Aviva Data Privacy Statement June 2023

1 Purpose

1.1 Our Data Privacy Statement sets out the Aviva Group's commitment to process personal data in a compliant and fair way. It identifies the framework in place across the Group to implement this approach, including an overview of the key elements applicable to data privacy. This statement applies across the Aviva Group, specifically our core markets in the UK, Canada and Ireland.

1.2 Aviva publishes a number of public documents and commitments about its approach to compliance. This statement provides an overview of the key elements applicable to data privacy.

1.3 Our privacy policies, required by law, set out in more detail how we process personal data to offer our products and services, such as what we collect, use, share, retain and individuals' rights in respect of their data. Please see the appropriate page: UK, Ireland, Canada, Aviva Investors.

2 Background

2.1 Our Purpose at Aviva is "be with you today for a better tomorrow". In the operation of our business, our customers, colleagues and other stakeholders trust us to process their personal data responsibly, ethically and keep it secure.

2.2 We comply with laws and regulations and adhere to key regulators' requirements and principles in the countries and markets in which we operate. Failure to do so could damage the trust that individuals place in us, expose Aviva to regulatory sanctions including large financial fines and increase the risk of litigation, or prevent us from processing some or all personal data needed to deliver products to our customers.

2.3 We have policies and systems in place to ensure the highest standards of business integrity in our dealings with our customers, colleagues, communities and partners as well as regulators. However, we understand the importance of complying with internal requirements because it is the right thing to do, and it is an integral part of our culture. Operating a strong control environment helps us demonstrate that people are right to trust us and that we will use their data with their best interest at heart.

3 Governance and risk management

3.1 Personal data is processed in accordance with Aviva Group Data Privacy and Business Protection Standards. The Standards support our Risk Management Framework and sets out the way that Aviva Group wishes to operate globally. It is the responsibility of business CEOs to ensure that their business operates in line with the minimum requirements set out in Aviva business standards, including any internally or externally outsourced activities.

3.2 Primary responsibility for the delivery of the strategy regarding protection of personal data rests with the business Data Accountable Executives, who must ensure that appropriate internal controls are in place and operating effectively and that colleagues are adequately trained. The business is supported in meeting this responsibility by business unit data governance and data privacy specialists and the Group Data Governance and Privacy team.

3.3 Aviva Board and Group and business-level committees determine the strategy and focus areas.

3.4 Risk and compliance functions report to the Aviva Boards to ensure the strategy is adhered to and that we maintain a strong performance.

3.5 In addition, our Data Protection Officers independently report to appropriate Board committees on data privacy matters.

3.6 Key aspects of the data privacy framework include:

- Oversight and governance
- Risk controls tested annually at a minimum (more frequently if required based on the nature of the risk)
- Communication and training
- Due diligence on and risk rating of third-party relationships
- Confidential data treatment, retention controls and record-keeping
- Independent assurance and testing in addition to ongoing assurance activities within a 'three lines of defence' model

4 Personal data

4.1 Personal data means any information relating to the customer or another living individual who is identified or identifiable by us.

4.2 We have a duty to protect all the personal data we hold and to be clear and transparent about the way this data is used. Our Customer Data Charter outlines the way in which we keep personal data safe and secure and how we use it to improve our products and services.

4.3 Our Privacy Policies explain what personal data we collect about individuals and how we use it. We regularly review and, where necessary, update our privacy policies and communicate any changes as appropriate.

4.4 Individuals have legal rights under data protection law, which may differ depending on their country, state or jurisdiction. All individuals have the right to access the data we hold about them and request rectification or deletion of their data. We have processes in place to identify and fulfil these requests in accordance with data privacy law and regulation and to ensure that we manage data rights requests in a safe and compliant way.

4.5 Colleagues are trained to be able to identify and if appropriate manage personal data breaches such as recording the breach, taking steps to contain any risks and making appropriate notifications to regulators and individuals where required and in a timely manner.

5 Colleague Responsibilities

5.1 We require our businesses to have in place frameworks, processes, and tools to ensure colleagues learn and maintain the required skills and knowledge.

5.2 As a minimum, these skills and knowledge frameworks must include:

- Statutory or mandatory learning that is central to all colleagues.
- Regulatory learning requirements in-line with the expectations of the role.

5.3 More specifically, training on data privacy and cyber security is provided to all colleagues annually through our learning platform. Colleagues with specialist and high-risk roles receive additional training.

5.4 We have controls to ensure all information obtained by colleagues concerning Aviva – its businesses, practices, operations and employees – is only used for legitimately carrying out their duties and using only approved Aviva IT equipment.

5.5 Colleagues are encouraged to report any concerns of improper behaviour within the workplace locally or through our 'Speak Up' processes. Examples may be a breach of the Aviva Business Ethics Code or activity which appears illegal, criminal or unethical, including breaches of data requirements such as theft, deliberate/accidental loss or unethical use. Colleagues must attest to the Business Ethics Code on an annual basis.

6 Suppliers

6.1 Aviva requires appropriate contracts and agreements to be established, incorporating clearly defined performance levels, duties and responsibilities, obligations, and rights of both parties (as appropriate).

6.2 Our risk assessments determine if a contract needs to be actively and regularly managed to ensure contractual obligations and service levels are achieved, including Aviva's own obligations. We ensure appropriate action is taken if the supplier is not carrying out activities effectively and in compliance with applicable laws and regulation.

7 Related Aviva Policies

- People business standard (PDF 51KB)
- Procurement and outsourcing business standard (PDF 126KB)
- UK Customer Data Charter (PDF 66KB)
- The Aviva Business Ethics Code 2022 Living Our Values (PDF 2.8MB)
- Speak Up Charter (PDF 403KB)
- Human Rights Policy
- Aviva UK Privacy Policies