Data Privacy

How Aviva protects customer data

| Retirement | Investments | Insurance | Health |

AVIVA

Data Privacy

How Aviva protects customer data

Introduction

The General Data Protection Regulation (GDPR) came into effect and has a significant impact for all organisations. The legislation significantly strengthens the rights of data subjects and gives clear requirements for data controllers to have accountability, responsibility and oversight of data privacy practices.

This document summarises our approach to data protection, and provides answers to frequently asked questions.

If you have any questions on this, please get in touch with your usual point of contact.

Please note that this document is not advice. It reflects only the interpretation of Aviva UK Insurance in relation to Data Protection Legislation as at July 2023, which may be subject to change. This document is for general information purposes only and does not cover every piece of activity pertinent to the legislation. Aviva takes no responsibility for any decisions or actions taken as a result of the information given and it should not be relied upon in place of legal or other professional advice

Contents

1. UK General Data Protection Regulation

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 for the data processed for the purposes of these contracts. The employer, who passes data to Aviva is a controller for the data it holds and passes to us. As the data passes 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 we provide to employers to assess and communicate with their employees about auto-enrolment prior to the pension being established. For this, we will be a data processor on behalf of the employer. Please note that once the member's policy is either established or the employee opts-out, Aviva will be a data controller.

Defined benefit trust based schemes

- Where trustees are investing scheme assets through an insurance policy, we are the data controller for the policy.

Money purchase trust based schemes

- Where trustees invest through a product provided through a platform service or insurance policy, we will act as a data controller for the purposes of processing data for the product.

Master Trust pensions

- These schemes will follow the approach set out for money purchase schemes.

Bulk Purchase Annuity

- Aviva is controller for data processed for the purposes of the insurance policy.

Group protection

- The employer and/or trustee is a controller for the data passed to Aviva. Aviva is controller for data processed for the purposes of the insurance policy, and any data 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 reflected in our corporate agreements and we won't enter in to variations to these agreements in relation to personal data.

Individual Medical Insurance and Individual Protection

- Aviva has medical insurance contracts in place with individuals. To supply insurance as per the contract Aviva collects data from the individual. This means both the individual who passes data to Aviva and vice versa are both independent data controllers. Aviva is the data processor for the data collected.

2. Aviva's data governance framework

2.1 What is our data governance framework?

Aviva's data governance framework sets out the minimum requirements for managing the activities, policies and processes that support our 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 tells us what data we have, where and how we store it, what purpose we use it for and whether we are retaining and destroying it in line with legal and regulatory requirements.

2.2 What is our data governance standard?

Aviva's data governance standard is based around eight principles, covering the end-to-end information lifecycle from the point 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. We're embedded these practices into the risk management framework.

The information lifecycle

Principle 1: Accountable
A data governance accountable executive oversees and leads 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/Uses
Transferring, sharing or using Aviva's data will be done in a manner that can evidence the 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 our global data privacy standard?

Aviva's global data privacy standard sets out the mandatory control objectives and controls for protecting the personal data we collect and process for customers, staff, shareholders and third parties. It also lays out the minimum requirements necessary to be sure the personal data we process is appropriately protected. We do this in line with legal and regulatory requirements, supplemented by local policies and procedures for the different jurisdictions in which we operate.

This standard defines nine Aviva data privacy principles, which follow global privacy laws. It aims to embed appropriate data privacy controls allowing us to use personal data for legitimate purposes. It also protects personal data and the individual's rights and freedoms with regard to their personal data.

Aviva data privacy principles

Accountability
Each business unit is responsible for ensuring the appropriate resources and controls are in place to comply with this standard. This includes evidencing compliance.

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 do we limit personal data processing to what is necessary for the agreed purpose?

Data owners within each business unit must review personal data to make sure the data is 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. If such personal data is no longer needed, it must be deleted or anonymised subject to applicable guidelines.

2.5 What are our business protection standards?

Our business protection standards set out our control objectives and controls for business protection across Aviva. This makes sure we achieve appropriate and consistent levels of governance, control and risk management for 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 and outsourcing requirements.

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

3. Breaches and security incidents

3.1 How do we manage security incidents?

We have a dedicated global cyber security operations centre, which includes a security incident management team, who will deal with any security incident.

To help with detecting and investigating security incidents, the team use a number of threat intelligence sources and forensic services. If an investigation uncovers a data breach affecting one or more of our customers, the security incident management team will liaise with the relevant relationship manager to inform the customer and any regulatory bodies.

3.2 What processes do we have in place to manage data privacy breaches?

We have 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. This includes the identification, reporting, notification and resolution of any data privacy breaches in line 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 they tell us of any potential or actual data privacy breaches immediately.

We log data breach's of all ratings and use the root cause analysis to identify and improve any systemic improvements that can be made in our wider system/relationships.

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

We keep internally and externally audited business continuity management documentation to help 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.

We're committed to protecting our customers and the interests of our 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
- try to meet our obligations to customers and regulators
- protect our reputation
- minimise the exposure to our business position
- return to normal operations as soon as practicable.

We'll do this by giving appropriate command and control to our major incident and crisis leadership teams.

3.4 Do we have a process in place to back up client data?

For data held on Aviva-owned platforms, we perform daily incremental back-ups and full weekly back-ups. We monitor this to make sure it happens.

We also synchronously mirror all critical data across our data centres. We would use a copy of this data if we needed to begin disaster recovery. We make an additional data copy every day to DXC data centre in Reading across dedicated, secure network links. We would use back-up media as a last resort should the mirrored copy become corrupted.

Where data is held on third party platforms, we have contracts in place with the service providers to make sure they back data up in line with the criticality of the service. The service providers must also perform regular tests to make sure they can restore the data if anything happens.

Aviva uses a cloud service based within GDPR EU compliant nation in which data is stored and multiple platforms operate from. This is based in Ireland and the data backed up in Germany.

4. Information security framework

4.1 Our information security framework

We have aligned our information security control framework to industry best practices, such as the Information Security Forum (ISF) Standard of Good Practice for Information Security and ISO 27001.

As part of the Third Party Information Security Assurance process, we carry out annual assessments of all our critical suppliers. This includes referencing independent SOC1/SOC2 Reports and ISO27001 Certifications, where available, as well as PCI DSS Certifications for those suppliers who process Dr/Cr Card Payments on behalf of Aviva.

As part of Aviva's 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 Do we have a process for detecting and managing any inappropriate or unauthorised IT activity?

We have a security incident and event monitoring tool in place 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 do we 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 must be authorised by either the individual's line manager or the system owner. A central IT access team sets up authorised access. The mandatory information security controls outline the processes for access provisioning, as well as processes for amending and deleting access. Line managers and system owners must carry out six monthly access reviews to make sure access is still appropriate, removing access 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 secure Virtual Private Network (VPN) between the remote user and Aviva and all information passed across the VPN is encrypted. Access is restricted to authorised users and managed through a soft token installed on the user's laptop. We uses Cisco AnyConnect Secure Mobility and multi-factor authentication is in operation.

Where users have Aviva supplied mobile phones with access to email, we use a mobile device management solution to secure any data access, together with remote wiping if a mobile device is lost.

4.5 What security controls are in place to protect our computers and networks?

We've secured our network perimeter with firewalls and intrusion detection/prevention systems and software. We've installed data loss prevention software to monitor external email and web traffic to ensure personal data is not sent outside of the organisation to unauthorised persons. We restrict internet access to approved website categories. We block personal webmail and file sharing services by default.

We protect all endpoint devices and servers with anti-malware software configured to look for signature updates multiple times a day. Devices are scanned daily. In addition, we patch all operating systems 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 Do we perform penetration testing and vulnerability scanning of its network and systems?

We carry out penetration testing of critical applications and infrastructure annually and whenever there is a significant change to that infrastructure. Any critical vulnerabilities identified must be remediated before the system/application goes live. All testing is carried out by Check or Crest accredited third parties. We perform internal vulnerability scans every week and network equipment, servers and workstations every month. If we identify any vulnerabilities, we will fix them in line with their severity.

4.7 How do we encrypt mobile data?

We have a cryptographic standard which outlines when to use encryption and what algorithms and minimum key lengths are acceptable. All emails containing confidential information will be sent using either Blue Padlock Encryption or enforced TLS where this is in place with the third party. 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 use wireless networks, and if so how are they secured?

We have a segregated corporate and guest wireless network. The corporate network is restricted to Aviva personnel and computers only and automated wireless intrusion detection/intrusion prevention systems (WIDS/WIPS) are in place to detect, alert, report, contain and prevent unauthorised wireless access. WPA2- Enterprise encryption is in place. Guest wireless access allows users to access the Internet only.

4.9 What security measures are in place to protect client data within our offices?

All access to Aviva premises is restricted to authorised personnel through 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. 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 Do we handle cloud technology and usage?

We do store some customer data in the cloud and we're moving to a more cloud-based approach. The data remains in region. For Europe, that means Dublin and/or Frankfurt, which complies with the UK GDPR requirements.

4.11 Do we have any offsite data centres where client data is stored, and how are these protected?

We've contracted with third party data centre providers for offsite data centre services. These companies are ISO27001 certified and provide us with annual SOC2 reports for 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.

4.12 How do we assess contingent workers or third party suppliers who have access to Aviva client data or systems?

Before bringing on new suppliers, we require potential supplier to provide details of their security framework, as well as go through a vetting process led by our procurement teams. Once we select a supplier, we put contractual agreements in place. This includes requirements for maintaining security programmes aligned to industry best practice standards (like ISO27001) and any legal and regulatory requirements applicable to the services provided.

Our Third Party Information Security Assessment teams carry out yearly assessments of all key suppliers with access to Aviva data to make sure they continue to comply with the terms of the contract.

5. Employees

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

We assess all staff and contingent workers before they start work with Aviva. This includes but is not restricted to

- 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.

There is a confidentiality clause in the staff contract of employment. For senior management, there are additional checks around media, regulatory requirements and directorships.

5.2 What training do we provide to staff and contingent workers on security awareness, data protection and compliance with Data Privacy?

Our business units have an embedded programme of education and awareness for all employees and contingent workers for the requirements of the data governance framework, policies and processes and applicable privacy legislation and regulation.

We deliver training through modules, presentations, which may be provided by external organisations, and other appropriate materials. We keep an individual record of training for all our staff.

Mandatory training

- Aviva employees and contingent workers complete online essential learning CBTs every year. This training ensures all relevant employees are aware of our data governance and business standards, policies and processes.
- All those who hold formally assigned data governance roles complete specific data governance training modules.
- Third parties with access to Aviva data are expected to embed Aviva's data governance into their training modules.

6. Transfers of personal data

6.1 Do we hold clients personal data outside the UK?

We use many third parties to support Aviva's processing of data and a number of these third parties (or their sub-contractors) process personal data outside of the EEA. We have the appropriate contractual measures in place to cover this and conduct due diligence and assurance on our third parties.

6.2 Do we transfer data to US?

Where a company will be transferring personal data originating from the UK or EU. To a third party located in jurisdiction without an adequate data protection regime we will take the following steps:

- Enter into new EU SCC
- Carry out a transfer risk assessment.

7. Data classification

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

We have a documented information classification and handling technical specification which defines the four levels of classification applied to all data - secret, confidential, internal and public. We use software to support this technical specification, which prompts users to label emails, documents and other end user applications with the appropriate classification based on the type of data being recorded.

We use identification software paired with manual reviews to assess outgoing emails and confirm they are appropriately classified.

7.2 How do we identify and protect sensitive personal data?

We treat all personal data as confidential. Only users within Aviva required to support clients would have access to the applications and systems used to process client data. We review all access every six months to make sure it remains appropriate.

Where we send confidential information across untrusted networks (eg, email or other web-based mechanisms), we'll encrypt it using either TLS, HTTPS or SFTP as appropriate. We may also password protect documents to provide an additional level of security.

8. Individual personal data rights

8.1 Do we have a process in place to manage subject access requests?

We have a subject access procedure in place as required under data protection law. This process meets Data Privacy 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 do we support customers exercising their personal data rights?

We have documented procedures in place to ensure we deliver processes which meet Data Privacy requirements for the fulfilment of individuals' rights. Our procedures make sure all staff can recognise and comply with individuals exercising their personal data rights, in line with local laws and regulations.

Personal data rights

A data subject will have the following rights under UK 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 Do we have a data retention policy?

Our documented guidelines set out our retention requirements for managing our data in line with legal and business commitments, including current and legacy product terms and conditions. They apply to all records, regardless of media or format. All data used for administering policies, is also subject to ongoing data quality assessments.

We have identified different business activities which act as triggers, after which we no longer need to process data. These triggers are aligned to events in a policy lifecycle, including quotation, policy maturity, cancellation, claim and transfer. Each of these event triggers a retention period, partly determined by our administration experience around the event, and also aligned to any legislative requirements where applicable. The retention period also takes account of limitation periods, within which legal actions must start to ensure we keep sufficient information to cover these incidences.

10. Disposal

10.1 What controls do we have in place to securely dispose of paper records?

All Aviva offices have secure confidential waste bins to collect any paper records that are no longer required. Each day, these bins are emptied and the secure bags stored in a locked cage ready for onsite shredding by an approved, certified, audited third party.

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

We have a contract in place with a third party accredited company who securely destroy hardware, including decommissioned hard drives. This includes securely wiping the drives to CESG standards before destroying the hardware itself. We carry out annual audits of both third parties involved in the secure disposal of media (paper and electronic).

10.3 Home working & disposal of Data

Following the increase of home working due to COVID19, Aviva have completed a full review of our Working from home policy along with the implementation of further controls and processes in respect of Data Security in the home working environment, all Aviva employees are currently signing home working Attestations and they are encouraged If taking any notes relating to our customers to take these electronically whenever possible. In cases whereby electronic notes cannot be taken notes these should be securely stored and locked away. We are also ensuring (subject to National/Local lockdown) any notes relating to our customers are to be taken to an Aviva office for secure destruction in one of our confidential waste bins or secure storage facilities. All employees are aware that under no circumstances should any handwritten notes be destroyed in the home environment unless destroyed by a shredder.

11. Engagement with third parties

We may sub-contract administrative services to a third-party service provider, sub-processor or sub-contractor. In these instances, we'll put appropriate contracts and security controls in place to protect customer data and ensure compliance with UK GDPR obligations.

We've reviewed existing contacts to ensure ongoing compliance. For new contracts, we'll make sure the third party is UK GDPR compliant from the start.

Our sub-contractors will change over time and some of the organisations we share information with may be outside the European Economic Area ("EEA").

We always carefully manage the transfer of information outside the EEA to protect customers privacy rights:

- We have an intra-group agreement with members of the Aviva group covering transfers within the Aviva group. This contractually obliges each member to make sure personal data receives an adequate and consistent level of protection wherever it's transferred within the group.
- Where we transfer data to non-Aviva group members or other companies providing us with a service, we'll obtain contractual commitments and assurances to protect personal data.
- We'll only transfer personal data to countries recognised as providing an adequate level of legal protection or where we're satisfied alternative arrangements are in place to protect our customers privacy rights.

12. Fair Processing Notice

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority with firm reference number 185896) is the main pension provider responsible for your Personal Information (known as the controller).

We collect and use Personal Information about you in relation to our retirement and investments products and services. Personal Information means any information relating to you or another living individual who is identifiable by us. The type of Personal Information we collect and use will depend on our relationship with you and may include more general information (e.g. your name, date of birth, contact details) or more sensitive information (e.g. details of your health).

Some of the Personal Information we use may be provided to us by a third party. This may include information already held about you within the Aviva group, information we obtain from publicly available records, third parties and from industry databases, including fraud prevention agencies and databases. Where you are a member of an occupational or workplace pension scheme, or if you join a savings product through your employer, we may obtain information from, and share information with, the employer who set up your pension or savings product, the trustees of the pension and any third parties who are providing services to you or them.

This notice explains the most important aspects of how we use your Personal Information, but you can get more information by viewing our full privacy policy at aviva.co.uk/privacypolicy or requesting a copy by writing to us at: The Data Protection Team, Aviva, PO Box 7684, Pitheavlis, Perth PH2 1JR. If you are providing Personal Information about another person you should show them this notice.

We use your Personal Information for a number of purposes including providing our products and services and for fraud prevention.

We also use profiling and other data analysis to understand our customers better, e.g. what kind of content or products would be of most interest, and to predict the likelihood of certain events arising, e.g. to assess risk or the likelihood of fraud.

We may sometimes make decisions using automated decision making. More information about this, including your right to request that certain automated decisions we make have human involvement, can be found in the “Automated Decision Making” section of our full privacy policy.

We may use Personal Information we hold about you across the Aviva group for marketing purposes, including sending marketing communications in accordance with your preferences. If you wish to amend your marketing preferences please contact us at: contactus@aviva.com or by writing to us at: Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD. More information about this can be found in the “Marketing” section of our full privacy policy.

Your Personal Information may be shared with other Aviva group companies and third parties (including service providers and regulatory and law enforcement bodies). We may transfer your Personal Information to countries outside of the UK but will always ensure appropriate safeguards are in place when doing so.

You have certain data rights in relation to your Personal Information, including a right to access Personal Information, a right to correct inaccurate Personal Information and a right to erase or suspend our use of your Personal Information. These rights may also include a right to transfer your Personal Information to another organisation, a right to object to our use of your Personal Information, a right to withdraw consent and a right to complain to the data protection regulator. These rights may only apply in certain circumstances and are subject to certain exemptions. You can find out more about these rights in the “Data Rights” section of our full privacy policy or by contacting us at dataprt@aviva.com.

13. Aviva Registered Addresses

All Aviva entity addresses and registration details listed below:

- Aviva PLC - Registered Office: St Helen's, 1 Undershaft, London EC3P 3DQ. Registered in England Number 2468686. VAT number 105 4373 00.
- Aviva Life & Pensions UK Limited - Registered in England, No. 3253947 with its registered address at Aviva, Wellington Row, York, YO90 1WR.
- Aviva Health UK Limited - Registered in England Number 2464270. Registered Office: 8 Surrey Street Norwich NR1 3NG. Authorised and regulated by the Financial Conduct Authority. Firm Reference Number 308139.
- Aviva Insurance Limited - Registered in Scotland, No. 2116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 202153. Member of the Association of British Insurers.
- Aviva Pension Trustees UK Limited - Registered in England No. 2407799. Registered Office: Aviva, Wellington Row, York, YO90 1WR. Authorised and regulated by the Financial Conduct Authority. Firm Reference Number 465132.
- Aviva Annuity UK Limited - Registered in England, No. 3253948. Registered Office: Aviva, Wellington Row, York, YO90 1WR. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Member of the Association of British Insurers. Firm Reference Number 202991.
- Aviva Life Services UK Limited - Registered in England, No. 2403746. Registered Office: Aviva, Wellington Row, York, YO90 1WR. Authorised and regulated by the Financial Conduct Authority. Firm Reference Number 145452.
- Aviva Equity Release UK Limited - Registered in England, No. 3286484. Registered Office: Aviva, Wellington Row, York, YO90 1WR. Authorised and regulated by the Financial Conduct Authority. Firm Reference Number 310433.

Contact details

If you have any questions or wish to exercise your rights, please contact our Data Protection team.
Write to: The Data Protection Team, Aviva, Pitheavlis, Perth, PH2 0NH
Email us: DATAPRT@aviva.com
Online form: https://www.aviva.co.uk/legal/subject-access-request/

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

PPEN32/S GN61006 07/2023