a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Verwerking van persoonsgegevens en informatieveiligheid

1. Inleiding

Deze brochure is een aanvulling op de privacyverklaring van a.s.r. Ze gaat dieper in op hoe ASR Levensverzekering N.V. als pensioenuitvoerder omgaat met vertrouwelijke informatie.

ASR Levensverzekering N.V. (hierna a.s.r.) is onderdeel van ASR Nederland N.V. Wij gaan op een veilige manier om met vertrouwelijke informatie, waaronder persoonsgegevens. We houden ons aan de geldende (privacy) wetgeving, internationale standaarden en gedragscodes die hier branche-breed invulling aan geven. Alle medewerkers van a.s.r. hebben de eed of belofte afgelegd, waarmee zij verklaren integer en betrouwbaar te zullen handelen. Daarnaast toetst a.s.r. de betrouwbaarheid en integriteit van nieuwe medewerkers door middel van een pre-employment screening.

Dit document beschrijft de juridische rollen die de werkgever en a.s.r. hebben. Daarnaast bevat dit document informatie over hoe risicomanage-ment, informatiebeveiliging, uitbestedingsmanagement en toezicht zijn ingericht.

Dit document behandelt niet alle aspecten van informatiebeveiliging. Voor verdere vragen over dit document kunt u contact opnemen met uw contactpersoon bij a.s.r.

2. a.s.r. zelfstandig verwerkingsverantwoordelijke

a.s.r. is een financiële instelling die valt onder de Wet op het financieel toezicht en die als pensioenuitvoerder valt onder de Pensioenwet. Op basis van de Algemene verordening gegevensbescherming (AVG) is a.s.r. verwerkingsverantwoordelijke. Vanuit deze en andere wetten hebben wij een verantwoordelijkheid om zorgvuldig met persoonsgegevens om te gaan.

Bij het tot stand komen van een pensioenregeling onderscheiden we de volgende elementen:

- De werkgever en de werknemer komen een pensioenovereenkomst overeen. De werkgever is daarbij verwerkingsverantwoordelijke.
- De werkgever vraagt een offerte aan bij a.s.r. Vanaf dit stadium worden er persoonsgegevens van werknemers uitgewisseld tussen de werkgever en a.s.r. De werkgever en a.s.r. zijn daarin beiden zelfstandig verwerkingsverantwoordelijken voor het eigen deel van de gegevensverwerking. Zowel de werkgever als a.s.r. bepalen namelijk afzonderlijk van elkaar het doel van en de middelen voor de verwerking van deze persoonsgegevens. Omdat zowel de werkgever als a.s.r. onafhankelijke verwerkingsverantwoordelijken zijn, kan er geen verwerkersovereenkomst (waarbij de ene partij de verwerkingsverantwoordelijke is en de andere partij de verwerker) tussen beide partijen gesloten worden. Branchebreed wordt dit inzicht gedeeld, zie bijvoorbeeld paragraaf 7.9.1 (pagina 45) van de Gedragscode Verwerking Persoonsgegevens Verzekeraars.
- De werkgever en a.s.r. sluiten vervolgens een uitvoeringsovereenkomst. Ook hierin zijn de werkgever en a.s.r. beiden zelfstandig verwerkingsverantwoordelijken.

In de uitvoeringsovereenkomst, in het pensioenreglement en in de privacyverklaring informeren wij betrokkenen over de doelen en middelen van de verwerking van de persoonsgegevens die wij ontvangen om de pensioenregeling uit te voeren.

Kortom, vanaf het moment dat persoonsgegevens zijn verstrekt voor het vragen van een offerte of voor de uitvoering van het pensioencontract, is a.s.r. zelfstandig verantwoordelijk voor een zorgvuldige verwerking van de gegevens. Uiteraard met inachtneming van de toepasselijke wet- en regelgeving.

3. Toezicht

Wij staan onder meer onder toezicht van De Nederlandse Bank (DNB) en hebben daarom ons IT Riskframework ingericht op het informatiebeveiligingsmodel van DNB zoals deze beschreven staat in de "Good Practice Informatie Beveiliging 2019/2020". Dit model van DNB bevat de thema's:

- Governance
- Organisation
- People
- Processes
- Technology
- Facilities
- Outsourcing
- Testing en Risk Management Cycle

Hier zijn vervolgens 58 beheersingsmaatregelen aan opgehangen. Periodiek toetsen we onszelf op deze onderdelen en jaarlijks voeren we het self assessment van DNB uit om te bepalen of we voldoen aan deze 58 beheersingsmaatregelen waar DNB op toeziet. Verdere informatie over dit informatie beveiligingsmodel en het toezicht dat DNB hierop uitvoert, is te vinden op de website van DNB.

4. Risicomanagement

a.s.r. heeft een risicomanagementsysteem dat bestaat uit verschillende elementen:
- Risicostrategie
- Risico governance
- Systemen en data
- Risicobeleid en procedures
- Risicocultuur en Risicomanagementproces

We hanteren het "three lines of defence model" in ons risicomanagementsysteem. Dit draagt bij aan de versterking van de risicocultuur, het nemen van verantwoordelijkheid voor het beheersen van risico's en aan interne beheersing. Dit model bestaat uit de volgende drie lijnen:

1. De eerste verdedigingslinie voert de bedrijfsactiviteiten uit en is verantwoordelijk voor de bijbehorende risico's. Binnen de bedrijfsonderdelen zijn Privacy-experts aangesteld die hier uitvoering aan geven.
2. De tweede verdedigingslijn bestaat uit de Risk Management functie, de Actuariële Functie en de Compliance Functie. De gehele tweede lijn opereert onafhankelijk van de eerste verdedigingslijn en geeft invulling aan de "countervailing power". De Functionaris Gegevensbescherming ziet vanuit de tweede lijn toe op de naleving van de privacyregels.
3. De derde lijn, Audit, is verantwoordelijk voor een onafhankelijke beoordeling van de doeltreffendheid van het risicomanagement-systeem, het interne controlesysteem en van de toereikendheid van de governance.

Deze scheiding van taken en verantwoordelijkheden met betrekking tot het opstellen van beleid en het goedkeuren van beleid, het implementeren en naleven van beleid en de controle op de naleving van beleid geeft waarborgen voor effectieve risicobeheersing.

5. Informatieveiligheid

a.s.r. heeft een algemeen informatiebeveiligingsbeleid met verschillende specifieke richtlijnen op de onderstaande domeinen:

- Personeel en Informatie
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging
- Beveiliging in bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie
- Ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten en bedrijfscontinuïteit
- Naleving

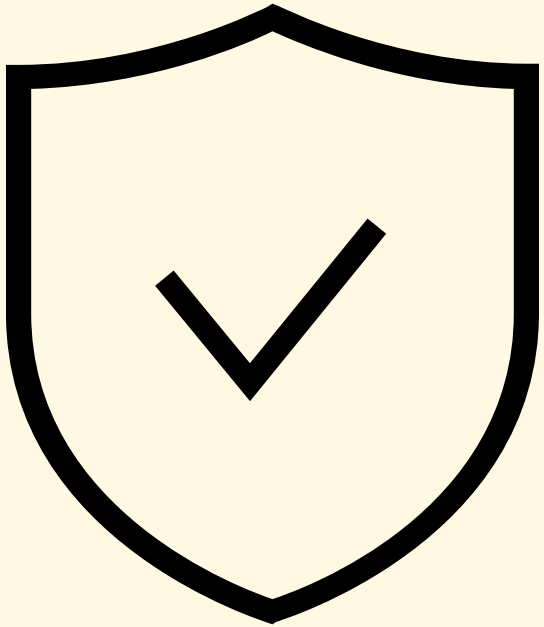
Deze informatiebeveiligingsrichtlijnen zijn concreet gemaakt in diverse standaarden en werken door in de te volgen processen, te gebruiken tooling en in de minimale vereisten waar informatiesystemen en IT-componenten aan dienen te voldoen. a.s.r. IT&C heeft een ISAE 3000 type 2 assurance rapport.

Daarnaast hanteren wij een IT Risk Framework (ITRF). Dit beschrijft alle inhoudelijke aspecten van informatiebeveiliging. Het ITRF is ‘principle based’ en geeft kaders aan de organisatie bij het in uitvoer brengen van dit beleid. Bij het opstellen van het ITRF is gebruik gemaakt van marktconforme standaarden en best practices, waaronder COBIT 2019, ISO 2700x, NIST Cybersecurity-framework, SOC1- en SOC2-principes, PCI DSS, COSO, BS 25999, ISO 31000, ITIL en PMF.

6. Partners waar a.s.r. mee samenwerkt

Wij werken in de bedrijfsvoering samen met diverse partners. We sluiten verwerkersovereenkomsten met partners die binnen de AVG als verwerker worden aangemerkt. Ons beleid is om persoonsgegevens, waaronder opslag van gegevens, te verwerken binnen de Europese Economische Ruimte (EER). In uitzonderlijke gevallen waarbij verwerkers zich buiten de EER bevinden, zorgen we ervoor dat de bescherming van persoonsgegevens gewaarborgd is. In dit geval gebruiken we bijvoorbeeld de Modelcontractbepalingen (Europese modelcontractbepalingen).

a.s.r. voert een uitgekiend beleid om met diverse partners tot een optimale en integere samenwerking te komen. We bewaken voortdurend onze contracten en service-overeenkomsten. We beheersen de risico's zodat we een goed gecontroleerde en integere bedrijfsvoering kunnen waarborgen. Onderdeel hiervan is de beoordeling van ISO 27001 certificeringen of ISAE 3000 type 2 en ISAE 3402 type 2 rapportages van partners.



a.s.r.
Pensioenen
Archimedeslaan 10
3584 BA Utrecht
www.asr.nl

ASR Levensverzekering N.V., KVK 30000847 Utrecht

58164_0823