Telephone: 0345 366 5445
www.platform1online.com

Platform One
a premium service for private investors

DATA PROTECTION
&
PRIVACY POLICY

May 2018

Contents

1. Introduction

Like the Data Protection Act (DPA) that it will replace, the European General Data Protection Regulation (GDPR) applies to 'personal data' with a core principle of giving citizens and residents more control of their personal data. Personal data includes (but is not limited to) such details as name, address, telephone number, date of birth, etc.

The GDPR applies to both automated personal data and to manual filing systems where personal data are stored and accessible.

This data protection & privacy policy provides information about the way Platform One, and other organisations that we work with, manage and protect personal data.

Throughout this policy, 'personal data' means any information relating to an identified or identifiable natural person (a 'data subject') and the term 'individual' will be used in place of the more formal 'data subject'.

In this data protection & privacy policy, it is our aim to present the information using clear and plain language and in a manner that is concise, transparent, easily accessible and intelligible.

We aim to keep our policy under regular review and we'll place any updates on our website (www.platform1online.com).

2. Our Data Protection Principles

Platform One shall apply the following general principles in managing and protecting personal data so that it will be:

- processed lawfully, fairly and in a transparent manner in relation to the individual;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed and in accordance with the rules of our regulators, the Financial Conduct Authority (FCA);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, applying and using appropriate technical or organisational measures and constraints;
- managed in accordance with individuals' rights under GDPR - the right to request access to and rectification or erasure of personal data or restriction of processing concerning the individual or to object to processing as well as the right to data portability – unless such rights contradict regulations that Platform One is subject to.

3. Roles & Responsibilities

There are three important roles within the GDPR:

- 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;
- 'Sub-Processors' or 'Third Party Processors' mean a natural or legal person, public authority, agency or other body who, under the direct authority of the Controller or Processor, are authorised to process personal data.

This distinction is important because there are specific legal responsibilities that apply to those roles. The GDPR places specific legal obligations on Processors and Sub-Processors; for example, they are required to maintain records of personal data and processing activities and they will have legal liability if they are responsible for a personal data breach. The GDPR places other obligations on Controllers, such as:

- ensuring that contracts with Processors comply with the GDPR;
- providing information to individuals about the processing of their personal data;
- facilitating the exercise of individuals' rights.

Platform One's main business model is based on investment clients who are introduced by Independent Financial Advisors (IFAs). Each IFA signs a contract with Platform One who will have been chosen by the IFA to perform specific processing on the clients' personal data. The contracts that each IFA signs also specify any Sub-Processors and the processing they will perform.

Thus, in such cases, the Controller would normally be the IFA because the IFA provides the individual with financial planning advice and determines the purposes and means of the processing of the personal data, including the choice of Platform One and custodian business processes and systems. In those cases, Platform One would normally be the Processor and any custodian that Platform One uses would be the Sub-Processor.

Similarly, when a client signs up with a Trustee or Product Provider, the Trustee or Product Provider would also normally be the Controller.

The main cases when Platform One is the Controller are a) in the rare case when an individual uses Platform One without using an IFA and, b) when Platform One is dealing with the personal data of its employees. In these cases, Platform One is also the Processor.

4. Information Individuals Will Receive

The GDPR requires Controllers to provide individuals with information whenever any personal data relating to them is collected or received. The following information must be provided (possibly in the form of a privacy notice):

- The name and contact details of the organisation;
- The name and contact details of their representative (if applicable);
- The contact details of their data protection officer (if applicable);
- The purposes of the processing;
- The lawful basis for the processing;
- The legitimate interests for the processing (if applicable);
- The categories of personal data obtained (if the personal data is not obtained directly from the individual it relates to);
- The recipients or categories of recipients of the personal data;
- The details of transfers of the personal data to any third countries or international
- organisations (if applicable);
- The retention periods for the personal data;
- The rights available to individuals in respect of the processing;
    - The right to withdraw consent (if applicable);
    - The right to request (from the Controller) access to and rectification or erasure of personal data;
    - The right to restrict processing concerning the data subject or to object to processing;
    - The right to lodge a complaint with a supervisory authority;
- The source of the personal data (if it is not obtained from the individual it relates to);
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data;
- The details of any automated decision-making, including profiling (if applicable).

5. When Individuals Will Receive Information

The Controller shall provide the information referred to in Section 4:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- if the personal data are to be used for communication with the individual, at the latest at the time of the first communication with that individual; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed to that recipient.

The information does not need to be provided every time personal data is received from an (or sent by) an individual – the obligation is to inform an individual if they haven't previously been provided with such information. Thus, some Controllers might elect to send this information to existing clients as a 'one-off' exercise.

6. Personal Data Collected

Due to the nature of our business and of our partners' businesses, the personal data required will typically relate in some way to individuals' personal and financial circumstances. In the case where a new client is being introduced, the personal data would need to be sufficient to facilitate anti-money laundering and identity verification rules and regulations. In some cases, personal data may also include special categories of such as data about an individual's health if this is necessary for the provision of the service(s).

Where special category data is required, an adviser firm should have obtained explicit consent to collect and process that data.

7. Why Does Platform One Collect Personal Data?

The primary legal basis that Platform One has for the processing of personal data is for the performance of a contract we have with another company such as an adviser firm. One of those firms (acting as Controller) should notify the individual (investor) of the legal basis for using personal data when that personal data is provided or received. Such data is essential for us to be able to carry out the services that are expected of us effectively. Without the personal data described, Platform One and the other companies we work with would be unable to fulfil our contractual, legal and regulatory obligations.

For many adviser firms, the legal basis for processing personal data will be one or more of the following reasons: consent, performance of a contract, legal obligations or legitimate interests. If the firm does not have one or more of these grounds as a basis for processing the data, then the individual may review and question the need to provide the data.

8. Who We Might Share Personal Data With

We share personal data with a custodian, depending upon the service involved. A different custodian is used for each service (i.e. our UK Service, International Service, International Plus Service and our Global Service each use a different custodian). The Controller will provide individual investors with specific details at an appropriate point in time (typically at the time of new client application or specific product application).

We will ensure that the contracts that Platform One has with such Sub-Processor companies are in accordance with GDPR and to ensure that the nature and purpose of the processing is clear, that they are subject to a duty of confidence in processing personal data and that they'll only act in accordance with appropriate instructions.

When it is necessary for personal data to be sent to or collected by another party (such as a SIPP or other product provider), we'll use appropriate security measures to protect the personal data.

To fulfil our obligations in respect of prevention of money-laundering and other financial crime we may send personal data to third party agencies for identity verification purposes.

We will not share personal data with companies outside the Platform One Group of companies without seeking prior consent.

To comply with legal and financial regulations (including audit), we might need to share personal data details with HMRC, the FCA and accountancy or legal firms.

9. Period of Personal Data Retention

In principle, Platform One shouldn't hold personal data for longer than is required under the terms of our contract for services with an adviser firm (or in some cases with specific individuals). However, we are subject to regulatory requirements to retain data for specified minimum periods (normally a minimum of 5 years).

We also reserve the right to retain data for longer than this due to the possibility that it may be required to defend a future claim (not necessarily against us). Consequently, we may hold personal data indefinitely.

10. Other Obligations

Breach Notification

Under the GDPR, a 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Processors will also be required to notify their customers and the Controllers, "without undue delay" after first becoming aware of a data breach.

11. Complaints & Communications

If you are unhappy with how personal data is processed, you can write to the relevant Controller or, if you think the issue is more pertinent for Platform One, you can email the Platform One Data Protection Adviser via info@platform1online.com

You also have a right to lodge a complaint with the supervisory authority for data protection. In the UK this is:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire, SK9 5AF

Platform One Group Ltd. is registered in England and Wales (№ 09197677). Platform One Ltd. is regulated by the Financial Conduct Authority (№ 542059).

If you have any questions about our data protection & privacy policy or information we hold about you, please contact our Data Protection Adviser, email info@platform1online.co.uk or write to us at Platform One Group Ltd, Cedar House, 3 Cedar Park, Cobham Road, Wimborne, Dorset, BH21 7SB.