

# **Privacybeleid**

## **Stichting Bedrijfstakpensioenfonds Waterbouw**

Augustus 2021

<b>1.</b>	<b>Inleiding</b>	<b>3</b>
1.1	Doelstelling privacybeleid	3
1.2	Reikwijdte	3
1.3	Wettelijke kaders	3
1.4	Definities	3
1.5	Beheer privacybeleid	4
1.6	Implementatie en evaluatie	4
<b>2.</b>	<b>Visie op privacy</b>	<b>5</b>
<b>3.</b>	<b>Aanpak</b>	<b>7</b>
3.1	Privacystatement	7
3.2	Rechten van betrokkenen	7
3.3	Gegevensbeveiliging	7
3.4	Privacybewustzijn medewerkers	8
3.5	Verwerkingsregister	8
3.6	Privacy by Design	9
3.7	Meldplicht datalekken	9
3.8	Data Protection Impact Assessment (DPIA)	10
3.9	Verwerkersovereenkomst	10
<b>4.</b>	<b>Governance</b>	<b>12</b>
4.1	Algemene uitgangspunten	12
4.2	Rollen en verantwoordelijkheden	12
4.3	Functionaris Gegevensbescherming (FG)	13
<b>5.</b>	<b>Kwaliteitsbewaking</b>	<b>14</b>
5.1	Communicatie	14
5.2	Borging	14
5.3	Controle en naleving	14

## 1. Inleiding

Stichting Bedrijfstakpensioenfonds Waterbouw (hierna: BPF Waterbouw) werkt als verplicht gesteld bedrijfstakpensioenfonds dagelijks met persoonsgegevens van deelnemers, gewezen deelnemers, pensioengerechtigden en, bij hun overlijden, van hun eventuele nabestaanden. Voor een professionele dienstverlening is het essentieel dat we deze gegevens goed beschermen. Betrokkenen moeten er op kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan. Hierbij spelen wet- en regelgeving een belangrijke rol. De Algemene Verordening Gegevensbescherming (AVG) stelt eisen aan de verwerking en opslag van informatie.

### 1.1 Doelstelling privacybeleid

BPF Waterbouw wil met dit privacybeleid een eerlijke, veilige en fatsoenlijke verwerking van persoonsgegevens door BPF Waterbouw realiseren. Met dit beleid geven wij een duidelijke richting aan privacy en laten we zien dat we privacy waarborgen, beschermen en handhaven.

Het doel van dit beleidsdocument is om duidelijk te maken wat wet- en regelgeving over persoonsgegevens betekent voor BPF Waterbouw, voor alle betrokkenen en belanghebbenden bij het fonds en voor iedereen die voor of met BPF Waterbouw werkt.

### 1.2 Reikwijdte

Dit beleid is van toepassing op de gehele organisatie van BPF Waterbouw en heeft betrekking op alle verwerkingen van persoonsgegevens die binnen de organisatie plaatsvinden.

### 1.3 Wettelijke kaders

Voor de omgang met persoonsgegevens gelden bij BPF Waterbouw de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming;
- Uitvoeringswet AVG
- Pensioenwet;
- Wet verplichte deelneming in een bedrijfstakpensioenfonds 2000;
- Wet op de loonbelasting 1964;
- Archiefwet;

### 1.4 Definities

De volgende begrippen spelen een centrale rol bij de privacy wet- en regelgeving:

- **Persoonsgegevens**  
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.
- **Bijzondere persoonsgegevens**  
Zeer gevoelige gegevens zoals iemands ras, godsdienst, seksuele leven, politieke opvatting, gezondheid, lidmaatschap van een vakvereniging en strafrechtelijk gedrag worden aangemerkt als bijzondere persoonsgegevens. Hiervoor biedt de wet een hogere mate van bescherming.

- **Betrokkene**  
Degene over of van wie de persoonsgegevens worden verwerkt.
- **Verantwoordelijke (of: verwerkingsverantwoordelijke)**  
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
- **Verwerking**  
Een bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens, zoals verzamelen, vastleggen, ordenen, structureren, opslaan, raadplegen, verstrekken, verspreiden, afschermen, wissen of vernietigen.
- **Verwerker**  
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.
- **Subverwerker**  
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat wordt ingeschakeld door de verwerker om ten behoeve van de verantwoordelijke persoonsgegevens te verwerken.

### *1.5 Beheer privacybeleid*

Het privacybeleid is ondersteunend aan de doelstelling van BPF Waterbouw om de gegevens van betrokkenen en belanghebbenden zoveel mogelijk te willen beschermen. Het privacybeleid stelt echter ook beperkingen en grenzen aan de dienstverlening die BPF Waterbouw kan bieden. Immers de informatie mag alleen worden gebruikt voor het doel waarvoor zij ter beschikking werd gesteld aan BPF Waterbouw in het kader van de uitvoering van de pensioenovereenkomst. Het privacybeleid grijpt in op nagenoeg alle aspecten van de uitvoering van de pensioenregeling.

Het privacybeleid is een bijlage van de ABTN en is als download beschikbaar gesteld op de website van BPF Waterbouw.

### *1.6 Implementatie en evaluatie*

Dit beleid is op 25 mei 2018 in werking getreden. Eenmaal per jaar wordt beoordeeld of dit beleid geactualiseerd moet worden. Als daartoe aanleiding is, zal actualisatie eerder plaatsvinden. Een laatste actualisatie heeft plaatsgevonden op 2 augustus 2021.

## 2. Visie op privacy

BPF Waterbouw zorgt vanzelfsprekend goed voor de aan het fonds toevertrouwde gegevens. Daarbij speelt niet alleen het feit dat sprake is van een wettelijke verplichting maar dit is ook noodzakelijk voor het behoud van het vertrouwen van alle belanghebbenden en betrokkenen bij het fonds. Zij moeten er op kunnen vertrouwen dat wij zorgvuldig met hun persoonsgegevens omgaan.

Het centrale beginsel dat BPF Waterbouw hanteert luidt als volgt:

**Wij verwerken persoonsgegevens in overeenstemming met de wet en doen dat op behoorlijke, zorgvuldige en transparante wijze.**

We concretiseren dit beginsel met de volgende uitgangspunten:

### 1. Zodra we hun persoonsgegevens verwerken, informeren we betrokkenen volledig en duidelijk.

Met ‘volledig’ bedoelen wij dat we alle relevante informatie, zonder terughoudendheid aanbieden. ‘Duidelijk’ betekent dat de informatie beknopt, begrijpelijk en goed vindbaar is.

Op het moment dat BPF Waterbouw start met de ontvangst van persoonsgegevens van betrokkenen, rechtstreeks, via de werkgever of via een derde partij zoals een ander pensioenfonds, UWV of belastingdienst, dan informeren we hen via een zogenaamde privacystatement. Deze verklaring bevat de essentie van de verwerking. Dit privacystatement staat op de website van BPF Waterbouw en wordt op verzoek ook aan de betrokkene toegezonden.

### 2. Belanghebbenden en betrokkenen hebben de regie over hun persoonsgegevens

Belanghebbenden en betrokkenen bij BPF Waterbouw hebben zoveel mogelijk de controle over hun eigen persoonsgegevens. BPF Waterbouw is daarom transparant over de wijze waarop zij deze gegevens verwerkt en respecteert de rechten van betrokkenen op bijvoorbeeld inzage, bezwaar en verwijdering.

### 3. Persoonsgegevens zijn bij ons veilig

BPF Waterbouw zorgt voor een passende beveiliging van de persoonsgegevens die ze verwerkt. Hierbij maken we gebruik van een risico-gebaseerde aanpak. We beschermen persoonsgegevens tegen verlies, ongeautoriseerde toegang, openbaarmaking of wijziging. Medewerkers van BPF Waterbouw gaan zorgvuldig om met persoonsgegevens. Alleen medewerkers die dat nodig hebben voor hun werk, hebben toegang tot gegevens van belanghebbenden en betrokkenen.

### 4. We verzamelen alleen de persoonsgegevens die we nodig hebben voor ons doel (dataminimalisatie), we verwerken deze niet voor een ander doel (doelbinding) en bewaren de gegevens niet langer dan noodzakelijk (bewaartermijnen).

BPF Waterbouw stelt per verwerking het doel vast en verzamelt geen gegevens die niet nodig of relevant zijn om dit doel te behalen. We gebruiken de persoonsgegevens alleen voor andere doeleinden als deze verenigbaar zijn met het oorspronkelijke doel. BPF Waterbouw bewaart gegevens niet langer dan noodzakelijk. Hiervoor zijn bewaartermijnen vastgesteld in overeenstemming met het advies van de Pensioenfederatie. De naleving van deze bewaartermijnen vindt plaats voor wat betreft het verwijderen van fysieke dossiers. Voor wat betreft digitale dossiers is handhaving van de bewaartermijnen afhankelijk van de mogelijkheden die de gebruikte automatiseringspakketten bieden. BPF Waterbouw gaat met de leveranciers van

de pakketten in gesprek om te realiseren dat een goede en controleerbare naleving van de handhaving van de bewaartermijnen ook voor de digitale dossiers kan worden gerealiseerd. Het doel van de verwerking en de bewaartermijn zijn vastgelegd in het verwerkingsregister.

5. **BPF Waterbouw verwerkt (c.q. laat verwerken) alleen persoonsgegevens als daarvoor een rechtmatige grondslag is.**

BPF Waterbouw kan elke verwerking baseren op één van de wettelijke zes grondslagen die de AVG beschrijft. Deze grondslagen zijn:

1. Uitdrukkelijke toestemming van de betrokkene;
2. Het uitvoeren van een overeenkomst met de betrokkene;
3. Het voldoen aan een wettelijke verplichting;
4. Een gerechtvaardigd belang van de organisatie;
5. Er is een vitaal belang voor de betrokkene of een ander natuurlijk persoon;
6. Het vervullen van een overheidstaak/ het algemeen belang.

De grondslag per verwerking is vastgelegd in het verwerkingsregister.

6. **Bij nieuwe diensten of de toepassing van nieuwe technologieën zorgen we ervoor dat privacy vanaf het begin wordt meegenomen in de ontwikkeling hiervan.**

7. **Bij (potentiele) datalekken handelen we snel en zorgvuldig**

Een datalek is een inbreuk op de beveiliging van persoonsgegevens, waardoor persoonsgegevens niet beschikbaar zijn, in handen van onbevoegden komen, verloren raken of ongeoorloofd gewijzigd worden. BPF Waterbouw houdt een register bij van de (potentiele) datalekken. We melden een datalek binnen 72 uur aan de Autoriteit Persoonsgegevens.

8. **De privacyrisico's voor betrokkenen houden we zo laag mogelijk**

BPF Waterbouw beoordeelt de gegevensverwerkingen aan de hand van de impact die deze hebben voor de betrokkenen. Als er sprake is van hoge risico's voor betrokkenen, voeren wij een Data Protection Impact Assessment (DPIA) uit.

Hierbij worden o.a. de proportionaliteit (de inbreuk op de betrokkenen mag niet onevenredig zijn in verhouding tot het doel) en de subsidiariteit (het doel kan niet op een manier worden gerealiseerd die minder risicovol is voor de betrokkenen) van de verwerking geanalyseerd.

9. **We delen alleen gegevens met externe organisaties als zij voldoende veiligheidswaarborgen geven.**

Wij delen alleen persoonsgegevens met externe organisaties (verwerkers) die garanderen dat zij behoorlijk omgaan met de hen toevertrouwde gegevens. Hiervoor maken we gebruik van verwerkerovereenkomsten, die afgesloten worden voordat we gegevens delen met betreffende verwerkers.

10. **Wij verstrekken geen persoonsgegevens aan personen of organisaties buiten de Europese Economische Ruimte.**

Het is toegestaan om binnen de EER persoonsgegevens te delen (mits voldaan wordt aan de vereisten van de AVG). In de situatie van BPF Waterbouw is dit echter niet aan de orde.

### 3. Aanpak

Om ervoor zorg te dragen dat onze privacy-visie gerealiseerd wordt, heeft BPF Waterbouw een aanpak opgesteld. Dit hoofdstuk bevat een beschrijving van de inhoudelijke maatregelen die BPF Waterbouw uitvoert om onze ambities op het gebied van privacy in de praktijk te brengen.

#### 3.1 *Privacystatement*

BPF Waterbouw heeft een privacy statement opgesteld om betrokkenen te informeren wanneer wij van hen gegevens gaan verzamelen. Dit privacystatement bevat de volgende onderdelen:

- Onze identiteit en contactgegevens;
- De contactgegevens van de Privacy Officer van BPF Waterbouw;
- De doeleinden waarvoor wij de persoonsgegevens verwerken;
- De grondslag voor de verwerking;
- De bewaartermijnen van de door ons verwerkte gegevens;
- De (soorten) ontvangers aan wie wij de gegevens verstrekken;
- De (soorten) persoonsgegevens die wij ontvangen en verwerken.

Het privacystatement:

- Wordt aan betrokkenen bekend gemaakt bij de start van de verwerking van gegevens;
- Wordt vermeld op de website van BPF Waterbouw;
- Wordt op verzoek van betrokkenen toegezonden.

#### 3.2 *Rechten van betrokkenen*

De betrokkenen van wie wij informatie verwerken, hebben in principe de volgende rechten:

- recht op informatie;
- recht van inzage;
- recht op rectificatie;
- recht op gegevenswissing en vergetelheid;
- recht van beperking van verwerking;
- recht op dataportabiliteit (recht om gegevens over te dragen);
- recht op bezwaar;
- recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming.

Aan de invulling van deze rechten werken wij mee zolang de gerechtvaardigde belangen van het fonds, de uitvoering van de pensioenregeling of de rechten van anderen daardoor niet in het geding komen.

BPF Waterbouw heeft op haar website het privacystatement gepubliceerd waarin o.a. de rechten van betrokkenen worden weergegeven en de wijze waarop deze kunnen worden geëffectueerd. Wanneer een betrokkene een verzoek indient, zullen wij binnen één maand na ontvangst een reactie geven. BPF Waterbouw heeft een intern proces ingericht voor de afhandeling van de rechten van betrokkenen.

#### 3.3 *Gegevensbeveiliging*

Het beveiligen van persoonsgegevens is verbonden met de informatiebeveiliging binnen BPF Waterbouw. Informatiebeveiliging richt zich niet alleen op persoonsgegevens, maar behelst de gehele informatievoorziening van BPF Waterbouw. De doelstelling van informatiebeveiliging is het waarborgen van de betrouwbaarheid van de informatievoorziening en het verbeteren van de continuïteit van bedrijfsprocessen. Dit bestaat uit:

- Beschikbaarheid: ervoor zorgen dat informatie(systemen) zoals vereist en wanneer nodig voor de doelstellingen van BPF Waterbouw beschikbaar zijn;
- Integriteit: het beschermen van informatie(systemen) tegen niet geautoriseerde en/of (on)opzettelijke wijzigingen die de juistheid, volledigheid en inhoudelijke betrouwbaarheid van informatie in gevaar kunnen brengen;
- Vertrouwelijkheid: het beschermen van informatie tegen toegang door onbevoegden en niet geautoriseerde openbaarmaking.

Om dit te bewerkstelligen, heeft BPF Waterbouw een risico gebaseerde aanpak op informatiebeveiliging. Met behulp van een risico-inventarisatie hebben we de informatiebeveiligingsrisico's in kaart gebracht en beoordeeld. Op basis daarvan hebben we een aantal beheersmaatregelen vastgesteld. Dit zijn zowel technische als organisatorische maatregelen. Ook het informatiebewustzijn van medewerkers speelt hierin een rol. Het bovenstaande is vastgelegd in het informatiebeveiligingsbeleid en het uitgewerkt in het informatiebeveiligingsplan.

### *3.4 Privacybewustzijn medewerkers*

Beleid en technische en organisatorische maatregelen zijn niet voldoende om privacy risico's uit te sluiten. Het is minimaal even belangrijk om voortdurend aandacht te besteden aan privacybewustzijn bij medewerkers.

Daarom worden medewerkers op verschillende momenten en in verschillende vormen in aanraking gebracht met en wordt bij hen aandacht gevraagd voor privacy en security. Dit bestaat onder andere uit:

- Privacy en security gedragsregels;
- Presentaties;
- Best practices en voorbeelden;
- Discussie over risico's en hoe daarmee om te gaan.

### *3.5 Verwerkingsregister*

BPF Waterbouw houdt een register van verwerkingsactiviteiten bij voor alle verwerkingen van persoonsgegevens. Het verwerkingsregister bevat de volgende onderdelen:

- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers (waaronder verwerkers) aan wie de gegevens worden verstrekt;
- De (beoogde) bewaartermijnen;
- Een beschrijving op hoofdlijnen van hoe de gegevens beveiligd zijn.



### 3.6 Privacy by Design

Bij het ontwikkelen van nieuwe diensten en technologieën past BPF Waterbouw Privacy by design toe. Dat houdt in dat we privacy vanaf het begin van het ontwerpproces meenemen door na te denken over de benodigde technische en organisatorische maatregelen en die in te bouwen in processen en systemen. Wij hanteren hierbij de zeven algemeen geldende uitgangspunten van Privacy by design.

---

#### Principes Privacy by design

- 1 **Voorkomen is beter dan genezen**  
Door het nemen van preventieve in plaats van reactieve maatregelen, blijven privacy risico's zo klein mogelijk. Met Privacy by design ben je privacy incidenten voor.
  - 2 **Privacy als default setting**  
Producten en diensten zijn standaard ingesteld om de hoogste mate van privacy te garanderen. Zo min mogelijk persoonlijke data wordt verwerkt. Dit wordt ook wel 'Privacy by default' genoemd.
  - 3 **Privacy geïntegreerd in het ontwerp**  
Privacy by design zorgt ervoor dat privacy een kerncomponent wordt van je producten of diensten. Tijdens de ontwikkeling wordt privacy een integraal onderdeel van het product of dienst, zonder afbreuk te doen aan de functionaliteit daarvan.
  - 4 **Niet afdingen op functionaliteit**  
Door privacy in de ontwikkelingsfase in te bouwen in de systemen hoeft er geen afweging gemaakt te worden tussen privacy en andere functionaliteiten.
  - 5 **Beveiliging voor gehele levenscyclus**  
Gedurende de gehele levenscyclus van persoonsgegevens, van verzamelen tot vernietigen, wordt er rekening gehouden met privacy.
  - 6 **Zichtbaarheid en transparantie**  
Privacy by design staat voor openheid en transparantie over het verwerkingsproces van persoonsgegevens. Dit creëert vertrouwen bij alle betrokken partijen en zorgt tevens voor accountability.
  - 7 **Respect voor privacy van betrokkene**  
Wellicht het belangrijkste aspect van privacy by design is dat de gebruiker of klant centraal staat. De belangen van de betrokkenen staan altijd op de eerste plek door het aanbieden van sterke standaard instellingen, transparantie, duidelijke communicatie en gebruiksvriendelijke mogelijkheden.
- Ann Cavoukian, 1990**
- 

Voorbeelden van toepassingen van Privacy by design die BPF Waterbouw uitvoert zijn het anonimiseren, het pseudonimiseren, het aggregeren van gegevens en dataminimalisatie.

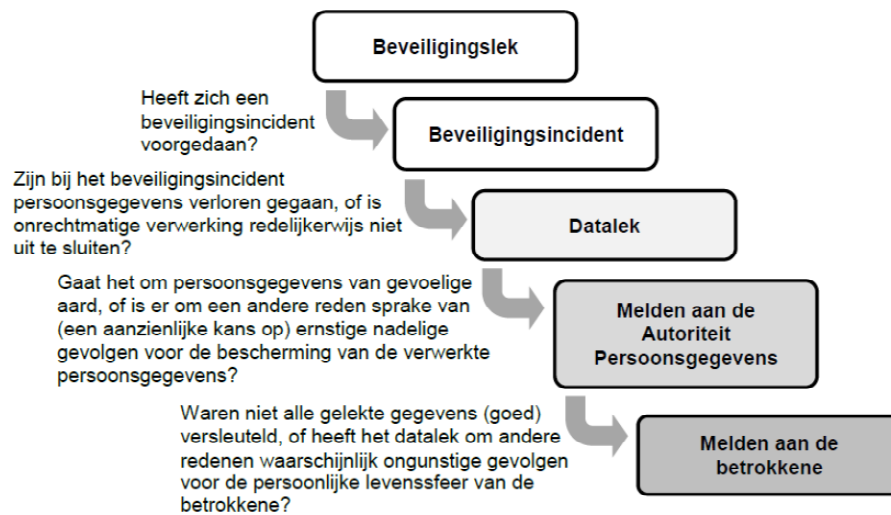
### 3.7 Meldplicht datalekken

BPF Waterbouw heeft een meldpunt voor datalekken, waar medewerkers datalekken kunnen melden. Medewerkers zijn verplicht om een (vermoedelijk) datalek en andere privacy incidenten direct te melden bij de Privacy Officer.

Voorbeelden van datalekken zijn:

- Een kwijtgeraakte onversleutelde USB-stick met persoonsgegevens;
- Uitgeprinte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen;
- Inbraak in een computer met persoonsgegevens;
- Naar onbevoegden sturen van een overzicht met persoonsgegevens.

Hierbij hanteren we volgende afwegingen:



bron: Autoriteit Persoonsgegevens

BPF Waterbouw houdt een register bij van de (potentiele) datalekken waar we mee te maken hebben. We melden een datalek binnen 72 uur aan de Autoriteit Persoonsgegevens en indien nodig, melden wij ook aan de betrokkene.

### 3.8 Data Protection Impact Assessment (DPIA)

BPF Waterbouw voert bij risicovolle gegevensverwerkingen een data protection impact assessment (DPIA) uit.

Er is sprake van een risicovolle verwerking als:

- Er systematisch en uitvoerig persoonlijke aspecten worden geëvalueerd (zoals bij profiling). Dit is bij BPF Waterbouw **niet** van toepassing;
- Er op grote schaal bijzondere persoonsgegevens worden verwerkt. Dit is bij BPF Waterbouw niet van toepassing omdat bijzondere persoonsgegevens (arbeidsongeschiktheid) slechts op **beperkte** schaal worden verwerkt;
- Er op grote schaal en systematisch mensen worden gevolgd in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht). Dit is bij BPF Waterbouw **niet** van toepassing.

Een mogelijke DPIA bevat:

- Een systematische beschrijving van de gegevensverwerking;
- Een beschrijving van de doeleinden en als dat van toepassing is, ook van onze gerechtvaardigde belangen;
- Een beoordeling van de noodzaak en proportionaliteit, gerelateerd aan de doeleinden. Is het verwerken van persoonsgegevens op deze wijze noodzakelijk om het doel te bereiken? Is de inbreuk op de privacy van betrokkenen niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacyrisico's voor de betrokkenen;
- De beoogde maatregelen om de risico's aan te pakken en aan te tonen dat we aan de AVG voldoen.

De proceseigenaar is verantwoordelijk om de DPIA uit te laten voeren. Deze wordt geadviseerd door de Privacy Officer.

De resultaten van de DPIA worden besproken met de directie en worden voorzien van een advies van de Privacy Officer.

### 3.9 Verwerkersovereenkomst

In de verwerkersovereenkomsten die we afsluiten, staan de volgende onderwerpen vastgelegd:

- Algemene beschrijving van het onderwerp, de duur, de aard en het doel van de verwerking. Het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en plichten van de verwerkingsverantwoordelijke;
- De verwerking vindt in beginsel uitsluitend plaats op basis van de schriftelijke instructie van de verantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken;
- Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht.
- De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen;
- De verwerker schakelt geen subverwerkers in zonder voorafgaande schriftelijke toestemming van de verantwoordelijke. De verwerker legt aan een subverwerker dezelfde verplichtingen op als de verwerker richting de verantwoordelijke heeft. Dit wordt vastgelegd in een subverwerkersovereenkomst;
- De verwerker helpt de verantwoordelijke om te voldoen aan zijn plichten, zoals wanneer betrokkenen hun privacyrechten uitoefenen (o.a. het recht op inzage, correctie, vergetelheid en dataportabiliteit) en bij het melden van datalekken;
- Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens;
- De verwerker werkt mee aan audits van de verantwoordelijke of van een derde partij.

## 4. Governance

Om een succesvol privacybeleid te realiseren, is het van belang dat er duidelijkheid bestaat over wie waarvoor verantwoordelijk is. Dit hoofdstuk heeft betrekking op de privacy governance van BPF Waterbouw en geeft de relevante privacy rollen en verantwoordelijkheden weer.

### 4.1 Algemene uitgangspunten

- Het bestuur is eindverantwoordelijk voor alle gegevensverwerkingen bij BPF Waterbouw. De verantwoordelijken worden in de lijn belegd. Iedere medewerker heeft, overeenkomstig zijn rol, een eigen verantwoordelijkheid;
- Privacy is een lijnverantwoordelijkheid. Dit betekent dat leidinggevendenden de primaire verantwoordelijkheid dragen voor een zorgvuldige verwerking van persoonsgegevens op hun afdeling/eenheid. Dit bevat ook de keuze voor de maatregelen en de uitvoering en handhaving ervan;
- Privacy is ieders verantwoordelijkheid. Van medewerkers wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens.

### 4.2 Rollen en verantwoordelijkheden

Onderstaande RACI-tabel bevat de relevante rollen en verantwoordelijkheden in het kader van het ontwikkelen, monitoren en uitvoeren van het privacybeleid.

Taken		Bestuur	Directie	IT	PO
<b>Plan</b>	Opstellen privacybeleid	A	R	C	C
	Privacy statement	A	R	C	C
<b>Do</b>	Verwerkingsregister	A	C	C	R
	DPIA	A	C	C	R
	Rechten van betrokkenen	A	R	C	C
	Gegevensbeveiliging	A	R	C	C
	Training privacybewustzijn	A	R	I	C
	Meldplicht datalekken	A	C	C	R
	Privacy by Design	A	R	C	C
	Verwerkers-overeenkomsten	A	R	C	C
<b>Check</b>	Monitoren en toetsen naleving privacybeleid	A	R	R	R
	Onderhouden en bijstellen privacybeleid	A	R	C	C

<b>R</b>	<b>Responsible.</b> Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.
<b>A</b>	<b>Accountable.</b> Eindverantwoordelijke. Degene aan wie verantwoording wordt afgelegd, die bevoegd is en goedkeuring geeft, die het eindoordeel velt en eventueel vetorecht heeft.
<b>C</b>	<b>Consulted.</b> Wordt voorafgaand aan de besluitvorming geraadpleegd.
<b>I</b>	<b>Informed.</b> Wordt achteraf geïnformeerd. Eénrichtingsverkeer.

### 4.3 Privacy Officer

Strikt juridisch gezien is er geen eenduidige uitspraak mogelijk of pensioenfondsen (en / of hun pensioenuitvoerder) een Functionaris Gegevensbescherming moeten aanstellen. Of deze verplichting geldt moet worden getoetst aan een aantal criteria. Bepalend is of “de verantwoordelijke of de verwerker hoofdzakelijk grootschalige verwerkingen uitvoert van bijzondere categorieën van gegevens of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten. Naar de letter genomen lijkt hiervan geen sprake bij BPF Waterbouw. Om die reden heft BPF Waterbouw besloten om geen Functionaris Gegevensbescherming aan te stellen maar te kiezen voor een Privacy Officer. De Privacy Officer heeft de volgende taken:

- Toezien op de naleving van het privacy beleid en de privacy maatregelen;
- Informeren en adviseren over privacywet en -regelgeving;
- Coördinatie van de afhandeling van eventuele datalekken volgens de geldende procedure;
- Het (laten) uitvoeren van audits om de werking van de privacy maatregelen te controleren;
- Als aanspreekpunt optreden voor en samenwerken met de AP.
- Inventariseren gegevensverwerkingen;
- Bijhouden van een openbaar register van (niet van melding vrijgestelde) gegevensverwerkingen;
- Afhandelen klachten over het gebruik van persoonsgegevens;
- Fungeren als deskundig aanspreekpunt voor betrokkenen mbt verwerking van persoonsgegevens;

De Privacy Officer legt rechtstreeks verantwoording af aan het bestuur.

## 5. Kwaliteitsbewaking

Dit hoofdstuk beschrijft de activiteiten die BPF Waterbouw onderneemt om het privacybeleid duurzaam te verankeren in de organisatie.

### *5.1 Communicatie*

Dit privacybeleid wordt naar alle medewerkers gestuurd en naar ingehuurde derden.

Verder wordt er uitvoerig met en naar medewerkers gecommuniceerd over privacy bij BPF Waterbouw.

### *5.2 Borging*

Privacy is geïntegreerd in de totale bedrijfsvoering van BPF Waterbouw.

- Vast onderwerp in werkoverleggen;
- In portefeuille van directie en bestuur;
- Opgenomen in procesbeschrijvingen, richtlijnen, een gedragscode, werkinstructies;
- Onderdeel van functiebeschrijvingen.

### *5.3 Controle en naleving*

De Privacy Officer houdt toezicht op de naleving van het privacybeleid. Indien een medewerker van BPF Waterbouw bewust in strijd handelt met dit beleid, dan kan dat leiden tot sancties, binnen de kaders van de wettelijke mogelijkheden.