General Data Protection Regulations
Policy

All Square Finance Limited is a Claims Management Company regulated by Claims Management Regulation Authority in respect of regulated claims management activities CRM31952. The regulated business provides claims services to consumers to help recover redress in respect of Payment Protection Insurance, Self-Invested Personal Pensions and other financial products. The list of consumer claims services both regulated and unregulated is not exhaustive.

Our claims services are provided to private individuals by way of consented contact and legitimate interest once the individual appoints us to make a claim on their behalf. Throughout the GDPR policy documents these individuals are referred to as either 'clients' or 'consumers'. Both clients and consumers contacted by All Square Finance Limited provide their personal data to be contacted to discuss a potential claim and to manage their claim in contract with All Square for the provision of their service.

We make contact with our clients in contract and with potential clients using data purchased from legitimate and compliant data suppliers, by advertising and through website domains www.allsquare.co.uk and www.sippclaims.uk

The nature of our business is such that it is required to comply with The General Data Protection Regulations 2016 with effect from 25th May 2018.

Daniel Hall

Data Protection Officer
May 2018

INDEX

SECTION 1 GDPR OVERVIEW

To Comply with GDPR we aim to evidence (list is not exhaustive) that:

- Data is processed lawfully, fairly and transparently
- Is collected for an explicit and legitimate purpose.
- Is accurate, up to date and retained only for as long as it is necessary
- Data held is relevant and limited to what is necessary
- Robust security systems are maintained and tested.

To achieve our GDPR implementation we have taken the decision to interpret the EU GDPR 2016 to make all necessary amendments to comply. Our GDPR consultation commenced in November 2017 and was initiated onsite in February 2018 with the assistance of Lia Richardson of SK Compliance Services.

We disposed of all data that has not been subject to a claims service contract and established a relationship with a new data supplier. We carried out significant due diligence and established suitable processes to ensure that we secure provable consent on all client data. Prior to the introduction of our GDPR compliance strategy we had robust due diligence processes in place to test data consents across random samples of data as required by our regulator, The Ministry of Justice.

Our ongoing aim is to exceed the requirements of our regulatory regime and to embrace the concept of consent within the context of the GDPR throughout our business.

Consent should be freely given, specific, informed and an unambiguous indication of the Data Subject (DS) wishes. Single opt ins tick boxes are not considered sufficient we ensure that the DS is made fully aware of what it is they are opting into. The service we provide naturally requires that we share data with banks, regulators and other third parties; we advise the DS who we are sharing their data with. We also work with form fills on our websites. The data suppliers we use also operate prize websites and adverts on other third-party domains. All client contact is designed to provide the consumer with access to our Privacy Policies and the data we capture via any capture forms are recorded appropriately.

We use data suppliers and online webforms to obtain consumer consent to contact them in relation to a mis-sold PPI policy or a Self-Invested Personal Pension. The data subject can indicate how they wish to be contacted and in the case of a SIPPS enquiry we send a claim pack to the consumer which allows them time to read our terms and conditions, read and sign a form of authority and return the form to us so that we may make a SIPPS enquiry on their behalf

We name any brand where we share the consumer data with a firm to do marketing for us or to make follow up calls after the consumer has given their initial consent. At the time of writing this policy we noted that the GDPR may conflict with our regulator rules that relate to agency principles: An agent must work to your brand we therefore avoid working with any un-authorised firms when seeking out clients wishing to contract for regulated claims management services.

This policy document aligns our existing Data Protection and PECR compliance strategies to the GDPR and initiates with effect from 25th May 2018. We have updated all Privacy Policies to accommodate the increased data subject rights of GDPR and have also updated our Cookie Notices. We have conducted GDPR consultation with all Third-Parties who touch our consumer data.

SECTION 2 FAIR & LAWFUL PROCESSING

The person responsible for Data Protection at All Square Finance Limited is the Managing Director Daniel Hall who is available by email daniel.hall@allsquare.co.uk

All Square Finance Limited processes consumer data lawfully based on one of the following:

a) The data we are processing is fully consented for All Square Finance Limited and/or the associate trading names as registered with our regulator The Ministry of Justice to process. The consents we hold to contact data subjects are provable in accordance with Article 6 1 a) of GDPR and, all due diligence on our data suppliers has been carried out.

b) We process customer data for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject in accordance with Article 6 1 b) of GDPR;

c) By way of a legitimate interest in accordance with Article 6 1 f) of GDPR.

Where we obtain data direct form the data subject we are the sole data controller. Purchased data is transferred to All Square Finance Limited securely; the data supplier retains provable consents and is therefore a joint controller. To carry out our services effectively we may share data with other data processors however, we provide our data subjects with details of our data processors.

Our aim is to provide clear and transparent information about how we use personal data. Where we record personal details for a specific purpose our customers are directed to our Privacy Policy published on our websites www.allsquare.co.uk and www.sippclaims.uk and across our social media accounts or third-party websites where we collect data. We may also provide details of our Privacy Policy by email, by way of a hover box or with a consent notice at a privacy point within our process.

If we hold personal information that relates to a Vulnerable Consumer make sure this is prominent within our customers private data file so that when their data is processed staff are aware and consider the individuals circumstance/s to assist the customer understand the process, we need to follow to provide our service.

We provide our Privacy Policy in other formats for individuals who are unable to access the Privacy Policies through our web-based resources. We can provide paper copies of our

Privacy Policy where necessary to an authorised carer or relative. We also comply with the Equality Act 2010 to help individuals who need assistance with reading due to language barriers, partial sight, blindness or any other adjustment. If you experience any day to day problems that may affect your ability to understand our Privacy Policy your carer or a family member should be able to assist you. Your appointed representative may call us on 0113 323 9955 to discuss how to set up an authority to assist the individual concerned.

SECTION 3 PROCESSING PURPOSE

We process data to contact consented individuals to enquire about Mis-sold Payment Protection Insurance and on mis-sold Self Invested Personal Pensions or similar.

During processing, calls are recorded and where the data subject provides information the call is appropriately dispositioned and thereafter processed in accordance with the disposition. As part of any marketing process carried out by a call centre we engage in full TPS checking every 28 days and suppress data accordingly.

Where a data subject appoints us to provide services we engage clients in accordance with our terms of business which are available in the footer area of our website www.allsquare.co.uk and sippclaims.uk

Once we are in contract with a data subject we then have a 'legitimate purpose' for the processing of that data subject's personal data. We will only ask you for information that is relevant for the service we provide.

Because of the service we provide we process information that relates to your personal finances and may also process information about your health by way of 'pre-existing health conditions'. We also share your data with banks, lenders, the Financial Ombudsman, investors, administrators and occasionally other third-party service providers.

We do not transfer any personal data to any third-party countries outside of the EU.

Of the data, we market we retain that data processed in accordance with Article 6 1 a) for no longer than 12 months. Where a data subject contracts with us, the data is retained as required by law but for no longer than 6 years after the conclusion of the service provided. Where reasonably practicable data is archived and/or minimised so not to be identifiable as the data subject unless required by law or is subject to a Subject Access Request.

We operate robust organisational security systems which are available upon request as documented in our Information Security Management System.

In the event of a complaint or breach relating to any aspect of our Data Protection our records will be made available to the relevant supervisory authority.

SECTION 4 SUBJECT ACCESS REQUEST POLICY

You have the right to request access to the personal data that we hold about you. The definition of personal data is any personal information held on record anywhere by All Square Finance Limited not just in electronic format but in any paper file or structured file we hold containing your data. It includes information held in correspondence and other formats.

You have the right to be advised whether your personal data is being processed and access to your data. On receipt of you're a Subject Access Request we will provide:

- Details of the purpose of processing;
- The category of your personal data being processed;
- Details of recipients or categories of recipients with whom your data may have been shared or disclosed;
- How long your data will be stored;
- Details of where your data was sourced if you did not give us your data;
- Details of any automated decision making or profiling;
- Information regarding right to rectification, erasure, restriction and objection
- The right to make a complaint to the Supervisory Authority

You may make a Subject Access Request, also known as a SAR by writing to us with your name, contact number, email address and where applicable an account reference number. You should write to The Data Protection Officer at: All Square Finance Limited Unit 1C Riparian Way, The Crossings Business Park, Cross Hills, Keighley, West Yorkshire, BD20 7AA alternatively you mail email us at daniel.hall@allsquare.co.uk

The process of dealing with Subject Access Requests can be difficult especially during times of high demand. We continue to design and implemented specific systems, policies and internal procedures to be as efficient as we can in locating and providing a copy of the information we hold about you. The following information is provided so that you can understand how we process your request:

On receipt of your request we will check your identity, this may require us to call you in person to ensure we are in receipt of the correct information. We will check your identity using our usual procedure or by asking you to forward a copy of identification documents to us.

We take your data protection seriously so must be satisfied that we are releasing data to the correct person.

If you have a condition that means you cannot make your request we can accept a SAR from a third party authorised by you to make the request on your behalf, such as a carer. If you are submitting a Subject Access Request on behalf of someone else you must be able to satisfy us that you have the authority to do so by providing us with a signed letter of authority from the person you are acting for which should provide the full name, date of birth and address of the person acting on your behalf. We may ask to see proof of identity of your representative.

If the person or organisation making the request on your behalf has Power of Attorney (POA) you will be asked to provide us with a copy of the POA.

Once we have received you SAR satisfactorily, including all relevant proof of your identity (As detailed above) we will provide you with the information you have requested free of charge within 30 days from the data of a satisfactory request. We will provide you with full details of the information we hold about you along with copies of **the specific** information you have requested.

Important Note: If your request is made by electronic means including by email, unless you specify otherwise, the information will be provided to you in electronic form and not in paper format. Once we have fulfilled our obligation we maintain a log of your request to demonstrate data subject rights compliance.

If you require further copies we may charge you a reasonable fee to cover our administration costs. There are specific circumstances where we may not have to respond to a SAR, these are provided in our 'Subject Access Request Refusal Policy'

We have a bespoke Customer Relationship Management (CRM) system that holds your data within a unique data file relevant only to you. A member of staff can search for your data using the correct parameters designed for that function and once the correct information is available your identity is confirmed before the system is then activated to issue your information request to you.

SECTION 5 ERASURE POLICY

We have an obligation to extend the 'The right to be Forgotten' in circumstances that apply and to erase your personal data without undue delay.

This erasure policy gives you an overview of situations when your personal data may not be able to be fully erased. Our services deal with legal claims and require certain information to be retained even when you ask to be forgotten. In cases where we cannot carry out a full erasure of your personal data we may minimise, anonymise and then archive your data to a safe, secure location which is only accessible by our Data Protection Officer and our IT Director so;

If we have processed and submitted a claim on your behalf there are certain circumstances where the retention of your personal data is still necessary in relation to the purpose for which your data was processed. It is therefore unlikely that we will be able to do a full erasure of your personal data because of the legal aspects associate to the claims process, and because we may be required to provide information to our regulators at any given time. Whilst we may no longer need your data for processing your data may be needed to establish, bring or defend a legal claim. Once your case has concluded and a period of 6 years since conclusion has passed, your data will then be erased.

You can request erasure without undue delay in the following circumstances:

1. If we hold your data from one of our sales campaigns to which you have previously consented and where you have never contracted with <Insert Co Name>, you can withdraw your consent and asked that your personal data be erased;

2. If we hold your data and you object to your data being processed on the basis that we have no legitimate interest in the processing of your data;

3. If your data has been unlawfully processed by us;

4. We are required to delete your data to comply with our obligation to the Supervisory Authority*;

If we have shared or made your personal data public on receiving request to erase your personal data, we will take reasonable steps to inform the controllers of shared data that you have requested that your personal data be erased. We will request that all links, copies and replications of your data be erased.

When we erase your data, we will also erase any 'Do Not Call' (DNC) status that you may have requested. A DNC status ensures that your personal data is supressed and not called by us again but by erasing your data, we lose your suppression data which means that if you are not on the TPS register, you may end up being contacted by us during a new sales campaign against another consent that you may have made or make in the future. This advice will be provided to you on receipt of an erasure request

SECTION 6 DATA PORTABILITY POLICY

If you start the claims process with All Square Finance Limited then decide to use a different CMC we will have no obligation to transfer any information/data established as part of our claims processing to the other CMC. We are only obliged to provide your alternate CMC with the original data you provided not data we have established as a result of work we have carried out. Changing CMC's mid-claim can considerably slow down the resolution of any potential claim and may give rise to a charge for 'work done' as set out in our terms of business.

Transfer of personal data from the UK to a data processor who is either in the UK or is in any other EU or non-EU country.

As a UK based data controller providing a claims management service we only transfer data within the UK, EU or EEA to other data processors to process your personal data. Each of the data processors that process transferred data have a written contract under which they agree to act only on instructions from us the data controller. The data processors we transfer data to must comply with obligations which specifies that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

The contract also contains details of the processing to be carried out, details of the data processor's obligations, and certain other details.

As part of our claims service we may need to transfer personal data we hold to a location within/outside the UK, to someone either in the UK, EU, or EEA or to a country outside the UK, EU, or EEA, so that they can carry out processing of that data on our behalf.

For example we may on occasion engage a data processor to receive or access our customer data so that we can provide you with certain services we use to run our business, e.g. IT or administrative services. Our providers agree that they may not make any other use of the data or disclose it to any third party. All data is transferred lawfully to protect the individuals whose personal data is being transferred.

Data Transfer Outside the EU

It is highly unlikely that we will transfer your personal data outside the EU or EEA however, if this were to be introduced we have due diligence processes in place to make sure the destination country provides an adequate level of protection for the rights and freedoms of the individuals concerned.

SECTION 7 OBJECTION, RESTRICTION TO PROCESSING & RECTIFICATION POLICY

You have the right to object or restrict the processing of your data in the following circumstances:

i) The accuracy of your data is in contention;
We will restrict processing your data whilst we correct and verify your data.

ii) You have reason to believe that processing is unlawful; We will restrict processing your data whilst we carry out an investigation about the lawful processing of your data.

iii) You do not want your data to be erased, instead you want us to restrict the use of your data.

In the case of restriction, while your data is subject to restriction we will continue to store your data securely as set out in our Information Security Management System (ISMS) Policy. Your data will only be processed with your consent where there is a legal claim that needs to be established, pursued or defended or in circumstances where another person's rights need to be protected or for reasons of public interest.

We will notify you when the restriction is due to be lifted.

Rectification

If the information we hold about you is inaccurate you should email our Data Protection Officer daniel.hall@allsquare.co.uk with the correct information and request that your information be corrected. You have the right to rectification of inaccurate personal data about you, this includes having incomplete data completed. Our Officer will ensure you data is corrected without undue delay.

SECTION 8 STAFF TRAINING – GDPR DATA SUBJECT RIGHTS

Full staff training has been carried out across the Allay Group and is documented accordingly. An audit of our third parties has been carried out to ensure that they have trained their staff and where we are not satisfied that this is the case, the third party has been written to with notice to rectify their shortfall.

Our staff training records are retained as required by our regulator

SECTION 9 COMPLAINTS RELATING TO DATA PROTECTION

If you are unhappy with the way in which your personal data has been handled, you are asked to contact our Data Protection Officer to discuss your concerns.
Please contact

daniel.hall@allsquare.co.uk or write to

All Square Finanace Ltd
Unit 1C Riparian Way,
The Crossings Business Park,
Cross Hills, Keighley,
West Yorkshire, BD20 7AA.

We will deal with your complaint in accordance with our complaints procedure which is available on our website www.allsquare.co.uk and sippclaims.uk

If you are still unhappy with any aspect of Data Protection you are entitled to make a compliant to the ICO.

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

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510