AEGON

> 2022

Data protection at Aegon NL

Information relevant to employers and advisors of insurance and pension products offered by Aegon Levensverzekering N.V., Aegon Cappital B.V. and/or Aegon Schadeverzekering N.V.

Introduction

This document provides a general overview of data protection at Aegon The Netherlands (Aegon NL). The information relates to products that are administered by the legal entities Aegon Nederland N.V., Aegon Levensverzekering N.V., Aegon Hypotheken B.V., Aegon Schadeverzekering N.V. and Aegon Cappital B.V.

Data protection at Aegon NL is considered the combination of both Privacy and Information security policies and activities. This document provides a general overview of the Information security principles which Aegon NL has implemented.

This document aims to provide information that Aegon NL has appropriate protection in place regarding data protection, and to specifically describe a number of Information security procedures that Aegon NL has which aim at not disclosing information or performing any actions that will put any Aegon NL customers or customer data at risk or breach regulatory requirements.

This document cannot address all data protection concerns. You can always contact us, if you have any questions regarding the security within Aegon NL. Feel free to reach out to your contact at Aegon NL or send an email to privacy@aegon.nl.

Tabel of contents

1. Principles to manage and underline trust 4

- 1.1 Aegon NL as a data controller 4
- 1.2 Governance 4
- 1.3 Data Privacy Notice 5
- 1.4 Sectoral information sharing 5

2. Information Security Policy 6

- 2.1 Information Security Standards 6
- 2.2 Organization of Information Security 6
- 2.3 Information Asset Management 6
- 2.4 Human Resource Security 6
- 2.5 Physical and Environmental Security 7
- 2.6 Communications and Operations Management 7
- 2.7 Identity and Access management 8
- 2.8 Information Systems Acquisition, Development and Maintenance 9
- 2.9 Information Security Incident Management 10
- 2.10 Business Continuity Management 10
- 2.11 Compliance 11
- 2.12 Risk Management 11

3. Information Security Awareness 12

1. Principles to manage and underline trust

Our commitment is to be a trusted insurance company, based on the values of maintaining the confidentiality, integrity and availability of our customers' data. Our methods are built upon an executive commitment to ensure and improve the security of our services including:

- Defence-in-depth: multiple controls and technologies are applied to limit the possibility of any single point of failure.
- Investment: Aegon NL invests in personnel, tools, processes and technologies to manage, analyse and improve our security effectiveness.
- Transparency: trust cannot be maintained without open communications regarding the performance of our services, reliability and security; to which end we strive to be an industry leader in transparency.

1.1 Aegon NL as a data controller

Aegon NL is considered to be a data controller under the GDPR regime and subsequent Dutch privacy laws. Aegon NL is an insurance provider within the meaning of the Dutch Financial Supervision Act. Additionally, Aegon NL is a pension provider within the meaning of the Dutch Pensions Act. As a result, Aegon NL has to comply with various laws and regulations regarding insurance and pension contracts. In addition, insurance contracts tend to result in liabilities that result in payments long after the initial contract expired.

The purposes of the data processing by Aegon NL are defined in the contracts that employers have with us. The primary location of data processing activities conducted by Aegon NL are our data centres. It is our policy to process our data within Europe.

The role of the employer

Aegon NL considers employers to be data controllers under the GDPR regime.

The role of the advisor

Aegon NL considers advisors to be data controllers under the GDPR regime. Employers and advisors should formally agree on their respective roles and subsequently, the purposes and legal basis of data processing. Employers should pay attention to advisors that also act as an administrator on insurance or pension contracts and ensure appropriate safeguards. We advise employers to obtain proper legal advice whether your relationships with your advisor requires a data processing agreement.

1.2 Governance

Aegon NL has dedicated Security and Privacy departments which support the organization in achieving information security and data protection maturity levels appropriate for a financial institution like Aegon NL.

Three lines of defence

Aegon NL operates according to the three lines of defence model:

- **First line of defence are our business** functions and are accountable for the risks and controls within our first line functions. Aegon's Security and Privacy departments are positioned as first line roles.
- **Second line of defence is our Operational Risk and Compliance Team** who develop and implement risk frameworks and monitor the risk management process, ensuring risks are managed appropriately
- **Third line of defence is Internal Audit** who are an independent assurance function who review all activities across Aegon NL providing assurance via internal audits.

Certifications and audits

Aegon is a financial institution regulated by the Dutch National Bank (DNB) and is subject to regular independent financial and IT system audits by independent third party auditors.

Aegon is not ISO/ICE 27001 certified. The information security activities within the organization are guided by multiple internal and external frameworks, such as the Aegon Security Framework, the Aegon IT Control Framework and guidance from DNB in this area. Our information security practice does however work along the principles of the ISO/ICE 27001 standard. Aegon regularly performs internal checks to ensure that procedures are followed and security controls are effective. Also external, independent audits are performed to that end on a regular basis.

Aegon's key IT service provider – Global Technology Services (GTS) – is SSAE16 SOC 1 Type II audited on an annual basis. Audit reports are also obtained for other material outsourcing parties.

1.3 Data Privacy Notice

For further information on data protection at Aegon NL, we refer to our privacy and cookie notice on www.aegon.nl/over-ons/privacy

1.4 Sectoral information sharing

Aegon NL participates in multiple national (sectoral) cooperation initiatives on information security, such as in the Dutch Insurance-ISAC and the Dutch I-CERT initiative.

2. Information Security Policy

As stated above, this document provides a general overview of information security at Aegon NL and is not a complete list of all the processes, control measures and activities we perform within the organization to ensure a mature level of information security. The Aegon Security Framework addressed all relevant area's of information security as also outlined in the ISO/ICE 27001 standard. This framework is the foundation of information security within Aegon NL.

The Aegon NL information security policy is reviewed and published annually and covers the following domains:

- Information security policies
- Organization of information security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

2.1 Information Security Standards

The Information Security Standards set out the minimum requirements to which business units must adhere when implementing controls to comply with the Information Security Policy.

2.2 Organization of Information Security

- Information Security Roles and Responsibilities
- Governance and management of third Parties, for which Aegon NL has an outsourcing policy
- Ownership of data, applications and value chains

2.3 Information Asset Management

To classify and protect the processing of (strictly) confidential information Aegon NL has defined four data classification categories:

- Public
- Internal
- Confidential
- Strictly Confidential

Data is classified and based on classification specific controls which are implemented to ensure correct processing per class of data and to prevent unauthorised access and data loss. Confidential and strictly confidential data processed in third party environments (on premise at third party, in the cloud) is in most cases encrypted in transit and at rest. Only authorised Aegon NL employees have access to that data.

2.4 Human Resource Security

Aegon NL has a Pre-Employment Screening process in place to check identity and background of all potential employees or employees of service providers. Before employment can begin, Aegon NL will perform a pre-employment screening which includes:

- Reference checks
- Credit and criminal history
- Additional checks as needed for specific roles

2.5 Physical and Environmental Security

Data Centre Security

Access to our data centre and operations floors is restricted through a card key system and monitored on a 24x7 basis. All data centre visitors are required to present identification, sign the visitor's log and be escorted by an Aegon NL employee at all times while in the data centre.

A limited subset of individuals within each data centre have access to the data centre operations floor where the core technology equipment resides. Access privileges to the data centre are granted based on an individual's job responsibility and will be reviewed periodically. Employees who have data centre access, are reviewed at least annually.

Environmental Controls

The data centres have equipment to protect against and/or limit damage due to theft, fire, lightening, flooding, loss of electricity and temperature fluctuations. Smoke and heat detectors and a sprinkler system are located throughout each building.

Aegon NL Offices

All entry and exit points are protected by CCTV. Operational entrances are staffed by security personnel and have physical barriers such as turnstiles where only authorised employees with a key card can access the buildings. Fire exits and entrances not in operation are protected by intruder alarm systems. In addition, the following safeguards have been implemented:

- Physical Security Perimeter Requirements
- Physical Entry Controls Securing Public Access, Delivery and Loading Areas
- Protecting Against External and Environmental Threats
- Clear desk and clear screen guidance

2.6 Communications and Operations Management

Aegon NL and Global Technology (GTS) are business units within the Aegon group of companies.

GTS provides Aegon NL with IT services such as:

- Desktop/ laptops
- Messaging & other productivity applications
- Remote Access
- Servers
- Network Security
- Data Centres
- Service/ access request system
- Security administration

Aegon NL manages:

- Aegon NL specific business applications
- Third parties
- Information security management process

Hardening and Patching

Servers are built to a hardening standard based on the CIS Benchmark to establish consistent processing environment, and optimized Security configuration standards for Windows, UNIX, and Linux servers.

Server teams monitor security patches and vendor announcements. All security patches are applied to the server test environments before being applied to production in a scheduled manner based on the security patch criticality.

Network, Servers & workstations

Endpoint security (including antivirus) software is installed on all of our workstations and servers. The network is monitored for potential security intrusions or malware attacks. Alerts are investigated and follow the Aegon NL Incident Management Process under which appropriate remedial action will be initiated where necessary. In addition, network device configurations are monitored daily.

Logging and Monitoring

Access and changes to critical computer system, databases, and network devices are logged. Audit logs are kept for monitoring purposes and are stored longer than the reconciliation period for misuse analyses. Other activities performed include:

- Monitoring System Use
- Protection of Log Information
- Administrator and Operator Logs
- Fault Logging

Aegon NL's Security Information and Event Management (SIEM) system records security events from network devices and alerts the Security Operations Centre (SOC) who respond accordingly.

Anti-malware controls

An email 'hygiene service' filters out emails which are identified as spam, malware or having other suspicious characteristics to prevent infection of our network with malicious software.
All employees access the Internet through a proxy that prevents access to certain categories such as adult, webmail or file sharing sites. The web proxy also blocks access to websites with a poor reputation such as those identified as a phishing or malware distribution site.

Workstations and servers have anti-malware software that scan files upon access in addition to regularly scheduled scans.
Aegon NL also uses a network security solution that will detect suspicious activity (e.g. anomalous network connection attempts) on the Aegon NL internal network.

Other activities performed within the communications and operations domain:

- Procedures and Responsibilities In Respect of IT Operations
- Third Party Delivery Management
- Systems Planning and Acceptance
- Protection Against Malicious and Mobile Code
- Network Security Management
- Media Handling (digital and non-digital)
- Secure Exchange of Information

2.7 Identity and Access management

We manage the identity of our employees through a central HR system which interfaces with an Active Directory to ensure appropriate and timely management of employee user accounts.

User access management

A standard procedure is in place for provisioning, managing and revoking user access rights to applications and data. This procedure is supported by a central identity and access management system. This procedure includes periodical checks on existing access to critical systems and data. This ensures that staff only have access to systems and data that are required for their work. All user access can only be requested by an authorised operational manager. Each request is processed through a central access control system to guarantee assigning only approved business roles to ensure segregation of duties based on the least privileged principle.

Mover-leaver process

Aegon NL has processes in place to ensure access to the network and to systems is in accordance with their role within the company. In case of any role changes, access rights are automatically revoked and reassigned

Periodic review

Access to systems and applications used to support critical business processes and/or containing (strictly) confidential information is reviewed quarterly. For these systems the privileged access rights, e.g. System and database administrators, functional mangers, network and operating system access is reviewed quarterly.

Private Network Access

Aegon ensures that only authorised devices can connect to Aegon NL's private network.

Remote Access

Remote access requires two-factor authentication comprising login ID/Password and a generated one-time passcode. Laptops can establish a VPN in order to access services on our private LAN. Without a laptop, remote access via a VPN connection with data leak controls is enabled so that files cannot be transferred (i.e. uploaded or downloaded) and copy and paste functionality is disabled.

Laptops and Mobile Devices

Aegon NL laptops use full disk encryption. Writing to removable media (e.g. USB drives) is disabled. Where sensitive data requires physical transfer using electronic media such as USB or external hard drives encryption is applied and procedures employed to ensure the safe transfer from sender to recipient. Users can access email from personal devices using a secure mobile device management solution which applies encryption of data, secure transmission, two-factor (device certificate and password) authentication, remote wipe and other security features such as no copy and paste functionality.

General User and Data Leakage Controls

By default Aegon NL users:

- Have restricted workstation policies. For example, software cannot be installed and there are no local administrative privileges.
- Can only access authorised website categories. For example, file transfer and webmail sites cannot be accessed.
- Cannot save data to external storage media except encrypted devices provided by Aegon NL

2.8 Information Systems Acquisition, Development and Maintenance

Software Development Lifecycle

Aegon NL applies 'security-by-design' principles, based on OWASP top10 /SANS. The Software development process is designed to minimise any known vulnerabilities within the technological capabilities of Aegon NL by subjecting software to security tests and are finalized by penetration testing performed by third party experts (e.g. Deloitte).

Vulnerability scanning and Penetration testing

Windows and UNIX/LINUX servers are scanned weekly for vulnerabilities. Aegon NL's external IP addresses are scanned regularly by GTS and a third party.
For critical and web-based applications a penetration test is performed annually or when there is a significant change.

Cyber threat management

Within Aegon the Global Security Operations Centre tracks new and emerging information security threats to the organization. This is done using a variety of means, such as:

- Utilizing Threat Intelligence to identify threats, threat actors and tools that may be used against Aegon NL.
- Participate in Intelligence Sharing Communities, by sector, country and globally.
- Stage 'Red Team' operations to validate controls and Incident Response plans.

Third Party Services

Aegon NL conducts information security due diligence on third parties. The process involves assessing the potential information security impacts associated with the service and the level of information security maturity of the third party. The potential impact associated with the service determines the level of detail and assurance gathered. Aegon NL assigns vendor managers to ensure ongoing governance and monitoring of key suppliers.

Environments and test Data

Within Aegon NL development, test and acceptance environments are separated from the production systems. Access to production data is restricted. Developers, testers, functional managers and other employees with elevated access rights do not have access to production environments. Anonymised or synthetic test data will be used if personal data is required for testing purposes.

Decommissioning

A process ensures that all equipment and media that contain sensitive data are cleansed and properly disposed of. Drives are either physically destroyed or wiped by a specific software program so that no data is retrievable. Hardware is securely destroyed by a third party disposal company, subject to the environmental and safety standards. All equipment disposals of GTS supported assets are monitored by GTS management for compliance on a quarterly basis.

2.9 Information Security Incident Management

All data breaches and security incidents must be reported as soon as they are identified. Aegon NL has a standardized security incident response process. and takes part in the Global Security Incident Reponse Programme. The response process starts with the logging of a security event (which may be an incident). There are escalation routes depending on the severity of the incident and whether it affects other Aegon NL business units. An incident with a significant impact will be escalated to the Business Disruption Management Team (BDMT). An security incident that affects multiple business units is escalated to the Global Security Incident Response Team (GISIRT) and handled in close cooperation with all business units within Aegon NL.

2.10 Business Continuity Management

Within Aegon NL we perform Business Impact Assessments for all processes and systems to determine how to handle backup and recovery for all our systems and data.

Disaster recovery

We have a storage infrastructure which supports replication and recovery which is monitored 24/7. A disaster recovery test is conducted semi-annually.

Backups

Backups are scheduled and performed according to baselines. Backup failures are monitored and resolved through the incident management process.

Crises Management Team

Aegon NL has a disaster recovery plan in place and crises management teams for all business units. For major incidents which affect multiple business units a global crisis management team is in place.

2.11 Compliance

Information Assets within Aegon NL are reviewed to determine the asset's level of compliance with relevant business, legal, regulatory, or industry requirements. Aegon NL identifies control measures to avoid violations of criminal and civil law, statutory, regulatory or contractual obligations, and of any information security requirements.

2.12 Risk Management

Aegon NL has an information security risk management process in place which establishes the requirements for identifying, assessing, managing and monitoring information security risks in line with the Aegon NL risk tolerance. The process provides a consistent and formal approach to manage information security risks, to control impacts from systemic or emerging threats, to avoid serious damage to information assets or Aegon NL operations and reputation, and to implement controls to prevent future occurrences.

Decisions on the management, treatment, identification, qualification and prioritization of risks will be made based on the business objectives of Aegon NL and in the best interest of its clients.

3. Information Security Awareness

An extensive employee awareness program is in place. All year round different information security awareness activities take place including:

- a minimum test score after completing an information security ELearning course
- quarterly phishing simulations/tests against a (rotating) sample of our users in order to identify who needs additional awareness/training
- Information Security awareness presentations given by internal and external security experts.

www.aegon.nl

20220106