STICHTING PENSIOENFONDS VAN DE GROLSCHE BIERBROUWERIJ

Stichting Pensioenfonds van de Grolsche Bierbrouwerij
www.grolschpensioenfonds.nl

AZL N.V. verzorgt de administratie:
Postbus 4471, 6401 CZ Heerlen
T 088 - 116 2000
E pf-grolsch@azl.eu

Privacybeleid

Stichting Pensioenfonds van de Grolsche Bierbrouwerij

Versie 29 maart 2023

Privacybeleid Pensioenfonds

Inhoud

Inleiding

Persoonsgegevens worden verzameld met als doel het goed uitvoeren en administreren van de pensioenadministratie. Dit privacybeleid vormt het vertrekpunt voor Privacy Management binnen het pensioenfonds. Stichting Pensioenfonds van de Grolsche Bierbrouwerij (hierna: het pensioenfonds) voert een beleid dat gericht is op behoorlijke en zorgvuldige gegevensverwerking in overeenstemming met de wet. Het pensioenfonds mag niet meer gegevens verwerken dan noodzakelijk is voor het doel. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale gegevensuitwisseling vergen aanpassing van de bescherming van gegevens en de waarborging van privacy. Het pensioenfonds is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft.

1. Algemeen

1.1 Definities

De volgende begrippen worden gebruikt vanuit de AVG-wetgeving:

Een persoonsgegeven:	Alle gegevens die gaan over natuurlijke personen en waaraan je een natuurlijk persoon als individu kunt herkennen. Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere categorieën van persoonsgegevens. Het gaat specifiek om: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
Verwerken van Persoonsgegevens:	Elke bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via automatische procedé, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere wijze van ter beschikking stellen, aligneren of combineren wissen of vernietigen van gegevens;
Verwerkings-verantwoordelijke:	Een persoon of organisatie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Het pensioenfonds is gewoonlijk de verwerkingsverantwoordelijke en bepaalt in ieder geval het doel van de verwerking en heeft ook de zeggenschap over de wijze van verwerken. In dit beleid wordt voortaan de term verantwoordelijke gebruikt;
Verwerker:	De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie. De belangrijkste verwerker voor het pensioenfonds is de pensioenuitvoeringsorganisatie.
Betrokkene:	De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Voor het pensioenfonds zijn de belangrijkste betrokkenen de aanspraak- en pensioengerechtigden, (ex)-leden van fondsgremia, natuurlijke personen.
Toezichthouder(s):	het pensioenfonds staat onder toezicht van verschillende toezichthouders zoals de Autoriteit Persoonsgegevens (AP), de Autoriteit Financiële Markten (AFM), en De Nederlandsche Bank (DNB).
Gegevensbeschermings-effectbeoordeling:	Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment.

1.2 Visie, scope en doel

Visie
Het pensioenfonds beschouwt privacy als een duurzaamheidsthema, gekoppeld aan thema's zoals governance, integriteit, kwaliteit en klantgerichtheid. De ambitie is het bereiken van een cultuur waarbinnen naleving van privacywetgeving vanzelfsprekend is.

Scope
De primaire doelgroep van dit beleid zijn alle functionarissen van het pensioenfonds. Van hen wordt verwacht dat zij bewust omgaan met privacy en zich intensief inspannen voor het voorkomen van privacy incidenten. Bij het ontwikkelen van informatiesystemen en diensten wordt het privacy-element vanaf het ontwerp als voorwaarde meegenomen (Privacy by Design). Het pensioenfonds zorgt ervoor dat passende privacy verhogende technologieën kunnen worden ingezet. Daarnaast zal maximale transparantie worden nagestreefd ten aanzien van het gebruik van persoonsgegevens en zullen klantvriendelijke privacy instellingen zoveel mogelijk worden ingezet (Privacy by Default).

Doel
Het privacybeleid heeft tot doel:

a. uniforme en specifieke gedragslijnen te geven voor het pensioenfonds voor het verwerken van persoonsgegevens;
b. inzicht geven aan personen van wie persoonsgegevens door het pensioenfonds verwerkt (zullen) worden;

Het doel van het privacybeleid van het pensioenfonds komt tot uiting door:
- rechtmatige, behoorlijk en transparant verwerking;
- verwerking voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
- toereikende, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;
- juiste en zo nodig geactualiseerde verwerking;
- een redelijke bewaartermijn die gekoppeld is aan het doel van de verwerking;
- dusdanige technische of organisatorische maatregelen waardoor een passende beveiliging is gewaarborgd

Het privacybeleid is van toepassing op de (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens door het pensioenfonds in het kader van de pensioenuitvoering, alsook op de handmatige verwerking van persoonsgegevens door het pensioenfonds in het kader van de pensioenuitvoering, op voorwaarde dat de persoonsgegevens zijn opgenomen in een bestand of bestemd zijn om daarin te worden opgenomen.
Het pensioenfonds legt het doel en de wijze van de verwerking van persoonsgegevens vast.

1.3 Raakvlakken met andere beleidsstukken

Het privacybeleid heeft raakvlakken met het IT-beleid, het beleid omtrent het bewaren van gegevens, riskmanagement en uitbesteding.

1.4 Herkomst en categorieën persoonsgegevens

De persoonsgegevens van de volgende betrokkenen	**verkrijgt het pensioenfonds van**
(gewezen) deelnemers	• de werkgever • de Basisregistratie Persoonsgegevens • het Uitvoeringsinstituut Werknemersverzekeringen • de betrokkene
partners en kinderen van (gewezen) deelnemers	• de werkgever • de (gewezen) deelnemer • de betrokkene • de Basisregistratie Persoonsgegevens
ex-partners en nabestaanden van (gewezen) deelnemers	• betrokkene • de Basisregistratie Persoonsgegevens
functionarissen van het pensioenfonds (zoals leden van het bestuur, verantwoordingsorgaan)	de betrokkene
dienstverleners (zoals actuaris)	de betrokkene.

Het pensioenfonds verwerkt persoonsgegevens uit de volgende categorieën.

Categorie	**Voorbeelden**
Personalia	Naam, adres geboortedatum, leeftijd, geslacht, burgerlijke staat, kinderen, telefoon, salaris en e-mail
Identificatiegegevens	identiteitskaartnummer, paspoort, rijbewijsnummer en/of pensioennummer
Financiële gegevens	bankrekeningnummer, salarisgegevens, dienstverbanden en alle andere pensioengevende componenten
Pensioengegevens	hoogte pensioenaanspraken of pensioenrechten
Registratie op portal en website	Digitale pot en interactiegegevens

In principe verwerkt het pensioenfonds geen bijzondere categorieën van persoonsgegevens, behalve informatie over iemands gezondheid (een arbeidsongeschiktheidspercentage in geval van premievrijstelling), waarvoor een grondslag zoals vermeld in de AVG en/of Uitvoeringswet Algemene Verordening gegevensbescherming is benodigd om deze gegevens te mogen verwerken. Denk bijvoorbeeld aan uitdrukkelijke toestemming van betrokkene of een wettelijke regeling die dat mogelijk maakt. Hetgeen ook geldt voor strafrechtelijke gegevens en het Burgerservicenummer (BSN), waarvan de verwerking alleen geschiedt voor zover dat is toegestaan op basis van een specifiek wettelijke grondslag. Daarnaast kennen we nog een categorie gevoelige gegevens, zoals bijvoorbeeld financiële of locatiegegevens. Indien er bijvoorbeeld een datalek plaatsvindt, waarbij gevoelige gegevens zijn gelekt, dan dient er in ieder geval melding bij de Autoriteit Persoonsgegevens plaats te vinden en mogelijk ook aan betrokkenen.

2. Wettelijk kader

2.1 Achtergrond van het beleid

In dit privacybeleid wordt beschreven hoe concreet uitvoering wordt gegeven aan de op het pensioenfonds van toepassing zijnde privacyvoorschriften van de Algemene Verordening Gegevensbescherming (AVG) ofwel General Data Protection Regulation (GDPR) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).
Door dit privacybeleid geeft het bestuur van het pensioenfonds invulling aan haar wettelijke verantwoordelijkheid om te voorzien in privacybeleid volgens artikel 24 lid 2 van de AVG. Daarbij heeft het bestuur zich mede gebaseerd op de “Guidance verwerking persoonsgegevens pensioenfondsen” van de Pensioenfederatie.

2.2 Principes voor de verwerking van persoonsgegevens

Elke verwerking door het pensioenfonds moet rechtmatig zijn. Om rechtmatig te zijn moet de verwerking te baseren zijn op tenminste één van de onderstaande grondslagen.

<u>Rechtmatigheid en transparantie</u>
Het pensioenfonds verkrijgt de persoonsgegevens onder andere op grond van
1. de pensioenovereenkomst tussen de werkgever en de betrokkene;
2. de uitvoeringsovereenkomst die de werkgever met het pensioenfonds heeft gesloten;
3. het pensioenreglement;
4. verzoek tot waardeoverdracht;
5. het bekleden van een functie voor het pensioenfonds;
6. overeenkomst van opdracht of dienstverlening of toestemming;
7. wet- en regelgeving.

Het pensioenfonds verzamelt en verwerkt slechts de persoonsgegevens die nodig zijn voor de volgende doeleinden:
1. De uitvoering van de pensioenovereenkomst tussen de betrokkene en de werkgever;
2. Het uitvoeren van het pensioenreglement;
3. Het uitvoeren van de uitvoeringsovereenkomst;
4. Het functioneren als pensioenfonds;
5. Het gerechtvaardigd belang van de betrokkene of de aangesloten werkgever, met name als het gaat om gegevens die van belang zijn voor de uitvoering van regelingen;
6. De wettelijke verplichting die op het pensioenfonds rust.

Het pensioenfonds verzamelt en verwerkt persoonsgegevens niet voor andere doeleinden, zoals marketing en profilering.

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Voor betrokkenen moet inzichtelijk zijn waarom en op welke manier persoonsgegevens worden verwerkt. Het pensioenfonds moet hier helder en toegankelijk over communiceren in een zogenoemd privacy statement en in de eerste communicatie met betrokkenen, zoals bij het verzenden van de Pensioen 1-2-3.

<u>Behoorlijkheid</u>
De verwerking wordt beperkt tot wat noodzakelijk is om de doeleinden te bereiken. Persoonsgegevens worden indien mogelijk geaggregeerd, geanonimiseerd en gewist. De opslagperiode van de persoonsgegevens is beperkt en worden termijnen gehanteerd voor het wissen of periodiek toetsen van de persoonsgegevens.

De verwerking van persoonsgegevens zal relevant zijn voor de doeleinden waarvoor ze worden gebruikt en, voor zover nodig, voor deze doeleinden, juist, volledig en up-to-date zijn.

2.3 Doorgifte van persoonsgegevens aan derden

De pensioenuitvoerder zal de beschikbaar gestelde persoonsgegevens en/of andere informatie uitsluitend in de hiervoor genoemde doeleinden gebruiken. Deze persoonsgegevens en/of andere informatie wordt niet aan derden verstrekt, tenzij de verstrekking noodzakelijk is om de overeengekomen gekomen opdracht met het fonds te verrichten of als de pensioenuitvoerder/het fonds daartoe verplicht is op grond van de wet en/of dit noodzakelijk is in het kader van een gerechtelijke procedure. Enkel de medewerkers van de pensioenuitvoerder die daartoe geautoriseerd zijn hebben toegang tot de persoonsgegevens van het fonds.

2.4 Doorgifte van persoonsgegevens naar andere landen

Het pensioenfonds kan persoonsgegevens doorgeven (bijvoorbeeld in het kader van de opslag van) naar landen binnen de Europese Economische Ruimte (EER) of buiten de EER, indien:

1) de Europese Commissie heeft besloten dat een betreffend land passende waarborgen biedt ter bescherming van de persoonsgegevens, of;
2) op grond van een modelovereenkomst die de Europese Unie heeft goedgekeurd die is afgesloten met een partij in een land buiten de EER.

Het pensioenfonds zal geen persoonsgegevens overbrengen naar of toegankelijk maken vanuit een land buiten de EER, behoudens uitdrukkelijke schriftelijke toestemming van de betrokkene.

3. Governance

3.1 Structuur

Het pensioenfonds is verantwoordelijk voor de persoonsgegevens.
Het pensioenfonds verwerkt persoonsgegevens of laat deze door een verwerker verwerken in overeenstemming met de AVG.

Om tot een adequate afdekking van de geïdentificeerde risico's te komen heeft het pensioenfonds de volgende taken en verantwoordelijkheden belegd bij de onderstaande functies:

Functie	Verantwoordelijkheid
Bestuur	• Het bestuur van het pensioenfonds is eindverantwoordelijk voor het (laten) naleven van wetgeving en realiseert door goedkeuring van dit privacybeleid en de nadere uitwerking hiervan via procesbeschrijvingen het wettelijk vereiste niveau van bescherming van persoonsgegevens. • Rekenschap (laten) afleggen over privacybeleidsvoering via het jaarverslag.
Taken van de betreffende bestuurders met het aandachtsgebied privacy	• Hebben de 'lead' in interpretatie van privacywetgeving voor het pensioenfonds. • Adviseren het bestuur van het pensioenfonds en proceseigenaren op het gebied van privacy-compliance. • Monitoren de opvolging en eventuele wijzigingen van wet- en regelgeving. • Begeleiden het proces rondom privacyklachten om deze tot een goed einde te brengen (ombudsmanfunctie). • Adviseren de uitvoeringsorganisatieorganisatie bij privacy-incidenten. • Beoordelen of een nieuwe partij/uitbesteding voldoet aan de vereisten op het gebied van privacywetgeving en het privacybeleid van het fonds.
Visitatiecommissie	• Toetst het goed en betrouwbaar functioneren van de interne organisatie van het pensioenfonds. Het risico van privacy incidenten dient, zeker daar waar het gaat om voor privacy gevoelige processen, standaard te worden meegenomen in alle audits van systemen, processen en procedures.

3.2 Functionaris Gegevensbescherming (FG)/ Privacy Officer (PO), bestuur

Het pensioenfonds heeft geen Functionaris gegevensbescherming aangesteld en is hiertoe wettelijk niet verplicht. Het pensioenfonds borgt op andere manieren dat de verwerking van persoonsgegevens geschiedt volgens dit privacybeleid.

Toelichting
Een FG is verplicht gesteld in het geval:
a) van een overheidsinstantie of overheidsorgaan;
b) regelmatige en stelselmatige en grootschalige observatie onderdeel is van de kernactiviteiten; of
c) grootschalige verwerking van bijzondere categorieën van persoonsgegevens (zoals gegevens betreffende gezondheid) en van strafrechtelijke persoonsgegevens onderdeel is van de kernactiviteiten.

De hiervoor genoemde punten a, b en c zijn niet aan de orde is. Het pensioenfonds verwerkt wel op grootschalige wijze persoonsgegevens, maar de grootschaligheid heeft geen betrekking op bijzondere persoonsgegevens. Voor de uitvoering van het arbeidsongeschiktheidspensioen en de vrijstelling van premiebetaling bij arbeidsongeschiktheid wordt het arbeidsongeschiktheidspercentage verwerkt.

Binnen het bestuur van het pensioenfonds ten minste twee bestuurders privacy als specifiek aandachtsgebied.

3.3 Inschakeling van verwerker

Het pensioenfonds heeft de administratie uitbesteed aan een verwerker: AZL N.V.
Het pensioenfonds vergewist zich ervan dat de verwerker persoonsgegevens verwerkt in overeenstemming met de wet en dat diens privacybeleid niet strijdig is met het privacybeleid van het pensioenfonds. Het pensioenfonds heeft hiertoe een verwerkersovereenkomst met de verwerker gesloten.

Indien gebruik wordt gemaakt van de diensten van een Verwerker zal met deze Verwerker een (verwerkers)overeenkomst worden gesloten, waarin schriftelijk of in een andere, gelijkwaardige vorm onder meer wordt vastgelegd dat passende technische en organisatorische maatregelen ter beveiliging van die persoonsgegevens moeten worden genomen. Het pensioenfonds zal bij (onder)uitbesteding van taken aan verwerkers in de pensioensector naleving van de Gedragslijn Verwerking persoonsgegevens Pensioenfondsen opleggen.

3.4 Accountant, actuaris

In verband met controles ten behoeve van de certificering en accountantsverklaring hebben de actuaris en accountant toegang tot de persoonsgegevens. De persoonsgegevens worden in beginsel geanonimiseerd. Zij waarborgen de geheimhouding door middel van de opdrachtbevestiging dan wel het contract.

3.5 Verzekeraar

Het pensioenfonds heeft de risico’s van overlijden verzekerd bij de verzekeraar en draagt in verband met die verzekering slechts de daarvoor benodigde persoonsgegevens over aan de verzekeraar. De persoonsgegevens worden geleverd op basis van de herverzekeringsovereenkomst en niet geleverd op basis van de uitvoeringsovereenkomst. Gelet hierop is geen verwerkingsovereenkomst nodig.

4. Risico's

Het bestuur is verantwoordelijk voor het beheersen van privacyrisico's en het voldoen aan het privacybeleid. In het uitbestedingsbeleid van het fonds is vastgelegd aan welke kwaliteitsvoorwaarden ene partij moet voldoen. Alvorens tot uitbesteding van werkzaamheden wordt overgegaan, voert het fonds een risicoanalyse uit waarbij ook de privacyrisico's zijn meegenomen indien het een verwerker betreft.

Om tot een solide en effectief privacybeleid te komen zijn de volgende privacy risico's geïdentificeerd:

- Het risico dat het pensioenfonds persoonsgegevens verzamelt zonder een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde;
- Het risico dat het pensioenfonds persoonsgegevens verwerkt zonder rechtmatige grondslag;
- Het risico dat gegevens worden verwerkt zonder toestemming van de betrokkene wanneer er een rechtmatige grondslag ontbreekt en/of dat het pensioenfonds (vertrouwelijke) persoonsgegevens verstrekt aan derden zonder voorafgaande toestemming van de betrokkene;
- Het risico dat het pensioenfonds de kwaliteit van de persoonsgegevens onvoldoende heeft gewaarborgd (actueel, juist en volledig).
- Het risico dat het pensioenfonds de rechten van betrokkene op de inzage, verbetering, aanvulling, verwijdering en/of afscherming van zijn/haar persoonsgegevens niet nakomt.
- Het risico dat door het pensioenfonds geen, onjuiste of onvolledige melding is gedaan bij de verantwoordelijke bestuurders en/of de Autoriteit Persoonsgegevens over het type gegevens, doel en de ontvangers/bewerkers waar de persoonsgegevens voor worden verwerkt.
- Het risico dat betrokkene niet geïnformeerd is dat zijn/haar persoonsgegevens door het pensioenfonds of een derde worden verwerkt.
- Het risico dat persoonsgegevens worden gedeeld met en/of ongeoorloofd worden verwerkt door een derde zonder dat er voldoende aanvullende afspraken zijn gemaakt over die verwerking (adequate verwerkingsovereenkomst)).
- Het risico dat het pensioenfonds persoonsgegevens na afloop van de bewaartermijn niet afdoende vernietigt of verwijdert.
- Het risico dat het pensioenfonds persoonsgegevens verliest.
- Het risico dat het pensioenfonds niet of niet tijdig de toezichthouder en betrokkenen op de hoogte stelt van een datalek.
- Het risico dat het pensioenfonds ongeoorloofde toegang verstrekt tot (bijzondere) persoonsgegevens door partijen of personen (intern/extern) die deze gegevens niet expliciet nodig en/of mogen hebben voor de uitoefening van hun taken.
- Het risico dat data van het pensioenfonds niet beschikbaar zijn.
- Het risico dat data van het pensioenfonds gemanipuleerd worden en niet meer integer zijn.
- Het risico dat de vertrouwelijkheid van data van het pensioenfonds wordt geschonden.

Bovenstaande risico's kunnen zich voordoen bij onvoldoende borging van het privacybeleid en kunnen gevolgen hebben voor de organisatie. Deze gevolgen kunnen worden opgesplitst in de volgende drie schadecategorieën.

Reputatieschade: Privacy risico's waardoor het imago van het pensioenfonds schade lijdt door het bekend worden van feiten of omstandigheden of door publieke beeldvorming, als gevolg waarvan het vertrouwen in de organisatie wordt geschaad.

Juridisch en regelgevingschade: Privacy risico's waardoor het pensioenfonds te maken krijgt met inspecties of juridische procedures, met als gevolg sancties of (andere) onvoorziene uitgaven. Dit kan aan de orde zijn als het vermoeden bestaat dat het beleid op het gebied van privacy van het pensioenfonds niet toereikend is.

Operationele schade: Privacy risico's waardoor het pensioenfonds tekort schiet op het vlak van privacy management. Ook kan administratieve overbelasting ontstaan, bij de werkgever, wanneer privacy problemen aanleiding geven tot misverstanden en daaraan gekoppelde gedragingen, individuele klachten, verzoeken of claims.

4.2 Privacy Impact Analyse (PIA)

Met een PIA (ook wel gegevensbeschermingseffectbeoordeling genoemd) worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Het pensioenfonds laat deze uitvoeren indien een gegevensverwerking een hoog privacyrisico oplevert voor betrokkenen. Volgens de AVG is hiervan sprake indien het pensioenfonds:

- systematisch en uitvoerig persoonlijke aspecten evalueert (gebaseerd op geautomatiseerde verwerking), waaronder profilering en waarop besluiten worden gebaseerd waaraan rechtsgevolgen voor betrokkenen zijn verbonden;
- op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Voorts heeft de Autoriteit Persoonsgegevens een lijst met soorten verwerkingen opgesteld waarvoor het uitvoeren van een PIA is verplicht vóórdat met het verwerken van persoonsgegevens wordt begonnen. Deze lijst is niet uitputtend en het pensioenfonds moet zelf beoordelen of de verwerking een hoog privacy risico oplevert voor betrokkenen.
Nu is de situatie dat het pensioenfonds nagenoeg alle processen waarbij persoonsgegevens worden verwerkt, heeft uitbesteed. De belangrijkste verwerker is AZL N.V. en deze pensioenuitvoerder voert standaard een PIA uit bij een gewijzigd of nieuw proces met een verwacht hoog risico voor de betrokkenen. Het pensioenfonds neemt, desgewenst, kennis van de ingevulde PIA's. Op deze wijze houdt het pensioenfonds zicht op processen met een hoog privacyrisico voor betrokkenen en krijgt het inzicht welke maatregelen er worden genomen om geconstateerde privacyrisico 's te mitigeren.

5. Privacy management

5.1 Beveiliging en geheimhouding

Het pensioenfonds zorgt er al bij het ontwerpen van producten en diensten voor dat persoonsgegevens goed worden beschermd (Privacy by design). De gegevens worden goed beveiligd. Dat kan bijvoorbeeld door het verlenen van autorisaties aan daartoe aangewezen personen en het pseudonimiseren (dan wel anonimiseren) van persoonsgegevens.
Privacy by default: de standaardinstellingen zijn zodanig dat de privacy zoveel mogelijk wordt gewaarborgd. Bij voorkeur geen opt-out regime, maar opt-in: alleen als een deelnemer zich ergens voor heeft aangemeld, ontvangt hij informatie.

Het pensioenfonds houdt de persoonsgegevens geheim voor onbevoegden en personen die niets met de verwerking van doen hebben.

Het pensioenfonds deelt uw persoonsgegevens met verschillende andere partijen als dit noodzakelijk is voor het uitvoeren van de pensioenovereenkomst en/of om te voldoen aan wettelijke verplichtingen. Met partijen die uw gegevens in onze opdracht verwerken sluiten wij een verwerkersovereenkomst. Op die manier zorgen wij voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Het pensioenfonds blijft verantwoordelijk voor deze verwerkingen en verwerkt uw gegevens niet buiten de EU.

De uitvoering van de pensioenadministratie is uitbesteed aan AZL N.V. (AZL). AZL beschikt daarom over uw Persoonsgegevens. Het pensioenfonds heeft afspraken gemaakt over de wijze waarop AZL met uw gegevens om gaat, met wie zij uw gegevens mogen delen en hoe uw gegevens beveiligd zijn. Om de pensioenadministratie van het pensioenfonds goed uit te kunnen voeren maakt AZL gebruik van verschillende partijen die afhankelijk van uw situatie uw persoonsgegevens ontvangen (subverwerkers). AZL zorgt bij deze subverwerkers voor minimaal hetzelfde beveiligingsniveau zoals afgesproken met pensioenfonds Grolsch.

De partijen waarmee uw persoonsgegevens gedeeld kunnen worden, zijn onder te verdelen in de volgende categorieën:

- Toezichthouders
- Overheidsinstanties
- Uitkeringsinstanties
- Incasso-/debiteurenpartijen
- Herverzekeraars
- (Voormalige) werkgever(s) en hun gemachtigden
- Mailingverwerkers/Drukkerijen
- Archiefopslagen
- Controlepartijen bijvoorbeeld voor het uitvoeren van looncontroles
- ICT database/website beheer- en onderhoudsbedrijven
- IT Securitybedrijven
- Onderzoekspartijen
- Accountants/actuariskantoren voor assurancedoeleinden
- Andere pensioenuitvoerders

5.2 Ketenverantwoordelijkheid

Het pensioenfonds vergewist zich ervan dat de door haar ingeschakelde verwerkers persoonsgegevens beschermt met passende organisatorische en/of technische beveiligingsmaatregelen die redelijke waarborgen bieden tegen risico's van verlies of

ongeautoriseerde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens.
Het pensioenfonds verlangt hiervoor van de verwerker een verwerkersovereenkomst en dat de verwerker met subverwerkers een verwerkersovereenkomst heeft gesloten.

5.3 Datalekken

Het pensioenfonds waarborgt dat bij het verwerken van (persoons)gegevens, in welke vorm dan ook, in ieder stadium van de verwerking passende technische en organisatorische maatregelen getroffen zijn volgens een op het risico afgestemd beveiligingsniveau, om te voorkomen dat datalekken zich voordoen.

Er is sprake van een datalek als:
- er inbreuk wordt gemaakt op de beveiliging, en
- daarbij persoonsgegevens verloren zijn gegaan, of als redelijkerwijs niet is uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt.

Het pensioenfonds registreert alle datalekken.

Het pensioenfonds meldt een datalek aan de Autoriteit Persoonsgegevens als
- het datalek persoonsgegevens van gevoelige aard betreft, zoals:
    - gegevens over de financiële of economische situatie: salaris en pensioengegevens;
    - gebruikersnamen en inlogcodegegevens die kunnen leiden tot persoonsfraude, zoals BSN, paspoort of identiteitskaart of rijbewijs.

of
- er een aanzienlijke kans is dat er ernstige nadelige gevolgen zijn voor de bescherming van persoonsgegevens.

Indien een datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van een betrokkene, zal het pensioenfonds ook de betrokkene van het datalek op de hoogte stellen.

Het pensioenfonds vergewist zich ervan dat een verwerker datalekken registreert en doorgeeft aan de Autoriteit Persoonsgegevens en de betrokkene.

5.4 Register van de verwerkingsactiviteiten

Het pensioenfonds houdt een register van de verwerkingsactiviteiten bij die onder zijn verantwoordelijkheid plaatsvinden.
Dat register bevat in ieder geval alle volgende gegevens:
a) de naam en de contactgegevens van het pensioenfonds;
b) de verwerkingsdoeleinden;
c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e) doorgiften van persoonsgegevens aan een derde land of een internationale organisatie,
f) de beoogde termijnen waarbinnen de verschillende categorieën van gegevens zullen worden gewist;
g) een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het register is in elektronische vorm opgesteld.
Desgevraagd stelt het pensioenfonds het register ter beschikking van de Autoriteit Persoonsgegevens.

5.5 Bewaartermijn persoonsgegevens

Het pensioenfonds bewaart persoonsgegevens van deelnemers en pensioengerechtigden in ieder geval tot 7 jaar na overlijden of pensioendatum (bij waardeoverdracht).
De reden hiervoor is dat een vordering van pensioen niet verjaart tijdens het leven van een pensioengerechtigde, waardoor de gegevens in ieder geval gedurende die periode nodig zijn, onder meer om een eventuele juistheid van een pensioen aan te tonen, of om te kunnen aantonen dat een claim onterecht is.

Het pensioenfonds bewaart persoonsgegevens van degenen met wie het pensioenfonds een arbeidsovereenkomst heeft of die voor het pensioenfonds werkzaam zijn of een functie bij het pensioenfonds bekleden tot vijf jaar na het einde van de arbeidsovereenkomst of de werkrelatie, of het beëindigen van het bekleden van de functie.

Na het verstrijken van de bewaartermijn zal het pensioenfonds de persoonsgegevens vernietigen, anonimiseren, pseudonimiseren of overbrengen naar een bestemming ten behoeve van archiefbeheer en ter waarborging van geschillenbeslechting.

5.6 Rechten van de betrokkene

De AVG geeft aan de betrokkene een aantal rechten.

<u>Algemeen</u>
Het pensioenfonds draagt er zorg voor dat betrokkene in beginsel kosteloos zijn rechten kan uitoefenen.

Het pensioenfonds stelt het doel van het verzoek en de identiteit van de betrokkene vast. Indien het onvoldoende duidelijk is dat de betrokkene het verzoek heeft gedaan, vraagt het pensioenfonds aanvullende informatie op om de identiteit van de betrokkene vast te stellen.
Het pensioenfonds reageert binnen een maand inhoudelijk op het door de betrokkene ingestelde verzoek. De termijn van een maand wordt opgeschort zolang de betrokkene niet heeft voldaan aan het verzoek tot aanvullende informatie.

Het pensioenfonds reageert binnen een termijn van maximaal 3 maanden te nemen indien er sprake is van:

- een complex verzoek; of
- een grote hoeveelheid verzoeken

Dit ter beoordeling van het pensioenfonds. Het pensioenfonds bericht de betrokkene over deze termijn binnen een maand en geeft daarbij een onderbouwing.

Indien het pensioenfonds naar eigen oordeel van mening is dat een verzoek van kennelijke ongegronde of buitensporige aard is, weigert het pensioenfonds het verzoek te behandelen of brengt, na afstemming met betrokkene, kosten in rekening. Het pensioenfonds zal betrokkene hierover schriftelijk informeren met toelichting op het besluit en de mogelijkheid voor betrokkene om een klacht bij de Autoriteit Persoonsgegevens in te dienen of beroep bij de rechter in te stellen.

Het pensioenfonds stelt partijen met wie de persoonsgegevens gedeeld zijn en die worden gerectificeerd, gewist of beperkt, op de hoogte van de wijzigingen binnen redelijke termijn. Dit informeren blijft achterwege wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

Informatie over Verwerking Persoonsgegevens
Het pensioenfonds informeert de betrokkene over de verwerking van persoonsgegevens op een transparante wijze en in begrijpelijke taal, zodat de betrokkene de verwerking kan beoordelen en zijn rechten afdoende kan uitoefenen. Dit is uiterlijk op het moment van eerste contact met betrokkene middels de pensioenuitingen conform Pensioen 1-2-3.

Indien de persoonsgegevens worden opgevraagd bij de betrokkene zelf wordt de betrokkene volledig en voorafgaand aan de opvraging hierover geïnformeerd.

Indien de persoonsgegevens worden verkregen van een derde dan informeert het pensioenfonds de betrokkene voorafgaand in de privacyverklaring op de website van het pensioenfonds.

De informatieplicht vervalt als de betrokkene reeds geïnformeerd is, het informeren in de praktijk onmogelijk is of onevenredige inspanningen vergt.

Recht van inzage
De betrokkene heeft het recht om van het pensioenfonds uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens. Het pensioenfonds verstrekt de betrokkene op diens verzoek een kopie van de persoonsgegevens die worden verwerkt.

Indien de betrokkene om bijkomende kopieën verzoekt, kan de het pensioenfonds op basis van de administratieve kosten een redelijke vergoeding aanrekenen.

Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

Recht op rectificatie
Als de persoonsgegevens niet juist zijn dan heeft de betrokkene het recht om deze onverwijld en uiterlijk binnen 1 maand te wijzigen. Indien de persoonsgegevens onvolledig zijn heeft de betrokkene het recht om deze aan te vullen.

Als de betrokkene terecht een beroep doet op dit recht dan stelt het pensioenfonds iedere ontvanger van de gegevens, zoals de belastingdienst, het UWV en subverwerkers, hiervan op de hoogte.

Het pensioenfonds stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Het pensioenfonds verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Recht op gegevenswissing (”recht op vergetelheid”)
Het pensioenfonds bewaart persoonsgegevens in ieder geval tot 7 jaar na overlijden of pensioendatum (bij waardeoverdracht). Het pensioenfonds wist in deze periode de persoonsgegevens niet.
De persoonsgegevens zijn in deze periode nodig voor het doeleinde waarvoor ze zijn verzameld of verwerkt. Bovendien heeft het pensioenfonds persoonsgegevens nodig om een eventuele juistheid van een pensioen aan te tonen, of om te kunnen aantonen dat een claim onterecht is.

Het pensioenfonds werkt daarom alleen mee aan het wissen van persoonsgegevens als een van de volgende gevallen van toepassing is:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld;
- de betrokkene trekt eventuele zijn toestemming in waarop de verwerking berust en het pensioenfonds geen andere rechtsgrond heeft;
- de betrokkene maakt bezwaar tegen de verwerking en er zijn geen (gerechtvaardigde) rechtsgronden voor de verwerking;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan het Unierecht of het Nederlands recht.

Wanneer het pensioenfonds de persoonsgegevens openbaar heeft gemaakt en verplicht is op verzoek de persoonsgegevens te wissen, neemt het pensioenfonds, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om iedere ontvanger aan wie persoonsgegevens zijn verstrekt, ervan op de hoogte te stellen dat de betrokkene het pensioenfonds heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Het pensioenfonds stelt de iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke wissing van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Het pensioenfonds verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

<u>Recht op beperking van de verwerking</u>
De betrokkene heeft het recht om het pensioenfonds te beperken in de verwerking van persoonsgegevens, indien:

a) de juistheid van de persoonsgegevens gemotiveerd wordt betwist door de betrokkene;
b) de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
c) het pensioenfonds de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
d) de betrokkene bezwaar heeft gemaakt tegen de verwerking op basis van gerechtvaardigd belang. De beperking geldt dan tot duidelijk is of de gronden van het pensioenfonds voor de verwerking zwaarder wegen dan die van de betrokkene tegen de verwerking.

Indien de verwerking is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat van de Europese Unie.

Het pensioenfonds stelt betrokkene die een beperking van de verwerking heeft verkregen, op de hoogte van de opheffing van de beperking van de verwerking, voordat de beperking wordt opgeheven.

Het pensioenfonds stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

Wanneer het pensioenfonds de persoonsgegevens aan een derde heeft verstrekt voor verwerking, stelt het pensioenfonds deze van het bovenstaande op de hoogte.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)
De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan het pensioenfonds heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder dat hij daarbij wordt gehinderd door het pensioenfonds, indien (i) de verwerking berust op toestemming, en (ii) de verwerking geschiedt via geautomatiseerde systemen.

Het pensioenfonds draagt er zorg voor dat, indien dit technisch mogelijk is, de gegevens rechtstreeks naar de andere verwerkingsverantwoordelijke worden doorgezonden.

Recht van bezwaar
De AVG geeft de betrokkene het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, als die verwerking plaatsvindt

- op basis van de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag of
- voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde,
- ingeval van profilering op basis van een van beide hiervoor genoemde gronden.

Gebruik van rechten
De betrokkene kan het verzoek om gebruik te maken van zijn recht schriftelijk of per email indienen bij het pensioenfonds door zijn verzoek te richten aan :
Stichting Pensioenfonds van de Grolsche Bierbrouwerij
Postadres: Postbus 4471, 6401 CZ Heerlen (AZL)
Helpdesk: 088 – 1163 005
Mail: pf-grolsch@azl.eu
Het pensioenfonds beoordeelt of het verzoek rechtmatig is en of het excessief is.

Uiterlijk binnen een maand na de ontvangst van het verzoek voldoet het pensioenfonds aan het verzoek of laat het pensioenfonds weten of het verzoek is afgewezen met de reden van de afwijzing.

5.7 Klachten

Betrokkene kan volgens de klachtenregeling een klacht indienen bij het pensioenfonds indien betrokkene een klacht heeft met betrekking tot de verwerking van zijn persoonsgegevens.
Contactgegevens:
Stichting Pensioenfonds van de Grolsche Bierbrouwerij
Postadres: Postbus 4471, 6401 CZ Heerlen (AZL)
Helpdesk: 088 – 1163 005
Mail: pf-grolsch@azl.eu

Komt de betrokkene er niet uit met het pensioenfonds, dan kan hij zijn klacht voorleggen aan de Autoriteit Persoonsgegevens.

6. Evaluatie en wijziging

6.1 Evaluatie

De procedures die zijn beschreven in deze privacyverklaring vormen het huidige beleid op het gebied van de bescherming van persoonsgegevens, per 29 maart 2023.

Het pensioenfonds evalueert en past dit beleid zo nodig aan, indien daarvoor aanleiding is op basis van andere gebruiken, wijzigende wet- en regelgeving en aanwijzing van de Autoriteit Persoonsgegevens.