DowgateWealth

Data Protection Policy

Document Governance

Policy Owner	Compliance Officer
Team Owner	Compliance
Review Cycle	Annually
Approving Person	Head of Compliance
Date Approved	25.04.2024

Version Control

Version	Date	Change Rationale	Author
1.0	04.2023	New standalone Policy	Compliance Officer
1.1	04.2023	Review	Compliance Analyst
1.2	04.2023	Approval	Head of Compliance

Associated Documents

Data Protection Procedures
Staff Handbook
Information Security Policy
Records Retention Policy
Compliance Manual

Contents

1. Purpose

This Policy document confirms the application of 'Data Protection' legal requirements to 'Dowgate', which for this Policy includes Dowgate Wealth Limited. This Policy should be read in conjunction with associated procedural documents so that a thorough understanding is received to enable Data Protection activities to be completed correctly.

This Policy, and associated procedures, only covers requirements in respect of 'personal data' and therefore does not cover data or information more generally which is covered in related Policies and procedures.

2. Audience

This Policy should be read by all relevant Dowgate employees and consultants and is accessible to all employees.

3. Regulations

Dowgate is regulated by the Information Commissioners Office (ICO) and therefore must follow their guidelines as to ensure Data Protection requirements are met.

On 27 April 2016 the European Union enacted the General Data Protection Regulation (2016/679/EU) which was duly adopted into United Kingdom (UK) law. On 23 May 2018 the Data Protection Act (DPA) came into force confirming legal requirements on firms but with slight amendments due to 'Brexit', the UK's exit from the European Union.

The ICO, the UK's regulator for Data Protection, has interpreted legislation to provide guidelines (not rules) for all firms processing personal data to follow. For firms to satisfy legal requirements they must follow guidelines and ensure adequate controls processes are put in place.

The purpose of the UK DPA is to ensure an individual's personal data or information is protected, subject to their individual consents.

4. Risks

Firms are required to put in place robust control processes to ensure that personal data is processed appropriately. Failure to put in place adequate measures may result in outcomes having a detrimental affect on individuals which includes both clients and employees. Personal data is a lucrative business for criminals who will try to obtain personal data for their own gain and in this regard, you should refer to Dowgate's Information Security Policy. Loss of personal data will affect both an individual's wellbeing as well their personal and financial affairs resulting in complaints.

Consequently, should Dowgate not perform adequate Data Protection activities when applicable, the firm may be subject to various supervisory actions depending on materiality including substantial fines. Employees and consultants not completing adequate Data Protection activities as required may be subject to processes as detailed within the staff handbook.

5. Dowgate's Approach to Data Protection

Dowgate takes the responsibility of processing individual's personal data and complying with the legal requirements seriously. Dowgate will only process personal data for its intended purpose and only retain personal data for as long as is needed. Dowgate has put in place a framework to protect and manage personal data accordingly. Dowgate will endeavour to satisfy requests from clients and employees in respect of their personal data.

6. What is 'Personal Data'?

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Examples of personal data include:

- Name
- Address
- IP addresses / Cookies
- Photos
- Date of births, etc.

Personal data may also include special categories of personal data which is more sensitive and therefore requires a higher level of protection. Dowgate may only process them in more limited circumstances. This means sensitive personal data about an individual's:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where this is used for identification purposes)
- Health data
- Sex life
- Sexual orientation
- Criminal convictions and offences

7. Data Protection Principles

The UK DPA sets out seven key principles and are the foundation for the underlying framework and guidelines.

7.1 Lawfulness, Fairness and Transparency

> 'Firms must identify valid grounds under the UK DPA (known as a 'lawful basis') for collecting and using personal data. Firms must ensure that they do not do anything with the data in breach of any other laws. Firms must use personal data in a way that is fair. This means firms must not process the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned. Firms must be clear, open, and honest with people from the start about how they will use their personal data'.

Dowgate has identified the lawful basis for collecting and using personal data which is detailed within its Privacy Notices for both clients and employees. Notices are provided at the start of their relationship with Dowgate. Periodic control processes have been built to ensure the lawful basis remains correct when there are changes to its proposition and services generally.

7.2 Purpose Limitation

> 'Firms must be clear about what their purposes for processing are from the start. Firms need to record their purposes as part of their documentation obligations and specify them in their privacy information for individuals. Firms can only use the personal data for a new purpose if either this is compatible with their original purpose, they get consent, or they have a clear obligation or function set out in law.'

Dowgate has identified the 'purposes' for processing personal data which is detailed within its Privacy Notices for both clients and employees along with the Legal basis. Notices are provided at the start of their relationship with Dowgate. Periodic control processes have been built to ensure the purposes remains correct when there are changes to its proposition and services generally.

7.3 Data Minimisation

> 'Firms must ensure the personal data they are processing is:
>
> - adequate – sufficient to properly fulfil your stated purpose;
> - relevant – has a rational link to that purpose; and
> - limited to what is necessary – Firms do not hold more than they need for that purpose.'

Dowgate only requests personal data for its business requirements and legal purposes. Dowgate will not retain personal data outside of its intended purposes. The Record of Processing activities (ROPA) document details the types of personal data collected against the business activity.

7.4 Accuracy

> 'Firms should take all reasonable steps to ensure the personal data they hold is not incorrect or misleading as to any matter of fact. Firms may need to keep the personal data updated, although this will depend on what you are using it for. If firms discover that personal data is incorrect or misleading, they must take reasonable steps to correct or erase it as soon as possible. Firms must carefully consider any challenges to the accuracy of personal data.'

Dowgate has put in place control processes to ensure personal data is reviewed periodically so that data items remains accurate and up to date.

7.5 Storage Limitation

> 'Firms must not keep personal data for longer than they need it. Firms need to think about – and be able to justify – how long they keep personal data. This will depend on their purposes for holding the data. Firms need a policy setting standard retention periods wherever possible, to comply with documentation requirements. Firms should also periodically review the data they hold, and erase or anonymise it when they no longer need it. Firms must carefully consider any challenges to their retention of data. Individuals have a right to erasure if they no longer need the data. Firms can keep personal data for longer if they are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.'

Dowgate has in place a Records Retention Policy which details the time periods for information to be retained. The Policy is supported by ROPA register which confirms different types of personal data items processed and the purposes for processing this data. In addition, an Information Asset Register (IAR) confirms the security arrangements in place associated with systems which process personal data.

7.6 Integrity and Confidentiality (Security)

> 'Firms must ensure that they have appropriate security measures in place to protect the personal data you hold. This is the 'integrity and confidentiality' principle of the DPA – also known as the security principle.'

Dowgate has put in place information security systems and processes to protect all information manages including personal data. These security systems are reviewed and upgraded periodically

as to ensure the risk of incidents is low. In addition, security systems are tested to assess the adequacy of systems in use.

7.7 Accountability

> 'The accountability principle requires firms to take responsibility for what they do with personal data and how they comply with the other principles. Firms must have appropriate measures and records in place to be able to demonstrate compliance.'

Dowgate through this Policy and procedure documents confirms individual responsibilities for Data Protection activities and has put in place processes to ensure compliance with legislation and ICO guidelines.

8. Data Protection Processes

Dowgate has detailed their Data Protection processes within the related procedure document to confirm a framework of which this Policy is part of. The procedures and related forms mirror sections in the ICO's 'accountability framework' and detail the requirements applicable to Dowgate.

9. Incidents and Breaches

Employees and consultants who do not completed Data Protection activities when required or correctly must inform their Line Manager and Compliance so the issue may be managed accordingly. Should an employee or Consultant lose or misdirect an individual's personal data they must inform their Line Manager and Compliance immediately.

10. Training

Employees and consultants will receive training by becoming familiar with this Policy and associated procedural documents. A specific e-learning training on Data Protection is also provided. Compliance may also provide specific training on a need's basis. Should any employee or consultant have any queries regarding Data Protection or the contents of this Policy they should contact Compliance prior to completing associated activities.

11. Responsibilities

Dowgate employees and consultants are responsible for processing Personal Data in line with this Policy and procedures. Compliance is responsible for this Policy and its maintenance including the procedures. Compliance is also responsible for providing training when required and recording any breaches as applicable.

12. Assurance

Dowgate will complete assurance periodically to ensure all employees are adequately completing Data Protection activities.

13. Record Keeping

Dowgate will record Data Protection activities and keep these in line with associated record retention policies.