



Privacybeleid

Stichting Pensioenfonds Flexsecurity

10 november 2023

Inhoudsopgave

1.	Inleiding	3
2.	Regelgeving en definities	4
3.	Risicomanagement ten aanzien van privacy	5
4.	Algemene uitgangspunten privacybeleid	8
5.	Rechtmatige verwerking	9
6.	Doeleinden van de verwerking	11
7.	Welke persoonsgegevens verwerken wij?	12
8.	Hoe verwerken wij uw persoonsgegevens?	13
9.	Verwerking van bijzondere persoonsgegevens	15
10.	Rechten van betrokkenen	16
11.	Overige onderwerpen	19
12.	Naleving en klachten	23
13.	Verantwoording, evaluatie en aanpassing	24
14.	Inwerkingtreding	25

1. Inleiding

Stichting Pensioenfonds Flexsecurity (hierna: Flexsecurity) heeft als statutaire doelstelling om te voorzien in de opbouw van pensioenen en het verzekeren van risico's ten behoeve van deelnemers in dienst van de werkgever en hun nagelaten betrekkingen. Voor het uitvoeren van die taken moeten we persoonsgegevens van onze deelnemers en andere betrokkenen verwerken. Deze mensen moeten erop kunnen vertrouwen dat Flexsecurity, binnen de kaders van de geldende wet- en regelgeving, op een veilige en zorgvuldige manier omgaat met de persoonsgegevens van zijn betrokkenen.

In de missie, visie en strategie van Flexsecurity wordt het innovatief gebruik van data als strategisch speerpunt benoemd. Ons streven is om de data die het pensioenfondsfonds beheert, zodanig in te zetten dat hiermee de dienstverlening aan deelnemers en werkgevers wordt verbeterd. Veel van deze data hebben betrekking op persoonsgegevens. Het is daarom van belang dat de bescherming van deze persoonsgegevens optimaal geregeld is en dat we aan alle wettelijke waarborgen op dat punt voldoen.

De Algemene verordening gegevensbescherming (AVG) biedt deze waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van persoonsgegevens. Daarmee vormt de AVG de basis voor de manier waarop wij omgaan met persoonsgegevens. In dit privacybeleid hebben we vastgelegd op welke wijze wij omgaan met uw persoonsgegevens en uw privacy.

2. Regelgeving en definities

In dit privacybeleid beschrijven wij hoe wij als pensioenfonds uitvoering geven aan de privacyvoorschriften van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Daarbij houden wij aan ons aan de uitwerking die de Pensioenfederatie heeft opgesteld in de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen. De Pensioenfederatie heeft deze Gedragslijn opgesteld om een passende en werkbare vertaling te geven van de regels van de AVG naar de praktijk van pensioenfondsen.

In de regelgeving en in ons privacybeleid worden een aantal begrippen gebruikt die van belang zijn bij de toepassing van de regels. We lichten hieronder de belangrijkste definities toe.

Betrokkene is de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene wiens persoonsgegevens worden verwerkt in opdracht van Flexsecurity.

Verwerker is de persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie, in dit geval Flexsecurity. Onze belangrijkste verwerker is pensioenuitvoeringsorganisatie AZL. Daarnaast worden ook andere partijen incidenteel als verwerker ingeschakeld, bijvoorbeeld voor het verzenden van mailings.

Persoonsgegevens zijn 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; de combinatie van naam, adres, geboortedatum).

Bijzondere persoonsgegevens zijn persoonsgegevens van gevoelige aard, zoals 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. Flexsecurity legt geen bijzondere persoonsgegevens vast, met uitzondering van gegevens over gezondheid die relevant zijn als een deelnemer arbeidsongeschikt is, aangezien dit de hoogte van de pensioenopbouw bepaalt.

Verwerking is alles wat met een persoonsgegeven gedaan wordt, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Verwerkingsverantwoordelijke is een persoon of organisatie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Flexsecurity is de verwerkingsverantwoordelijke en bepaalt het doel van de verwerking van persoonsgegevens. Ook heeft Flexsecurity zeggenschap over de manier waarop persoonsgegevens worden verwerkt.

3. Risicomanagement ten aanzien van privacy

Bij de bepaling en uitvoering van het beleid probeert Flexsecurity de mogelijke risico's die zich kunnen voordoen zo goed mogelijk te beheersen. Niet alle risico's zijn te vermijden en sommige risico's zoeken we juist bewust op. De kunst van risicomanagement is om de juiste balans te vinden en alert te blijven op risico's die zich mogelijk kunnen voordoen. Flexsecurity heeft een beleid voor integraal risicomanagement vastgesteld waarin risico's en beheersingsmaatregelen zijn vastgelegd. Op het gebied van bescherming van persoonsgegevens spelen een aantal risico's. In dit hoofdstuk wordt aangegeven wat onze risicobereidheid is, welke risico's aan de orde kunnen zijn en hoe wij deze risico's beheersen.

3.1 Risicobereidheid

De risico's ten aanzien van persoonsgegevens kunnen op meerdere plekken in ons risicomanagement voorkomen. In de indeling die wij hiervoor hanteren zal het hoofdzakelijk gaan om governance- en compliancerisico's en uitvoeringsrisico's. Op de eerste hoofdcategory is onze risicobereidheid laag, op de tweede category is de risicobereidheid gematigd. In het algemeen kan gesteld worden dat onze risicobereidheid ten aanzien van persoonsgegevens laag is. Met andere woorden: we zullen alles in het redelijke doen om risico's ten aanzien van persoonsgegevens te voorkomen. Bij het bepalen van de maatregelen die daarvoor nodig zijn, vormen de kosten een factor. Het volledig garanderen van een foutloze operatie is onmogelijk en het streven daarnaar zou onevenredig veel geld kosten. We accepteren daarom een minimaal risico ten aanzien van de bescherming van persoonsgegevens. Mocht uit incidenten, zoals bijvoorbeeld datalekken, blijken dat de realiteit niet in overeenstemming is met onze risicobereidheid, dan zullen we aanvullende maatregelen treffen.

3.2 Mogelijke risico's

Om de privacyrisico's effectief te kunnen beheersen is het noodzakelijk om de risico's te kennen die zich op het gebied van bescherming van persoonsgegevens kunnen voordoen. De volgende privacyrisico's zijn daarbij door ons geïdentificeerd:

- Het risico dat wij persoonsgegevens verzamelen zonder een duidelijk bepaald, omschreven en gerechtvaardigd doeleinde.
- Het risico dat wij persoonsgegevens verwerken zonder rechtmatige grondslag.
- Het risico dat wij meer gegevens verwerken dan strikt noodzakelijk (minimale gegevensverwerking).
- Het risico dat wij gegevens verwerken zonder toestemming van de betrokkene wanneer er een rechtmatige grondslag ontbreekt.
- Het risico dat wij (vertrouwelijke) persoonsgegevens verstrekken aan derden zonder voorafgaande toestemming van de betrokkene.
- Het risico dat wij de kwaliteit van de verwerkte persoonsgegevens onvoldoende waarborgen (actueel, juist en volledig).
- Het risico dat wij de rechten van betrokkene op de inzage, verbetering, aanvulling, verwijdering en/of afscherming van zijn/haar persoonsgegevens niet nakomen.

- Het risico dat wij een onjuiste of onvolledige melding doen bij de privacy officer over het type gegevens, het doel en de ontvangers/verwerkers waar de persoonsgegevens voor worden verwerkt.
- Het risico dat betrokkene door ons niet geïnformeerd is dat zijn/haar persoonsgegevens door ons 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 (verwerkingsovereenkomst met geheimhouding, beveiligingsniveau etc.).
- Het risico dat wij persoonsgegevens na afloop van de vastgestelde bewaartermijnen niet afdoende vernietigen of verwijderen.
- Het risico dat wij persoonsgegevens verliezen.
- Het risico dat wij niet of niet tijdig de toezichthouder en betrokkenen op de hoogte stellen van een datalek.
- Het risico dat wij ongeoorloofde toegang verstrekken tot (bijzondere) persoonsgegevens en/of vertrouwelijke bedrijfsgegevens 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 onze data, waaronder persoonsgegevens, niet beschikbaar zijn.
- Het risico dat onze data gemanipuleerd worden en niet meer integer zijn.
- Het risico dat de vertrouwelijkheid van onze data wordt geschonden.

3.3 Mogelijke schade

Bovengenoemde risico's kunnen zich voordoen bij onvoldoende borging van het privacybeleid en kunnen nadelige gevolgen hebben voor de betrokkenen zelf en voor Flexsecurity. De gevolgen voor de betrokkenen kunnen betrekking hebben op zaken als verlies van vertrouwelijkheid van gegevens, identiteitsfraude, financiële fraude en reputatierisico. De mogelijke gevolgen voor Flexsecurity kunnen worden opgesplitst in de volgende drie schadecategorieën.

Reputatieschade

Privacyrisico's waardoor het imago van Flexsecurity schade lijdt door het bekend worden van feiten of omstandigheden of door publieke beeldvorming, waardoor het vertrouwen in het pensioenfonds wordt geschaad.

Juridische schade

Privacyrisico's waardoor het pensioenfonds te maken krijgt met of juridische procedures of onderzoeken, 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 niet toereikend is.

Operationele schade

Privacyrisico's waardoor het pensioenfonds tekortschiet op het vlak van privacymanagement. Ook kan administratieve overbelasting ontstaan wanneer privacyproblemen aanleiding geven tot misstanden en daaraan gekoppelde gedragingen, individuele klachten, verzoeken of claims. Het onvoldoende borgen van het privacybeleid kan tevens de kans op cybercriminaliteit doen toenemen waardoor incidenten zoals bijvoorbeeld datalekken kunnen ontstaan.

3.4 Risicobeheersing

Het privacybeleid van Flexsecurity is erop gericht om de genoemde risico's te elimineren dan wel te beheersen en de genoemde schade zoveel als mogelijk te voorkomen. Verder worden in het privacybeleid maatregelen genoemd die wij kunnen/zullen nemen als de risico's zich desondanks voordoen.

4. Algemene uitgangspunten

Flexsecurity verwerkt uw persoonsgegevens in overeenstemming met de geldende wet- en regelgeving. Wij respecteren de beginselen die in de wetgeving zijn vastgelegd op het gebied van proportionaliteit, subsidiariteit en vertrouwelijkheid. Wij verwerken uw persoonsgegevens op een transparante, behoorlijke en zorgvuldige wijze. Wij baseren iedere verwerking van persoonsgegevens op een in geldende wet- en regelgeving opgenomen grondslag.

Verwerking van persoonsgegevens door Flexsecurity moet voldoen aan de volgende negen beginselen. Persoonsgegevens moeten altijd:

1. Rechtmatig worden verwerkt;
2. Beperkt tot het doel waarvoor zij zijn verkregen, op behoorlijke wijze worden verwerkt met als uitgangspunt minimale gegevensverwerking;
3. Ten aanzien van de betrokkene op transparante wijze worden verwerkt;
4. Toereikend en relevant zijn en beperkt tot het noodzakelijke in verband met de doelen waarvoor zij worden verwerkt;
5. Correct en up-to-date zijn (waar nodig bijgehouden worden);
6. Niet langer worden bewaard dan noodzakelijk in verband met de doelen waarvoor zij worden verwerkt en vervolgens worden vernietigd of geanonimiseerd;
7. Verwerkt worden met inachtneming van de rechten van de betrokkenen;
8. Passend beveiligd en vertrouwelijk behandeld worden;
9. Alleen worden verstrekt aan andere derden indien wettelijk toegestaan of vereist en op grond van een verwerkersovereenkomst en eventuele aanvullende vereiste bepalingen.

Wij verzamelen en verwerken uw persoonsgegevens voor welbepaalde en uitdrukkelijk omschreven doeleinden. Daarnaast mogen wij, in overeenstemming met geldende wet- en regelgeving, persoonsgegevens verder verwerken als dit verenigbaar is met het oorspronkelijke doel waarvoor de persoonsgegevens zijn verzameld. Dat betekent dat wij uw persoonsgegevens kunnen verwerken als dat plaatsvindt in het kader van de opbouw en uitkering van uw pensioen.

Wij doen uitsluitend verwerkingen van persoonsgegevens die toereikend zijn, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking"). We beperken ons dus tot de gegevens die wij redelijkerwijs nodig hebben voor de uitvoering van onze pensioenregelingen. Als blijkt dat de persoonsgegevens niet juist zijn, worden ze geactualiseerd of gewist. Wij hebben beleid bepaald ten aanzien van de kwaliteit en juistheid van persoonsgegevens, de bewaartermijnen die we hanteren en de verwijdering van persoonsgegevens. We leggen onze verwerkingen vast in een daartoe bestemd verwerkingsregister dat periodiek wordt geactualiseerd.

Wij geven invulling aan de rechten die de betrokkenen hebben ten aanzien van de verwerking van persoonsgegevens. Dit is uitgewerkt in hoofdstuk 8 van dit beleidsdocument.

5. Rechtmatige verwerking

Wij mogen uw persoonsgegevens alleen verwerken als hier een rechtmatige basis voor bestaat. Om rechtmatig te zijn moet de verwerking te baseren zijn op tenminste één van de rechtsgrondslagen die in de AVG zijn vastgelegd en die relevant zijn voor pensioenfondsen. Of een rechtsgrondslag van toepassing is, hangt onder meer af van het doel dat wij met de verwerking nastreven.

In de AVG zijn meerdere relevante rechtsgrondslagen voor een verwerking door pensioenfondsen terug te vinden:

- de betrokkene heeft toestemming verleend voor de verwerking (bijv. door een toestemmingsverklaring te ondertekenen voor het ontvangen van een nieuwsbrief); of
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waar de betrokkene partij bij is; of
- de verwerking is noodzakelijk om te voldoen aan de wettelijke verplichting waaraan het pensioenfonds gehouden is (bijvoorbeeld het melden van pensioengegevens van deelnemers en/of pensioenontvangers aan sociale zekerheids- of fiscale instanties); of
- de verwerking heeft gerechtvaardigde belangen tot doel die het pensioenfonds nastreeft (bijv. fysieke beveiliging, IT- en netwerkbeveiliging); of
- de verwerking is noodzakelijk is om de vitale belangen van de betrokkene te beschermen (bijv. om beveiligings- of gezondheids- en veiligheidsredenen).

Flexsecurity verwerkt uw persoonsgegevens meestal op basis van de tweede grondslag; de noodzaak voor de uitvoering van een overeenkomst waar de betrokkene partij bij is. Deze overeenkomst is de pensioenovereenkomst die de werkgevers en werknemers in de uitzendsector zijn overeengekomen. Door de verplichtstelling van deze pensioenovereenkomst is deze overeenkomst op u van toepassing. De verzameling en verwerking van uw persoonsgegevens is erop gericht om de uitvoering van uw pensioenregeling mogelijk te maken. Hiervoor hoeft u dus geen voorafgaande toestemming te geven.

Bij het nemen van besluiten over de gerechtvaardigde verwerking van persoonsgegevens zullen wij altijd een aantoonbare afweging maken waarbij de rechten en vrijheden van de betrokkenen worden afgewogen tegen ons gerechtvaardigde belang van de verwerking. Naast het bepalen van ons eigen belang, zal tevens relevant zijn of de verwerking dan noodzakelijk is en of de inbreuk in verhouding staat het doel van de voorgenomen verwerking. Als wij persoonsgegevens op basis van deze grondslag verwerken, zullen wij de betrokkenen wijzen op het recht van bezwaar. Als wij de verwerking baseren op gerechtvaardigde belangen informeren wij de betrokkenen over wat deze gerechtvaardigde belangen zijn. Dit kan bijvoorbeeld van toepassing zijn bij de verwerking van persoonsgegevens van partners en ex-partners.



Wanneer wij bijzondere persoonsgegevens verwerken, kan dit alleen als er een wettelijke grondslag is of de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang. Een voorbeeld hiervan is de verwerking van gegevens ten aanzien van arbeidsongeschiktheid, die wij nodig hebben om de regelingen bij arbeidsongeschiktheid te kunnen uitvoeren. Daarbij verwerken wij geen gegevens over de aard van de arbeidsongeschiktheid, maar wel over de toepasselijke wettelijke regeling en het arbeidsongeschiktheidspercentage.

6. Doeleinden van de verwerking

Flexsecurity verwerkt persoonsgegevens uitsluitend voor de specifieke doelen of voor andere specifiek in de toepasselijke wet toegestane doelen. In onze privacyverklaring, die te vinden is op onze website, staat uitgelegd op welke gronden, en voor welk doel wij uw persoonsgegevens verwerken.

Dit betekent dat wij uw persoonsgegevens niet voor het ene doel verzamelen om vervolgens voor een ander doel te kunnen gebruiken. Als het op enig moment nodig is om het doel waarvoor wij de gegevens verwerken te veranderen, dan wordt de betrokkene geïnformeerd over het nieuwe doel voordat die verwerking plaatsvindt. Eventueel kan de betrokkene hiertegen bezwaar maken.

Daarnaast dient de verwerking behoorlijk te zijn. Alleen het feit dat wij ons aan de wet houden betekent nog niet dat de verwerking daarmee ook behoorlijk is. Hierbij kan gedacht worden aan de situatie dat wij misbruik zouden maken van een bepaalde machtspositie en verwerking als zodanig zouden afdwingen bij de betrokkene. Ook passen wij het uitgangspunt van minimale gegevensverwerking toe. Wij mogen geen gegevens verwerken die niet nodig of niet relevant zijn voor de vastgestelde doeleinden.

Primair verwerken wij uw persoonsgegevens om uw pensioen zo goed mogelijk te kunnen uitvoeren en administreren. Ook verwerken wij uw persoonsgegevens voor naleving van wet- en regelgeving en wettelijke voorschriften, waaronder wetgeving op het gebied van identificatieplicht, fiscale wetgeving en sociale zekerheidswetgeving. Zo zijn wij verplicht om uw pensioengegevens te verstrekken aan de Stichting Pensioenregister voor mijnpensioenoverzicht.nl, zodat de informatie op deze website actueel en correct blijft. Ook verstrekken wij op basis van een wettelijk voorschrift jaarlijks gegevens van onze deelnemers aan het Centraal Bureau voor de Statistiek (CBS).

Flexsecurity communiceert bij voorkeur digitaal. Daarvoor maken wij gebruik van de e-mailadressen die wij van uw werkgever ontvangen. Wij mogen uw e-mailadres gebruiken voor onze (verplichte) pensioencommunicatie. Als u hier bezwaar tegen maakt, zullen wij de pensioencommunicatie schriftelijk verstrekken.

De AVG kent een aantal andere doeleinden voor verwerking van persoonsgegevens, zoals het verzamelen van persoonsgegevens in relatie tot historische, statistische en wetenschappelijke doeleinden en het verzamelen van persoonsgegevens in het kader van relatiemanagement en Direct Marketing activiteiten. Flexsecurity gebruikt deze doeleinden niet voor de verwerking van persoonsgegevens. Mocht daar op enig moment wel sprake van zijn, dan worden de betrokkenen hierover voorafgaand geïnformeerd.

7. Welke persoonsgegevens verwerken wij?

Wij verzamelen persoonsgegevens uit verschillende bronnen. In de onderstaande tabel geven we de herkomst en categorieën van persoonsgegevens weer:

De persoonsgegevens van de volgende betrokkenen	verkrijgt het pensioenfonds van
(gewezen) deelnemers	<ul style="list-style-type: none"> • de werkgever • de Basisregistratie Persoonsgegevens • het Uitvoeringsinstituut Werknemersverzekeringen • de betrokkene
partners en kinderen van (gewezen) deelnemers	<ul style="list-style-type: none"> • de betrokkene • de Basisregistratie Persoonsgegevens
ex-partners en nabestaanden van (gewezen) deelnemers	<ul style="list-style-type: none"> • de betrokkene • de Basisregistratie Persoonsgegevens
functionarissen van het pensioenfonds (zoals leden van het bestuur, verantwoordingsorgaan)	<ul style="list-style-type: none"> • de betrokkene
dienstverleners (zoals uitbestedingspartijen)	<ul style="list-style-type: none"> • de betrokkene

Wij verwerken verschillende soorten persoonsgegevens. Daarbij hanteren we de volgende categorieën:

Categorie	Toelichting	Voorbeelden
Identificerende gegevens	Zoomen direct in op een individu	Naam, geboortedatum, overlijdensdatum
Kwalificerende gegevens	Zeggen wat over een persoon	Leeftijd, geslacht, salaris, burgerlijke staat
Procesgegevens	Helpen de gegevensverwerking met betrekking tot een persoon in goede banen te leiden	Bankrekeningnummer, deelnemersnummer
Juridische gegevens	Gegevens die bij wet of jurisprudentie als privacygevoelig zijn aangemerkt of waarvan het gebruik wettelijk is beperkt	BSN

8. Hoe verwerken wij uw persoonsgegevens?

In dit hoofdstuk geven wij een nadere toelichting bij de manier waarop wij uw persoonsgegevens verwerken en de afwegingen die wij daarbij maken.

8.1 Transparante verwerking

Wij zorgen ervoor dat de betrokkene begrijpt:

- wie de gegevensbeheerder is (Stichting Pensioenfonds Flexsecurity);
- voor welke doelen de gegevens verwerkt zullen worden;
- hoe de gegevens verwerkt zullen worden;
- degenen aan wie de gegevens verstrekt kunnen worden;
- waarnaar de gegevens zullen worden overgedragen of vanaf waar ze toegankelijk zullen zijn; en
- wat de rechten van betrokken zijn ten aanzien van hun gegevens volgens de geldende wet- en regelgeving.

Alleen als er een disproportionele inspanning nodig zou zijn om dit duidelijk te maken, of wanneer de betrokkene zich hiervan aantoonbaar al bewust is, laten we dit achterwege. Alle relevant informatie staat in onze privacyverklaring die te vinden is op onze website. De privacyverklaring wordt periodiek geëvalueerd en zo nodig aangepast.

8.2 Geschikt, relevant en beperkt tot het noodzakelijke in verband met de doeleinden

Wij verzamelen en verwerken persoonsgegevens alleen voor zover dat noodzakelijk is voor de doelen van het pensioenfonds. Alle persoonsgegevens die niet nodig zijn voor deze doelen, worden niet verzameld. De verwerking van persoonsgegevens blijft beperkt tot gegevens die in redelijkheid geschikt en relevant zijn voor het desbetreffende doel, namelijk de uitvoering van uw pensioenregeling.

Wij hebben redelijke maatregelen getroffen om uw persoonsgegevens niet langer in een vorm te bewaren die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.

8.3 Correct en up-to-date

Ons uitgangspunt is dat de persoonsgegevens correct zijn en worden waar nodig en mogelijk worden bijgehouden. Wij hebben maatregelen getroffen om de juistheid van persoonsgegevens te controleren, op het moment van verzamelen en met regelmatige tussenpozen erna en uiteraard ook als de persoonsgegevens tussentijds worden aangepast. Persoonsgegevens die aantoonbaar onjuist of misleidend zijn, zijn niet correct. Daarom treffen we maatregelen om de juistheid van persoonsgegevens te controleren, op het moment van verzamelen en met regelmatige tussenpozen erna.

8.4 Niet langer bewaren dan noodzakelijk

Wij bewaren uw persoonsgegevens tot zeven jaar na overlijden of uw pensioendatum (in geval van waardeoverdracht of afkoop van een klein pensioen). De reden voor deze lange bewaartermijn is dat een vordering op pensioen niet verjaart tijdens het leven van een rechthebbende. Om vast te kunnen stellen of een pensioenaanspraak juist is vastgesteld of om vast te kunnen stellen of een claim op pensioen terecht is, zullen wij het in hoofdstuk 10 genoemde recht om "vergeten te worden" (gegevenswissing) in beginsel niet honoreren, ook wanneer uw pensioenkapitaal is overgedragen of afgekocht. Uw persoonsgegevens zijn gedurende een redelijke termijn na het bereiken van de pensioendatum nodig voor het doel waarvoor ze zijn verzameld of verwerkt. Wij werken daarom alleen mee aan het verwijderen van persoonsgegevens als dat moet op grond van onrechtmatige verwerking of een wettelijke verplichting.

Persoonsgegevens die wij niet wettelijk verplicht hoeven te bewaren (bijvoorbeeld voor belastingdoeleinden) of persoonsgegevens die wij niet mogen bewaren op grond van juridische of complianceredenen, worden vernietigd. Niet-correcte of verouderde gegevens worden zo snel mogelijk vernietigd of gewist, tenzij deze vanwege de bewaartermijn bewaard moeten worden.

9 Verwerking van bijzondere persoonsgegevens

In principe verwerken wij geen bijzondere persoonsgegevens voor de uitvoering van de pensioenregelingen. De enige uitzondering betreft informatie over iemands gezondheid die relevant is voor de vaststelling van de juiste pensioenaanspraken. Een voorbeeld is het arbeidsongeschiktheidspercentage dat nodig is voor het vaststellen van het recht op premievrije voortzetting van de pensioenopbouw. Als eis geldt altijd dat er een grondslag zoals vermeld in de AVG en/of de UAVG nodig is om deze gegevens te mogen verwerken.

Voor de identificatie van deelnemers en de koppeling met administraties van andere instanties registreren wij het Burgerservicenummer (BSN), waarvan de verwerking alleen plaatsvindt voor zover dat is toegestaan op basis van een specifiek wettelijke grondslag. Ook beperken we het gebruik van het BSN in de gegevensuitwisseling zoveel als mogelijk.

Bij ingang van het pensioen registeren we een kopie van het identiteitsbewijs dat noodzakelijk is om de rechthebbende te kunnen identificeren.

10 Rechten van betrokkenen

Wij verwerken persoonsgegevens op redelijke wijze en met inachtneming van de rechten van de betrokkene. We hebben, conform de AVG, procedures vastgelegd om een aantal rechten van betrokkenen ten aanzien van hun persoonsgegevens te bevorderen. In dit hoofdstuk worden deze rechten van betrokkenen behandeld.

10.1 Recht op inzage

De betrokkene heeft het recht om duidelijkheid te verkrijgen over het al dan niet verwerken van zijn of haar persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens. Wij verstrekken de betrokkene op diens verzoek een kopie van de persoonsgegevens die wij verwerken. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in elektronische vorm verstrekt.

10.2 Recht op rectificatie

Als de door ons verwerkte persoonsgegevens niet juist zijn, dan heeft de betrokkene het recht om deze te wijzigen. Als de persoonsgegevens onvolledig zijn heeft de betrokkene het recht om deze aan te vullen. Als de betrokkene terecht een beroep doet op dit recht en er correctie en/of aanvulling van gegevens plaatsvindt, dan stellen wij iedere ontvanger van de gegevens, zoals de Belastingdienst, het UWV en verwerkers, hiervan op de hoogte.

Wij stellen 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. Wij verstrekken de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

10.3 Recht om "vergeten te worden" (gegevenswissing)

Wij bewaren persoonsgegevens tot 7 jaar na overlijden of pensioendatum (in geval van waardeoverdracht of afkoop van een klein pensioen). In deze periode wissen wij de persoonsgegevens niet. Wij werken 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 de toestemming in waarop de verwerking berust;
- de betrokkene maakt bezwaar tegen de verwerking en er zijn geen dwingende gerechtvaardigde gronden voor de verwerking;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan het Unierecht of het Nederlands recht.

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

Wij stellen iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke wissing van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Wij verstrekken de betrokkene informatie over deze ontvangers als de betrokkene hierom verzoekt.

10.4 Recht op beperking van de verwerking

De betrokkene heeft het recht om ons te beperken in de verwerking van persoonsgegevens, indien:

- a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene;
- b) de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en/of 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. 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.

Wanneer de verwerking is beperkt, zullen wij de persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerken met toestemming van de betrokkene, wanneer dit op juridische gronden verplicht is 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.

Wij stellen de 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. Wij stellen 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 wij de persoonsgegevens aan een derde hebben verstrekt voor verwerking, stellen wij deze derde van het bovenstaande op de hoogte.

10.5 Recht op overdraagbaarheid (portabiliteit)

De AVG geeft betrokkene het recht om zijn persoonsgegevens geautomatiseerd geleverd te krijgen en om ze te laten doorleveren aan een derde. Dat recht bestaat indien de gegevens zijn verkregen op basis van toestemming van betrokkene of een overeenkomst tussen de verantwoordelijke en de betrokkene en de verwerking via geautomatiseerde procedures wordt verricht. Omdat bij ons pensioenfonds daar alleen in zeer specifieke gevallen sprake van zal zijn, zal een beroep van betrokkenen op dit recht in de regel worden afgewezen, tenzij er aantoonbaar sprake is van bijzondere omstandigheden die een afwijking noodzakelijk maken.

10.6 Recht van bezwaar tegen de verwerking

De AVG geeft de betrokkene het recht om, vanwege redenen die verband houden met zijn specifieke situatie, bezwaar te maken tegen de verwerking zijn of haar 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.

10.7 Recht niet te worden onderworpen aan geautomatiseerde besluiten, waaronder profilering

Flexsecurity maakt geen gebruik van profilering in de gegevensverwerking.

10.8 Gebruik maken van rechten

Om gebruik te maken van de rechten die beschreven zijn in dit hoofdstuk, kan de betrokkene een verzoek indienen bij Flexsecurity. Dit verzoek kan zowel schriftelijk als via e-mail ingediend worden. De uitvoeringsorganisatie zal uw verzoek in behandeling nemen. AZL heeft vanaf de ontvangst van het verzoek een maand de tijd om te beoordelen of het verzoek gerechtvaardigd is. Als dat binnen een maand niet lukt, dan moet in ieder geval binnen een maand worden gemeld waarom het niet lukt en kan de termijn met maximaal twee maanden worden verlengd.

Als het verzoek niet wordt opgevolgd, dan wordt dit binnen een maand meegedeeld met de reden van weigering en informatie over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en beroep in te stellen bij de rechter. Er zal moeten worden vastgesteld dat de betrokkene zelf het recht inroept. Dit kan gebeuren aan de hand van verschillende gegevens, zoals naam, adres en woonplaatsgegevens en klantnummer.

Het inroepen van rechten is in beginsel kosteloos, maar als het verzoek kennelijk ongegrond of buitensporig is mag Flexsecurity redelijke kosten vragen voor het inwilligen van het verzoek of het verzoek weigeren. Met AZL zijn afspraken hoe de verzoeken van betrokkenen worden behandeld.

11 Overige onderwerpen

In dit hoofdstuk wordt ingegaan op andere verplichtingen en procedures in het kader van de AVG en bescherming van persoonsgegevens.

11.1 Register van verwerkingen

Flexsecurity houdt een register van alle verwerkingen bij waar het Fonds de verantwoordelijke voor is. Dit register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt. Daarbij moet gedacht worden aan:

- De naam en contactgegevens van de verantwoordelijke en, mogelijk, de gezamenlijke verantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Ook de ingeschakelde verwerkers moeten een verwerkingenregister aanhouden, waarin inzichtelijk wordt gemaakt welke categorieën verwerkingen voor het pensioenfonds worden uitgevoerd. De registers moeten op verzoek aan de Autoriteit Persoonsgegevens worden verstrekt. De registers dienen als bewijs dat het pensioenfonds en de verwerkers de AVG naleven. Om die reden moeten de registers schriftelijk worden vastgelegd.

11.2 Uitbesteding aan (sub)verwerkers

Flexsecurity is als verwerkingsverantwoordelijke de partij die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De verwerker is de partij die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. De verwerker heeft een uitvoerende taak en heeft geen zeggenschap over de wijze van verwerken. Essentieel is dat de gegevens alleen in opdracht van de verantwoordelijke mogen worden verwerkt en niet voor eigen doeleinden door de verwerker. Het gaat om uitbestede / gedelegeerde verwerkingsactiviteiten, die een verantwoordelijke ook zelf had kunnen verrichten. Het belangrijkste voorbeeld is het verwerken van de pensioenadministratie van het pensioenfonds door een pensioenuitvoeringsorganisatie.

Als Flexsecurity werkzaamheden uitbesteedt waarbij persoonsgegevens worden verwerkt, dan wordt er een verwerkersovereenkomst afgesloten. In deze overeenkomst worden de doeleinden en voorwaarden voor de verwerking van de persoonsgegevens vastgelegd. Daarnaast worden de duur, de aard van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen vastgelegd. De verwerker mag de persoonsgegevens niet voor eigen (commerciële) doeleinden gebruiken. Als een instructie een inbreuk oplevert op de AVG stelt de verwerker het pensioenfonds hier onmiddellijk van op

de hoogte. Personen in dienst van of werkzaam voor een verwerker hebben een geheimhoudingsplicht.

De verwerker garandeert passende technische en organisatorische maatregelen om de verwerking te beveiligen; daarbij wordt rekening gehouden met eisen over de beveiliging, de vertrouwelijkheid, de integriteit en de beschikbaarheid van de gegevens. Ook worden eisen vastgelegd ten aanzien van logische toegangscontrole, fysieke maatregelen voor toegangsbeveiliging; automatische logging van alle handelingen rond de persoonsgegevens, pseudonimisering en encryptie (versleuteling) van digitale bestanden met persoonsgegevens, organisatorische maatregelen voor toegangsbeveiliging, controle op toegekende bevoegdheden en een procedure voor het melden van datalekken. Na afloop van de opdracht verwijderd de verwerker de persoonsgegevens of geeft de persoonsgegevens terug aan het pensioenfonds. Ook verwijderd de verwerker alle kopieën, tenzij er een wettelijke verplichting is om de gegevens te bewaren.

Niet met alle partijen waarmee persoonsgegevens worden uitgewisseld wordt een verwerkersovereenkomst gesloten. Instanties zoals het CBS, de Belastingdienst en het UWV aan wie persoonsgegevens worden aangeleverd, verwerken deze gegevens op grond van hun eigen (wettelijke) taken en zijn zelf verantwoordelijke voor de gegevensverwerking.

De verwerker mag geen sub-verwerker(s) inschakelen zonder voorafgaande schriftelijke toestemming van Flexsecurity. De verwerker legt aan een sub-verwerker in een verwerkersovereenkomst dezelfde verplichtingen op als Flexsecurity met de verwerker is overeengekomen.

11.3 Datalekken

Bij een datalek gaat het om in handen komen van persoonsgegevens bij ongeautoriseerde personen, als gevolg van een inbreuk op de beveiliging. Bij een datalek worden persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, hetgeen dus niet de bedoeling is van het Fonds. Voorbeelden van datalekken zijn: een brief die verzonden wordt naar een adres waar de betrokkene niet meer woont, een e-mail naar een adres dat door een andere persoon gebruikt wordt, een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

In het geval van een geconstateerd datalek moet de verantwoordelijke, dus Flexsecurity, dit zo snel als mogelijk, maar in ieder geval binnen 72 uur melden aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico voor betrokkenen inhoudt. Als dat niet tijdig lukt, dan moet het pensioenfonds hiervoor een verklaring kunnen geven. Als er sprake is van een hoog risico is en het pensioenfonds geen maatregelen meer kan nemen om het risico te beperken, dan moeten naast de Autoriteit Persoonsgegevens ook de betrokkenen zelf worden geïnformeerd, zodat die eventueel voorzorgsmaatregelen kunnen treffen. De Autoriteit Persoonsgegevens kan het pensioenfonds ook verplichten tot melding aan de deelnemers.

11.4 Privacy Impact Analyse (PIA)

Met behulp van een PIA (ook wel gegevensbeschermingseffectbeoordeling genoemd) beoordeelt het pensioenfonds de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van de privacy. Het pensioenfonds laat een PIA uitvoeren als er sprake is van een gegevensverwerking met een hoog privacyrisico voor betrokkenen. De Autoriteit Persoonsgegevens heeft een lijst met soorten verwerkingen opgesteld waarvoor het uitvoeren van een PIA verplicht is vóórdat met het verwerken van persoonsgegevens wordt begonnen. Deze lijst is niet uitputtend en het pensioenfonds moet zelf beoordelen of de verwerking een hoog privacyrisico oplevert voor betrokkenen. Flexsecurity heeft vrijwel alle processen waarbij persoonsgegevens worden verwerkt, uitbesteed aan uitvoeringsorganisatie AZL. Deze verwerker voert standaard een PIA uit bij een gewijzigd of nieuw proces met een verwacht hoog risico voor de betrokkenen. Flexsecurity neemt kennis van de ingevulde PIA's. Op deze wijze houden wij zicht op processen met een hoog privacyrisico voor betrokkenen en krijgen wij inzicht welke maatregelen er worden genomen om geconstateerde privacyrisico 's te beperken.

11.4 Audits & Monitoring

De verwerker werkt mee aan periodieke audits die door of namens Flexsecurity worden uitgevoerd. De verwerker stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de aan hem als verwerker opgelegde verplichtingen. Flexsecurity zorgt ervoor dat de verwerkersovereenkomsten voldoen aan de gestelde eisen en ziet toe op de naleving daarvan.

11.5 Verwerkingen buiten de EU/EER

De AVG is van toepassing op pensioenfonds die persoonsgegevens (doen) verwerken van betrokkenen in de Europese Unie, ongeacht of de verwerking plaatsvindt in de Europese Unie. Flexsecurity en zijn verwerkers passen de privacyregels dus ook toe als gegevens worden verwerkt buiten de Europese Unie, bijvoorbeeld via cloud computing. Contracten met IT-dienstverleners die niet in de Europese Unie gevestigd zijn, worden dus aangepast aan de AVG. Bij doorgifte van persoonsgegevens buiten de EU gaat het pensioenfonds na of doorgifte is toegestaan. In principe hanteert Flexsecurity als beleid dat er geen verwerking van persoonsgegevens plaatsvindt buiten de EU/EER.

11.6 Privacy officer

Flexsecurity verwerkt op beperkte schaal bijzondere persoonsgegevens die betrekking hebben op de gezondheid van de deelnemers die (gedeeltelijk) arbeidsongeschikt zijn. Deze gegevens bestaan uitsluitend uit de toepasselijke arbeidsongeschiktheidspercentages van de betreffende deelnemers. Het pensioenfonds verwerkt geen andere bijzondere persoonsgegevens en heeft om die reden geen Functionaris Gegevensbescherming (FG) aangesteld.

Wel heeft het fonds een privacy officer aangesteld. De privacy officer heeft de volgende taken en verantwoordelijkheden:

- Adviseren van het bestuur over kwesties die verband houden met privacy;
- Aanbevelen van wijzigingen op dit beleid om ervoor te zorgen dat het voldoet aan toepasselijke wettelijke eisen en dat het blijft voldoen aan de behoeften van het pensioenfonds;
- Samenwerken, indien gewenst, met relevante afdelingen / personen bij uitvoeringsorganisatie AZL en eventuele andere verwerkers van persoonsgegevens;
- Toezicht houden op naleving van dit beleid door het pensioenfonds en zijn verwerkers en subverwerkers;
- De ontwikkelingen op het gebied van privacy bijhouden en op de hoogte blijven van toepasselijke wetten, Nederlandse verplichtingen en regulerende richtsnoeren en best practices in verband met compliance op het gebied van privacy;
- Een overzicht bijhouden van de privacy impact assessments (gegevensbeschermingseffectbeoordelingen) en deze nauwgezet volgen en op verzoek verdere begeleiding en advies geven;
- De implementatie van passende technische en organisatorische maatregelen bevorderen en hierover adviseren om 'privacy by design' of 'by default' te garanderen;
- Fungeren als belangrijkste contactpersoon voor de Autoriteit Persoonsgegevens of andere bevoegde autoriteit ten aanzien van de persoonsgegevens en voor personen die hun rechten jegens het pensioenfonds willen uitoefenen;
- Het register voor de verwerkingen van het pensioenfonds bijhouden en erop toezien dat de verwerkers van het pensioenfonds ook een register voor de verwerkingen van het pensioenfonds bijhouden.

De privacy officer behoort tot de tweede lijn in de risicobeheersing van het fonds en rapporteert rechtstreeks aan het bestuur.

12 Naleving en klachten

12.1 Naleving en toezicht

De Autoriteit Persoonsgegevens heeft als wettelijke taak om de naleving van de verplichtingen op grond van de AVG te monitoren en te handhaven. De Autoriteit Persoonsgegevens beschikt daarvoor over verschillende bevoegdheden, zoals het doen van onderzoeken, het verkrijgen van toegang tot alle bedrijfsruimten en middelen van gegevensverwerkingen. In geval van een onderzoek door de Autoriteit Persoonsgegevens zal Flexsecurity daaraan zijn medewerking verlenen.

De Autoriteit Persoonsgegevens heeft de bevoegdheid tot het opleggen van corrigerende maatregelen, oplopend van een waarschuwing, een last om betrokkenen te informeren, tot een verwerking te beperken, tijdelijk dan wel definitief. Tenslotte kan er, afhankelijk van de aard, ernst en duur van de overtreding, een boete worden opgelegd, oplopend tot 20 miljoen Euro. Het is daarom van belang dat het pensioenfonds, de (sub)verwerkers en alle anderen de AVG naleven.

12.2 Klachten en bezwaar

Indien een betrokkene van mening is dat de verwerking van zijn of haar persoonsgegevens inbreuk maakt op de AVG, heeft de betrokkene het recht om bezwaar te maken. Daarvoor zijn twee procedures mogelijk:

- Het indienen van een klacht indienen bij het pensioenfonds. Het pensioenfonds heeft een Klachtenreglement dat voorziet in behandeling van klachten en bezwaren en in een beroepsprocedure bij de Geschillen Instantie Pensioenfondsen. Het klachtenreglement is te vinden op de website van Flexsecurity.
- Een bezwaarprocedure bij de Autoriteit Persoonsgegevens. De betrokkene heeft ook het recht om direct een klacht bij de Autoriteit Persoonsgegevens in te dienen. De Autoriteit Persoonsgegevens stelt een onderzoek in en stelt de klager in kennis van de voortgang en het resultaat van de klacht, alsmede van de mogelijkheid tot voorziening in rechte, ook tegen de Autoriteit Persoonsgegevens zelf. De Autoriteit Persoonsgegevens faciliteert de indiening van een bezwaar kosteloos. Een betrokkene die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de AVG, heeft het recht om van de verantwoordelijke en/of de verwerker een schadevergoeding te ontvangen voor de geleden schade. Betrokkene kan daarbij een orgaan, organisatie of vereniging inschakelen om de klacht in te dienen dan wel de schadeclaim in te stellen.

Het beleid van Flexsecurity is erop gericht om juridische beslechting van geschillen zoveel als mogelijk te voorkomen door het zoeken naar een minnelijke oplossing.

13 Verantwoording, evaluatie en aanpassing

Flexsecurity legt jaarlijks verantwoording af over het gevoerde beleid ten aanzien van privacybescherming in een privacyrapportage die door uitvoeringsorganisatie AZL wordt opgesteld. Daarnaast wordt in het jaarverslag verantwoording afgelegd over het gevoerde beleid, eventuele incidenten en datalekken en de beleidsmatige aspecten rondom privacy.

Evaluatie en herziening van het privacybeleid vindt ten minste een maal per drie jaar plaats en zoveel vaker indien het bestuur dit noodzakelijk acht.



14 Inwerkingtreding

Dit privacybeleid is vastgesteld op 10 november 2023 en per diezelfde datum in werking getreden.