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

Processing of personal data and information security

1. Introduction

This brochure supplements the privacy statement of a.s.r. It describes in greater detail how ASR Levensverzekering N.V. and ASR Premiepensioen-instelling N.V., in their capacities as pension providers, treat confidential information.

Both ASR Levensverzekering N.V. and ASR Premiepensioeninstelling N.V. (hereinafter referred to as "a.s.r.") are subsidiaries of ASR Nederland N.V. a.s.r. treats confidential information, including personal data, with due care and security. In doing so, a.s.r. adheres to the applicable privacy legislation, international standards, and codes of conduct that govern data protection industry wide. All employees of a.s.r. have taken an oath, by which they have declared that they will act with integrity. In addition, a.s.r. performs a background check and integrity screening on all its new employees (pre-employment screening).

In this document, we describe the roles the employer and a.s.r. have under the law. This document also addresses a.s.r.'s risk management, information security, outsourcing management, and supervision policies.

This document is non-exhaustive. It does not cover all aspects of information security. a.s.r. has the policy that it does not respond to in-depth inquiries from external parties about information security. That said, your contact person at a.s.r. will be happy to answer any questions you may have about this document specifically.

2. a.s.r. as a data controller

a.s.r. is a financial institution under the Dutch Financial Supervision Act and a pension provider under the Dutch Pensions Act. Based on the General Data Protection Regulation (GDPR), a.s.r. qualifies as a data controller. Based on these and other rules and regulations, a.s.r. is responsible for treating personal data with due care.

Establishing a pension scheme involves the following steps:

- The employer and the employee agree on a pension agreement. The employer qualifies as the data controller in this context.
- The employer requests a quote from a.s.r. From this stage onwards, personal data of employees is exchanged between the employer and a.s.r. The employer and a.s.r. each qualify as independent data controllers for their own part of the data processing. They each separately determine the purpose and means of processing the personal data. Since both the employer and a.s.r. qualify as independent controllers, they cannot conclude a data processing agreement (where one party qualifies as the controller and the other party qualifies as the processor). This opinion is shared throughout the sector (e.g. see Section 7.9.1 (pp. 43-44) of the Dutch Code of Conduct for the Processing of Personal Data by Insurers).
- The employer and a.s.r. ultimately conclude an administration agreement, in which process the employer and a.s.r. each again qualify as independent data controllers.

In the administration agreement, in the pension regulations, and in the privacy statement, a.s.r. will address the purpose and means of the processing of the personal data it receives to administrate the pension scheme.

In short, from the moment personal data is provided for the purposes of issuing a quote or administrating a pension contract, a.s.r. is independently responsible for processing this data with due care and with due observance of the applicable laws and regulations.

3. Supervision

a.s.r. is subject to the supervision of the Dutch Central Bank (DNB). For this reason, the a.s.r. IT Risk Framework is based on DNB's information security model as described in the Good Practice Information Security 2019/2020. This DNB model covers the following themes:

- Governance
- Organization
- People
- Processes
- Technology
- Facilities
- Outsourcing
- Testing
- Risk Management Cycle

DNB has defined 58 control measures to go with these themes. a.s.r. periodically performs self-assessments for these themes in addition to performing the annual self-assessment dictated by DNB to determine whether it complies with the 58 control measures that are subject to central bank supervision. For more information about this information security model and its supervision by DNB, please visit the DNB website.

4. Risk management

a.s.r. has a risk management framework, which is based on the following pillars:
- Risk strategy
- Risk governance
- Systems and data
- Risk policy and procedures
- Risk culture
- Risk management process

a.s.r. uses the three-lines-of-defence model in its risk management framework. This contributes to strengthening the risk culture, taking responsibility for managing risks and internal control. The three lines in this model are:

1. First line of defence: this line conducts the operations and is responsible for the associated risks. Privacy experts have been appointed within the business units to address the risks.
2. Second line of defence: this line consists of the Risk Management function, the Actuarial function, and the Compliance function. The second line operates independently of the first line of defence and exercises the countervailing power. The Data Protection Officer, who is part of the second line, monitors compliance with the privacy rules.
3. Third line of defence: this line is made up of the Audit function, which is responsible for performing an independent assessment of the effectiveness of the risk management system, the internal control system, and the governance procedures.

The segregation of duties and responsibilities regarding policy making and policy approval, policy implementation and compliance, and policy compliance monitoring ensures effective risk management.

5. Information security

a.s.r. has a general information security policy, which has been further elaborated in specific guidelines, in the following domains:

- Staff and information
- Management of company assets
- Access security
- Cryptography
- Physical security
- Security in business operations
- Communication security
- Business development
- Development and maintenance of information systems
- Supplier relationships
- Management of information security incidents
- Information security aspects and business continuity
- Compliance in practice

The information security guidelines in the domains mentioned above have been transposed into a body of standards. These are applied in work processes and instructions, tooling, and minimum requirements of information systems and IT components. a.s.r. IT&C is ISAE 3000 Type 2-certified.

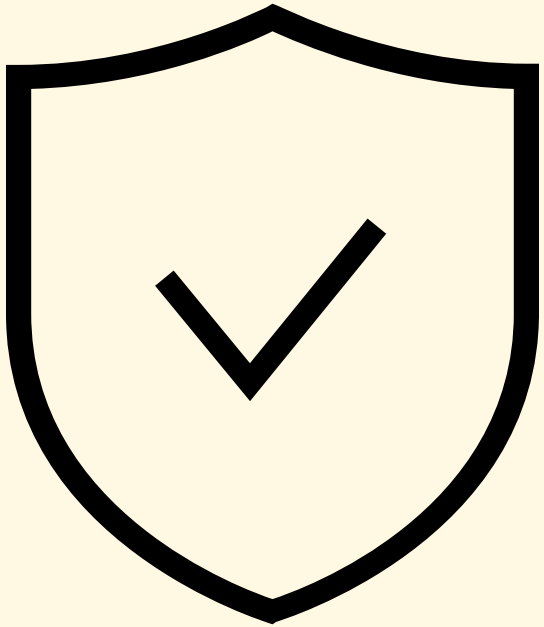
In addition, a.s.r. has in place an IT Risk Framework (ITRF), which describes all substantive aspects of information security. The ITRF is principles-based and provides context for the organization in implementing the information security policy. Market-based standards and best practices were used as inputs in the ITRF, including COBIT 2019, ISO 2700x, NIST Cybersecurity framework, SOC1 and SOC2 principles, PCI DSS, COSO, BS 25999, ISO 31000, ITIL, and PMF.

6. Partnerships

a.s.r. has several outsourcing partnerships. a.s.r. has signed processing agreements with several partners who qualify as data processors under the GDPR. a.s.r. has the policy that personal data is processed and stored within the European Economic Area (EEA).

In exceptional cases where processors are located outside the EEA, a.s.r. ensures that the protection of personal data is guaranteed. In this case a.s.r. uses, for example, the Standard Contractual Clauses (European model contractual clauses).

a.s.r. has a policy to achieve optimal and honest cooperation with various partnerships. Contracts and service agreements are continuously monitored and risks are managed, so that controlled and sound business practices are guaranteed. Within this scope, a.s.r. reviews its partners' ISO 27001 certifications or ISAE 3000 Type 2 and ISAE 3402 Type 2 reports.



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

ASR Levensverzekering N.V., KVK 30000847 Utrecht

58164EN_1123