande en/of nieuwe uitbestedingsovereenkomsten, gedurende de gehele looptijd van die overeenkomsten.

Het beleid uitbesteding en inkoop is van toepassing op alle naar het oordeel van het bestuur uitbestede, bedrijfskritische of belangrijke activiteiten en processen aan derde partijen van het pensioenfonds. Kritieke of belangrijke functies zoals gedefinieerd onder DORA, die zijn uitbesteed aan ICT-derden, vallen per definitie onder dit beleid.

Het pensioenfonds besteedt niet uit:

- 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;
- werkzaamheden waarvan uitbesteding de verantwoordelijkheid van het pensioenfonds voor de organisatie en beheersing van bedrijfsprocessen en het toezicht daarop kan ondermijnen;
- indien de uitbesteding een belemmering kan vormen voor een adequaat toezicht op de naleving van het bij of krachtens de Pensioenwet bepaalde.

## 3 Strategieën als leidraad

Er is een aantal strategieën die de leidraad vormen voor het Uitbestedings- en inkoopbeleid en bepalen de richting voor het behalen van de doelstelling van het pensioenfonds. Het biedt een consistent kader voor het vaststellen van beleid, waarin duidelijke richtlijnen en principes worden geformuleerd die het pensioenfonds helpen risico's te beheersen, kosten te optimaliseren en de kwaliteit van dienstverlening te waarborgen. Door de strategie als fundament te gebruiken, kan het beleid flexibel inspelen op veranderingen in de markt en tegelijkertijd zorgen voor een robuuste en verantwoorde bedrijfsvoering.

Het betreft de volgende strategieën:

- strategie IT-risicobeheer ICT-derden;
- multi-vendor strategie;
- extistategie.

### Strategie IT-risicobeheer ICT-derden

In het kader van uitbesteding en inkoop van ICT-diensten heeft het pensioenfonds een robuuste strategie voor IT-risicobeheer met betrekking tot ICT-derden. Deze strategie heeft als doel om de continuïteit, kwaliteit en integriteit van de uitbestede IT-processen te waarborgen, terwijl tegelijkertijd de risico's van uitbesteding effectief worden beheerd.

### Multi-vendor strategie

Het pensioenfonds erkent de voordelen van een multi-vendor strategie, waarbij verschillende leveranciers worden ingezet om specifieke diensten en producten te leveren. Deze aanpak biedt flexibiliteit, verhoogt de concurrentie en kan bijdragen aan betere prestaties en kosten beheersing. Echter onderkent het pensioenfonds ook de uitdagingen van deze strategie, aangezien de markt voor ICT-dienstverleners beperkt is en er niet veel geschikte leveranciers zijn om uit te kiezen.

#### Exitstrategie

De exitstrategie richt zich op het waarborgen van een gecontroleerde, risicoloze en efficiënte beëindiging van contracten met uitbestedingspartners en leveranciers. Deze strategie is bedoeld om de continuïteit van de dienstverlening en de bescherming van de belangen van het pensioenfonds en haar deelnemers te garanderen bij het beëindiging van een samenwerking.

## 4 Risicoanalyse

Het bestuur voert periodiek een analyse van de uitbestedingsrisico's uit en past het beleid uitbesteding en inkoop aan als de uitkomsten van de analyse daartoe aanleiding geven. Daarnaast voert het bestuur per (her)nieuwe uitbesteding een specifieke risicoanalyse uit.

## 5 Belangenverstrengeling

Bij besluitvorming omtrent uitbesteding neemt het bestuur de relevante bepalingen van de gedragscode van het pensioenfonds met betrekking tot het melden van een (potentieel) belangenconflict in acht. Hiermee wordt voorkomen dat een besluit wordt genomen op basis van andere belangen dan die van het pensioenfonds, of de schijn hiervan wordt gewekt.

## 6 Selectieproces

Het pensioenfonds waarborgt een effectief proces bij het selecteren van externe partijen aan wie processen of activiteiten worden uitbesteed. Dit selectieproces omvat in ieder geval de volgende onderdelen:

- Risicoanalyse;
- Longlist;
- Request for Information;
- Shortlist;
- Request for Proposal;
- Selectiebesluit;
- Onderhandelingen.

## 7 Criteria voor de selectie van een uitbestedingsrelatie

De uitbestedingsrelatie voldoet, voor zover relevant, minstens aan de volgende criteria:

- de duurzaamheid van de dienstverlening en het voortbestaan van de dienstverlener zijn gewaarborgd door een integraal financieel gezonde toestand en een goede administratieve en interne organisatie;
- voor zover het de uitbesteding van het vermogensbeheer en de pensioenadministratie betreft, beschikt de uitbestedingsrelatie bij voorkeur over een ISAE 3402 verklaring type II of daaraan gelijkwaardige certificeringen;
- het bestuur vraagt bij de uitbestedingsrelatie op welke processen niet onder de ISAE 3402 of vergelijkbare certificering vallen en vergewist zich ervan op welke wijze de uitbestedingsrelatie de kwalitatieve uitvoering van deze processen borgt;
- de uitbestedingspartij houdt zich bij uitbesteede bedrijfsprocessen of- activiteiten aan de daarvoor geldende wet- en regelgeving, Voor ICT-derden, en met name die kritieke of belangrijke functies uitvoeren, betekent dit tevens dat zij moeten voldoen aan de aanvullende vereisten zoals gesteld in DORA;

- de uitbestedingsrelatie beschikt over de kwaliteiten die voor een goede uitvoering van de uitbestede bedrijfsprocessen of –activiteiten nodig zijn en voldoet aan eventuele door het bestuur specifiek gestelde kwaliteitsaanduidingen;
- heeft een gedragscode, een incidentenregeling en een klokkenluidersregeling ingevoerd;
- heeft – indien van toepassing op het type onderneming van de uitbestedingsrelatie – een beloningsbeleid vastgesteld dat in overeenstemming is met de daarvoor geldende wet- en regelgeving of de door de toezichthoudende instantie gestelde eisen of normen;
- de uitbestedingsrelatie beschikt over de nodige certificeringen en/of vergunningen;
- de kwaliteit en continuïteit van de uitvoering van de uitbestede bedrijfsprocessen en activiteiten zijn gedurende de periode van uitbesteding gewaarborgd;
- de uitbestedingsrelatie heeft voorzien in een proces van continue bijwerken van “back-ups” van bestanden en mutaties daarin en in een adequaat noodstelsel bij onvoorziene omstandigheden;
- de uitbestedingsrelatie stelt het bestuur onmiddellijk in kennis van incidenten;
- de uitbestedingsrelatie verstrekt voor zover relevant de toezichthouder alle relevante informatie;
- de uitbestedingsrelatie biedt de toezichthouder de mogelijkheid om (onafhankelijk) onderzoek ter plaatse te doen of te laten doen;
- de uitbestedingsrelatie is te allen tijde bereikbaar en is op het hoogste niveau aanspreekbaar.

## 8 Waarborgen en normen voor de kwaliteit van uitbestede werkzaamheden

De kaders waarbinnen de werkzaamheden zijn/worden uitbesteed, zijn/worden vastgelegd in schriftelijke overeenkomsten. Deze overeenkomsten voldoen aan alle juridische eisen.

In deze overeenkomsten worden de uitgangspunten van de selectie ook nog vastgelegd:

- De verantwoordelijkheid voor de uitbestede processen blijft bij het bestuur
- Expliciete rechten en verplichtingen van het bestuur/pensioenfonds en de uitbestedingsrelatie
- Verwijzing naar het beleid uitbesteding en inkoop met daarin benoemd o.a. doelstellingen en risicobereidheid
- Een regeling bij een eventuele benodigde overdracht van rechten en plichten van de uitbestedingsrelatie
- Afspraken over aansprakelijkheid
- Vastlegging van eigendom van vermogen, gelden, effecten, gegevens en systemen
- Mogelijkheden om wijzigingen aan te brengen in de manier waarop werkzaamheden worden uitgevoerd
- Een overzicht van kosten
- Vermelding van de opstelling van een Service Level Agreement
- Afspraken over diensten bij eventuele doorbesteding
- Afspraken over niet extra werkzaamheden die tot mogelijk additionele kosten kunnen leiden
- De voorwaarde dat er altijd aan de geldende wet- en regelgeving wordt voldaan door de uitbestedingsrelatie waardoor het pensioenfonds blijvend voldoet aan de pensioenwet- en regelgeving
- Afspraken over evaluatie, herziening, escalatie en beëindiging
- Vastlegging van de geldigheid
- Vastlegging van rechtskeuze en forumkeuze

- Aanvullende bepalingen vanuit DORA, specifiek voor ICT-derden die kritieke of belangrijke functies uitvoeren, waaronder aanvullende vereisten en controles ter borging van operationele weerbaarheid.

Het bestuur ziet er gedurende de gehele periode van uitbesteding op toe dat blijvend wordt voldaan aan de criteria die bij de selectie van de uitbestedingsrelatie en de schriftelijke overeenkomst golden. In de uitbestedingsovereenkomst wordt in ieder geval geregeld hetgeen bij of krachtens de Pensioenwet wordt voorgeschreven en worden bepalingen opgenomen over:

- de van toepassing zijnde wettelijke voorschriften of andersoortige voorschriften op het gebied van de bescherming van persoonsgegevens en andere vertrouwelijke gegevens;
- de beveiliging van de bestanden van het pensioenfonds, de toegang tot deze bestanden en de in verband daarmee afgegeven en af te geven autorisaties;
- de aansprakelijkheid voor en de kosten van fouten die bij de uitvoering van de uitbestede werkzaamheden worden gemaakt.

In de uitbestedings- of inkoopovereenkomst met kritieke of belangrijke ICT-derden wordt in ieder geval geregeld hetgeen bij of krachtens DORA wordt voorgeschreven en worden aanvullende bepalingen overgenomen die onder andere betrekking hebben op:

- de opname van gedetailleerde risicobeheersmaatregelen gericht op de bescherming van kritieke en belangrijke functies;
- het toevoegen van een DORA-addendum, waarin specifieke beveiligingsmaatregelen, herstelprocedures en aanvullende eisen verder gaan dan de basisvereisten;
- het aantonen door partijen dat zij voldoen aan de nalegingsvereisten van DORA, met inbegrip van continuïteitsbeheer en crisisplanning;
- strengere afspraken over de registratie, rapportage en afhandeling van (cyber)incidenten en klachten;
- strikte normen voor gegevensbescherming en privacy, inclusief procedures voor gegevensintegriteit, authenticiteit en vertrouwelijkheid;
- de expliciete vastlegging van mogelijkheden voor periodieke externe audits en penetratietests om de naleving van beveiligingsmaatregelen te verifiëren.

### **SLA**

Een gedetailleerde beschrijving van de uitbestede werkzaamheden ten aanzien van de pensioenadministratie of het vermogensbeheer, is vastgelegd in een service level agreement (SLA). In de SLA zijn de uitbestede werkzaamheden gekoppeld aan specifieke kwaliteitsnormen op het gebied van tijdigheid, juistheid en volledigheid. Het serviceniveau en de overeengekomen sancties wanneer niet aan de gestelde normen is voldaan worden in de SLA verwoord. Ten aanzien van specifieke werkzaamheden (pensioenbeheer, vermogensbeheer, vastgoedbeheer, custody) kunnen te leveren prestaties nog nader in de bijlagen van de SLA omschreven zijn.

## **9 Monitoring en evaluatie**

Het bestuur monitort en evalueert voldoende frequent, afhankelijk van de soort uitbesteding, of de wijze waarop de uitbestede bedrijfsprocessen en activiteiten worden uitgevoerd nog in overeenstemming is met de gemaakte afspraken. Deze monitoring en evaluatie kan gebeuren door:

- Monitoring van de periodieke SLA-rapportage door de uitbestedingsrelatie;
- Monitoring van de voorwaarden en afspraken in de schriftelijke overeenkomsten;
- Monitoring van de ISAE-3402 rapportage van de uitbestedingsrelatie;
- het betrekken van het verslag en de verklaring van de waarmede actuaire en het verslag van de accountant van het pensioenfonds;
- periodiek overleg tussen de uitbestedingsrelatie en het bestuur van het pensioenfonds;
- monitoring door periodieke audits en site visits bij de uitbestedingsrelatie.
- Vastlegging van de prestaties, incidenten en klachten worden genoteerd met vermelding van de gemaakte analyses.

- Uitgewerkte actiepunten worden traceerbaar opgevolgd
- Op basis van de bevindingen worden, indien nodig, overeenkomsten en Service Level Agreements aangepast.

DORA stelt specifieke eisen aan de monitoring van uitbestedingsrelaties met ICT-derden. DORA verplicht het pensioenfonds om de digitale operationele weerbaarheid te waarborgen en stelt specifieke eisen aan de monitoring van uitbestedingsrelaties met ICT-derden. Hierbij wordt onderscheid gemaakt tussen reguliere en kritieke of belangrijke ICT-derden.

Het pensioenfonds evalueert de uitbestedingspartners jaarlijks naast de reguliere monitoring die gedurende het jaar plaatsvindt. In de evaluatie wordt nagegaan of de uitbestedingspartners nog aan de wensen, doelstellingen en eisen van het pensioenfonds voldoen, waar bij ICT-derden ook gekeken wordt naar de vereisten van digitale operationele weerbaarheid zoals vastgelegd in DORA.

## 10 Inwerkingtreding

Dit document kan worden aangehaald als “Beleid uitbesteding en inkoop Stichting Pensioenfonds Ecolab”. Het beschreven beleid is vastgesteld door het bestuur op 13 maart 2025, treedt in werking per dezelfde datum en vervangt alle vorige versies. Dit Beleid uitbesteding en inkoop kan worden gewijzigd bij besluit van het bestuur.