DATA PROTECTION AND SECURITY POLICY

Introduction

The General Data Protection Regulation (GDPR) applies from 25th May 2018. It aims to protect the privacy of all EU citizens and prevent breaches of their personal data. It applies to all organisations controlling or processing personal data.

The protection of personal data is not a new requirement but the GDPR tightens a number of the existing requirements and adds to the principles of data protection.

Simplicity Pensions Limited (SPL) is a data processor under the terms of the GDPR and must comply with the provisions of the GDPR as they relate to data processors. This Policy sets out how we ensure compliance with the requirements of the GDPR.

The basis under which we process personal data

We may process personal data to enable us to provide Client Services as specified and detailed in Client Agreements, Letters of Appointment or other such instructions received from our clients in writing, including those received via email.

Our formal purpose for the processing of the data is that of 'legitimate interest', acting on behalf of our clients to assist them in the provision of pension and other workplace employee benefits.

We may process the data for as long as is necessary under the terms set out in any Client Agreement, Letter of Appointment or other such instructions, and as set out in our Terms of Business.

We may process data to provide some or all of the following Client Services:

- pension automatic enrolment services, including the assessment of eligibility under the workplace pensions automatic enrolment regulations and the provision of generic information to pension providers for the costing of a group pension arrangement;
- pension and benefit consulting and secretarial services, including the reporting of membership information, liabilities and statistics to employers and pension scheme trustees, and the provision of information to pension and employee benefits providers or associated or sub-contracted third-party employee benefit consultancy and advisory firms for the purposes of costing of group pension and/ or employee benefits arrangements;
- pension and employee benefit arrangements governance services, administration services and financial management services including the calculation of benefits due to an employee or pension scheme member and/ or their dependants and beneficiaries, required annual processes, accounting functions and the preparation and production of annual Reports and Accounts, actuarial valuations, updates and costings, and employee, pension scheme and employee benefit scheme member calculations;
- provision of data to associated or sub-contracted third party data controllers or processors for the purposes of the administering and financial management of pension and employee benefit arrangements.

DATA PROTECTION AND SECURITY POLICY

What data we process

The scope of the personal data that we process depends on the nature of the Client Services provided, and may include some or all of the following in relation to employee and/ or pension and benefit scheme members:

- name, contact details (postal address, email address, mobile and telephone numbers), gender, date of birth, occupation, description of physical or mental health and identifiers such as National Insurance number, pension or member reference number and employee number (where applicable);
- family, lifestyle and social circumstances such as details about partnership and marital history, details of family and dependants;
- employment details such as salary, earnings, full-time / part-time status, pensionable pay, length of service, employment dates and career history, attendance records, job title and job responsibilities;
- financial records such as any other income, pension savings, personal insurances (such as life assurance, medical, health, illness and accident), pension payments, tax code and other State benefits;
- any information regarding direct dealings with us.

Where the data is stored and how we keep this data secure

Data is stored primarily in electronic soft copy means but may also be stored in hard copy format. All electronic data is held locally on SPL desktop and laptop PCs and from time to time, on SPL-provided mobile phones, as well as being held in cloud-based back-up solutions.

All SPL PC equipment runs the Microsoft Windows 10 operating system with all updates automatically downloaded and installed when available. Access to the data is via unique login to the Windows 10 environment and is restricted to SPL personnel only. The hard drives containing personal data are encrypted.

All electronic files are automatically backed up and stored in a secure online cloud-based solution.

All SPL-provided mobile phones have security measures enabled and can only be accessed by correctly entering the security information or via finger-print recognition. Phone data can be erased remotely in the event that the phone is lost or stolen. No data is normally held on a phone for more than two weeks.

All SPL IT and mobile phone equipment is protected against the latest online and email threats through the use of comprehensive antivirus, firewall and anti-phishing technology.

DATA PROTECTION AND SECURITY POLICY

Where personal data held in soft copy format is shared with clients and other third-parties, this is pseudonymised where possible and the data is password protected with passwords being sent via separate transmission. Where possible, passwords are sent via an alternative means to the data itself (i.e. SMS or encrypted messaging services). In some circumstances, it may be possible to anonymise data and this is undertaken where possible.

Where personal data is stored in hard copy format, these are within client specific files which are kept in locked filing cabinets. Access to these cabinets is restricted to SPL personnel. Hard copy files may only leave the premises' of SPL personnel in the event that they are required at a client's premises for the fulfilment of the Client Services. We operate a clear-desk policy.

All SPL personnel are provided with data protection training and are made aware of the security protocols that SPL adheres to. Failure to comply with these may result in disciplinary action.

Use of sub-contractors and sub processors

We may use sub-contractors from time to time to provide agreed the Client Services. Third-party suppliers may also be used in the fulfilment of the Client Services. We ensure that any sub-contractors and third-party suppliers (who will act as sub processors) meet and operate within the requirements of the GDPR and have adequate data protection and security protocols in place.

Data retention

Personal data is held only for the purposes of fulling the Client Services. Non-sensitive personal data will normally be retained throughout the period during which the Client Services are provided. This will usually be for at least the duration of the initial contract term agreed under the Client Agreement; data may be retained thereafter should the Client Services continue to be provided following the expiry of the initial term.

At the end of the provision of Client Services and in the absence of any written instruction from the client to return or securely destroy the data, the data will continue to be held securely and in archive for the minimum period required by law or a period of 12 (twelve) months from the end of the provision of the Client Services. Retained data will continue to be subject to our data security policy. At the end of the period, or at any time at the written request of the client, the data will be returned or securely deleted, except where this is required to be maintained by law or other regulatory requirements, and/ or for the purposes of defending against a complaint or claim.

Any sensitive personal data will be returned or securely destroyed no later than the end of the provision of services, except where this is required to be maintained by law or other regulatory requirements, and/ or for the purposes of defending against a complaint or claim.

DATA PROTECTION AND SECURITY POLICY

Data sharing

Personal data will be held only for the purposes of fulling the Client Services and will not be shared with other parties other than for the purposes of the Client Services or as required by law and the provisions of the GDPR.

In the event that we receive a valid 'subject access request' from an employee or scheme member of a client, we will notify the client in their capacity as Data Controller and agree the responsibility for responding to the request.

Data breaches

In the event of a personal data breach, we will notify the relevant client/s as soon as practically possible after becoming aware of the breach and within no later than 48 hours. We will assist the client/s in providing information and the circumstances regarding the breach as per Article 33 of the GDPR to the supervisory authority.

Data processing outside of the EU / EEA

SPL's office and places and business and staff are based in the UK. Therefore, in the normal course of business, personal data will not usually be transferred to or accessed from outside the EEA.

However, data may on occasion be stored on servers outside the EU or EEA where third-party email hosting services or cloud-based backup solutions are used. Where this may be case, we ensure that the international organisation ensures an adequate level of protection.

On occasion SPL's personnel may need to access data whilst outside of the EEA – this may be case in the event of a member of staff taking an SPL laptop on holiday with them and undertaking work whilst away. In this event, all data will be subject to the IT security policy as set out in this Policy and the member of staff will be required to keep the laptop with them or adequately secured and locked at all times.

Internal responsibility for data protection compliance

We are not required to appoint a Data Protection Officer. The designated person responsible for data protection and security within SPL is Martin Ralph.