AVIVA
Good thinking

Helping you understand data governance

Your guide to the current rules and best practice for safeguarding data

Contents

The importance of safeguarding your data

Data is a vital business asset. It helps us make more informed business decisions about how we support customers and enables us to provide them with better choices.

Data governance gives ownership and oversight of how data is being looked after throughout its lifecycle. Through the growing use of digital technologies and evolving lifestyle changes, our customers are producing more data than ever before – making robust governance, driving good data management and security practices in the business, more important than ever. The way data is used and maintained is a key responsibility and is fundamental to the way we look after our customers, whether digitally or otherwise. We're responsible for managing a substantial amount of customer data – and it's essential we collect and care for it in an open and transparent way.

It's a legal requirement to keep data secure and up to date which can be challenging as the volume of data grows every day. That's why, at Aviva, we're keen to share our knowledge and do whatever we can to promote best practice.

How these guidelines can help

Aviva UK General Insurance has developed these best practice guidelines to assist partners, brokers and suppliers in the management of customer data related to Aviva's business.

The management of the integrity, quality, security and availability of data by organisations should enable them to make more informed decisions and, in turn, reduce data related costs whilst mitigating regulatory and reputational risk.

This document shares current best practices relating to data, as well as the most relevant current legislation and regulation. In addition to complying with current practices, organisations should also consider future regulation and legislation, such as General Data Protection Regulation (GDPR), and the appropriate actions that you need to take to ensure compliance. As with the example of GDPR, the regulator is likely to be far stricter and the penalties far greater if you don't comply.

As a legal entity, you're accountable for your own processes and procedures to ensure you adhere to regulation and legislation. Please make sure you review your processes and make any adjustments necessary.

As your trusted partner, Aviva's here to help. If you have any queries, please get in touch at **datamatters@aviva.com**

What do these guidelines include?

- Data protection regulation
- Roles and responsibilities
- Data management
- Data security
- Data breach and issue management

Throughout this guidance paper are links to additional sources of information. It’s recommended that you explore these and review them against your current practices.

Disclaimer: The content of this document is for guidance and illustrative purposes only. These guidelines are neither advice nor a checklist to be used prescriptively to manage data or mitigate data loss. We’d recommend consultation with your IT security, legal and risk department/contacts to conduct and implement comprehensive data governance.

Data regulation

All types of organisations hold and process details about individuals and legislation concerning the protection of personal data has been around for many years. Holding your customers' personal data is a big responsibility. This section contains a summary of the key legislation and regulatory bodies involved with the rights of individuals and how their personal and sensitive data is used, handled and protected.

Legislation	Key aspects
Data Protection Act 1988 (DPA)	The Act defines UK law on the processing of personal data on identifiable living people, controlling how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is: • used fairly and lawfully • used for limited, specifically stated purposes • used in a way that is adequate, relevant and not excessive • accurate • kept for no longer than is absolutely necessary • handled according to people's data protection rights • kept safe and secure • not transferred outside the European Economic Area without adequate protection.
EU General Data Protection Regulation (GDPR)	• This EU regulation was passed in May 2016 and addresses data protection in the digital age, giving the same rights across the EU, regardless of where people's data is processed. This comes into force in May 2018. • The Brexit decision initially clouded the position for the UK but we know now that the government has confirmed the UK will implement GDPR. The Information Commissioner's Office (ICO) has stated that it's committed to assisting businesses and public bodies prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. • Fines up to 4% of the global turnover of an organisation can be applied.
Privacy and Electronic Communications Regulations (PECR)	The PECR sit alongside the DPA and give specific privacy right to people in relation to electronic communications. • There are specific rules on: - marketing calls, emails, texts and faxes - cookies (and similar technologies) - keeping communications services secure - customer privacy in relation to traffic and location data, itemised billing, line identification and directory listings.

Legislation	Key aspects
Solvency II Directive	A Directive in European Union law that codifies and harmonises the EU insurance regulation. Primarily this concerns the amount of capital that EU insurance companies must hold to reduce the risk of insolvency. The regulation applies to all data used in the calculation of capital and Technical Provisions including all premium, exposure and claims data. It is therefore critical these sets of data are: • appropriate • complete • accurate • consistent

Regulatory body	Role
Information Commissioner's Office (ICO)	The ICO is the UK's independent body tasked with providing practical advice to organisations on how they should handle data protection matters and upholding information rights in relation to: • the DPA • the PECR • the Freedom of Information Act. The ICO holds a number of powers in respect of breaches of the DPA. These powers are not mutually exclusive and the ICO will use them in combination where justified by the circumstances. They include: • **taking action against organisations and individuals**, committing them to a course of action that improves its compliance • **criminal prosecution** • **non-criminal enforcement**, serving notices that require organisations to take specified steps to comply with the law • **audit and monetary penalties** of up to £500,000 for serious breaches of the DPA (occurring on or after 6 April 2010).
Financial Conduct Authority (FCA)	The FCA use a wide range of enforcement powers – criminal, civil and regulatory – to protect consumers and to take action against firms or individuals that don't meet FCA standards. The FCA's remit covers much more than data privacy but they can take action that includes: • withdrawing a firm's authorisation • prohibiting individuals from carrying on regulated activities • suspending firms or individuals from undertaking regulated activities • issuing fines • making a public announcement when disciplinary action is taken, publishing details of warning, decision and final notices.

All Aviva General Insurance activities must be in adherence with the DPA, as must those of our brokers, partners and suppliers. You should also follow more detailed data protection guidance and processes which will exist within your own business.

For more information on the DPA, you can access readily available material online, including the ICO's guidance.

The regulation and legislation included is correct at the time of publication. However, we recommend you continue to keep checking in case any changes are made or new regulation and legislation is introduced.

Roles and responsibilities

When it comes to managing data effectively it's important that responsibilities are assigned – but there's no 'one size fits all' approach. The roles within organisations will be proportional to the size of your business and the type of data handled. It is, however, important that roles are clear and defined. For example your Data Protection Officer (DPO) should be of suitable seniority, with appropriate knowledge of data protection in relation to your business. If you don't have a titled DPO you should have someone assigned to a role which manages risks related to data and ensures adherence to data legislation.

Your DPO's responsibilities should include:

- ensuring appropriate control assurance is in place for data protection
- reporting and acting promptly in the event of any **data incidents**
- developing and implementing a plan of activity to remediate any issues promptly
- championing the importance of data protection requirements and best practice to all employees within your organisation.

Your DPO should be known both within your organisation and to Aviva. Within Aviva, we have a Senior Data Protection Officer who is supported by DPOs and a network of 'champions', all with specific roles, that collectively help ensure appropriate data protection controls are in place and working effectively.

It's important that all people handling data receive training appropriate to their role on a regular basis. Dependent on the size of your organisation you may have forums in place to ensure appropriate oversight and escalation for the management of data.

Data management

Data creation/collection

Data is created or collected for a stated purpose with the recorded consent of the customer. Legislation is in place to protect a consumer's rights. This includes a right to privacy and the option to refuse the use of cookies and similar technologies.

ICO have developed useful guidelines that cover current legislative requirements and codes of best practice for both privacy and cookie policies:

- **Privacy Notices Code of Practice** – this provides details of why and how individuals must be aware of their right to privacy whenever information is collected about them, whether directly or indirectly. This Code includes clear details of the legal requirements and how to provide privacy notices.
- **Guidance on the use of cookies and similar technologies** – this provides practical advice for compliance with PECR, covering the legal requirements for storing information, and accessing information stored on a user's device, as well as explaining forms of consent and any exceptions to obtaining consent.

Looking to the future, the GDPR will require an 'unambiguous' affirmative consent and the consent must be active. An affirmative, active consent means ticking a box on a website or selecting an option that clearly indicates consent to the processing. 'Silence, pre-ticked boxes or inactivity' are inadequate to prove consent.

Data use

The DPA includes clear parameters for the appropriate use and holding of personal and sensitive data.

Within your organisation the use of data should be appropriately controlled. Best practice behaviours include the development, application and ongoing review of data processes and privacy impact assessments. These practices should be proportional to the types of data used, the scale of your business, and the permissions and consents given by the customer.

Processes should include:

- **mandatory conditions to restrict or prescribe the use of data**. These should be recorded, for example, in a **Business Data Dictionary**
- **any amendments to, or exemptions from, these conditions of use**. Again, such information should be recorded in a centralised place such as a Business Data Dictionary. This should be actively used for capturing the use of data and thereby safeguarding consistency and minimising the risk of misuse
- **proactive enforcement of all applicable conditions of use**. By ensuring users of data are aware of all applicable conditions they can remain compliant and avoid misuse and breaches of consents from occurring
- **periodic testing of compliance with conditions of use**. Where there are no means available to prevent misuse, testing must occur using suitably representative samples of data and usage
- **reporting of any violation of a condition of use**. Your organisation's DPO must be notified as soon as a violation is discovered. In turn, that person should consider their **data incident management** practices and any improvements that need implementing.

Data quality

The business decisions and actions we take are based on the information we have, so it's crucial that the quality of that information is managed and accurate. Before considering data quality management, it's important to consider how quality may be eroded. This could be as a result of:

- inappropriate structures in databases
- errors and omissions when data is initially collected
- reduced accuracy over time
- movement between systems and databases.

The Data Management Association (DAMA) – the international organisation for data management professionals – recommends **data quality** be assessed in terms of six dimensions.

Data quality dimension	Definition
Completeness*	The proportion of stored data against the potential of '100% complete'.
Uniqueness	No data item, record, data set or database will be recorded more than once, based upon how that item is identified.
Timeliness*	The degree to which data represents reality from the required point in time.
Validity	Data is valid if it conforms to the syntax (format, type, range) of its definition.
Accuracy*	The degree to which data correctly describes the 'real world' object or event being described.
Consistency	The absence of difference, when comparing two or more representations of a thing against a definition.

*Completeness, Timeliness and Accuracy are also a requirement of the DPA.

Data should be considered against these quality dimensions according to the level of its criticality. Best practice effective implementation would include controls to manage data quality. For example, non-critical data may not be used for decision-making or servicing customers and should therefore not be developed and reviewed as robustly as business critical data. Aviva strives to reflect all six dimensions for its critical data and has data quality controls in place to monitor it.

Records Management

Records Management is the discipline that encompasses rules and processes for creating and managing your records and information.

A record is anything made or received by an organisation that is evidence of the Company's operation. Records take many forms such as paper, electronic or other media. Examples include documents, photos, audio records, database fields, e-mail, voicemails and instant messages.

Legislation requires certain records be retained for a defined period of time and for no longer than is absolutely necessary.

As best practice, organisations should have policies and procedures in place for the management of their records. These should include:

- **Records Management Policy**
  Your policy should include Retention Guidelines to define the retention and destruction timescales for all records based on legal and regulatory requirements – reducing the risk of non-compliance. You also need to have a clear rational for the retention periods defined within your guidelines. We can provide a sample guideline template that you can use if you wish.

- **Records Management Procedures**
  These procedures explain the processes in place for the implementation of your Records Management policy. They need to include the identification of your records to enable:

  - implementation of embargoes
  - the provision of records as part of legal proceedings, regulatory inspections, or audits.
  - readiness for the destruction of records when they near the end of their retention cycle
  - the secure disposal and destruction of records

Further data management guidance

You can easily find more information on data management from a range of sources, such as:

- The UK branch of the Data Management Association (DAMA) at **www.damauk.org**
- Internal Organisation for Standardisation (ISO) which has developed various standards relating to data management – including data quality, records management, information classification and data security.

Data security

It's your responsibility to ensure your information and information systems are effectively protected from unauthorised access, use, disclosure, disruption, modification or destruction. Effective data security should include mechanisms that are easy enough for all stakeholders to abide by on a daily operational basis.

As best practice you'll have developed and implemented your own data security policy which would reflect your needs and those of external stakeholders. This section will provide guidance on:

- standards
- classification
- administration
- auditing.

Standards

Your data security standards should include controls, procedures and guidance within your organisation for effective safe handling and access to data. These standards will be appropriate to the scale of your organisation and the type of information handled, and are likely to include:

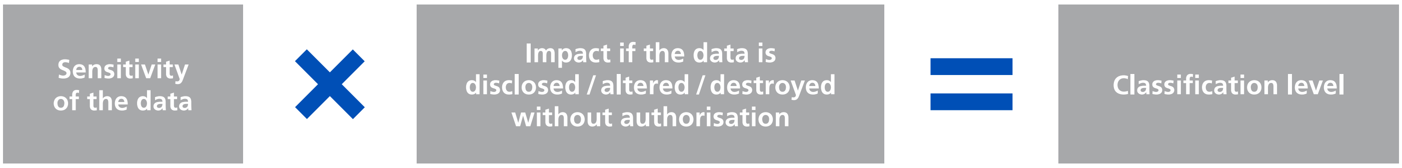
- defined data security controls and procedures
- physical protection
- management of data access
- monitor authentication and access behaviour
- proactive prevention tools.

Classification

Why should information be classified?
So that:

- the appropriate level of security can be put in place
- the level of risk of unauthorised disclosure or access is clear.

How should data be classified?
It's recommended that all communication of information includes clear classification. This classification of data should be based on the level of sensitivity of the data and the impact if that data is disclosed, altered or destroyed without authorisation.



Sensitivity of the data × Impact if the data is disclosed / altered / destroyed without authorisation = Classification level

What terms of classification could be used?
Various terms are in use across organisations, for example ‘public’, ‘internal use’, ‘confidential’, and ‘regulatory handling’.

Whilst you may already have your own classifications defined, the table below details how, at Aviva, we classify our data into four categories:

Classification	Characteristics of the information
Secret	If the information is disclosed intentionally or unintentionally, modified or lost the survival of the business could be threatened, or the competitive advantage, share price or value of the business could be impacted. **Labelling: ‘SECRET’ to be clearly visible at top and bottom of each page when printed**
Confidential	The information is intended for a specific, restricted audience and intentional or unintentional disclosure, modification or loss could damage the business, its share price or its customers. **Labelling: ‘CONFIDENTIAL’ to be clearly visible on each page when printed, electronic copies to be protected when shared**
Internal	The information is intended to be shared without restriction internally and its intentional or unintentional disclosure to unauthorised parties would result in only limited impact to the business or its reputation. **Labelling: ‘INTERNAL’ to be clearly visible on each page when printed**
Public	The information is available for external release or can be obtained from public records that are intentionally in the public domain. **Labelling: ‘PUBLIC’ to be clearly visible on each page when printed**

Exchanges of customer data should only be undertaken with a valid, restricted audience and security measures should be followed. Details of the best practice security approaches acceptable to Aviva follow in the ‘Overseeing your data’ section of these guidelines.

Overseeing your data

Why is administration important?

Effective administration will enable you to be confident that only the right people have access to your information within your own business and when sharing it with third parties (which also includes Aviva). Again, your administrative functions should be proportional to the size of your business and the type of information you hold. Your administrative practices should be recorded in your data standards, policies and procedures.

Access

It's important to maintain rigorous access controls for your applications, systems, networks and devices as well as physical access to your premises and confidential information.

Your procedures for staff should cover access rights to physical information assets and systems in which users, passwords, and permissions are managed. Processes should reflect new entrants, leavers or employees who change role as a minimum.

Please ensure everyone in your business is aware of the criticality of not leaving information unattended or insecurely stored:

- Laptops and any form of information that is secret, confidential or contains personal identifiable information should be secured overnight
- During working hours devices should be locked and information should not be left openly available if unattended.

Best practice suggests you have processes in place to manage both internal and external risks of misappropriate access, use, disclosure, disruption, modification or destruction.

Sharing of information

Data sharing is the reciprocal exchange of information, encompassing:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established reason
- exceptional, one-off decisions to share data for any of a range of purposes.

Whenever data is transferred to a third party the security of that data is paramount to protect our customers and the reputations of all parties.

Best practice for the sharing of sensitive corporate or personal data suggests that it:

- be securely protected with appropriate physical, technical, and organisational safeguards to prevent unauthorised or unlawful processing, and accidental loss, destruction or damage
- not be transferred to another legal entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.

Before sharing data with a third party, ask yourself the following questions.

- Does the data need to be sent?
- Is the data sensitive to the business and/or is personal data included?
- What encryption needs to be applied?
- Is the recipient the correct person to receive the data?

Encryption is a way of converting electronic data from being readable to being unreadable. The only way to transfer it back is with a unique key, thus ensuring only authorised persons are able to view the data. There are many techniques that can be used to do this, including WinZip, Password Protection and Transport Layer Security (TLS). The table below provides an overview of these techniques:

Encryption method	Overview
WinZip	WinZip is a file compression software package which has the added facility to secure attachments sent via email. If the encryption facility is enabled, WinZip encrypted attachments can only be opened by a recipient who has the same software and the password, which must be sent separately. Best practice would require electronic transfers containing confidential data to be encrypted. Please note, there are other similar software protection packages available that you could also use.
Password protection	Microsoft Office documents such as Excel and Word can be password protected so that the holder of the password can open and/or modify them. Password protecting files does not automatically encrypt them and the level of encryption varies depending on the version of software held.
Transport Layer Security (TLS)	Enforced TLS is a protocol that provides security and data integrity over computer networks such as the internet and is used in applications dealing with email, web-browsing and instant messaging. Emails sent via TLS are secured in transit, but on reaching the recipient's email servers the content can still be read by anyone who has access to the email. It's recommended that passwords are also used where there is a need to restrict access to a specified recipient. Wherever possible, TLS should be considered and discussed with your usual point of contact as best practice where regular transfers of confidential data are expected.

Auditing

Depending on the size and complexity of your organisation, planned reviews should be undertaken to ensure your processes are adhered to and best practice is consistently applied.

If you have any queries regarding this document please contact **datamatters@aviva.com**

Data breach and issue management

What is a data breach?

A breach is a failure of any part of the business to comply with an FCA – or other regulatory body – rule, guideline and/or principle, and is a breach of the DPA.

Examples include, but are not limited to:

- any breach of your Security Controls
- loss or theft of information
- unauthorised access either from inside or outside your network
- any malicious software or viruses downloaded to your computers.

Which result in loss or compromise of your customers' information.

Aviva must be notified as soon as you're aware of any breach impacting Aviva data. This can be done through your usual Aviva contact and via email to datamatters@aviva.com

What is a data issue?

An issue is where a process has failed but by chance the information hasn't been compromised. This also includes process failures which have the potential to be systemic. A data issue is an issue with an impact on or connection to data.

An example of a data issue is where personal information is sent by post to the wrong address, but the address is not a known address and the information is returned unopened.

Glossary and abbreviations

Business data dictionary

A central dictionary or glossary of data terms used within a business. For each data term it would typically include the meaning/description, security classifications and any additional important information such as where the data resides.

Cookies

Cookies are small text files which contain a small amount of information that is downloaded to your computer or mobile device when you visit a website. When you visit the website again, or visit another website which recognises that cookie, your device is able to communicate with the website and the website can read the information held in that cookie.

Cookies can be used to help you efficiently browse websites and to save you time by not having to re-enter your details each time you visit. They allow the website provider to provide you with information and show you content relevant to you. Cookies are also used to analyse how customers interact with websites so their customer journey can be improved.

DAMA

Data Management Association, an international organisation for data management professionals.

Data

All electronic and physical data, owned or used.

Data processing

ICO definition:

"…obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data,

b) retrieval, consultation or use of the information or data,

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

d) alignment, combination, blocking, erasure or destruction of the information or data."

Data Quality

Data is generally considered high quality if it's fit for the intended uses in operations, decision-making and planning.

You should use the quality dimensions to assess the quality of data.

DPA

Data Protection Act 1998

Encryption

The process of converting information or data into a code, predominantly to prevent unauthorised access.

Encryption of email messages protects the content from being read by entities other than the intended recipients. Email encryption may also include authentication.

Encrypting an email doesn't automatically encrypt any attachment, although the encryption to the email would have to be broken before you could access the attachment. Encrypting both the email and the attachment would give two layers of security but may not always be necessary.

GDPR	General Data Protection Regulation
ICO	Information Commissioner’s Office
ISO	International Organisation for Standardisation
PECR	Privacy and Electronic Communications Regulations

If you have any queries regarding this document, please contact our Data Governance Office at datamatters@aviva.com

| Retirement | Investments | **Insurance** | Health |

For Intermediary use only. Aviva Insurance Limited, Registered in Scotland Number 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.

AVIVA
Good thinking