



Stichting Pensioenfonds van de KAS BANK

Beleid bescherming persoonsgegevens

Disclaimer

De meest recente en goedgekeurde versie van deze regeling staat in de folderstructuur van het pensioenfonds in de folder Beleidsdocumenten/ Privacybeleid.

Wees erop attent dat geprinte documenten snel verouderd kunnen zijn.

Copyright

Alle informatie en afbeeldingen uit dit beleidsdocument staan onder copyright en zijn eigendom van Stichting Pensioenfonds van de KAS BANK (hierna SPKB) tenzij anders aangegeven. Dit beleid is enkel bedoeld voor intern gebruik door betrokkenen bij SPKB.

Geen enkele informatie of afbeelding uit dit beleid mag worden gekopieerd, gereproduceerd, gepubliceerd, gedownload of verspreid in zijn geheel of gedeeltelijk naar een persoon of organisatie buiten SPKB. Uitzondering hierop bestaat indien vooraf per e-mail of anders schriftelijke toestemming is gegeven door het bestuur van SPKB.

Documentbeheer

Naam	Beleid bescherming persoonsgegevens Stichting Pensioenfonds van de KAS BANK
Versie	3.1
Vindplaats	I-schijf SPKB folder Implementatie GDPR
Uitgiftedatum	Initiële uitgifte datum 26 oktober 2018, nieuwe uitgifte 27 juni 2025
Taal	Nederlands
Gelieerde documenten	Privacy Statement

Eigenaar
SPKB

Toepassingsgebied
Alle vestigingen – alle functies

Betrokken afdelingen

Afdeling	Verantwoorde- lijke manager	Vertegenwoordigd door	Status	Datum
Compliance	Frank Lurling	Saskia Doekhie	Beleids voorbereider	22 juli 2018
DPO SPKB	Peter van der Knaap		SPKB specifieke aanpassingen uitgevoerd	25 oktober 2018
DPO SPKB	Peter van der Knaap		Periodieke evaluatie	22 september 2021
DPO SPKB	Daphny Batstra p/o Peter van der Knaap		Periodieke evaluatie	11 september 2023
Compliance	Compliance team AethiQs	Marlou Heijs	Evaluatie	11 november 2024
Compliance	Compliance team AethiQs	Marlou Heijs	Jaarlijkse evaluatie	19 juni 2025

Goedkeuringen

		Versie	Datum	
Bestuur SPKB	☒ Yes ☐ No	3.0	22 november 2024	
Bestuur SPKB	☒ Yes ☐ No	3.1	27 juni 2025	

Inhoudsopgave

Inhoudsopgave	4
1 Introductie.....	6
1.1 Achtergrond.....	6
1.2 Doelstelling	6
1.3 Afbakening, reikwijdte en toepassingsgebied	7
1.4 Context/afhankelijkheid.....	7
1.4.1 Gelinkt beleid	7
1.4.2 Gelinkte administratieve en organisatieprocessen	7
2 Definities	8
3 Governance	11
3.1 Three lines model	11
3.1.1 Eerstelijns management.....	11
3.1.2 Tweedelijns management.....	12
3.1.3 Derdelijk.....	12
3.2 Beginselen voor verwerking	12
3.3 Verantwoordingsplicht.....	13
3.4 Legitieme gegevensverwerking	13
3.5 Verwerking voor andere doelen	14
3.6 Toestemming van betrokkene	15
3.7 Noodzakelijk voor de uitvoering van een overeenkomst.....	16
3.8 Noodzakelijk om te voldoen aan een wettelijke plicht.....	16
3.9 Noodzakelijk voor de behartiging van het gerechtvaardigde belang.....	16
3.10 Verwerking van bijzondere categorieën van persoonsgegevens	16
3.10.1 Verwerking van persoonsgegevens over ras en etnische afkomst.....	17
3.11 Verwerking van persoonsgegevens van betrokkenen.....	17
3.12 Rechten van betrokkenen	17
3.12.1 Standaardformulier en reactietermijn	18
3.13 Informatieplicht naar betrokkenen	18
3.14 Registerplicht.....	19
3.15 Verwerkersovereenkomst	19
3.16 Bewaartermijn	19
3.17 Speciale onderwerpen	19
4 Minimum Standaarden.....	23

5	Monitoring	23
6	Goedkeuringsproces	23
7	Herziening van beleid	23
8	Afwijken van beleid	24
9	Schenden van beleid	24
10	Inwerkingtreding	24

1 Introductie

In dit beleid worden de basisprincipes en maatregelen beschreven met betrekking tot de opslag, de verwerking en beveiliging van persoonsgegevens.

Met de vastlegging van dit beleid neemt SPKB haar verantwoordelijkheid om een rechtmatige en zorgvuldige omgang met persoonsgegevens te waarborgen dit in lijn met de verplichtingen uit de Algemene Verordening Gegevensbescherming (hierna ook: AVG), wet- en regelgeving en richtlijnen.

Alle betrokkenen binnen SPKB (bestuur, leden SPKB commissies, verantwoordingsorgaan en medewerker SPKB) worden geacht dit beleid en de bijbehorende procedures na te leven om zodoende de risico's met betrekking tot de verwerking van persoonsgegevens te minimaliseren.

1.1 Achtergrond

Het Pensioenfonds van de KAS BANK voert de pensioenregeling uit van CACEIS. Dat betekent onder meer dat het Pensioenfonds van de KAS BANK verantwoordelijk is voor het beleggen van de pensioenpremies die de werkgever en werknemers inleggen. Maar ook dat zij verantwoordelijk is voor het op tijd en correct communiceren en voor het uitbetalen van alle pensioenen.

Het pensioenfonds is een onafhankelijke stichting die wordt bestuurd door (oud) medewerkers van CACEIS Bank Netherlands branch (hierna CACEIS) en namens de gepensioneerde een collega die met pensioen gegaan is. Vanaf 1 mei 2023 is SPKB een gesloten fonds. Op enkele arbeidsongeschikte deelnemers na, zijn alle deelnemers per die datum inactief. Voor de wijze waarop met de gegevensbescherming van deze deelnemers wordt ingegaan, heeft het zijn van een gesloten fonds geen invloed.

1.2 Doelstelling

SPKB wil met dit beleid de privacyrisico's met betrekking tot de opslag en de verwerking van persoonsgegevens binnen haar bedrijfsprocessen juist, tijdig en volledig beheersen. Door het nemen van passende en effectieve maatregelen in lijn met het vastgestelde risico van de verwerking wil SPKB misbruik en ongeautoriseerd gebruik van de haar toevertrouwde persoonsgegevens voorkomen.

Overige doelstellingen van het beleid zijn:

- Een omschrijving van de categorieën persoonsgegevens die het fonds verwerkt
- kaders beschrijven om de risico's met betrekking tot de verwerking van persoonsgegevens te beheersen om zodoende een passend beschermingsniveau te bewerkstelligen;
- de gerechtvaardigde bedrijfsdoeleinden benoemen, waarvoor persoonsgegevens mogen worden verwerkt;
- de wijze waarop wordt voldaan aan de beginselen van verwerking van persoonsgegevens
- de taken en verantwoordelijkheden van afdelingen die persoonsgegevens verwerken benoemen;
- alle medewerkers belast met de verwerking van persoonsgegevens te informeren over: de verantwoorde verwerking van persoonsgegevens, de risico's met betrekking tot het verlies van persoonsgegevens en situaties waarin er mogelijk sprake is van een onrechtmatige verwerking van persoonsgegevens;
- De privacyrechten die betrokkenen van het fonds hebben en hoe zij die rechten uit kunnen oefenen.
- de kaders van voor de Privacy Statement voor op de internet website te beschrijven.

1.3 Afbakening, reikwijdte en toepassingsgebied

Dit privacybeleid is van toepassing op de verwerking van persoonsgegevens door SPKB als onderdeel van haar dienstverlening. SPKB heeft onderdelen van haar operationele processen van uitbesteed, de belangrijkste uitbestedingsrelatie is met AZL de pensioenuitvoerder en de vermogensbeheerders die in opdracht van SPKB handelen. SPKB steunt waar mogelijk op de architectuur, systemen, processen en beleidsdocumenten van haar externe partijen. De externe partijen moeten voldoen aan de normen van SPKB. Met de externe partijen worden door SPKB verwerkersovereenkomsten overeengekomen.

Dit beleid ziet toe op de verwerking van persoonsgegevens zoals geregeld en voortvloeiend uit de:

- Algemene Verordening Gegevensbescherming;
- Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Gedragslijn Verwerking Persoonsgegevens Pensioenfederatie.

Dit beleid is van toepassing op alle betrokkenen bij SPKB.

Dit beleid ziet toe op de volgende verwerkingen van persoonsgegevens:

- de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens en
- de handmatige verwerking van persoonsgegevens die in een bestand (kan ook een fysieke verzameling van gestructureerde gegevens betreffen) zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Onder dit beleid valt onder andere, de verwerking van persoonsgegevens van:

- deelnemers aan de pensioenregeling van CACEIS die voor 1 november 2020 in dienst gekomen zijn via SPKB, zowel de actieven als de niet actieven.
- gepensioneerden.
- Andere betrokkenen (Bestuur, commissieleden, verantwoordingsorgaan).

1.4 Context/afhankelijkheid

1.4.1 Gelinkt beleid

Ander relevant beleid en/of procedures voor het beheersen van risico's binnen SPKB zijn:

- Informatiebeveiligingsbeleid;
- het beleid aangaande het bewaren van data;
- en datakwaliteitbeleid.

1.4.2 Gelinkte administratieve en organisatieprocessen

SPKB heeft passende administratieve en organisatorische processen ingericht, waarmee de risico's gemitigeerd worden en de minimum standaarden uit dit beleid gewaarborgd kunnen worden.

In het kader van de verwerking van persoonsgegevens worden door onderstaande processen de volgende zaken gewaarborgd:

- Information Security Management, een adequate beveiliging van informatiesystemen;
- Access Management, een adequaat toegangsbeheer tot gegevens en informatie;
- Architecture Decision Making, een toets op het naleven van architectuur-principes en richtlijnen ingeval van veranderingen;
- Incident Management, het tijdig signaleren en oplossen van incidenten waaronder datalekken;

2 Definities

In het kader van dit beleid betekent:

AVG:

Algemene Verordening Gegevensbescherming

Beperken van de verwerking:

Het selecteren van opgeslagen persoonsgegevens met als doel de verwerking van deze persoonsgegevens te beperken;

Toelichting: Een betrokkene mag in bepaalde gevallen het recht van beperking van verwerking uitoefenen.

Bestand:

Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

Toelichting: Met een bestand wordt bedoeld een gestructureerd geheel van gegevens dat betrekking heeft op verschillende personen waarbij:

- de gegevens onderlinge samenhang moeten vertonen en
- het systeem systematisch toegankelijk moet zijn.

Dit is aan de orde bij de handmatige verwerking van persoonsgegevens die zijn opgenomen in een bestand of die na verwerking bestemd zijn om in een bestand te worden opgenomen. Een ongestructureerd handmatig dossier valt dus niet onder het begrip bestand.

Betrokkene:

Een natuurlijk persoon op wie de persoonsgegevens betrekking hebben, dan wel van wie bepaalde persoonsgegevens worden verwerkt.

Toelichting: een natuurlijk persoon is identificeerbaar, indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Bijzondere categorieën persoonsgegevens:

Gegevens waaruit:

- religieuze of levensbeschouwelijke overtuigingen;
- ras of etnische afkomst;
- politieke opvattingen;
- lidmaatschap van een vakbond blijkt en:
- genetische gegevens,
- biometrische gegevens met het oog op de unieke identificatie,
- gegevens over de gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Toelichting: Bijzondere categorieën persoonsgegevens zijn gegevens die gezien hun aard bijzonder gevoelig zijn. Verwerking hiervan kan voor een grote inbreuk op de privacy van de betrokken personen zorgen.

SPKB mag geen bijzondere persoonsgegevens verwerken, behalve als voor de verwerking er sprake is van een gerechtvaardigd belang.

Een inbreuk in verband met persoonsgegevens (datalek):

Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

EER:

Europese Economische Ruimte.

Toelichting: hiertoe behoren alle landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland.

Functionaris:

De Data Privacy Officer van SPKB.

Grensoverschrijdende verwerking:

Verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd of verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden.

Betrokkene:

Eenieder die in een bepaalde gezagsverhouding staat tot SPKB.

Minderjarige:

Natuurlijk persoon die de leeftijd van 18 jaar nog niet heeft bereikt.

Nationaal identificatienummer:

Een bij wet vastgesteld uniek nummer dat alleen gebruikt wordt voor in de wet voorgeschreven doelen. Hieronder valt ook het Burger Service Nummer (BSN), omdat het een uniek en tot de persoon herleidbaar nummer is.

Persoonsgegevens:

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Toelichting 1: als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

Voorbeelden van directe persoonsgegevens zijn:

- Voornaam, achternaam, adresgegevens, geboortedatum;
- Postcode en huisnummer;
- Identificatienummer;
- Telefoonnummers;
- Bankrekeningnummer in combinatie met de achternaam;
- Identificatiecookies;
- Internetprotocol (IP adres)

Toelichting 2: SPKB verwerkt geen persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten.

Privacy by design:

Al bij het ontwerpen van producten en diensten worden de persoonsgegevens goed beschermd.

Privacy default:

Technische en organisatorische maatregelen die genomen worden om ervoor te zorgen dat als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel.

Toestemming:

Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de betreffende verwerking van persoonsgegevens aanvaardt;

Toeziethouder:

Autoriteit Persoonsgegevens (AP).

Verwerker:

Degene, die ten behoeve van de verwerkersverantwoordelijke, persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Toelichting: Bij de verwerking van persoonsgegevens kan SPKB een verwerker inschakelen. De verwerker verwerkt uitsluitend in opdracht van SPKB de persoonsgegevens.

Verwerking van Persoonsgegevens:

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures.

Toelichting: In de praktijk kan een verwerking al snel een verwerking van persoonsgegevens zijn. Verwerkingen zijn in ieder geval het verzamelen, vastleggen, opslaan ordenen, structureren, 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.

Verwerkingsverantwoordelijke:

Een natuurlijke persoon of rechtspersoon, die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

Toelichting: Binnen dit beleid is SPKB de verwerkingsverantwoordelijke die 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. SPKB bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.

3 Governance

SPKB zal met het voldoen aan de vereisten uit IORP II gaan voldoen aan 'Three Lines model' (hierna: 3L), dat voortkomt uit het Risk Governance model. Binnen dit principe heeft iedere lijn haar eigen rol en verantwoordelijkheid. Dit hoofdstuk beschrijft het Three Lines principe en de verantwoordelijkheden van de afdelingen, die betrokken zijn bij de borging en uitvoering van dit beleid, onder meer de beginselen voor verwerking, hoe SPKB invulling geeft aan de verantwoordingsplicht, de rechten van betrokkenen en special onderwerpen.

Het Bestuur is eindverantwoordelijk voor de goede naleving van de AVG bij het verwerken van persoonsgegevens binnen de interne processen van SPKB.

3.1 Three lines model

Deze paragraaf beschrijft het Three Lines principe en de verantwoordelijkheden van de afdelingen, die betrokken zijn bij de borging en uitvoering van dit beleid.

3.1.1 Eerstelijns management

In het kader van het 3L, ligt bij het eerstelijnsmanagement (= het Bestuur) de verantwoordelijkheid voor het uitvoeren, naleven en de effectiviteit van dit beleid. Dit houdt onder meer in dat het management ervoor zorg draagt, dat de betrokkenen op de hoogte zijn van dit beleid en dat dit beleid op de juiste wijze wordt geïmplementeerd en geborgd.

Het eerstelijnsmanagement is als eigenaar van de bedrijfsprocessen verantwoordelijk voor de implementatie en naleving van de minimum standaarden van dit beleid in de bedrijfsprocessen.

Data Privacy Officer

De Data Privacy Officer (hierna: DPO) vervult een onafhankelijke toezichthoudende positie binnen SPKB. De DPO mag in het kader van de uitoefening van de controlebevoegdheden - indien relevant - ruimtes betreden, inzage vragen in dossiers en inlichtingen opvragen. SPKB stelt de DPO in de gelegenheid zijn taak naar behoren te vervullen en ziet erop toe dat de DPO geen nadeel ondervindt in de uitoefening van zijn taak. De Data Privacy Officer rapporteert aan het Bestuur.

De Data Privacy Officer is binnen SPKB in ieder geval verantwoordelijk voor:

- informeren en advisering van SPKB over de verplichtingen waaraan SPKB moet voldoen;
- het verzamelen van informatie om de verwerkingsactiviteiten te identificeren, te analyseren en te beoordelen;
- advisering over de noodzakelijkheid van de uitvoering van een Privacy Impact Assessment of gegevensbeschermingseffectbeoordeling en ziet toe op de uitvoering daarvan;
- het opstellen en herzien van het informatiebeveiligingsbeleid;
- de inventarisatie van de categorieën persoonsgegevensverwerkingen binnen SPKB;
- de controle van de inventarisatie van de automatiseringssystemen, waarin persoonsgegevensverwerkingen plaatsvinden;
- het bijhouden van een register waarin de persoonsgegevensverwerkingen worden geregistreerd;

- het opstellen van interne procedures met betrekking tot de verwerking van persoonsgegevens;
- de advisering over technologie en beveiliging, waaronder voorlichting over Privacy by Default en Privacy by Design;
- het verrichten van meldingen in het kader van de Meldplicht Datalekken aan de toezichthouder.

De Data Privacy Officer vervult een vraagbaakfunctie bij vragen en klachten van de business, medewerkers, leveranciers en klanten en treedt op als contactpersoon voor de toezichthouder. Hij kan aanbevelingen doen aan het Bestuur van SPKB in het kader van de beveiliging van de persoonsgegevens.

3.1.2 Tweedelijns management

Tot de tweede lijn behoren de (sleutel)functies Risicobeheer, Compliance en Actuarieel die toezien op het Financial en Non Financial Risk Management binnen SPKB.

Deze personen zijn medeverantwoordelijk voor:

- de advisering over de wet- en regelgeving op het gebied van bescherming van persoonsgegevens;
- de voorbereiding van intern beleid op basis van de wet- en regelgeving.
- de ondersteuning van de beleidsverantwoordelijke afdeling bij de uitvoering van het beleid;
- de monitoring van de uitvoering van het beleid door de eerste lijn;
- de beheersing van integriteitsrisico's op het gebied van bescherming van persoonsgegevens.
- assisteren bij het vergroten van de bewustwording op het gebied van bescherming van persoonsgegevens onder de medewerkers.

3.1.3 Derdelijns

Als derde lijn heeft de sleutelfunctiehouder interne audit de taak een onafhankelijk oordeel te geven over de effectiviteit van, de opzet en de werking van dit beleid. De sleutelfunctiehouder rapporteert over de uitkomsten aan de DPO en het Bestuur.

3.2 Beginselen voor verwerking

Binnen SPKB worden persoonsgegevens verwerkt van deelnemers aan het pensioenfonds en pensioengerechtigden.

Persoonsgegevens kunnen ook worden verwerkt als informatie wordt opgevraagd of een bezoeker de website bezoekt.

Voor de verwerking van persoonsgegevens hanteert SPKB het beginsel 'privacy-by-default'. Voor de activiteiten die SPKB zelfstandig als fonds uitvoert ziet SPKB erop toe dat bij de verwerking er een goede balans is tussen het belang van SPKB en het belang van de betrokkene.

Elke verwerking van persoonsgegevens voldoet aan de volgende beginselen:

1. verwerking van de persoonsgegevens vindt plaats in overeenstemming met de wet ("rechtmatigheid");

2. persoonsgegevens worden op een behoorlijke en transparante wijze verwerkt ("behoorlijkheid en transparantie");
3. persoonsgegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verwerkt ("doelbinding");
4. persoonsgegevens mogen niet verder worden verwerkt op een met gerechtvaardigde doeleinden onverenigbare wijze ("doelbinding");
5. persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking");
6. SPKB treft maatregelen om te waarborgen dat de te verwerken gegevens juist en actueel zijn ("juistheid");
7. persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor verwezenlijking van de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ("opslagbeperking");
8. door het nemen van passende technische of organisatorische maatregelen waarborgt SPKB dat persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is ("integriteit en vertrouwelijkheid").

3.3 Verantwoordingsplicht

SPKB is verantwoordelijk voor de naleving van deze beginselen en ziet erop toe dat de verwerking van persoonsgegevens aan deze beginselen voldoet (de verantwoordingsplicht).

Om aan deze verantwoordingsplicht invulling te geven heeft SPKB de volgende maatregelen genomen:

- er wordt een register van verwerkingsactiviteiten bijgehouden (de registerplicht);
- er is een Data Privacy Officer aangesteld;
- voorafgaand aan risicovolle verwerkingsactiviteiten wordt een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd er wordt op toegezien dat de toezichthouder onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit wordt geraadpleegd (voorafgaande raadpleging);
- bij het inrichten van verwerkingen wordt rekening te gehouden met het principe van privacy door ontwerp (privacy by design & default);
- er zijn passende beveiligingsmaatregelen getroffen met het oog op de bescherming van persoonsgegevens;
- er is een meldprocedure ingericht om in het geval van een datalek melding te doen bij de toezichthouder en onder bepaalde omstandigheden ook bij de betrokkenen;
- Verwerkersovereenkomsten zijn afgesloten met verwerkers;
- er wordt medewerking verleend aan informatieverzoeken van de toezichthouder.

3.4 Legitieme gegevensverwerking

SPKB ziet erop toe dat persoonsgegevens alleen rechtmatig worden verwerkt. Persoonsgegevens worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen die vooraf aan elke verwerking van persoonsgegevens zijn bepaald. In die gevallen waarin SPKB persoonsgegevens voor meerdere doelen tegelijkertijd verwerkt stelt zij de verschillende doeleinden duidelijk vast.

Daarnaast moet het doel van de gegevensverwerking gerechtvaardigd zijn. Hiervan is sprake als SPKB de verwerking in overeenstemming verricht met een van de volgende rechtsgrondslagen:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
- het aangaan en voor de uitvoering van overeenkomsten waarbij betrokkene partij is, vooral het uitvoeren van betalingen en andere financiële transacties;
- het uitvoeren van analyses met betrekking tot persoonsgegevens voor statistische en wetenschappelijke doeleinden;
- de uitvoering van bedrijfsprocessen, intern beheer en managementrapportering;
- controle activiteiten, zoals interne audits en onderzoeken uitvoeren, financieel beheer en boekhouding, implementeren van interne controlemechanismes op de bedrijfsvoering, centrale verwerkingsinfrastructuur, ter beschikking stellen voor efficiëntie doeleinden en persoonsgegevens verwerken voor managementrapportering en analyse;
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (de naleving van wettelijke verplichtingen, om te voldoen aan de wettelijke vereisten betreffende witwassen en de financiering van terrorisme);
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op SPKB rust (de verwerking van gegevens van betrokkenen in het kader van een normale bedrijfsvoering zoals het bijhouden van een dossiers, het voeren van een rechtenadministratie en doen van uitkeringen in het kader van pensioenaanspraken de overdracht van waarden, etc.

Een verwerking is rechtvaardig wanneer de verwerking noodzakelijk is voor de in bovengenoemde grondslagen genoemde doelen. Hierbij neemt SPKB het proportionaliteits- en het subsidiariteitsbeginsel in acht.

Bij de proportionaliteitstoets wordt een verwerking op twee elementen beoordeeld, te weten:

- de effectiviteit: d.w.z. de verwerking is proportioneel als met de gegevens het gestelde doel kan worden bereikt en
- de evenredigheid: d.w.z. dat het legitieme doel dat wordt nagestreefd in verhouding staat tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt.

Bij subsidiariteit toetst SPKB of het genoemde doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) kan worden bereikt.

Bij twijfel of een verwerking van persoonsgegevens in overeenstemming gebeurt met een van de hiervoor genoemde doeleinden, moet advies worden gevraagd aan de DPO.

3.5 Verwerking voor andere doelen

Indien SPKB de gegevens wil verwerken voor een ander doel dan het oorspronkelijke doel dan dient opnieuw te worden vastgesteld of de verzamelde gegevens:

1. toereikend;
2. ter zake dienend;
3. niet bovenmatig en
4. juist en nauwkeurig zijn.

SPKB verwerkt de gegevens ook voor andere dan de oorspronkelijke doelen in de volgende situaties:

1. een verenigbaar doel: persoonsgegevens mogen verder worden verwerkt voor andere doelen, als die doelen verenigbaar zijn met het oorspronkelijke verzameldoel.

Bij de beoordeling om te bepalen of een nieuw doel verenigbaar is, wordt gekeken naar een aantal elementen:

- het verband tussen het nieuwe doel en het oorspronkelijke doel.
 - de context waarin de persoonsgegevens zijn verzameld.
 - de aard van de persoonsgegevens;
 - de mogelijke gevolgen van de verwerking voor betrokkenen;
 - het bestaan van passende waarborgen
2. toestemming: betrokkene heeft toestemming gegeven voor de verdere verwerking (ook in het geval het doel van de verdere verwerking niet verenigbaar is met het oorspronkelijke doel).
 3. Er is een specifieke wettelijke grondslag.

3.6 Toestemming van betrokkene

Het komt voor dat SPKB persoonsgegevens verwerkt op basis van toestemming van de betrokkene. SPKB moet in dat geval kunnen aantonen dat de betrokkene of de wettelijk vertegenwoordiger, toestemming heeft gegeven voor de verwerking. Toestemming mag niet worden geacht vrijelijk te zijn verleend, indien de betrokkene geen echte of geen vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

Om te waarborgen dat er sprake is van een geldige toestemming ziet SPKB erop toe dat de toestemming aan een aantal voorwaarden voldoet, te weten:

- de toestemming is vrij gegeven d.w.z. betrokkene heeft de keuzemogelijkheid te weigeren dat er persoonsgegevens worden verwerkt;
- de toestemming moet specifiek en geïnformeerd zijn: SPKB verschaft de betrokkene duidelijke informatie over de redenen waarom SPKB de persoonsgegevens gaat verwerken (het doel), maar ook bij voorbeeld over andere zaken die van belang zijn om te zorgen dat de betrokkene voldoende informatie heeft om een goed geïnformeerd besluit te nemen.
- de toestemming is ondubbelzinnig gegeven voor de verwerking.
Dit blijkt uit een ondubbelzinnige wilsuiting of uit een ondubbelzinnige, actieve handeling van de betrokkene ("opt in").

SPKB ziet in bovenstaand geval erop toe dat betrokkene toestemming geeft via een schriftelijke verklaring. Deze verklaring moet op een begrijpelijke en gemakkelijke manier en in duidelijke en eenvoudige taal het onderscheid aangeven tussen dat waarvoor de betrokkene toestemming geeft en de andere aangelegenheden.

SPKB stelt de betrokkene vooraf op de hoogte dat de toestemming te allen tijde ingetrokken mag worden.

3.7 Noodzakelijk voor de uitvoering van een overeenkomst

SPKB mag persoonsgegevens verwerken als dit noodzakelijk is voor de uitvoering van een overeenkomst en waarbij de betrokkene zelf ook partij is. De verwerking van de persoonsgegevens hoeft niet het hoofddoel van de overeenkomst te zijn, maar de verwerking van de persoonsgegevens kan voortvloeien uit de uitvoering van de overeenkomst.

Persoonsgegevens mogen ook worden verwerkt in de pre-contractuele fase (vóór sluiting van de overeenkomst) als dit noodzakelijk is om op verzoek van de betrokkene maatregelen te kunnen nemen.

3.8 Noodzakelijk om te voldoen aan een wettelijke plicht

SPKB verwerkt ook persoonsgegevens als dit noodzakelijk is om te voldoen aan een wettelijke plicht. Verschillende wetten verplichten SPKB om persoonsgegevens te verstrekken aan bijvoorbeeld de belastingdienst of uitkeringsinstanties.

3.9 Noodzakelijk voor de behartiging van het gerechtvaardigde belang

SPKB verwerkt persoonsgegevens als dit noodzakelijk is voor de behartiging van het gerechtvaardigd belang van SPKB of van een derde, op voorwaarde dat de belangen, rechten en vrijheden van de betrokkene(n) niet zwaarder wegen.

SPKB maakt een zorgvuldige beoordeling om te bepalen of er sprake is van een gerechtvaardigd belang om te bepalen of de betrokkene, gelet op het moment en de context van de verzameling van de persoonsgegevens, redelijkerwijs mag verwachten dat zijn persoonsgegevens voor dit doel worden verwerkt.

Voorbeelden hiervan zijn verwerkingen die strikt noodzakelijk zijn voor het voorkomen van fraude.

SPKB is transparant over het gerechtvaardigde belang en maakt duidelijk:

1. voor welke doeleinden persoonsgegevens worden verwerkt,
2. welke persoonsgegevens voor deze doeleinden worden verwerkt,
3. welke persoonsgegevens met andere partijen worden gedeeld en
4. hoelang de persoonsgegevens worden bewaard.

De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de Verwerking van zijn Persoonsgegevens.

3.10 Verwerking van bijzondere categorieën van persoonsgegevens

SPKB verwerkt alleen bijzondere persoonsgegevens in een van de volgende gevallen:

- als de verwerking noodzakelijk is in het kader van de uitvoering van regels op het gebied van arbeids- en sociale zekerheidsrecht of toelaatbaar is volgens het toepasselijk lokaal recht;

- als de verwerking nodig is om een vitaal belang van een betrokkene te beschermen, maar alleen wanneer het onmogelijk is eerst de toestemming van betrokkene te krijgen;
- als de bijzondere gegevens kennelijk openbaar gemaakt zijn door betrokkene;
- als de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

3.10.1 Verwerking van persoonsgegevens over ras en etnische afkomst

Persoonsgegevens waaruit ras of etnische afkomst blijken worden door SPKB alleen in twee specifieke situaties verwerkt, te weten:

- met het oog op de identificatie van de betrokkene, alleen voor zover dit onvermijdelijk is om het gestelde doel te bereiken bijvoorbeeld: paspoortgegevens van een medewerker, bezoeker of klant worden verwerkt ten behoeve van het identificatiedoeleinde;
- persoonsgegevens waaruit ras of etnische afkomst blijken, mogen daarnaast alleen worden verwerkt wanneer het doel is personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen of feitelijke nadelen op te heffen.

3.11 Verwerking van persoonsgegevens van betrokkenen

SPKB verwerkt persoonsgegevens van betrokkenen op basis van onderstaande grondslagen:

1. indien er sprake is van een gerechtvaardigd belang van SPKB en
2. indien de verwerking noodzakelijk is om te voldoen aan wettelijke verplichtingen.

Bij een verwerking op basis van een gerechtvaardigd belang ziet SPKB erop toe dat:

1. alleen die gegevens worden verwerkt die noodzakelijk zijn voor het doel dat wordt beoogd;
2. een of alleen de noodzakelijke bijzondere gegevens worden verwerkt en
3. er voldoende waarborgen zijn ingebouwd om de identiteit van betrokkene te beschermen.

3.12 Rechten van betrokkenen

Betrokkene kan onderstaande rechten tegenover SPKB uitoefenen:

- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens en ‘het recht om vergeten te worden’;
- het recht op beperking van de gegevensverwerking;
- het recht op verzet tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (data-portabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

SPKB geeft gehoor aan deze rechten, en handelt in lijn met de voorwaarden en rechten en plichten zoals vastgelegd in de Gedragslijn Verwerking persoonsgegevens Pensioenfondsen van de Pensioenfederatie die in dat kader gelden. Indien de verzoeken van de betrokkene kennelijk ongegrond of buitensporig zijn (dit is onder andere het geval wanneer de betrokkene heel vaak achter elkaar exact hetzelfde vraagt) dan hoeft geen gehoor te worden gegeven aan deze rechten.

SPKB kan de uitvoering ten aanzien van verplichtingen en rechten van Betrokkenen en van de beginselen van Verwerking van Persoonsgegevens beperken conform de AVG alleen in geval van:

- a. het voorkomen, opsporen, onderzoeken en vervolgen van - overtredingen van wet- of regelgeving waaronder begrepen de samenwerking met- justitiële of toezichthoudende autoriteiten; of
- b. het beschermen en verdedigen van de rechten en vrijheden, met name:
 - i de veiligheid van personen, Pensioenfondsen en Pensioenuitvoeringsorganisaties, de sector alsook de nationale veiligheid;
 - ii de continuïteit en integriteit van de dienstverlening van Pensioenfondsen en Pensioenuitvoeringsorganisaties alsmede de sector;
 - iii de inning van civielrechtelijke vorderingen, bijvoorbeeld bij pensioenbeslag.

3.12.1 Standaardformulier en reactietermijn

Om de betrokkene de mogelijkheid te bieden om deze rechten uit te oefenen heeft SPKB een standaardformulier voor het indienen van een verzoek.

Er worden geen kosten in rekening gebracht voor het uitoefenen van deze rechten, tenzij het gaat om ongegronde of buitensporige verzoeken.

Binnen een maand na ontvangst van het verzoek wordt de betrokkene geïnformeerd over de uitvoering van het verzoek. Ook in het geval dat SPKB besluit geen gehoor te geven aan het verzoek van de betrokkene moet dit binnen een maand kenbaar worden gemaakt. Een weigering wordt gemotiveerd en de betrokkene wordt ingelicht over het klachtrecht bij de toezichthouder.

3.12.2 Complexe verzoeken

Voor complexe verzoeken of als het veel verzoeken betreft mag SPKB twee maanden extra de tijd nemen. De betrokkene wordt binnen een maand na ontvangst van het verzoek op de hoogte gesteld van deze extra tijd.

3.13 Informatieplicht naar betrokkenen

Op SPKB rust een informatieplicht naar alle betrokkenen dus ook naar de bezoekers van de website. SPKB informeert de betrokkene onder andere over wat met hun persoonsgegevens gebeurt en de manier waarop zij hun rechten met betrekking tot de verwerking van gegevens kunnen uitoefenen.

Er is een informatieplicht in onderstaande gevallen:

1. De gegevens worden bij de betrokkene zelf verzameld bijvoorbeeld:
 - ✓ wanneer de gegevens van een bezoeker aan de website worden verzameld;
 - ✓ een enquête wordt verstuurd aan klanten of
 - ✓ als gegevens van medewerkers worden geregistreerd.
2. De gegevens worden buiten de betrokkene om verkregen bijvoorbeeld;
 - ✓ de gegevens worden verkregen via andere personen of organisaties of
 - ✓ de gegevens worden verzameld op het internet.
3. De gegevens worden voor een ander doel gebruikt dan waarvoor ze oorspronkelijk verzameld zijn.

Er is geen informatieplicht naar de betrokkene als de gegevens bij de betrokkene zelf worden verzameld en de betrokkene al beschikt over de benodigde informatie. Dit is ook het geval als de persoonsgegevens buiten de betrokkene om worden verkregen en de betrokkene reeds over de informatie beschikt.

3.14 Registerplicht

Om aantoonbaar te maken dat SPKB aan de verplichtingen uit de AVG voldoet, houdt SPKB een register in elektronische vorm bij van de verwerkingsactiviteiten. Het register bevat een beschrijving van de verwerkingsactiviteiten en niet de persoonsgegevens zelf.

3.15 Verwerkersovereenkomst

In die gevallen waarin SPKB een verwerker inschakelt voor de gegevensverwerkingen wordt er een verwerkersovereenkomst afgesloten. In deze overeenkomst worden onder andere de volgende zaken geregeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de SPKB.
- Geheimhoudingsplicht verwerker
- Beveiliging bij de verwerker
- Afspraken over toestemming subverwerkers
- Verwijderen van gegevens na afloop dienstverlening
- audits

3.16 Bewaartermijn

Gegevens mogen niet langer bewaard worden dan noodzakelijk is voor de verwerking van de doeleinden. SPKB stelt vast of er redenen zijn op grond waarvan gegevens bewaard kunnen blijven. Indien wordt vastgesteld dat er voldoende redenen zijn om de gegevens te bewaren dan bepaalt SPKB welke bewaartermijnen gelden. SPKB houdt een overzicht bij van de bewaartermijnen.

SPKB bewaart in ieder geval persoonsgegevens in onderstaande gevallen:

- Voor de duur van de relatie: SPKB hanteert de van toepassing zijnde wettelijke bewaartermijnen.

SPKB mag geen gegevens verwerken waarvan de bewaartermijnen zijn verlopen, tenzij deze gegevens voor een ander, daarmee verenigbaar doel, mogen worden verwerkt (bijvoorbeeld voor statistische archivering). SPKB kan verzamelde persoonsgegevens verwerken voor statistische en voor trendanalyse doeleinden. De verwerkte informatie is daarna niet meer naar personen herleidbaar.

3.17 Speciale onderwerpen

3.17.1 Burgerservicenummer

SPKB gebruikt dit uniek identificatienummer alleen ter uitvoering van de wet of bij voor bij de wet bepaalde doeleinden.

3.17.2 Privacy by design en Privacy by default

SPKB ziet erop toe dat de principes Privacy by Design en Privacy by Default worden meegenomen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen als ook persoonsgegevens worden verwerkt.

Door erop toe te zien dat privacy en gegevensbescherming worden meegenomen bij de ontwikkeling wil SPKB ervoor zorgen dat bij verwerkingsactiviteiten een zo klein mogelijke inbreuk op de persoonlijke levenssfeer van de betrokkene wordt gemaakt. Het Privacy by design principe is uitgewerkt in IT-architectuurprincipes en richtlijnen.

Afhankelijk van het concrete geval neemt SPKB technische en organisatorische maatregelen om invulling te geven aan eerdergenoemde principes.

Bij het bepalen van de verwerkingsmiddelen en de verwerking houdt SPKB rekening met de volgende elementen:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking en
- de risico's voor de betrokkene.

Van belang is dat de te nemen maatregelen in verhouding staan tot de risico's en redelijk zijn met het oog op de stand van de techniek en de uitvoeringskosten noodzakelijk om de maatregelen te implementeren.

3.17.3 Privacy Impact Assessment of gegevensbeschermingseffectbeoordeling (DPIA)

Voor verwerkingen die een hoog risico inhouden voor de rechten en vrijheden van de betrokkenen voert SPKB een gegevensbeschermingseffectbeoordeling uit. In dat geval mag de voorgenomen verwerking pas plaatsvinden als de DPIA volledig is uitgevoerd en is afgerond, inclusief implementatie van de benodigde beheersmaatregelen.

Bij verwerkingen waarbij een hoog risico niet aanwezig is wordt geen gegevensbeschermingseffectbeoordeling uitgevoerd.

Voor de beoordeling van de risico's zijn onderstaande factoren van belang:

- de aard van de voorgenomen gegevensverwerking;
- de omvang, context en doelen van de verwerking en
- de bronnen van de risico's.

De resultaten van de gegevensbeschermingseffectbeoordeling worden bij het vaststellen van de maatregelen meegenomen om de belangen van betrokkene te beschermen. Wanneer de hoge risico's voor betrokkenen niet met redelijke maatregelen beperkt kunnen worden wordt de voorgenomen verwerking voorgelegd aan de toezichthouder.

Conform de Gedragslijn zal éénmaal in de 3 jaar, bezien worden of er noodzaak is de DPIA te actualiseren. Het toepassen van nieuwe technologieën maakt het tussentijds uitvoeren van een DPIA noodzakelijk, evenals het toepassen van nieuwe profileringsmethodieken.

3.17.4 Doorgifte van persoonsgegevens

Binnen de EER

Landen van de Europese Unie, Noorwegen, Liechtenstein en IJsland moeten zich ook houden aan de Verordening. Dit betekent dat SPKB gegevens naar deze landen mag sturen.

Buiten de EER

SPKB geeft alleen persoonsgegevens door aan landen buiten de Europese Unie als het betreffende land een adequaat niveau van gegevensbescherming kent.

Bij gebrek aan een adequaatheidsbeslissing of passende waarborgen is het in onderstaande situaties toegestaan om persoonsgegevens door te geven:

- er is een uitdrukkelijke toestemming van de betrokkene;
- de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en SPKB of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen;
- de doorgifte is noodzakelijk voor de sluiting of de uitvoering van een overeenkomst in het belang van de betrokkene met SPKB;
- de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;
- de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de doorgifte is verricht vanuit een bij wet ingesteld register dat bedoeld is om het publiek voor te lichten.

Als SPKB in bovengenoemd geval gebruik wil maken van de toestemming van de betrokkene moet SPKB transparant zijn over de risico's die verbonden zijn aan de doorgifte bij gebrek aan een adequaatheidsbeslissing of passende waarborgen. De toestemming van betrokkene moet specifiek zien op de doorgifte van persoonsgegevens aan derde landen of internationale organisaties.

3.17.5 Beveiliging en vertrouwelijkheidsvereisten

Om de persoonsgegevens die verwerkt worden te beveiligen heeft SPKB geregeld dat de door haar aangestelde outsourcing partijen passende technische en organisatorische maatregelen getroffen hebben. De maatregelen die SPKB heeft getroffen in het kader van het beveiligen van gegevens zijn vastgelegd in het informatiebeveiligingsbeleid/IT-beleid. Deze maatregelen waarborgen een beschermingsniveau dat is afgestemd op het risico dat gelopen wordt bij de verwerking.

Deze maatregelen bestaan onder andere uit:

- pseudonimisering en versleuteling van de persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Overige technische maatregelen zijn bijvoorbeeld het toepassen van encryptie, het opzetten van een firewall of het opslaan van gegevens in beveiligde omgevingen. Ten aanzien van organisatorische maatregelen heeft SPKB een autorisatiebeleid waarmee de toegang tot gegevens tot bepaalde medewerkers wordt beperkt.

3.17.6 Security Awareness

SPKB ziet erop toe dat betrokkenen die toegang hebben tot persoonsgegevens bekend zijn met dit beleid en de hieruit voortkomende vertrouwelijkheidsplichten. Het is belangrijk het bewustzijn van betrokkenen met betrekking tot beveiliging te bevorderen.

3.17.7 Datalekken

Een inbreuk in verband met persoonsgegevens of datalek is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of verwerkte persoonsgegevens.

Het fonds registreert en beoordeelt elk datalek (inbreuk op de beveiliging van persoonsgegevens. De DPO houdt een register bij van de datalekken. Daarbij wordt tenminste vastgelegd:

- de aard van het datalek met vermelding van de categorieën van betrokkenen en van persoonsgegevens alsook het aantal betrokkenen.
- de waarschijnlijke gevolgen van het datalek;
- de te nemen of getroffen maatregelen om de eventuele nadelige gevolgen van het datalek te beperken of op te heffen.

De DPO beoordeelt of een datalek gemeld wordt bij de Autoriteit Persoonsgegevens (AP). Indien het waarschijnlijk is dat het datalek een risico voor betrokkenen inhoudt, wordt het datalek door het pensioenfonds zonder onredelijke vertraging, en indien mogelijk binnen 72 uur na het ontdekken van het datalek door het fonds aan de AP gemeld.

De Verwerker informeert het fonds zo snel mogelijk nadat hij een datalek ontdekt heeft bij de Gegevensverwerking voor het fonds. Hierover zijn afspraken gemaakt welke zijn vastgelegd in de verwerkersovereenkomst, de dienstverleningsovereenkomst of de SLA.

Indien er sprake is van een datalek dat gemeld moet worden aan de AP wordt, indien het datalek waarschijnlijk een hoog risico voor de betrokkene inhoudt, ook melding gedaan aan de betrokkene.

Betrokkene wordt in ieder geval over volgende geïnformeerd:

- de aard van het datalek;
- de naam en contactgegevens van de Data Privacy Officer;
- de waarschijnlijke gevolgen van het datalek;
- de te nemen of getroffen maatregelen om de eventuele nadelige gevolgen van het datalek te beperken of op te heffen.

Melden aan de betrokkene kan achterwege blijven indien:

- er vooraf dan wel achteraf maatregelen genomen zijn die het risico voor betrokkene mitigeren, met name het versleutelen van de persoonsgegevens;
- er onevenredige inspanningen gemoeid zijn met de melding en met een openbare mededeling kan worden volstaan.

3.17.8 Privacy Statement en Cookies

SPKB heeft op haar website een Privacy Statement (Privacyverklaring) gepubliceerd, waarin SPKB haar identiteit kenbaar maakt en de doelen van de gegevensverwerking benoemd. Het Privacy Statement beschrijft aan bezoekers van de website de manier waarop SPKB omgaat met persoonsgegevens en welke soorten cookies SPKB gebruikt.

3.17.9 Uitbesteding van werkzaamheden

Bijzondere aandacht verdient de verwerking van persoonsgegevens bij uitbestedingstrajecten. SPKB heeft beleid dat erop toeziet dat een rechtmatige verwerking van persoonsgegevens plaatsvindt voor de aanvang van een uitbestedingstraject, tijdens en na het uitbestedingstraject.

4 Minimum Standaarden

In dit hoofdstuk staat een overzicht van de minimum standaarden die voortkomen uit dit beleid:

Op het gebied van de governance:

- SPKB heeft een beleidsdocument met betrekking tot de bescherming van persoonsgegevens;
- SPKB heeft een Data Privacy Officer benoemd.

Er is een procedure voor de afhandeling van de rechten van betrokkenen.

Op het gebied van een categorieën van gegevensverwerking:

- SPKB houdt een register bij van alle categorieën gegevensverwerkingen;

Voor de Meldplicht Datalekken:

- SPKB heeft een meldplicht datalekken procedure;
- SPKB heeft een overzicht van alle datalekken;

Voor de website van SPKB:

- SPKB heeft op de website een Privacy Statement en Cookie beleid staan;

Voor de Privacy by design en Privacy Impact Assessment:

- SPKB maakt bij functiewijzigingen waarbij zij zelf direct betrokken is gebruik van de privacy by design principes die door CACEIS uitgewerkt zijn in haar architectuurprincipes;
- SPKB heeft het Privacy impact assessment principe geborgd in haar Change Managementproces.

5 Monitoring

De sleutelfunctiehouder Internal Audit neemt in haar monitorings- en rapportageplanning een periodieke monitoring op dit beleid op.

SPKB verantwoordt zich over de naleving van de AVG, en meer specifiek over de Gedragslijn Verwerking Persoonsgegevens Pensioenfederatie. Het fonds verantwoordt jaarlijks over de mate waarin zij zich heeft gehouden aan de gedragslijn. Het bestuur besluit in welke mate hierover verantwoording wordt afgelegd in het jaarverslag.

6 Goedkeuringsproces

Dit beleid is opgesteld door DPO/compliance officer en geaccordeerd door het Bestuur van het pensioenfonds.

7 Herziening van beleid

Dit beleid wordt (in principe) iedere drie jaar herzien, in samenspraak met de DPO, tenzij er omstandigheden zijn voor een tussentijdse herziening.

8 Afwijken van beleid

Ingeval er omstandigheden zijn die een afwijking van het beleid kunnen rechtvaardigen, dan moet een speciale procedure worden gevolgd ter verkrijging van goedkeuring door het Bestuur.

Het Bestuur geeft schriftelijk de reden en noodzaak van afwijking van dit beleid aan en verzoekt de DPO om een advies.

9 Schenden van beleid

Schending van dit beleid kan resulteren in disciplinaire maatregelen van SPKB, conform het van toepassing zijnde sanctiebeleid van Human Resource voor zover er sprake is van verwijtbaar gedrag. Indien van toepassing zijnde regelgeving, richtlijnen of ander beleid wordt geschaad, dan kunnen ook toezicht-sancties en/of civiele en strafrechtelijke boetes en maatregelen worden opgelegd.

10 Inwerkingtreding

Dit beleid treedt in werking op 27 juni 2025 en is vanaf de datum van inwerkingtreding van toepassing.