SPIN

Privacybeleid

2026

Stichting Pensioenfonds
IBM Nederland

Inhoudsopgave

1 Inleiding 3

2 Doelstellingen van privacy en gegevensbescherming 3

3 Privacy-strategie 3

4 Verwerking van persoonsgegevens 4

5 Governance en verantwoordelijkheden 5

6 Technische en organisatorische beveiligingsmaatregelen 5

7 Uitbesteding en verwerking door externe partijen 6

8 Rechten van betrokkenen 7

9 Bewaartermijnen en archivering 8

10 DPIA's, datalekken, cyberincidenten en continuïteit 8

11 Monitoring, audits en evaluatie 9

Bijlage 1 RACI 10

Bijlage 2 Begrippen 11

Bijlage 3 Protocol Datalekken 12

Bijlage 4 Data Protection Impact Assessment 13

Bijlage 5 Bewaartermijnen 14

Bijlage 6 Privacyverklaring 15

1 Inleiding

Stichting Pensioenfonds IBM Nederland (SPIN) en in naam van SPIN worden in het kader van de uitvoering van de pensioenregeling persoonsgegevens verwerkt van (gewezen) deelnemers, pensioengerechtigden, werkgevers, medewerkers, bestuursleden en andere betrokkenen. Een zorgvuldige omgang met persoonsgegevens is essentieel voor het vertrouwen in de uitvoering van de pensioenregeling en voor de bescherming van de persoonlijke levenssfeer van betrokkenen.

SPIN is gehouden om persoonsgegevens te verwerken in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), de Pensioenwet, de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen 2023 van de Pensioenfederatie (de gedragslijn) en overige relevante wet- en regelgeving. Privacybescherming vormt een integraal onderdeel van de governance, risicobeheersing, informatiebeveiliging en continuïteitsbeheersing van SPIN. Dit privacybeleid beschrijft de uitgangspunten, verantwoordelijkheden en beheersmaatregelen die SPIN hanteert om persoonsgegevens op een rechtmatige, zorgvuldige en veilige wijze te verwerken. De omschrijving van de begrippen in dit beleid sluiten aan bij de definities van de AVG en van de gedragslijn. In bijlage 2 zijn de belangrijkste definities opgenomen.

Het privacybeleid sluit aan op het IT-beleid, het Business Continuity Plan (BCP), het uitbestedingsbeleid, het risicomanagementraamwerk en het Internal Control Framework van SPIN. Gezamenlijk vormen deze documenten het kader voor de beheersing van privacy-, informatiebeveiligings- en continuïteitsrisico's.

2 Doelstellingen van privacy en gegevensbescherming

SPIN streeft ernaar persoonsgegevens uitsluitend te verwerken voor gerechtvaardigde en expliciet omschreven doeleinden die samenhangen met de uitvoering van de pensioenregeling, de naleving van wettelijke verplichtingen en de ondersteuning van de bedrijfsvoering. Daarbij hanteert SPIN de uitgangspunten van rechtmatigheid, proportionaliteit, transparantie, dataminimalisatie en vertrouwelijkheid.

Het privacybeleid is van toepassing op de verwerking van persoonsgegevens waarbij SPIN in de zin van de AVG als verwerkingsverantwoordelijke gegevens verwerkt. Een verwerkingsverantwoordelijke is de partij die het doel (wat) en de middelen van de verwerking (hoe) vaststelt. De verwerkingsverantwoordelijke draagt de volledige juridische eindverantwoordelijkheid dat de privacyregels worden nageleefd

De verwerking van persoonsgegevens moet bijdragen aan een betrouwbare, zorgvuldige en toekomstbestendige uitvoering van de pensioenregeling. SPIN wil voorkomen dat persoonsgegevens verloren gaan, onrechtmatig worden verwerkt, ongeautoriseerd toegankelijk zijn of langer worden bewaard dan noodzakelijk. De bescherming van persoonsgegevens is daarom geïntegreerd in de inrichting van processen, systemen, uitbestedingsrelaties en continuïteitsmaatregelen.

SPIN hanteert een risicogebaseerde benadering waarbij privacy risico's onderdeel uitmaken van de reguliere risicomanagementcyclus. Bij nieuwe processen, systeemwijzigingen, uitbestedingen of wijzigingen in wet- en regelgeving wordt beoordeeld welke impact bestaat op de bescherming van persoonsgegevens en welke aanvullende beheersmaatregelen noodzakelijk zijn.

3 Privacy-strategie

SPIN beschouwt privacybescherming als een integraal onderdeel van verantwoord pensioenfondsbestuur. Persoonsgegevens worden uitsluitend verwerkt indien daarvoor een geldige grondslag bestaat en indien de verwerking

noodzakelijk is voor het betreffende doel. Daarbij wordt steeds beoordeeld of het doel niet op een minder ingrijpende wijze kan worden bereikt.
Bij de inrichting van processen en systemen wordt uitgegaan van de beginselen privacy by design en privacy by default. Dat betekent dat privacybescherming vanaf het ontwerp van processen, systemen en dienstverlening wordt meegenomen en dat standaardinstellingen zoveel mogelijk privacy-vriendelijk worden ingericht. De instellingen van de portal en website zijn zo ingericht dat betrokkene zoveel mogelijk zelf keuzes moet maken en keuzes niet voor ingevuld zijn. Waar mogelijk worden persoonsgegevens geanonimiseerd of gepseudonimiseerd en wordt de toegang beperkt tot medewerkers en externe partijen die deze gegevens nodig hebben voor de uitvoering van hun werkzaamheden.

SPIN maakt in belangrijke mate gebruik van uitbestedingsrelaties voor de ondersteuning van haar primaire processen en IT-dienstverlening. Met deze partijen worden contractuele afspraken gemaakt over de verwerking van persoonsgegevens, informatiebeveiliging, continuïteit, auditrechten, datalekken en naleving van de AVG. Daarbij blijft SPIN als verwerkingsverantwoordelijke verantwoordelijk voor de bescherming van persoonsgegevens.

4 Verwerking van persoonsgegevens

SPIN verwerkt persoonsgegevens uitsluitend als daarvoor een geldige wettelijke grondslag bestaat (toestemming, overeenkomst, wettelijke verplichting, vitaal belang, taak van algemeen belang of gerechtvaardigd belang). In de meeste gevallen heeft de grondslag te maken met de uitvoering van de pensioenovereenkomst, het voldoen aan wettelijke verplichtingen op grond van onder meer de Pensioenwet, fiscale wetgeving en socialezekerheidswetgeving of een gerechtvaardigd belang van SPIN. Indien verwerking plaatsvindt op basis van toestemming van de betrokkene, zorgt SPIN ervoor dat deze toestemming op de juiste wijze wordt verkregen en dat deze toestemming op ieder moment kan worden ingetrokken.

Het verwerken van persoonsgegevens vindt plaats binnen processen zoals pensioenadministratie, premie-inning, berekening en uitbetaling van pensioenen, communicatie met deelnemers, governanceprocessen, vermogensbeheer, financiële administratie, personeelsadministratie en de behandeling van klachten en geschillen. Bij de uitvoering van deze processen verwerkt SPIN persoonsgegevens van onder meer (gewezen) deelnemers, pensioengerechtigden, werkgevers, medewerkers, bestuursleden, leden van fondsorganen, externe adviseurs en nabestaanden. Afhankelijk van het doel van de verwerking kunnen onder andere identificerende gegevens, contactgegevens, gegevens over dienstverbanden, pensioenaanspraken, betaalgegevens, gegevens over partners en kinderen, gegevens over arbeidsongeschiktheid en andere gegevens die noodzakelijk zijn voor de uitvoering van wettelijke verplichtingen worden verwerkt.

Bijzondere categorieën persoonsgegevens, zoals gegevens over gezondheid of arbeidsongeschiktheid, worden uitsluitend verwerkt als daarvoor een specifieke wettelijke uitzondering bestaat en indien deze verwerking noodzakelijk is voor de uitvoering van de pensioenregeling of op grond van (andere) wettelijke verplichtingen. Het betreft onder meer aanspraken die afhankelijk zijn van de gezondheidstoestand van betrokkene. SPIN verwerkt dergelijke gegevens met een hoog beveiligingsniveau en beperkt de toegang tot medewerkers of externe partijen die deze gegevens strikt noodzakelijk nodig hebben voor de uitvoering van hun werkzaamheden.

SPIN verwerkt uitsluitend persoonsgegevens die noodzakelijk zijn voor het betreffende doel. Bij nieuwe verwerkingen of wijzigingen in bestaande processen wordt beoordeeld of de verwerking proportioneel is en of het doel niet met minder of minder gevoelige persoonsgegevens kan worden bereikt. Daarbij wordt expliciet aandacht besteed aan de beginselen van dataminimalisatie, doelbinding en opslagbeperking.

Om de juistheid, volledigheid en actualiteit van persoonsgegevens te waarborgen maakt SPIN gebruik van verschillende interne en externe gegevensbronnen. Gegevens kunnen onder meer worden ontvangen van werkgevers, deelnemers zelf, uitvoeringspartijen, overheidsinstanties en basisregistraties zoals de Basisregistratie Personen. SPIN neemt passende maatregelen om onjuiste of verouderde gegevens te corrigeren zodra blijkt dat gegevens niet langer juist of volledig zijn.

De verwerkingen van persoonsgegevens zijn vastgelegd in een verwerkingsregister. In dit register wordt onder meer vastgelegd welke categorieën persoonsgegevens worden verwerkt, voor welke doeleinden dit gebeurt, welke wettelijke grondslagen van toepassing zijn, welke bewaartermijnen gelden, welke interne en externe partijen bij de verwerking betrokken zijn en welke beveiligingsmaatregelen zijn getroffen. In bijlage 5 zijn de toepasselijke bewaartermijnen opgenomen. Het verwerkingsregister wordt beheerd door de Privacy Officer en jaarlijks gecontroleerd op actualiteit en volledigheid.

Indien persoonsgegevens voor een nieuw doel worden gebruikt, beoordeelt SPIN vooraf of deze verwerking verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Daarbij wordt rekening gehouden met de aard van de gegevens, de mogelijke impact voor betrokkenen, de relatie tussen het oorspronkelijke en nieuwe doel en de noodzaak van aanvullende waarborgen of toestemming.

Op de website staan een privacyverklaring en cookieverklaring waarin staat beschreven welke gegevens en op welke wijze SPIN deze verwerkt. De privacyverklaring en cookieverklaring zijn opgenomen in bijlage 6 en worden jaarlijks door de Privacy Officer herzien.

5 Governance en verantwoordelijkheden

Het Algemeen Bestuur is eindverantwoordelijk voor het privacybeleid en stelt de kaders vast waarbinnen persoonsgegevens worden verwerkt. Het Uitvoerend Bestuur is verantwoordelijk voor de implementatie, uitvoering en monitoring van het privacybeleid en ziet erop toe dat passende maatregelen worden getroffen om privacyrisico's te beheersen. Het privacybeleid valt onder het toezichtsgebied juridische zaken. Jaarlijks stelt het niet uitvoerend bestuur vast of de Gedragslijn is nageleefd en rapporteert daarover in het jaarverslag.
SPIN heeft de functie van Privacy Officer belegd bij de Manager Juridische Zaken. De Manager Juridische Zaken vervult in die hoedanigheid de rol van Privacy Officer en adviseert het Uitvoerend Bestuur en het Algemeen Bestuur over de naleving van de AVG, het privacybeleid en de Gedragslijn. De Privacy Officer ondersteunt de organisatie bij privacyvraagstukken, behandelt klachten, handelt datalekken af, onderhoudt het privacybeleid en andere gerelateerde documenten, onderhoudt het verwerkingsregister, adviseert over DPIA's en treedt op als contactpersoon inzake privacy gerelateerde zaken richting de Autoriteit Persoonsgegevens en andere toezichthouders.

De verantwoordelijkheid voor privacybescherming is nauw verbonden met de beheersing van IT-risico's, cybersecurity, datakwaliteit en continuïteit. Daarom werken de Privacy Officer, de Manager IT & Change, risicomanagement en de verantwoordelijke managers binnen de primaire processen nauw samen bij het identificeren, beoordelen en beheersen van privacy- en informatiebeveiligingsrisico's.

In bijlage 1 is de RACI-tabel opgenomen met daarin de belangrijkste processen en verantwoordelijkheden.
SPIN borgt de verantwoordingsplicht uit de AVG door besluiten, beoordelingen en beheersmaatregelen aantoonbaar vast te leggen. Daartoe behoren onder meer het verwerkingsregister, DPIA-besluiten en datalekregistraties.

6 Technische en organisatorische beveiligingsmaatregelen

SPIN treft passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies, onbevoegde toegang, wijziging, vernietiging of onrechtmatige verwerking. Daarbij wordt rekening gehouden met de aard van de persoonsgegevens, de risico's van de verwerking, de stand van de techniek en de afhankelijkheid van externe dienstverleners.

Bij indiensttreding worden nieuwe medewerkers geïnformeerd over het belang van privacy en het beleid van SPIN. Tevens worden periodiek bewustwordingssessies georganiseerd voor medewerkers en bestuur. Daarnaast is de gedragscode op de medewerkers van toepassing.

Binnen de kantoorautomatisering en de primaire processen wordt gebruikgemaakt van toegangsbeveiliging op basis van het need-to-know- en need-to-access-principe. Toegang tot systemen en gegevens wordt uitsluitend verleend aan medewerkers die deze toegang nodig hebben voor de uitvoering van hun functie. Voor kritieke systemen wordt gebruikgemaakt van multi-factor authenticatie, encryptie en beveiligde verbindingen.

SPIN maakt gebruik van beveiligde gegevensuitwisseling en ziet erop toe dat persoonsgegevens vertrouwelijk worden verwerkt. Apparatuur en systemen worden beveiligd tegen ongeautoriseerde toegang en belangrijke IT-diensten worden conform het internal control framework (ICF) beoordeeld op de effectiviteit van de getroffen beveiligingsmaatregelen. Daarbij wordt gebruikgemaakt van onafhankelijke assurance-rapportages, audits, penetratietesten en jaarlijkse evaluaties van leveranciers.

Privacy- en informatiebeveiligingsmaatregelen maken integraal onderdeel uit van het IT-beleid, het cybersecuritybeleid, AI-beleid en de continuïteitsmaatregelen van SPIN.

7 Uitbesteding en verwerking door externe partijen

SPIN maakt voor de uitvoering van haar werkzaamheden gebruik van externe dienstverleners. Deze uitbestedingsrelaties zijn noodzakelijk voor onder meer de ondersteuning van de pensioenadministratie, IT-dienstverlening, kantoorautomatisering, communicatieprocessen, actuariële dienstverlening, hosting, gegevensuitwisseling en vermogensbeheer. Partijen die persoonsgegevens verwerken namens SPIN, worden veelal aangemerkt als verwerker in de zin van de AVG. Ook is het mogelijk dat er sprake is van een zelfstandige of gezamenlijke verwerkingsverantwoordelijkheid.

SPIN blijft als verwerkingsverantwoordelijke eindverantwoordelijk voor de bescherming van persoonsgegevens die door externe partijen namens SPIN worden verwerkt. Daarom worden voorafgaand aan de samenwerking afspraken gemaakt over de wijze waarop persoonsgegevens worden verwerkt, beveiligd en beheerst. Deze afspraken worden vastgelegd in verwerkersovereenkomsten of andere contractuele documenten die voldoen aan de vereisten van de AVG.

In deze overeenkomsten wordt onder meer vastgelegd welke persoonsgegevens worden verwerkt, voor welke doeleinden dit gebeurt, welke beveiligingsmaatregelen van toepassing zijn, hoe wordt omgegaan met vertrouwelijkheid, datalekken, auditrechten, rechten van betrokkenen, subverwerkers en beëindiging van de dienstverlening. Daarnaast wordt vastgelegd dat persoonsgegevens uitsluitend mogen worden verwerkt op basis van schriftelijke instructies van SPIN en dat medewerkers van de verwerker gebonden zijn aan geheimhouding.

SPIN beoordeelt voorafgaand aan een uitbesteding of een externe partij voldoende waarborgen biedt voor een zorgvuldige en veilige verwerking van persoonsgegevens. Daarbij wordt onder meer gekeken naar de volwassenheid van de informatiebeveiliging, de aanwezigheid van assurance-rapportages, certificeringen, continuïteitsmaatregelen, incidentmanagement en de ervaring van de leverancier binnen de financiële sector of pensioensector.
Tijdens de looptijd van de dienstverlening monitort SPIN conform het ICF of externe partijen blijven voldoen aan de overeengekomen privacy- en beveiligingseisen. Hiervoor wordt gebruikgemaakt van periodieke evaluaties, leveranciersgesprekken, assurance-rapportages zoals ISAE3402-, SOC- en ISO-rapportages, auditbevindingen en incidentrapportages. Indien tekortkomingen worden geconstateerd, worden aanvullende maatregelen verlangd of verbeteracties afgesproken.

Indien een externe partij gebruikmaakt van subverwerkers, is daarvoor voorafgaande toestemming van SPIN vereist. SPIN beoordeelt daarbij of ook deze subverwerkers passende waarborgen bieden voor de bescherming van persoonsgegevens en of voldoende transparantie bestaat over de locaties waar gegevens worden verwerkt of opgeslagen.

Doorgifte van persoonsgegevens buiten de Europese Economische Ruimte vindt uitsluitend plaats indien daarvoor een geldige wettelijke grondslag bestaat en passende waarborgen zijn getroffen. Daarbij beoordeelt SPIN of het

beschermingsniveau in het betreffende land voldoende is en of aanvullende contractuele, organisatorische of technische maatregelen noodzakelijk zijn.

Bij beëindiging van een uitbestedingsrelatie worden afspraken gemaakt over het retourneren, verwijderen of vernietigen van persoonsgegevens en over de wijze waarop wordt vastgesteld dat gegevens daadwerkelijk uit systemen van de verwerker zijn verwijderd, tenzij wettelijke bewaarplichten verdere opslag vereisen.

8 Rechten van betrokkenen

SPIN informeert betrokkenen op transparante wijze over de verwerking van persoonsgegevens en over de rechten die zij op grond van de AVG kunnen uitoefenen. Betrokkenen hebben onder meer het recht op inzage, correctie, verwijdering, beperking van verwerking, overdraagbaarheid van gegevens en bezwaar tegen bepaalde verwerkingen. Betrokkenen kunnen kosteloos hun rechten uitoefenen.

Verzoeken van betrokkenen worden zorgvuldig beoordeeld en binnen de wettelijke termijnen afgehandeld. Voorafgaand aan de behandeling van een verzoek stelt SPIN de identiteit van de verzoeker vast om ongeautoriseerde verstrekking van persoonsgegevens te voorkomen. In beginsel worden verzoeken door de pensioenadministratie in behandeling genomen. De privacy officer geeft advies over de afhandeling en het Uitvoerend Bestuur neemt de beslissing over de afhandeling.

Indien SPIN een verzoek geheel of gedeeltelijk afwijst, wordt de betrokkene geïnformeerd over de reden van afwijzing en over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep in te stellen bij de rechter.

De procedures binnen het pensioenfonds die ervoor zorgen dat de betrokkenen deze rechten kunnen uitoefenen, zijn als volgt:

a. Informatieverstrekking

De betrokkenen worden geïnformeerd over de verwerking van op hen betrekking hebbende persoonsgegevens voordat deze door of ten behoeve van het pensioenfonds worden verwerkt. Deze informatie is beknopt, begrijpelijk en wordt verstrekt in de Nederlandse taal. Voor informatie over gegevens die aan SPIN verstrekt worden door derden, voldoet SPIN binnen een redelijke termijn (een maand) aan de informatieplicht. SPIN geeft onder meer via de Privacyverklaring op de website uitvoering aan de informatieplicht.

b. Recht op inzage:

Betrokkene heeft het recht om SPIN te vragen of zijn persoonsgegevens door SPIN worden verwerkt. Nadat de betrokkene een verzoek tot inzage heeft gedaan bij SPIN, deelt SPIN zo spoedig mogelijk, maar in ieder geval binnen 1 maand mee of SPIN persoonsgegevens betreffende de betrokkene verwerkt. Als dat het geval is, verstrekt SPIN binnen 1 maand na ontvangst van het verzoek aan de betrokkene een omschrijving van:

i. het doel of de doelen van de verwerking;
ii. de (categorieën) persoonsgegevens die worden verwerkt;
iii. de ontvangers of categorieën ontvangers; en
iv. informatie omtrent de herkomst van de persoonsgegevens.

Indien er sprake is van een complex verzoek of een grote hoeveelheid verzoeken dan kan SPIN de termijn met twee maanden verlengen. SPIN mag weigeren een kennelijk ongegrond of buitensporig verzoek in behandeling te nemen. Bij weigering ontvangt betrokkene informatie om een klacht in te dienen bij de AP en beroep in te stellen bij de rechter.

c. Recht op correctie, aanvulling en verwijdering:

Nadat een betrokkene zijn persoonsgegevens heeft ingezien, kan hij SPIN verzoeken om deze persoonsgegevens te corrigeren, aan te vullen of te verwijderen. Het pensioenfonds bericht de betrokkene binnen 1 maand na ontvangst van het verzoek of daaraan voldaan zal worden, waarbij een afwijzing gemotiveerd zal zijn. SPIN zal het verzoek van de betrokkene honoreren indien de persoonsgegevens feitelijk onjuist zijn, voor het doel of doeleinden van de verwerking

onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met de AVG worden verwerkt. Voor een verzoek tot verwijdering geldt daarnaast dat SPIN dit niet zal honoreren, voor zover dit in strijd is met een wettelijke verplichting. Bij honorering van het verzoek, zal SPIN de beslissing tot correctie, aanvulling of verwijdering binnen 1 maand uitvoeren.
d. Recht op beperking van verwerken: een betrokkene kan het recht op beperking van verwerking van persoonsgegevens verkrijgen (dat wil zeggen SPIN verzoeken tijdelijk het verwerken van persoonsgegevens te staken) indien:

i. de juistheid van de persoonsgegevens wordt betwist. De beperking geldt dan gedurende de periode die SPIN nodig heeft om de juistheid van de persoonsgegevens te controleren;
ii. de verwerking onrechtmatig is en de betrokkene zich verzet tegen wissen van de persoonsgegevens in plaats daarvan verzoekt om beperking van het gebruik, bijvoorbeeld omdat bij het wissen het “bewijs” dat nodig is voor het vorderen van een schadevergoeding verdwijnt;
iii. SPIN de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden maar de betrokkene deze nodig heeft voor de instelling van een rechtsvordering. Een betrokkene die een beperking van de verwerking heeft verkregen wordt door het pensioenfonds op de hoogte gebracht voordat de verwerking wordt opgeheven.

e. Recht op dataportabiliteit:
Voor die persoonsgegevens die een betrokkene zelf actief en bewust aan SPIN heeft verstrekt, kan er recht op dataportabiliteit (overdracht) bestaan. Indien van toepassing zullen de betreffende persoonsgegevens binnen 1 maand in een gestructureerd, gangbaar en machine leesbaar format worden verstrekt.

f. Recht van bezwaar:
Een betrokkene kan in enkele gevallen bezwaar maken tegen het verwerken van zijn persoonsgegevens in verband met bijzondere omstandigheden. SPIN staakt de verwerking van persoonsgegevens bij bezwaar tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen, rechten en vrijheden van de Betrokkene of verband houden met een rechtsvordering.

9 Bewaartermijnen en archivering

SPIN bewaart persoonsgegevens niet langer dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld, tenzij wettelijke verplichtingen, pensioenrechtelijke aanspraken, bewijsvoering, geschillenbeslechting of archivering een langere bewaartermijn vereisen.

Persoonsgegevens worden na afloop van de bewaartermijn vernietigd, geanonimiseerd of ontoegankelijk gemaakt, tenzij verdere opslag noodzakelijk blijft op grond van wet- en regelgeving of archiveringsdoeleinden. Bij herstel vanuit back-upomgevingen blijft het geldende retentie- en verwijderbeleid van toepassing.

Vanwege de langlopende aard van pensioenrechten en mogelijke aanspraken van deelnemers en nabestaanden kunnen voor bepaalde persoonsgegevens lange bewaartermijnen gelden. Daarbij houdt SPIN rekening met wettelijke verplichtingen, de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen en de noodzaak om pensioenrechten ook op lange termijn te kunnen reconstrueren en onderbouwen.

10 DPIA’s, datalekken, cyberincidenten en continuïteit

SPIN beoordeelt of verwerkingen van persoonsgegevens een verhoogd risico opleveren voor de rechten en vrijheden van betrokkenen. Wanneer sprake is van een verwerking met een waarschijnlijk hoog privacy risico voert SPIN voorafgaand aan de verwerking een Data Protection Impact Assessment (DPIA) uit. Het doel van een DPIA is om inzicht te krijgen in de aard, omvang, context en doeleinden van de verwerking en om vast te stellen welke risico’s bestaan voor betrokkenen en welke maatregelen noodzakelijk zijn om deze risico’s te beheersen.

Een DPIA wordt in ieder geval overwogen bij nieuwe systemen, omvangrijke wijzigingen in processen of systemen, nieuwe vormen van gegevensuitwisseling, grootschalige verwerking van persoonsgegevens, verwerking van bijzondere categorieën persoonsgegevens of het gebruik van nieuwe technologieën. Ook bij wijzigingen in wet- en regelgeving of veranderingen in de bedrijfsvoering wordt beoordeeld of een aanvullende DPIA noodzakelijk is.

Bij het uitvoeren van een DPIA beschrijft SPIN onder meer welke persoonsgegevens worden verwerkt, welke categorieën betrokkenen daarbij betrokken zijn, wat de doeleinden en wettelijke grondslagen van de verwerking zijn, welke systemen en processen worden gebruikt en welke risico's bestaan op het gebied van vertrouwelijkheid, integriteit, beschikbaarheid en rechtmatigheid van de verwerking. Daarnaast wordt beoordeeld welke technische en organisatorische maatregelen noodzakelijk zijn om de risico's voldoende te beperken.

De Privacy Officer ondersteunt de organisatie bij het uitvoeren van DPIA's en adviseert over de noodzaak, aanpak, en uitkomsten en periodieke herbeoordeling daarvan. Indien uit een DPIA blijkt dat sprake blijft van een hoog restrisico dat onvoldoende kan worden beperkt, wordt beoordeeld of overleg met de Autoriteit Persoonsgegevens noodzakelijk is voordat de verwerking wordt gestart. Een nadere toelichting over de noodzaak van DPIAs is opgenomen in bijlage 4.

SPIN beschikt daarnaast over procedures voor het beheersen van datalekken, cyberincidenten en continuïteitsverstoringen. Privacy-, IT- en continuïteitsincidenten worden geïntegreerd beoordeeld binnen het incidentmanagementproces van SPIN. Daarbij werken juridische zaken, IT, risicomanagement, de Privacy Officer en het crisismanagementteam samen om incidenten tijdig te detecteren, te beoordelen, te beheersen en te herstellen.

SPIN beschikt over een protocol meldplicht datalekken waarin de procedures voor het beoordelen en melden van een datalek zijn beschreven (Zie bijlage 3). Indien sprake is van een datalek dat risico's oplevert voor betrokkenen, wordt melding gedaan bij de Autoriteit Persoonsgegevens en indien noodzakelijk aan de betrokkenen zelf. Datalekken en cyberincidenten worden geregistreerd en geëvalueerd zodat structurele verbeteringen kunnen worden doorgevoerd in processen, systemen en beveiligingsmaatregelen.

11 Monitoring, audits en evaluatie

SPIN monitort de effectiviteit van het privacybeleid en de getroffen beheersmaatregelen. Privacy risico's maken onderdeel uit van de reguliere risicomanagementcyclus en worden meegenomen in rapportages aan bestuur en management.

De naleving van privacy- en informatiebeveiligingsmaatregelen wordt ondersteund door interne controles, awarenessprogramma's, audits, assurance-rapportages van leveranciers en periodieke evaluaties van processen en systemen. Waar nodig worden aanvullende maatregelen getroffen om risico's te beperken en de effectiviteit van beheersmaatregelen te verbeteren.

Het privacybeleid wordt minimaal eenmaal per drie jaar geëvalueerd en indien noodzakelijk aangepast naar aanleiding van wijzigingen in wet- en regelgeving, technologische ontwikkelingen, incidenten, uitkomsten van audits of veranderingen in de bedrijfsvoering van SPIN.

Dit Beleidsdocument treedt in werking op 10 november 2026

Aldus vastgesteld door het algemeen bestuur 10 november 2026 te Amstelveen.

Bijlage 1 RACI

In deze bijlage wordt een praktische invulling van de rollen en verantwoordelijkheden besproken in het complianceproces. Via het RACI-model (Responsible, Accountable, Consulted, Informed; zie uitleg onderaan) worden de verantwoordelijkheden en werkzaamheden per complianceproces aangegeven.

	Algemeen bestuur	Uitvoerend bestuur	NUB	Manager juridische zaken/ Privacy Officer	IT-manager	Risico-manager
Vaststellen privacybeleid	A	R	I	C	C/I	C
Vaststellen noodzaak DPIA		A		R	C	I
Uitvoeren privacybeleid		A		R	C	I
Toezicht op uitvoering privacy beleid			A	R	I	I
Vaststellen verwerkingsregister		A		R		I
Uitvoeren DPIA		A/R		C	C/I	I
Vaststellen privacyverklaring		A		R	C/I	I
Vaststellen procedure datalekken		A		C		C
Vaststellen datalek		A		R	I	C

Het model is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen die bij een project of lijnwerkzaamheden betrokken zijn weer te geven. In de matrix staan:
- op de horizontale as de namen van de personen of de functionele rollen, en
- op de verticale as de op te leveren resultaten, betrokken processen of activiteiten.

Het RACI-model staat voor:
- **R** (Responsible, NL: Verantwoordelijk)
  Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de actor die accountable is.
- **A** (Accountable, NL: Eindverantwoordelijk)
  Degene die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet de actor het eindoordeel kunnen vellen, vetorecht hebben. Er is slechts één actor Accountable.
- **C** (Consulted, NL: Geraadpleegd/Geadviseerd)
  Degene die (mede) richting geeft aan het resultaat, deze actor wordt voorafgaand aan beslissingen of acties geraadpleegd. Dit is tweerichtingscommunicatie.
- **I** (Informed, NL: Geïnformeerd)
- Degene die geïnformeerd wordt over onder andere de beslissingen, de voortgang en bereikte resultaten. Dit is éénrichtingscommunicatie.

Bijlage 2 Begrippen

Persoonsgegeven
Alle informatie over een geïdentificeerde of identificeerbare levende natuurlijke persoon (de Betrokkene) aan de hand een (online) identificator zoals een naam, een identificatienummer, locatiegegevens, of van één of meerdere elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Betrokkene(n)
Degene op wie een Persoonsgegeven(s) betrekking heeft/hebben zoals (gewezen) deelnemer, pensioengerechtigde of andere aanspraakgerechtigde (onder andere nabestaande).

Verwerkingsverantwoordelijke
Een natuurlijk persoon, of rechtspersoon, overheidsinstantie, een dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt. Dit is SPIN.

Verwerker
Eenieder die ten behoeve van en in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking
Elke bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen wissen of vernietigen van Persoonsgegevens.

Bijlage 3 Protocol Datalekken

1. Achtergrond

SPIN hecht grote waarde aan adequate beveiliging van haar data en heeft hier dan ook passende organisatorische maatregelen voor getroffen. Toch kan het voorkomen dat er een datalek optreedt bij SPIN of bij één van haar uitvoerders.

De meldplicht voor datalekken houdt in dat SPIN direct een melding moet doen bij de Autoriteit Persoonsgegevens indien er sprake is van een datalek, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Er dient tevens een melding te worden gedaan aan de betrokkene(n) wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Betrokkenen zijn de mensen van wie de persoonsgegevens zijn gelekt (bijvoorbeeld deelnemers of personeelsleden).

2. Wat is een datalek?

Een datalek is een inbreuk op de beveiliging die per ongeluk of onrechtmatig leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens. Mogelijke voorbeelden van datalekken zijn: een kwijtgeraakte laptop met persoonsgegevens, inbraak in een databestand of het versturen van een pensioenopgave naar de verkeerde deelnemer.

De meldplicht geldt bij een datalek, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een datalek kan zowel kwantitatief ernstig zijn (hoeveelheid data) als kwalitatief ernstig (gevoeligheid van gegevens).

3. Procedure melden datalekken SPIN

De verantwoordelijke voor het proces van melden van datalekken is de Manager Juridische Zaken. Alle mogelijke datalekken dienen dan ook initieel gemeld te worden bij de Manager Juridische Zaken met een kopie naar de Risicomanager en het Uitvoerend Bestuur.

Een melding doorloopt de volgende stappen:

1. Melding potentieel datalek bij de Manager Juridische Zaken.
2. Beoordeling door de Manager Juridische Zaken of er daadwerkelijk sprake is van datalek en of melding gedaan moet worden bij de Autoriteit Persoonsgegevens (art. 33 AVG). Bij twijfel wordt er contact gezocht met de Autoriteit Persoonsgegevens.
3. De beoordeling wordt geaccordeerd door een lid van het Uitvoerend Bestuur. De melding wordt zonder vertraging en zo mogelijk niet later dan 72 uur na ontdekking gedaan.[1]
4. Indien er sprake is van een datalek wordt door de Manager Juridische Zaken beoordeeld of het datalek bij de betrokkene gemeld moet worden (zie artikel 34 AVG).
5. Door de Manager Juridische Zaken wordt in samenspraak met de Risicomanager onderzocht of er maatregelen genomen moeten worden om gevolgen van het datalek te beperken.
6. In samenspraak met de Risicomanager wordt onderzocht of procedures aangepast moeten worden om nieuwe lekken te voorkomen.
7. De Risicomanager neemt het datalek op in het incidentenregister (zie artikel 33.5 AVG) en rapporteert het incident.
8. Indien een datalek gemeld is dan wordt een overzicht hiervan bewaard in de administratie. Dit overzicht bevat de feiten en gegevens van het datalek (oorzaak datalek, soort gegevens die gelekt zijn, het moment van ontdekking van het datalek, op welke wijze het datalek gedicht is, de melding aan de betrokkene e.d.).

4. Datalekken bij uitvoerders

Een datalek kan zich ook voordoen bij een partij aan wie SPIN zaken heeft uitbesteed. Met deze partijen, zijn afspraken gemaakt over hoe om te gaan met datalekken. SPIN heeft vastgesteld dat de uitvoerders procedures hebben opgesteld om te voldoen aan de wet rondom datalekken en dat de verantwoordelijkheden benoemd zijn binnen deze organisaties. Uitgangspunt blijft dat SPIN verantwoordelijk is voor het melden van datalekken.

[1] *Bij grootschalige datalekken met grote impact kan overwogen worden het bestuur te informeren.*

Bijlage 4 Data Protection Impact Assessment

Met een DPIA kan aangetoond worden dat bij hoog risicoverwerkingen aan de wet voldaan wordt. Een DPIA is een proces dat is gemaakt om een verwerking te omschrijven, de noodzakelijkheid en evenredigheid van een verwerking te onderzoeken en de risico's voor rechten en vrijheden van betrokkenen te managen (door deze te onderzoeken en passende maatregelen te bepalen).

Een DPIA is alleen verplicht als gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. De AVG noemt drie omstandigheden waarbij een DPIA verplicht is:

- systematisch en uitvoerig persoonlijke aspecten evalueren, waaronder profiling;
- op grote schaal bijzondere persoonsgegevens verwerken;
- op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Naast de drie situaties in de AVG genoemde situaties de geeft de AVG geen limitatief overzicht van verwerkingen met een hoog risico. De beoordeling vindt risico gebaseerd plaats. De geldende lijst van de Autoriteit Persoonsgegevens met verwerkingen waarvoor een DPIA verplicht is, is altijd leidend. Daarnaast gebruikt SPIN de negen criteria van de Europese privacytoezichthouders als hulpmiddel. In de regel wijst een verwerking die aan twee of meer criteria voldoet op een waarschijnlijk hoog risico en daarmee op de noodzaak van een DPIA. Afhankelijk van aard, omvang, context en doel van de verwerking kan ook één criterium voldoende zijn. Indien SPIN gemotiveerd besluit dat ondanks één of meer criteria geen DPIA nodig is, wordt deze afweging schriftelijk vastgelegd.

Aan hoe meer criteria de verwerking voldoet, hoe waarschijnlijker het is dat deze een hoog risico oplevert (en een DPIA verplicht is):

1. Beoordelen of scoren van betrokkenen. Veelal op basis van persoonskenmerken (waaronder profileren). Zoals kredietwaardigheidsscores, klantbeeld op websites;
2. Geautomatiseerde beslissingen;
3. Stelselmatige (en grootschalige) monitoring van openbaar toegankelijke ruimten;
4. Gevoelige gegevens verwerken;
5. Grootschalige gegevensverwerkingen: gezien de hoeveelheid betrokkenen, gegevens, tijdsduur en/of geografische reikwijdte;
6. Het koppelen van databases/ datasets: koppelen of combineren van persoonsgegevens afkomstig uit verschillende gegevensverwerkingen met andere doelen en/of andere verantwoordelijken;
7. Gegevens over kwetsbare personen;
8. Gebruik van nieuwe technologieën;
9. Blokkering van een recht, dienst of contract: gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

Bij projecten en materiële wijzigingen wordt altijd getoetst of een DPIA noodzakelijk dan wel wenselijk is. Bij twijfel wordt een DPIA uitgevoerd, omdat dit proces helpt om risico's systematisch in kaart te brengen en de aantoonbaarheid van naleving van de AVG te versterken. De AP heeft op basis van deze criteria een aanvullende lijst opgesteld van gegevensverwerkingen waarvoor een DPIA verplicht is:

1. Heimelijk onderzoek
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. Cameratoezicht
10. Flexibel cameratoezicht
11. Controle werknemers
12. Locatie gegevens
13. Communicatiegegevens
14. Internet of things
15. Profilering
16. Observatie en beïnvloeding van gedrag
17. Biometrische gegevens.

Bijlage 5 Bewaartermijnen

Voor bewaartermijnen wordt aansluiting gezocht bij wet- en regelgeving en het servicedocument bewaartermijnen van de Pensioenfederatie. Uitgangspunt is dat persoonsgegevens niet langer worden bewaard dan nodig is voor het doel waarvoor we ze verwerken. Hieronder is per gegevens categorie de bijbehorende bewaartermijn toegelicht. De termijnen worden bij herziening van het privacybeleid getoetst.

Voor het bewaren van persoonsgegevens van (gewezen) deelnemers, nabestaanden en pensioengerechtigden hanteert SPIN de volgende bewaartermijnen:

- 50 jaar na het eindigen van de deelnemersrelatie door afkoop of waardeoverdracht wanneer er geen sprake is van andere mogelijke aanspraak- of pensioengerechtigden, dan wel
- 50 jaar na het overlijden van alle aanspraak- en pensioengerechtigden of na het realistisch te bepalen vermoedelijke overlijden (bij niet-opgevraagde pensioenen) van alle mogelijke aanspraak- en pensioengerechtigden terzake een bepaald pensioenrecht of -aanspraak.

Voor wat betreft de bewaartermijnen van persoonsgegevens van sollicitanten en (voormalig) werknemers:
Sollicitanten:

- 4 weken na einde sollicitatieprocedure, tenzij anders overeengekomen, tot maximaal 1 jaar na einde sollicitatieprocedure.

Werknemers:

- Personeelsdossiers (aanstellingsdocumenten, loonbelastingverklaringen, kopie ID, gegevens over ziekteverzuim, correspondentie met financiële consequenties): in beginsel 5 jaar na einde dienstverband
- Overige documenten 2 jaar
- Niet-essentiële correspondentie wordt bij uitdiensttreding verwijderd
- Voor zover ziek uit dienst met een ZW of WIA-uitkering gedurende vijf jaar nadat de betrokkenheid/verantwoordelijkheid van de werkgever is geëindigd.

Voor wat betreft de bewaartermijn van gegevens van bestuursleden, leden van het verantwoordingsorgaan en externe leden van commissies (voor zover niet via een onderneming ingeschakeld):

- Bestuursleden en leden verantwoordingsorgaan (VO): afhankelijk van de gegevens minimaal 7 jaar na einde lidmaatschap (mede in verband met vergoedingen/administratieplicht stichting), kopie ID bewijs 7 jaar.
- Aspirant of afgewezen leden van bestuur en VO: twee jaar na afwijzing (i.v.m. verantwoordingsplicht) dan wel na afloop van de beoogde zittingstermijn na verkiezingen i.v.m. het mogelijk opvullen van tussentijdse vacatures.
- Externe leden van commissies voor een periode van 1 tot 7 jaar afhankelijk van de aard van de relatie.

Bijlage 6 Privacyverklaring

Stichting Pensioenfonds IBM Nederland verzamelt en verwerkt persoonsgegevens. Niet alleen om de pensioenovereenkomst goed uit te kunnen voeren, maar ook om te voldoen aan wettelijke en contractuele verplichtingen en om onze diensten te kunnen verbeteren. Contractuele bepalingen brengen mee dat wij hiervoor gegevens van u en van andere partijen moeten ontvangen. Wij verwerken de gegevens van (gewezen) deelnemers, (gewezen) partners, wezen, pensioengerechtigden, hun wettelijk vertegenwoordigers en de aangesloten werkgevers.

Wij gaan zorgvuldig om met uw gegevens. Wij zorgen dat we niet meer gegevens verzamelen dan nodig en dat onbevoegden geen toegang hebben tot gegevens. Wij hebben passende technische en organisatorische maatregelen getroffen om uw persoonsgegevens te beveiligen tegen diefstal, verlies of onrechtmatig gebruik. Wij zijn open en duidelijk over wat we doen en maken het voor u eenvoudig om uw gegevens in te zien en aan te passen. Wij werken niet op basis van geautomatiseerde besluitvorming.

Afhankelijk van uw situatie kunnen wij van de volgende partijen gegevens over u en/of uw dienstverband ontvangen:
- Basisregistratie Personen (BRP)
- (Voormalige) werkgever(s)
- Uitvoeringsinstituut Werknemersverzekeringen (UWV)
- Kamer van Koophandel (KvK)
- Andere pensioenuitvoerders
- U zelf
- Belastingdienst
- Het CAK
- Een door u ingeschakelde financiële planner
- Deurwaarders en andere gerechtelijke instanties die vorderingen op deelnemers beheren.

Wij kunnen de volgende (bijzondere) (persoons)gegevens verwerken:
- Voor- en achternamen
- Geslacht
- Geboortedatum
- Burgerservicenummer (BSN)
- Adresgegevens
- Telefoonnummer
- E-mailadres
- Pensioennummer
- Bankrekeningnummer
- Burgerlijke staat
- Gegevens over uw (voormalige) dienstverband(en)
- Salaris
- Aanspraken / pensioenrecht
- Indicatie gemoedsbezwaard
- Gegevens uit identiteitsdocumenten zoals het documentnummer of biometrische gegevens.
- Gegevens over arbeidsongeschiktheid
- Gegevens over uw kinderen
- Overige (persoons)gegevens die u actief verstrekt digitaal, in correspondentie en telefonisch
- IP-adres
- Internetbrowser en apparaat type
- Gegevens over uw activiteiten op onze website
- Voorkeurstaal
- Opname van telefoongesprekken van klantcontactmomenten
- Handtekening
- Bewijs van in leven/attest de vita
- Beleggingsprofiel/risicoprofiel

Waarom we uw gegevens nodig hebben
Stichting Pensioenfonds IBM Nederland is contractueel verplicht om de pensioenovereenkomst uit te voeren. Om dit op de juiste wijze te kunnen doen verwerken we uw (persoons)gegevens voor de volgende doelen:
- Vaststellen van de hoogte van en uitbetaling van pensioenaanspraken en -uitkeringen
- Berekenen, vastleggen en innen van premies
- Behandelen van klachten, geschillen of juridische procedures
- Voorkoming van fraude
- Statistische analyses

- Adequate communicatie met u

Delen met andere partijen

Stichting Pensioenfonds IBM Nederland 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. Deze partijen mogen alleen voor de afgesproken doeleinden uw persoonsgegevens verwerken en alleen in overeenstemming met de wet en onze uitdrukkelijke instructies. Op die manier zorgen wij voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Stichting Pensioenfonds IBM Nederland blijft verantwoordelijk voor deze verwerkingen. Stichting Pensioenfonds IBM Nederland verwerkt uw gegevens uitsluitend buiten de Europese Economische Ruimte indien daarvoor een geldige wettelijke grondslag bestaat en passende waarborgen zijn getroffen.

De uitvoering van de pensioenadministratie doet Stichting Pensioenfonds IBM Nederland zelf, met ondersteuning van ICT-, print-, post-, beheer- en andere dienstverleners. Uw gegevens worden daarvoor intern verstrekt aan medewerkers van het pensioenfonds. Leveranciers kunnen onder toezicht en verantwoordelijkheid van SPIN toegang hebben tot persoonsgegevens voor zover dat noodzakelijk is voor hun dienstverlening. Voor deze dienstverlening worden passende contractuele en beveiligingsafspraken gemaakt.
Naast bovenstaande dienstverleners is het mogelijk dat we (incidenteel)gegevens verstrekken aan andere dienstverleners. Al deze diensten staan in het teken van de uitvoering en verbetering van onze taak als pensioenuitvoerder. Daarbij hanteren wij geen commerciële doelstelling.
De partijen waarmee uw (persoons)gegevens gedeeld kunnen worden, zijn onder te verdelen in de volgende categorieën:

- Toezichthouders, zoals de Nederlandse Bank en de AFM
- Overheidsinstanties, zoals de belastingdienst, een gemeente, politie/justitie, CBS, rechterlijke macht
- Uitkeringsinstanties, zoals UWV
- 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 assurance doeleinden
- Ombudsman pensioenen
- Geschilleninstantie Pensioenfondsen
- Andere pensioenuitvoerders en de stichting pensioenregister

Hoe lang we uw gegevens bewaren

Stichting Pensioenfonds IBM Nederland bewaart uw persoonsgegevens niet langer dan strikt nodig is en binnen de wettelijke bepalingen om de doelen te realiseren waarvoor ze zijn verzameld. Omdat we te maken hebben met langlopende pensioenverplichtingen kan dat een hele lange periode zijn. We bewaren de persoonsgegevens die nodig zijn voor het uitvoeren van de pensioenovereenkomst in ieder geval totdat 50jaar zijn verstreken na het einde van uw recht op pensioen. Als wij uw gegevens niet meer nodig hebben, dan verwijderen, anonimiseren of beperken wij de gegevens.

Opnemen van telefoongesprekken

Stichting Pensioenfonds IBM Nederland kan telefoongesprekken opnemen. Deze opnames worden onder andere gebruikt voor trainings- en coachingsdoeleinden, maar ook voor onderzoek naar verdachte opdrachten en transacties of voor de bestrijding van fraude. De opgenomen telefoongesprekken worden niet langer bewaard dan noodzakelijk is voor bovenstaande doeleinden. Binnen de bewaartermijn heeft u recht op een weergave van het telefoongesprek.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien en aan te passen (corrigeren). In bepaalde gevallen kunt u ons daarnaast vragen om de verwerking van uw persoonsgegevens te beperken, uw gegevens te wissen of om uw gegevens over te dragen aan een andere zogenoemde verwerkingsverantwoordelijke.

Intrekken toestemming
Om uw pensioenregeling goed uit te kunnen voeren hebben wij bepaalde persoonsgegevens uiteraard nodig. Maar dit geldt niet voor alle gegevens die wij verwerken. U kunt ons daarom vragen om uw gegevens voor bepaalde situaties niet meer te gebruiken. Als u bijvoorbeeld niet wilt dat wij u bellen of e-mailen of als u een belangrijke persoonlijke reden heeft waarom u niet wilt dat wij uw gegevens gebruiken.

U kunt een verzoek tot inzage, correctie, beperking, verwijdering of overdracht sturen naar info@spin.nl. Dit e-mailadres kunt u ook gebruiken om uw toestemming voor het gebruik van uw persoonsgegevens in te trekken. Om er zeker van te zijn dat het verzoek door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs bij het verzoek mee te sturen. Zorg ervoor dat op deze kopie de pasfoto en het Burgerservicenummer (BSN) en MRZ code onherkenbaar zijn gemaakt. Dit ter bescherming van uw privacy. Stichting Pensioenfonds IBM Nederland zal zo snel mogelijk, maar uiterlijk binnen een maand, op uw verzoek reageren.

Klachtrecht
Als Stichting Pensioenfonds IBM Nederland niet voldoet aan uw verzoek tot inzage, correctie, beperking, verwijdering of overdracht van uw persoonsgegevens, dan kunt u hierover een klacht indienen bij de Autoriteit Persoonsgegevens. Mocht uw klacht niet naar tevredenheid worden opgelost, dan kunt u hiertegen in beroep te gaan bij de rechter.

Beveiliging
Stichting Pensioenfonds IBM Nederland neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging ervan tegen te gaan. Als u het idee heeft dat uw gegevens toch niet goed beveiligd zijn of dat er aanwijzingen zijn van misbruik, neem dan contact met ons op.

Links
Onze website bevat links naar andere websites. Deze privacyverklaring heeft geen betrekking op de gelinkte websites. Lees daarvoor de privacyverklaring van de gelinkte website.

Contact
U kunt ons en onze Privacy Officer bereiken via:

Website: www.spin.nl
Telefoonnummer: 020-3472722
E-mailadres: info@spin.nl
Postadres: Stichting Pensioenfonds IBM Nederland
Postbus 342
1180 AH AMSTELVEEN

Cookies
Stichting Pensioenfonds IBM Nederland maakt gebruik van cookies. Een cookie is een tekstbestandje dat op uw computer, tablet of mobiele telefoon wordt geplaatst als u de site raadpleegt. Cookies vergemakkelijken en versnellen het gebruik van de site. Lees meer over cookies in onze cookieverklaring.

Wijzigingen privacyverklaring voorbehouden
Stichting Pensioenfonds IBM Nederland behoudt zich het recht voor de privacyverklaring te wijzigen. Elke verandering wordt op deze pagina gepubliceerd. Wij raden u daarom aan om deze privacyverklaring regelmatig te lezen. Deze pagina is het laatst opgemaakt op 10 oktober 2026.

Cookieverklaring

Stichting Pensioenfonds IBM Nederland (SPIN) maakt voor haar publiek toegankelijke website www.spin.nl gebruik van cookies.

Cookies zijn kleine tekstbestandjes die op uw computer, tablet of mobiele telefoon worden geplaatst als u de site raadpleegt met daarin gegevens die wij over u hebben verzameld. Cookies vergemakkelijken en versnellen uw gebruik van de site. Cookies geven ons geen toegang tot uw computer. Wij vinden een zorgvuldige omgang met persoonsgegevens van groot belang. Persoonsgegevens worden door ons dan ook zorgvuldig verwerkt en beveiligd.

Doeleinden van de cookies

Via onze website plaatsen wij functionele en analytische cookies. Deze cookies worden voor verschillende doeleinden geplaatst. Functionele cookies zijn voor het functioneren van de site noodzakelijk. Deze cookies maken het bijvoorbeeld mogelijk dat u een taal kunt kiezen, contact met ons kunt opnemen en kunt inloggen in de mijn omgeving. Deze cookies

worden geplaatst door WordPress. SPIN is de verwerkingsverantwoordelijke voor de gegevensverwerking. WordPress is echter de feitelijk verwerkende partij.

Aanvullend op de functionele cookies, plaatsen wij ook analytische cookies. Analytische cookies vertellen ons onder meer in algemene zin hoeveel bezoekers er op de website komen en welke pagina's het meest worden bekeken. Deze informatie is nooit op u als individuele bezoeker terug te herleiden. Wij gebruiken deze statistieken alleen om te zien of de onderwerpen die wij belangrijk vinden ook wel voldoende worden herkend en bezocht.

Onze analytische cookies hebben wij privacyvriendelijk ingesteld. Dat betekent dat de gegevens alleen worden gebruikt voor geaggregeerde statistieken, niet worden gebruikt voor commerciële tracking of profilering en niet worden ingezet om individuele bezoekers te volgen. Voor zover analytische cookies geringe gevolgen hebben voor de persoonlijke levenssfeer, plaatsen wij deze op basis van ons gerechtvaardigd belang om de website goed te laten functioneren en te verbeteren.
Onderstaand treft u een overzicht aan van de analytische cookies die wij via uw browser op uw computer plaatsen:

Dienst	Soort doel	Type/naam	Bewaartermijn
Google Analytics	Analytisch	_ga	26 maanden
Google Analytiscs	Analytisch	_gat	Huidige sessie
Google Analytics	Analytisch	_gat	1 dag
Google Tag Manager	Analytisch	force current session	Huidige sessie
Google Tag Manager	Analytisch	force current user	1,5 maand
Google Tag Manager	Analytisch	force current day	Huidige sessie

In- en uitschakelen van cookies

Functionele en analytische cookies plaatsen wij automatisch via uw browser op uw computer. Voor het plaatsen van deze cookies hoeven wij geen toestemming van u te vragen, omdat wij hiervoor een gerechtvaardigd belang hebben en deze privacy vriendelijk zijn ingesteld. We zetten ze niet in vanuit een commercieel belang.

U kunt cookies via uw internetbrowser handmatig verwijderen of deze automatisch laten verwijderen wanneer u de website verlaat. Daarnaast kunt u uw internetbrowser zo instellen dat u een bericht krijgt als er een cookie wordt geplaatst. U kunt uw browser ook zo instellen dat cookies niet geplaatst mogen worden.

Indien u niet wilt dat wij cookies zonder uw toestemming op uw computer plaatsen, dan kunt u dit eenvoudig instellen in uw browser. Raadpleeg voor meer informatie de handleiding van uw webbrowser. Let op: het kan zijn dat de website niet naar behoren functioneert wanneer u de cookies heeft uitgeschakeld.

Categorieën van ontvangers

Sommige werkzaamheden besteden wij uit aan derde partijen. Deze derde partijen zijn zowel binnen als buiten de Europese Economische Ruimte gevestigd.

Contact

U kunt meer lezen over hoe wij met uw privacy omgaan in onze Privacyverklaring. Voor vragen over ons cookiebeleid of vragen omtrent inzage, verbetering, aanvulling, wijziging, afscherming, verwijdering of overdracht van uw persoonsgegevens kunt u te allen tijde contact met ons opnemen via onderstaande gegevens:

Telefoonnummer: 020-347 2722
E-mailadres: info@spin.nl
Bezoekadres: Van Heuven Goedhartlaan 121, Amstelveen
Postadres: Postbus 342 1180 AH Amstelveen