



SSAS Practitioner.com
The SSAS Specialist

Lowering Fees, Enhancing Retirement

DATA PRIVACY NOTICE

KEY DETAILS

Notice prepared by: SSAS Practitioner.com Limited
Approved by management on: 1st September 2020

Notice became operational on: 1st September 2020
Next review date: 1st September 2021



SSAS Practitioner.com
The SSAS Specialist

Lowering Fees, Enhancing Retirement

1 INTRODUCTION

SSAS Practitioner.com Limited needs to gather and use certain information about individuals.

We use your email contact details to remind you of issues that arise in the industry through our regular newsletters.

If you are not happy for us to contact you, please email us at info@ssaspractitioner.com. Otherwise we may contact you by email with regular newsletters, and other material directly relevant to the administration of your scheme.

We SSAS Practitioner.com Limited:

- Will use your data in accordance with the service agreement completed between the Trustees/Scheme Administrator and SSAS Practitioner.com Limited. The lawful basis for the processing is contract.
- Will only obtain special category data i.e. sensitive data or/and criminal offence data where necessary for reasons of substantial public interest, such as to comply with anti-money laundering and anti-terrorism financing regulations.
- We will use the information you provide to us to set-up the scheme with HMRC or take-over the running of the scheme and to set up various investments, including bank accounts.
- We will share the information provided to us with various providers, deposit holders and third parties appointed to act for the scheme, if necessary.
- We will use electronic verification providers to check data provided, to ensure we comply with anti-money laundering and anti-terrorism financing regulations.
- We will use third party providers for storing personal data, but will have a contract in place with these third party providers to ensure your data is stored securely.

SSAS Practitioner.com Limited take your privacy seriously and will only use your personal information to administer your scheme and to provide the products and services you have requested from us.

We have no intention of sharing data with any third parties for marketing purposes. These include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

We adopt a 'plain language' policy so that you can understand what we are doing with your personal data.



We consider data protection issues as part of the design and implementation of our systems, services and business practices.

This notice describes how this personal data must be collected, handled and stored to meet the company's data protection policy - and to comply with the law.

2 WHY THIS NOTICE EXISTS

This data privacy notice ensures SSAS Practitioner.com Limited complies with data protection law and follows good practice, protects the rights of staff, customers and partners, is open about how it stores and processes individuals' data and protects itself from the risks of a data breach. You may view our Data Protection Policy on request. Please note that we do not prepare Data Protection Impact Assessment Reports.

3 DATA PROTECTION LAW

General Data Protection Regulations (GDPR) are tailored by the Data Protection Act 2018. The Data Protection Act 2018 replaced the Data Protection Act 1998 and came into effect on 25th May 2018.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 2018 sits alongside the regulations, there are seven main principles as follows, that personal data shall:

1. Be processed lawfully, fairly and in a transparent manner.
2. Be obtained only for specific, explicit and legitimate purposes.
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Be accurate and kept up to date, every reasonable step being 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.
5. Be kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisations measure required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation').



-
6. Be 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, using appropriate technical or organisation measures ('integrity and confidentiality').
 7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (this is paragraph 1 in Article 5 (2) of the GDPR ('accountability')).

4 PEOPLE, RISKS AND RESPONSIBILITIES

4.1 POLICY SCOPE

This policy applies to:

- The office of SSAS Practitioner.com Limited.
- 'All staff' of SSAS Practitioner.com Limited.
- 'All other staff' - all contractors, suppliers, volunteers and (including but not limited to) any other person/persons working on behalf of SSAS Practitioner.com Limited.

It does not apply to any organisation outside that of SSAS Practitioner.com Limited.

The Data Controller that SSAS Practitioner.com Limited are registered with, is the Information Commissioner Office under Z2068455. SSAS Practitioner.com Limited is also the Data Processor (applies to all staff and all other staff as defined above acting on behalf of SSAS Practitioner.com Limited) and the Data Subjects are the Trustees/Scheme Administrators and any other potential beneficiaries in respect of the small self administered schemes in relation to a service agreement made between the Trustees/Scheme Administrator and SSAS Practitioner.com Limited together with all staff and all other staff of SSAS Practitioner.com Limited.

The Trustees of each small self administered scheme have to make a separate registration with the Information Commissioner under which the Trustees are the Data Controller and SSAS Practitioner.com Limited is the Data Processor and the data subjects are the Trustees/Scheme Administrators and any other potential beneficiaries in respect of the small self administered scheme. This should not be confused with the registration required in the paragraph above.

It applies to all data that the company holds relating to identifiable individuals, including special category data (sensitive data) and criminal offence data even if that information technically falls outside of the Data Protection Act 2018 and GDPR.

This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone Numbers.
- Any other information relating to individuals.

The lawful basis under the GDPR that SSAS Practitioner.com Limited use for processing data is contract. In respect of special category data or criminal conviction and offence data the condition for processing this is where necessary for reasons of substantial public interest.

Where SSAS Practitioner.com Limited uses third parties to assist in its processing of personal data, a written contract between SSAS Practitioner.com Limited and the third party will be put in place, in accordance with GDPR.

Under normal circumstances, we should not transfer individual personal data outside the European Economic Area (EEA) as individuals may then lose their protection under the GDPR. There are some circumstances where this is possible, but stringent rules apply and we would need to check the circumstances and the rules at the time to see whether allowable.

4.2 DATA PROTECTION RISKS

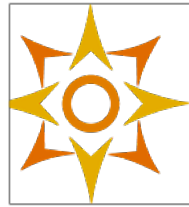
This policy helps to protect SSAS Practitioner.com Limited from some very real data security risks, including:

- **Breaches of Confidentiality** - For instance, information being given out inappropriately.
- **Failing to offer choice** - All individuals should be free to choose how the company uses data relating to them.
- **Reputational damage** - For instance, the company could suffer if 'hackers' successfully gained access to sensitive data.

4.3 RESPONSIBILITIES

Everyone who works for or with SSAS Practitioner.com Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.



SSAS Practitioner.com
The SSAS Specialist

Lowering Fees, Enhancing Retirement

However, the following people have **key** areas of responsibility:

Managing Director | Mr Peter Jones:

Is responsible for ensuring that SSAS Practitioner.com Limited meets its legal obligations.

Data Protection Officer | Mr Peter Jones:

Is responsible for:

- Keeping '*staff*' and '*other staff*' members (all employees, contractors, volunteers and any other person/s working for SSAS Practitioner.com Limited) updated about data protection responsibilities, risks and issues.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from *staff* (employees of SSAS Practitioner.com Limited) and '*other staff*' covered by this policy.
- Dealing with requests from individuals to see the data SSAS Practitioner.com Limited holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Being the first point of contact for the Information Commissioner.
- Our Data Protection Officer has due regard to the risks associated with processing operations, and takes into account the nature, scope, context and purpose of our processing.
- Monitoring compliance with GDPR and other data protections laws, our data protection policy and audits.

IT Manager | Mrs Kerry Smith:

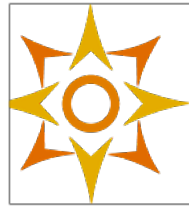
Is responsible for:

- 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 functioning *properly* (correctly and efficiently).
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

Marketing Manager | Mrs Ann Sturman:

Is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or any other media or social media outlets.
- Where necessary, working with other '*staff*' and '*other staff*' members to ensure marketing initiatives abide by data protection principles.



5 GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those that require it **for the purpose of their 'work'**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **SSAS Practitioner.com Limited will provide training** to all 'staff' to help them understand their responsibilities when handling data
- 'Staff' should keep all data secure, by taking sensible precautions and following the guidelines below.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of immediately and in the correct manner.
- 'Staff' **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

6 DATA COLLECTION

We may collect personal data set out in the table below through one or more of the following channels:

Personal Data Type	Source
First name	Website opt in forms, SSAS Application Forms, Trustee/Member Questionnaires, anti money laundering documents and HMRC Fit and Proper Declaration.
Last name	Website opt in forms, SSAS Application Forms, Trustee/Member Questionnaires, anti money laundering documents and HMRC Fit and Proper Declaration.
Postal Address	SSAS Application Forms, Trustee/Member Questionnaires, anti money laundering documents and HMRC Fit and Proper Declaration.
Email Address	Website opt in forms, SSAS Application Forms, Trustee/Member Questionnaires and HMRC Fit and Proper Declaration.
Telephone	SSAS Application Forms, Trustee/Member Questionnaires and HMRC Fit and Proper Declaration.
Date of Birth	Trustee/Member Questionnaires, anti-money laundering documents and HMRC Fit and Proper Declaration.
National Insurance Number	Trustee/Member Questionnaires and HMRC Fit and Proper Declaration.



Personal Unique Tax Reference Number	HMRC Fit and Proper Declaration
Occupation	Trustee/Member Questionnaire
Politically Exposed Person	Trustee/Member Questionnaire
Health	We may investigate this if we have concerns that client may be deemed a "vulnerable Client". We may initially ask questions verbally to try and access whether this needs further action and follow up with a written request for information

The personal data that we collect, will be limited to what is necessary for the purposes for which it is collected and will be used as follows:

- To contact you via newsletters about all relevant industry updates and legislation changes.
- Internal administrative purposes.
- To offer data to official third party organisations for legitimate business interests.

7 DATA STORAGE

These rules describe how and where data should be safely stored. Questions about the safe storage of data can be directed to the IT Manager or Data Protection Officer.

7.1 PAPER STORAGE

- Where data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. This also applies to data usually stored electronically but for work purposes has been printed out onto paper.
- When not required, the paper or files should be kept in a locked room, locked drawer or locked filing cabinet.
- 'Staff' or 'other staff' members should ensure that any paper or printouts including data are not left in a place where unauthorised people could see them. An example of this could be documents left on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

7.2 ELECTRONIC DATA STORAGE

- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed on a regular basis and never shared between employees.
- If data is stored on re-moveable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.



-
- Servers containing personal data should be sited in a secure location, away from the general office space.
 - Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
 - Data should never be saved directly to laptops or other mobile devices - such as smartphones and tablets.
 - All servers and computers containing data should be protected by approved security software and a firewall.

7.3 Communication

- Letters will be posted using Royal Mail.
- E-mail security is provided by one of our third party suppliers, with whom we have a contract.
- Staff are aware that when taking phone calls they need to identify the caller. They may ask you for two pieces of information to identify you such as your date of birth and postcode.
- When processing transactions, our staff may telephone to verify the receiving account details provided.

8 RETENTION PERIOD

Subject to your rights as a data subject and applicable data protection law, SSAS Practitioner.com Limited may process your personal data for a period of 6 years and will store the personal data for a minimum of 6 years as long as the subject is actively receiving and acting upon contact from SSAS Practitioner.com Limited. In respect of data held for anti-money laundering and anti-terrorism financing purposes, data will not be held for more than 5 years after the end of the business relationship. In any event, SSAS Practitioner.com Limited not hold data for longer than it is needed for the purposes for which it was gathered.

9 DATA USE

- Personal data is of no value to SSAS Practitioner.com Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.
- When working with personal data, 'staff' and 'other staff' members should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. Care should be taken when sending information by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic Area.
- 'Staff' and 'other staff' members should not save copies of personal data to their own computers. Always access and update the central copy of any data.

10 DATA ACCURACY

- The law requires SSAS Practitioner.com Limited to take reasonable steps to ensure data is kept accurate and up to date.
- It is the responsibility of all 'staff' and 'other staff' members who work with data to take reasonable steps to ensure it is kept accurate and up to date.
- Data will be held in as few places as necessary. 'Staff' and 'other staff' members should not create any unnecessary additional data sets.
- 'Staff' and 'other staff members' should take every opportunity to ensure that data is updated. For instance, by confirming a customers details when they call.
- SSAS Practitioner.com Limited will consider at all times making it easier for data subjects to update the information SSAS Practitioner.com Limited holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance if a client can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing managers responsibility to ensure marketing databases are checked against industry suppression files every six months.

11 YOUR RIGHTS AS A DATA SUBJECT

11.1 SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by SSAS Practitioner.com Limited are entitled to:

- Ask the purposes of our processing.
- Ask for the categories of personal data concerned, I.e. does this relate to special category or criminal offence data.
- Ask who are the recipients that we are disclosing your personal data to.
- Ask for a copy of your personal data.
- Ask how long we will store your personal data, or the criteria for determining how long we will store the data.
- Ask for your rights to request rectification, erasure or restriction or to object to such processing.
- Ask for the right to lodge a complaint with the Information Commissioner Office or another supervisory authority.



-
- Ask for information about the source of data, when not obtained directly from you.
 - Ask whether we use automated decision-making (including profiling).
 - Ask about the safeguards we provide if we transfer your personal data to a third country or international organisation.

If an individual contacts the company requesting this information, this is called a Subject Access Request.

We would suggest that subject access requests from individuals should be made by email addressed to the data protection officer at: peter.jones@ssaspractitioner.com. However, in accordance with GDPR these requests can be made verbally or in writing and do not have to be to a specific person or contact point, the request does not have to include the phrases 'subject access request' or Article 15 of the GDPR, but you do need to make it clear to us that you are asking for your own personal data. The data protection officer can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged nor will be refused access to each subject access request unless the request is deemed to be 'unfounded or excessive'. The data protection officer will aim to provide the relevant data within 14 days although the law stipulates a time period of 1 month to respond. This time limit, can be extended by a further two months if the request is complex or we have received a number of requests from you. If we wish to extend the time limit, we must let you know within one month of receiving the request and explain the reasons why.

Should any data request be refused, for example it would mean disclosing information about another individual who could be identified from that information, reasons why refusal was made and your right to make a complaint to the Information Commissioners Office will be provided to the individual, together with your ability to seek to enforce this right through a judicial remedy.

The data protection officer will always verify the identity of anyone making a subject access request before handing over the required information. A subject access request can be made via a third party, such as a solicitor acting on your behalf, we would expect to see either a letter of authority or a power of attorney in these circumstances, it is the third party's responsibility to provide evidence of their entitlement to obtain the information.



11.2 FURTHER RIGHTS

At any point whilst we are in possession of or are processing your personal data, you, the data subject, have the following rights (as well as the right to access your data as above (11.1)):

- **Right of rectification.** You have the right to correct data that we hold about you that is inaccurate or incomplete. The request can be made verbally or in writing. All reasonable steps will then be carried out to ensure that all data is updated immediately (refer to section 10.0 above). We have one month to respond to this request or (if later) within one month of receipt of the information requested to confirm the requester's identity (where a third party involved), although we will always try to respond sooner. We can extend the time limit by a further two months if the request is complex or we have received a number of requests from the individual. We will let you know within one month of receiving the request if we need to extend the time limit and explain why. If we rectify data that we have disclosed to other parties, then we will inform them of the rectification (as long as this does not involve disproportionate effort). We can refuse this request if we are satisfied our records are accurate, if the request is manifestly unfounded or excessive, in these circumstances you can make a complaint to the Information Commissioners Office or through judicial remedy.
- **Right to be forgotten.** This right is not absolute and can only be applied in certain circumstances, for example you can ask that the data that we hold about you, be erased from our records if the data is no longer necessary for the purposes which it was originally collected for processing, however, it may still need to be held onto for the purposes of anti-money laundering and anti-terrorism financing regulations and in this circumstance we would need to let you know why we cannot erase your data. We have one month to respond to this request or (if later) within one month of receipt of the information requested to confirm the requester's identity (where a third party involved), although we will always try to respond sooner. We can extend the time limit by a further two months if the request is complex or we have received a number of requests from the individual. We will let you know within one month of receiving the request if we need to extend the time limit and explain why. If not satisfied with our response, you can make a complaint to the Information Commissioners Office or through judicial remedy.
- **Right to Restrict Processing.** As good practice we might restrict the processing of data whilst considering its accuracy. We would not process the restricted data in any way except to stop it unless, we have the individual's consent, it is for the establishment, exercise or defence of legal claims, it is for the protection of the rights of another person or it is for reasons of important public interest. Other circumstances where this restriction might apply include where data has been unlawfully processed, where we no longer need the personal data but an individual has asked us to keep it in order to establish, exercise or defend a legal claim. We will let other parties know of the restriction of personal data where it has been



previously disclosed to them, unless this involves disproportionate effort. Usually this restriction will be temporary and we will notify you before we lift the restriction.

If you have asked us to restrict processing, we will let you know within one month of receiving the request, or (if later) within one month of receipt of the information requested to confirm the requester's identity (where a third party involved), although we will always try to respond sooner. If we need to extend the time limit and explain why, if not satisfied with our response you can make a complaint to the Information Commissioners Office or through judicial remedy.

- **Right of portability.** You have the right to have the data we hold about you transferred to another organisation and also to have data ported to us. We cannot do this through contract as our lawful basis, we would need **consent** from the individual to process this. If the personal data contains information about a third party, we will seek consent from the third party before porting the data. We will maintain a record of consent. SSAS Practitioner.com Limited will not be responsible for any subsequent processing carried out by the other organisation. We will ensure the data is transmitted securely and to the right destination. The data will be exported using a structured, commonly-used and machine readable format. If data is imported to us, we will only retain the data necessary for the purposes for which we process it. We can refuse the request for portability if we decide it is manifestly unfounded or excessive. If we refuse the request, we will inform you of the reasons why and your rights to make a complaint to the Information Commissioners Office or your ability to seek to enforce your right through a judicial remedy. We must respond to the request within at least one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requesters identity. We can extend the time limit by a further two months if the request is complex or we have received a number of requests from you, we must let you know the reason why the extension is necessary within one month of receiving the request.
- **Right to object.** You have the right to object to certain types of processing such as direct marketing emails and newsletters. In respect of direct marketing, this is an absolute right, there are no exemptions for us to refuse this request. You can also object where the processing relates to a public task or legitimate interests, but these are not an absolute right and we can refuse to comply with this request if we can demonstrate compelling legitimate ground for the processing, which override the interest, rights and freedoms of the individual or the processing is for the establishment, exercise or defence of legal claims. If the public task is for the necessary performance of a task carried out in the public interest, then you cannot object. If we do refuse the request, this may be because it is manifestly unfounded or excessive, we will inform you of the reasons why and your rights to make a complaint to the Information Commissioners Office or your ability to seek to enforce your right through a judicial remedy. We must respond to the request within at least one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requesters identity. We can extend the time limit by a further two months if the request is complex or we have received a number of requests from



you, we must let you know the reason why the extension is necessary within one month of receiving the request.

- **Right to object to automated processing including profiling.** This is automated individual decision-making made by automated means without any human involvement. **SSAS Practitioner.com Limited** do not use automated processing including profiling.

12 DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, The Data Protection Act 2018 and the GDPR allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances SSAS Practitioner.com Limited will disclose requested data.

Prior to this, however, the data control will ensure that the request is legitimate, and will seek assistance from the company's legal advisers where necessary.

13 EXEMPTIONS

We are aware that exemptions exist, we would not rely on these and would look at on an individual basis. Exemptions can apply where we are discharging a regulatory function, for example reporting to the National Crime Agency. Immigration exemptions would only ever be used where there are no viable alternatives, the specifics of the case and the guide from the Information Commissioner would be reviewed at the time to reach a decision.

14 PROVIDING INFORMATION

SSAS Practitioner.com Limited aims to ensure that individuals are aware that their data is being processed, and that they are understand how their data is being used and how to exercise their rights.

15 COMPLAINTS

In the event that you wish to make a complaint about how your personal data is being processed by SSAS Practitioner.com Limited, or how your complaint has been handled, please contact our Data Protection Officer in the first instance using the details below and we will endeavour to resolve your complaint. You also have the right to lodge a complaint with the Information Commissioners Office online (www.ico.org.uk/concerns) or by telephone on 0303 123 1113.



SSAS Practitioner.com
The SSAS Specialist

Lowering Fees, Enhancing Retirement



SSAS Practitioner.com Limited
Orchard Grange | Main Street | Foxton | Leicestershire | LE16 7RB
Freephone | 0800 112 3750
Fax | 0116 290 1910
Email | info@ssaspractitioner.com
W | www.ssaspractitioner.com

VAT Registration Number | 983834865
Data Controller Number | Z2068455
HMRC Practitioner Registration Number (ID) | 00017124

Registered with HMRC as a Trust and Company Service Provider | Reference 12587196
Registered with the Information Commissioner under Z2068455
Full PI Insurance held
Member of AMPS (Association of Member-Directed Pension Schemes)