General Data Protection Regulation (GDPR):

How Aviva protects customer data

| Retirement | Investments | Insurance | Health |

AVIVA

General Data Protection Regulation (GDPR):

How Aviva protects customer data

Introduction

On 14 April 2017, the EU Parliament adopted the "General Data Protection Regulation" ("GDPR") which will apply from 25 May 2018. GDPR will have a significant impact for all organisations and robust preparations are needed. At time of writing, there remain a number of legislative and regulatory uncertainties on GDPR principles. These are being written into UK law and the Data Protection Bill currently going through the parliamentary process, and may impact our delivery plans.

The existing rights of data subjects will be strengthened significantly under the new legislation. Individuals can request to have their data erased and given to them in a portable format. They can also refuse to be part of marketing activities and other processing activities in certain circumstances.

In addition, there are clear requirements for Data Controllers to have accountability, responsibility and oversight of data privacy practices and we must be able to demonstrate compliance with the regulation. The UK Regulators will be looking for assurance that there are strong data privacy risk and control frameworks in place.

This document is provided in response to frequently asked questions with regard to Aviva's approach to GDPR and Data Protection practice.

Queries relating to this document can be emailed to **AskGDPR@aviva.com**

Contents

1. General Data Protection Regulation (GDPR)

1.1 Is Aviva a Data Controller or Data Processor?

Group Personal Pension Schemes:

- Aviva has personal pension contracts in place with the individual members and is a data controller in respect of the data processed for the purposes of these contracts. Data is passed to Aviva by the employer. The employer is a controller in respect of the data it holds and passes to Aviva. As the data is passed to Aviva for the purposes of the contracts this is a controller to controller relationship.
- Auto-enrolment communication and technology services – this is an ancillary service provided by Aviva to employers to assess and communicate with their employees about auto-enrolment. Aviva will be undertaking processing as a data processor on behalf of the employer.

Defined Benefit Trust Based Schemes:

- Where trustees are investing scheme assets through an insurance policy Aviva will be the data controller in respect of the policy. For ancillary services Aviva may be carrying out a data processor role on behalf of the trustee as data controller. This will depend on the specific arrangement.

Money Purchase Trust Based Schemes:

- Where trustees invest through a product provided via a platform service or insurance policy, then Aviva will be acting as a data controller for the purposes of processing data for the product. For ancillary services Aviva may be carrying out a data processor role on behalf of the trustee as data controller. This will depend on the specific arrangement.

Master Trust Pensions

- These schemes will follow the approach set out above for Money Purchase schemes.

Bulk Purchase Annuity

- Aviva is controller in respect of data being processed for the purposes of the insurance policy. Where additional services are provided Aviva may be a data processor on behalf of the trustees in respect of those services.

Group Protection

- The employer and/or trustee is a controller in respect of the data passed to Aviva. Aviva is controller in respect of data being processed for the purposes of the insurance policy, and any data which is collected directly from members.

Group Private Medical Insurance

- In relation to corporate private medical insurance policies, both the corporate policyholder and Aviva act as independent Data Controllers and neither party processes personal data on behalf of the other. This is the position that is reflected in our corporate agreements and Aviva will not enter in to variations to these agreements in relation to personal data.

1.2 What action is Aviva taking to prepare for GDPR?

Aviva has an extensive and long-standing programme in place to address the requirements of the EU GDPR legislation and we are confident that we will be compliant with the principles of GDPR as from May. There still remain a number of legislative and regulatory uncertainties with the Data Protection Bill (which will write GDPR in UK Law) currently going through the parliamentary process, but we are confident that the approach we are taking on prioritising the rights of individuals will meet the needs our customers and comply with the legislation.

1. General Data Protection Regulation (GDPR)

Key activities

- Governance – we are reviewing all processes that support the demonstration of GDPR compliance. This will include storage of key information, committees, resources and training. Our Data Protection Officer will be in role and operational prior to May 2018 and we are currently rolling out a training programme to staff.
- Understanding our personal data – we have processes in place to document all personal data, across all processes as a key building block to help support delivery of other aspects of GDPR legislation.
- Conditions for lawful basis for processing (including consent) – we have assessed each activity undertaken that involves processing of personal data, and validated it is justified under a lawful basis, as set out in Article 6 of GDPR.
- Data subject rights – we are reviewing our procedures for existing data subject rights, to ensure they are compliant with GDPR legislation and that these rights can be fulfilled.
- Data portability – we will implement a process that allows for the porting of data, in receipt of a data subject request.
- Data subject access requests – we are putting an enhanced process in place to ensure we continue to fulfil data subject access requests and meet the requirements of GDPR legislation.
- Automated decision making – our processes will be reviewed for automated decisions with the necessary adjustments made to ensure compliance with GDPR.
- Data security – security controls will be reviewed in line with GDPR requirements. We will implement appropriate technical and organisational measures to continue to ensure appropriate levels of security are in place.
- Breach management – we are reviewing our current data breach procedures and will update to ensure GDPR compliance. This will be tested prior to May 2018.
- Data transfers – although GDPR does not make major changes to overseas transfers, we are reviewing all contracts to ensure compliance with the rules around data transfers.
- Special categories of data – we are reviewing all processes where special categories of data are used and will make any necessary adjustments, this may include the revision of customer notices.
- Data retention and deletion – we have a set of data retention guidelines in place. These guidelines apply to data records across our estate and will continue as part of GDPR ongoing compliance.
- Contracts – our existing contracts with third party service providers will be revised to ensure the correct GDPR obligations are in place. We have an ongoing process to ensure new contracts support GDPR compliant processing.

Aviva's GDPR Programme has developed a comprehensive Data Governance Framework. The guiding principle for this Framework is that our use of customer data has a clear and positive outcome for our customers. Further detail is provided in Q2.

2. Aviva's Data Governance Framework

2.1 What is Aviva's Data Governance Framework?

Aviva's Data Governance framework sets out the minimum requirements for managing the activities, policies and processes that support Aviva's data journey through the information lifecycle. The framework draws together the key components from the relevant policies, guidance and the three Business Standards:

- Data Governance Standard
- Global Data Privacy Standard
- Group Business Protection Standards

Embedding good data governance informs us of what data we have, where and how it is stored, what purpose we are using it for and whether we are retaining and destroying it in line with legal and regulatory requirements.

2.2 What is Aviva's Data Governance Standard?

Aviva's Data Governance Standard is based around eight principles covering the end-to-end information lifecycle from the point at which data is captured to the point it is destroyed.

Across Aviva there are practices and business standards in place which contribute to controlling specific elements of the information lifecycle; these practices are embedded into the Risk Management Framework.

The Information Lifecycle

Principle 1: Accountable –
A Data Governance Accountable Executive will oversee and lead Data Governance, delegating roles and responsibilities to appropriate individuals.

▼

Principle 2: Transparent –
Business Policies and processes will be documented and made available to all individuals and other interested parties as appropriate. Individuals will be trained appropriately for the role they perform.

▼

Principle 3: Collect/Create –
Data collected or created by Aviva will be constantly checked for quality to ensure the data lineage is sustained for internal and external transfers.

▼

Principle 4: Store/Secure –
A proportionate level of protection is applied to critical data assets in line with their Security Classification.

▼

Principle 5: Transfer/Use –
Transferring, sharing or using Aviva's data will be done in a manner that can evidence he information lifecycle, ensuring the correct justification for sharing is apparent and security controls are applied.

▼

Principle 6: Hold/Discover –
Data will be held in a manner which allows for timely efficient and accurate discovery.

▼

Principle 7: Retain/Archive –
Data will be held for the appropriate amount of time, in accordance with legal, regulatory and operational requirements.

▼

Principle 8: Destroy –
Secure destruction arrangements are in place for data that is no longer required in accordance with the applicable laws and Aviva's policies.

2. Aviva's Data Governance Framework

2.3 What is Aviva's Global Data Privacy Standard?

Aviva's Global Data Privacy Standard sets out the mandatory control objectives and controls for the protection of the personal data that Aviva collects and processes in relation to customers, staff, shareholders and some third parties. It sets out the minimum requirements necessary to ensure personal data processed by Aviva is appropriately protected, in line with legal and regulatory requirements, and is supplemented by local, policies and procedures applicable to the different jurisdictions in which Aviva operates.

This Standard defines nine Aviva Data Privacy Principles (which follow global privacy laws), with its objective to embed appropriate data privacy controls that allow Aviva to use personal data for legitimate purposes but which also protects personal data and ensures the protection of individuals' rights and freedoms with regards their personal data.

Aviva Data Privacy Principles

Accountability –
Each Business Unit is responsible for ensuring that the appropriate resources and controls are in place to comply with this Standard. This includes evidencing compliance with this Standard.

Fair and Legal Processing –
Personal Data shall be processed lawfully, fairly and in a transparent way.

Limited Purpose –
Personal Data shall be processed, including collected, for specified, explicit and legitimate purposes and not used for any other purpose.

Minimisation –
Personal Data shall be adequate, relevant and limited to only what is necessary for the purposes for which it is processed.

Accurate –
Personal Data shall be accurate and kept up to date.

Retention Limitation –
Personal Data shall be kept in an identifiable format for no longer than necessary for the purposes for which the Personal Data are processed.

Security, Integrity, Confidentiality –
Personal Data shall be kept secure to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Individual Rights –
Individual's Personal Data rights shall be respected.

Transfers –
Personal Data shall not be transferred to another country/ jurisdiction without appropriate safeguards in place.

2. Aviva's Data Governance Framework

2.4 How does Aviva limit personal data processing to what is necessary for the agreed purpose?

Data Owners within each Business Unit must review personal data to ensure the data remains up to date and accurate, and consider whether any processing is aligned to the purpose for which it was originally collected or any secondary legitimate purpose. To the extent that such personal data is no longer needed, data should be deleted or anonymised subject to applicable guidelines.

2.5 What are Aviva's Business Protection Standards?

Aviva's Business Protection Standard sets out Aviva's control objectives and controls for business protection across Aviva. This is to ensure that appropriate and consistent levels of governance, control and risk management are achieved in relation to Information Security, Physical Security and Business Continuity Management. These cover areas including:

- Access Control
- Acceptable use of Aviva equipment and data
- Information classification and handling
- Password Management and configuration
- Cryptography and Security Incident Management
- Selection and engagement of third party suppliers and vendors in line with Aviva's Procurement & Outsourcing requirements

All Aviva staff, contingent workers and third party service providers must comply with the controls that are relevant to their roles and responsibilities.

3. Breaches and Security Incidents

3.1 How are security incidents managed by Aviva?

Aviva has a dedicated Global Cyber Security Operations Centre which includes a Security Incident Management Team which will deal with any security incident.

To aid the detection and investigation of security incidents the Team will use a number of threat intelligence sources and forensic services. If as part of an investigation, it is discovered that there has been a data breach affecting one or more of Aviva's customers, the Security Incident Management Team would liaise with the relevant Relationship Manager to inform the customer, and any regulatory bodies accordingly.

3.2 What processes does Aviva have in place to manage data privacy breaches?

Aviva has Data Privacy Breach Reporting guidance in place, and local Incident Plans in each Business Unit. These Plans ensure appropriate organisational and technical measures are in place to protect personal data, including the identification, reporting, notification and resolution of any data privacy breaches in accordance with our internal policies and local laws and regulations.

We also have processes and contracts in place with our third party service providers to ensure all potential or actual data privacy breaches are immediately notified to Aviva.

3.3 Does Aviva have a business continuity plan in place to respond to a significant cyber security event or business disruption?

Aviva maintains internally and externally audited Business Continuity Management documentation which is designed to minimise disruption and maintain high levels of customer service in the event of a significant business disruption. These documents provide the framework for the initial response, control and co-ordination for any significant business disruption.

Aviva is committed to protecting its customers and the interests of its stakeholders. As part of that commitment, we rigorously employ a philosophy of Business Continuity Management that:

- Proactively assesses and mitigates against impending threats to the business
- Recognises the risks to continued operations that could arise from significant disruptions
- Mitigates the impact of such risks through timely and appropriate responses

In the event of a significant business disruption, (whether actual or impending) our focus will always be to:

- Ensure the safety and welfare of our personnel
- Endeavour to meet our obligations to customers and regulators
- Protect our reputation
- Minimise the exposure to our business position
- Facilitate a return to normal operations as soon as practicable

This is achieved by deploying appropriate command and control via our Major Incident and Crisis Leadership Teams.

3.4 Does Aviva have a process in place to back up client data?

For data held on Aviva-owned platforms, Aviva performs daily incremental back ups of its data. Full weekly backups are performed and all backups are monitored to ensure that they are performed. All critical data is synchronously mirrored across Aviva data centres and this copy of data would be used in the event of disaster recovery being invoked. An additional data copy is performed daily to DXC data centre in Reading across dedicated, secure network links. Backup media would be used as a method of last resort should the mirrored copy become corrupted.

Where data is held on third party platforms, contracts are in place with the Service Provider to ensure that Data is backed up in accordance with the criticality of the service, and regular tests are performed to ensure that data can be restored in the event of an incident occurring.

4. Information Security Framework

4.1 Aviva's Information Security Framework

Aviva is not accredited to any particular standard and has controls in place to integrate industry best practices based on formally recognised standards, such as ISO27001 and the Information Security Forum (ISF) Standard of Good Practice for Information Security.

As part of the Third Party Information Security Assurance process, Aviva carries out annual assessments of all of its critical suppliers, which include referencing independent SOC1 and SOC2 Reports, ISO27001 Certifications as well as PCI DSS Certifications for those suppliers who process Dr/Cr Card Payments on behalf of Aviva.

As part of Aviva Financial Reporting Controls Framework, Aviva internal Controls Testing Team and External Auditors carry out annual testing of key systems and processes to ensure that they are functioning in line with Global Mandatory Controls.

4.2 Does Aviva have a process for detecting and managing any inappropriate or unauthorised IT activity?

Aviva has a Security Incident and Event Monitoring tool in place which is used to provide automatic logs of systems access, including administrator access, successful and unsuccessful access attempts to the network and applications. The Group Cyber Security Operations Centre will receive alerts if there is any suspicious activity detected.

4.3 How does Aviva ensure that staff and contingent workers have the appropriate level of access to IT systems and clients personal data?

All access to Aviva systems is based on least privilege and has to be authorised by either the individual's line manager or the system owner. Authorised access is set up by a central IT Access Team. The Global Information Security Mandatory Controls outline the processes for access provisioning, as well as processes for deleting access. Line Managers and system owners are required to carry out six monthly access reviews to ensure that access is still appropriate, with access removed where this is no longer required.

4.4 How are off-site Aviva staff and contingent workers able to remotely access the Aviva network?

Aviva staff requiring remote access to the Aviva network have to use Aviva's approved mechanism. This creates a VPN between the remote user and Aviva and all information passed across the VPN is encrypted. Access is restricted to authorised users, and is managed through a soft token installed on the user's laptop. Aviva uses Cisco AnyConnect Secure Mobility.

Where users have Aviva supplied mobile phones which have access to email, Aviva uses a Mobile Device Management Solution to secure any data access, together with remote wiping in the event of a mobile device being lost.

4.5 What security controls are in place to protect Aviva's computers and networks?

Aviva's network perimeter is secured with firewalls and intrusion detection/prevention systems and software. Data Loss Prevention Software is installed to monitor email and web traffic to ensure that personal data is not sent outside of the organisation to unauthorised persons. Internet access is restricted to approved website categories. Personal Webmail and File Sharing Sites are blocked by default.

All endpoint devices and servers are protected by Anti-Malware software which is configured to look for signature updates multiple times a day. Devices are scanned daily. In addition all operating systems are patched in line with a documented Patch Management process, which includes testing in a non -production environment before being rolled out across all servers and endpoints.

4. Information Security Framework

4.6 Does Aviva perform penetration testing and vulnerability scanning of its network and systems?

Penetration testing of externally facing infrastructure is carried out whenever there is a significant change to that infrastructure and any critical vulnerabilities identified have to be remediated prior to the system/application going live. All testing is carried out by Check or Crest accredited third parties. In addition the Perimeter is scanned on a weekly basis. Network equipment, servers and workstations are scanned on a monthly basis. Any vulnerabilities identified have to be fixed in line with their severity.

4.7 How does Aviva encrypt mobile data?

Aviva has a Cryptographic Standard which outlines when encryption should be used and what algorithms and minimum key lengths are acceptable. All emails containing confidential information will be sent using either enforced TLS, or where this is not in place with the third party, opportunistic TLS. Data classified as confidential or above must be encrypted across untrusted networks. All portable media such as laptops and tablets have full disk encryption.

4.8 Does Aviva utilise wireless networks, and if so how are they secured?

Aviva has a segregated corporate and guest wireless network. The corporate network is restricted to Aviva personnel and computers only, and utilises WPA2. Guest wireless access permits users to access the Internet only.

4.9 What security measures are in place to protect client data within Aviva's offices?

All access to Aviva premises is restricted to authorised personnel through the means of proximity readers and photo ID cards. Reception areas are manned during business hours and all offices are covered by remote CCTV 24x7x365. Any visitors to Aviva offices have to be pre-approved and visitors have to provide Government photo ID on arrival and are escorted at all times when on site. Aviva operates a Clear Desk Policy in which all confidential documentation is secured under lock and key at the end of each day.

4.10 Does Aviva have any offsite data centres where client data is stored, and how are these protected?

Aviva has contracted with third party Data Centre providers for offsite data centre services. These companies are ISO27001 certified and provide Aviva with annual SOC1 Reports in respect of the services that they provide specifically to Aviva. These cover Information Security and Physical Security including access control, CCTV coverage, 24x7x365 monitoring and environmental controls such as heating, ventilation and air conditioning. The data centre staff have access to Aviva infrastructure, but do not have any application level access to any Aviva data.

4.11 How does Aviva assess contingent workers or third party suppliers who have access to Aviva client data or systems?

Prior to on-boarding new suppliers each potential supplier will be required to provide details of their security framework, as well as go through a vetting process led by Aviva's Procurement teams. Once a supplier is selected, contractual agreements are put in place which will include Security requirements for maintaining security programmes which are aligned to industry best practice standards such as ISO27001, as well as any legal and regulatory requirements applicable to the services being provided. Aviva Supplier Assurance teams are responsible for carrying out annual assessments of all suppliers who have access to Aviva data to ensure that they continue to comply with the terms of the contract.

5. Employees

5.1 What pre-employment checks does Aviva carry out for all new personnel or contingent workers?

All staff and contingent workers are assessed before they commence work with Aviva. This includes, but is not restricted to, the following:

- Proof of eligibility to work in the UK
- Two year activity verification
- Staff Fraud database check
- Credit check
- Basic criminal history check
- Previous employment history
- Conflict of Interest check

A confidentiality clause is contained in the staff contract of employment. For senior management there are additional checks around Media, Regulatory requirements and Directorships.

5.2 What training does Aviva provide to staff and contingent workers on security awareness, data protection and compliance with the GDPR?

Aviva Business Units must have an embedded programme of education and awareness for all employees and contingent workers in respect of the requirements of the Data Governance Framework, policies and processes and applicable privacy legislation and regulation.

Training may be delivered through training modules, presentations and training materials as appropriate, with a record of completed training maintained.

Mandatory training

- Online 'Essential Learning' CBTs are completed by Aviva employees and contingent workers on a yearly basis. This training ensures that all relevant employees are aware of Aviva's data governance and business standards, policies and processes.
- Data Governance role specific training modules are completed by all those who hold formally assigned Data Governance roles.
- Third parties with access to Aviva data are expected to embed Aviva's Data Governance into their training modules.

GDPR training

- Separate GDPR-focused training (e.g. documented guidance, CBTs and on-site presentations) is scheduled to ensure all relevant staff have an understanding of GDPR and what is required to ensure Aviva Business Units are GDPR compliant.
- This training will be completed ahead of May 2018 to ensure Aviva is able to respond appropriately to GDPR requirements from 25 May 2018.

6. Transfers of personal data

6.1 Does Aviva hold clients personal data outside the UK?

Aviva and our business partners may use service providers outside the UK for administration and IT purposes. Where this happens, the appropriate contracts and security controls are put in place to protect our customers' personal data.

7. Data classification

7.1 Does Aviva have a data classification system in place to ensure client data is appropriately identified and protected?

Aviva has a documented Information Classification and Handling Technical Specification which defines the four levels of classification applied to all data - Secret, Confidential, Internal and Public. This technical specification is supported by software which prompts users to label emails, documents and other end user applications with the appropriate classification based on the type of data being recorded.

7.2 How does Aviva identify and protect "sensitive personal data"?

All personal data is treated as Confidential, and only those users within Aviva who would be required to support clients would have access to the applications and systems used to process client data. All access is reviewed on a six monthly basis to ensure that it remains appropriate.

Where confidential information is sent across untrusted networks eg. e-mail or other web based transfer mechanisms; this will be encrypted in transit using either TLS, HTTPS or SFTP as appropriate. Documents may also be password protected to provide an additional level of security.

8. Individual Personal Data Rights

8.1 Does Aviva have a process in place to manage Subject Access Requests?

Aviva has a subject access procedure in place as required under Data Protection law. This process meets GDPR requirements and is managed by a central team with responsibility for overall coordination, including liaising with third party processors and the data subject.

8.2 How does Aviva support customers exercising their Personal Data Rights?

Aviva has documented procedures in place to ensure we deliver processes which meet GDPR requirements for the fulfilment of individuals' rights. Our procedures ensure that all staff are able to recognise and comply with individuals exercising their Personal Data Rights, in accordance with local laws and regulations.

Personal Data Rights

A data subject will have the following rights under GDPR:

- **The right to be informed**, typically through issue of a privacy notice
- **The right of access** to their personal data
- **The right to rectification**, where personal data is inaccurate or incomplete
- **The right to erasure** of their personal data at the end of the relevant retention period
- **The right to restrict processing** of personal data
- **The right to data portability**, allowing an individual to move their personal data across different services
- **The right to object to processing** of personal data, including for direct marketing
- **The right to challenge automated decision making**, including where applied in the context of profiling.

9. Retention of Personal Data

9.1 Does Aviva have a data retention policy?

Aviva has internally published Records Retention Guidelines, setting out best practice requirements for the management of legal commitments, including current and legacy product terms and conditions. The guidelines apply irrespective of the media or format in which records are held.

All personal data currently processed is required for product administration purposes and subject to ongoing data quality assessments and adherence to retention guidelines.

We have identified different business activities which act as triggers from where data no longer needs to be processed. These triggers are aligned to events which can occur in a policy lifecycle and include events such as quotation, policy maturity, cancellation and transfer. Each of these events will trigger a retention period which is partly determined by our administration experience around the event and is also aligned to any legislative requirement where applicable.

The retention period will take account of limitation periods within which legal actions must commence to ensure that sufficient information is available to consider such events where appropriate.

10. Disposal

10.1 What controls does Aviva have in place to securely dispose of paper records?

All Aviva offices are equipped with secure Confidential Waste Bins which are used to collect any paper records that are no longer required. Each day these bins are emptied and the secure bags are stored in a locked cage in readiness for onsite shredding by an approved, certified, audited third party.

10.2 What controls does Aviva have in place for the secure destruction of hardware that may contain confidential data, including client information?

Aviva has a contract in place with a third party accredited company who provide secure destruction of hardware, including hard drives, when they have reached the end of their service, and need to be decommissioned. This includes securely wiping the drives to CESG standards, before destroying the actual hardware itself. Aviva carries out annual audits of both third parties involved in the secure disposal of media (paper and electronic).

Aviva Life & Pensions UK Limited.

Registered in England No.3253947. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 185896.

Aviva Investment Solutions UK Limited.

Registered in England No. 6389025. Authorised and regulated by the Financial Conduct Authority. Firm Reference Number 515334.

These companies have their registered office at: Aviva, Wellington Row, York, YO90 1WR.

Telephone 0345 602 9189 – calls may be recorded.

aviva.co.uk

GN61006/PPEN32/S 03/2018

AVIVA