

# Pharon Data Protection Policy/Privacy Notice

## Introduction

Pharon gather your personal information to provide you with suitable advice based on your needs and objectives. We also use the data to enable us to process any recommendation by arranging products and services on your behalf.

Personal information is collected and dealt with appropriately whether collected on paper, stored electronically in a computer database, or recorded through any other medium. The data we collect includes Sensitive Data, such as health details.

The lawful and correct treatment of your personal information is paramount to the Pharon philosophy, ensuring we maintain the confidence of those with whom we deal. We therefore impose numerous safeguards to ensure your information is secure in compliance with the General Data Protection Regulation (GDPR).

## Consent

Before gathering any personal information, we will request your explicit consent. Before you give consent, please ensure you fully understand why your information is required, with whom it may be shared and how the information will be processed.

## Legitimate Interest

Where we do not achieve consent, we may still be required to process and store personal data as we have a legitimate interest in keeping details of the financial advice provided to clients. In particular our regulator the Financial Conduct Authority asks that we keep records for a certain period of time and in some cases indefinitely.

Where we have this legitimate interest and you object to the processing of personal information, we will discuss this with you and seek ways to resolve the situation. We will cease processing your data unless we are required to process the data in response to a legal or regulatory reason. In this case we may have to continue to process your data. In this event we will inform you immediately. We will of course keep data to a minimum where possible.

Pharon sometimes receives data about individuals from third parties, such as employers, product providers, accountants and solicitors. Pharon will only request explicit consent in this instance if further data is requested. The initial introducer will remain responsible for gaining consent on any personal information they receive and share. Pharon will rely on the legitimate interest rule to process this data.

## Disclosure

In the course of our work on your behalf we may be required to provide elements of the data we hold on you to relevant third parties for example and including:

1. Product Providers and investment companies
2. Credit Reference Agencies
3. The Financial Ombudsman
4. The Financial Conduct Authority
5. Central Government
6. Social and Welfare Organisations
7. Healthcare Professionals

We will only provide data where absolutely necessary. We will never sell the data or use it in a way that is not for the purpose of fulfilling our advisory service, or complying with legislation.

## Principles and your Rights

As a Pharon client, we abide by the following principles to ensure your rights are upheld:

1. We ensure your information is processed fairly, lawfully and in a transparent manner in accordance with the GDPR.
2. Your information will not be used for any other purpose than that which is required for the advising, processing, administrating and servicing of financial products and services.
3. At no point will we request information which is irrelevant or in excess to that required.
4. We strive to ensure the information you provide is accurate and kept up to date. You can access your personal information anytime you require. You also have the right to rectify any inaccurate or incomplete information. We will endeavour to supply you with a copy of your data in an acceptable format as soon as possible upon request.
5. Personal information and the record of any advice we have provided based on that information may be required to be retained indefinitely. This is to enable the proper and efficient handling of all future queries, regulatory enquiries or legal proceedings.
6. We will, upon your request, remove and delete all non-relevant information. As mentioned, Financial Advisory firms are required to retain certain relevant data to ensure compliance with FCA regulations.
7. Your information will not be shared with any country or territory outside the European Economic Area, unless we are certain they will maintain your data protection rights.
8. We have organisational measures in place to prevent unauthorised and/or unlawful processing of personal information.
9. We employ strict regimes preventing the accidental loss, destruction of, or damage to your personal data.

In addition, we will ensure that

1. All staff which handle your personal information are appropriately trained and understand their contractual responsibilities.
2. Any third party organisation with which we share information, also has adequate measures in place.
3. Our methods when handling personal information are described clearly. We will promptly answer any queries you may have.
4. You are informed of any breach involving your personal information without undue delay, including details of the likely outcome and remedial actions.
5. All individuals are treated equally and fairly, irrespective of age, religion, disability, gender, sexual orientation and ethnicity.
6. You are well informed of our complaint procedure, including your right to lodge a complaint with the regulatory authority. Any personal complaints will be kept confidential.
7. A review of this data protection policy/privacy notice is conducted at least annually.

## **Responsibilities**

The board of directors is ultimately responsible for ensuring we meet our legal obligations.

The compliance director, Elizabeth Rule, is responsible for:

- Updating the board on data protection responsibilities, risks and issues
- Reviewing data protection procedures and related policies
- Arranging data protection training for all staff
- Handling access requests from individuals who wish to see their stored personal data
- Approving all data protection statements and communications

The IT manager, Nick Holness, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functional

All staff responsible for handling and processing personal information are trained on data protection and given the staff handbook which informs them of their responsibilities to:

- Keep data secure by taking sensible precautions
- Ensure no data is shared with unauthorised people or organisations, both internally and externally
- Report any concerns regarding data security to the compliance director

Pharon has a “Data Security Policy” which is kept up to date and you may request a copy.

## **Duty of Disclosure**

Failing to provide accurate personal information could affect the suitability of the advice you receive. Please therefore ensure you are accurate and correct when disclosing personal information.

## **Contact**

If you have any questions, please refer to your financial adviser or ask to speak to Elizabeth Rule (Compliance Director) at:

Tel - 01227 787000

Email - e.rule@pharon.co.uk