**Privacy Policy**

Effective date: 23 May 2018

This policy concerns the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy.

 **Definitions**

**Personal Data**
Personal Data means data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession).

**Usage Data**
Usage Data is data collected automatically either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

**Cookies**
Cookies are small pieces of data stored on a User’s device.

**Data Controller**
Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
For the purpose of this Privacy Policy we are a Data Controller of your data.

**Data Processor (or Service Providers)**
Data Processor (or Service Provider) means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. We may use the services of various Service Providers in order to process your data more effectively.

**Data Subject**
Data Subject is any living individual who is the subject of Personal Data.

**User**
The User is the individual using our Service. The User corresponds to the Data Subject, who is the subject of Personal Data.

**Information Collection And Use**
We collect several different types of information for various purposes to provide and improve our Service to you.

**Types of Data Collected**
**Personal Data**
While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you (“Personal Data”). Personally identifiable information may include, but is not limited to:

– Email address
– First name and last name
– Phone number
– Address, ZIP/Postal code, City, Area
– Cookies and Usage Data

We may use your Personal Data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt out of receiving any, or all, of these communications from us by following the unsubscribe link or instructions provided in any email we send.

**Usage Data**
We may also collect information how the Service is accessed and used (“Usage Data”). This Usage Data may include information such as your computer’s Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

**Location Data**
We may use and store information about your location if you give us permission to do so (“Location Data”). We use this data to provide features of our Service, to improve and customise our Service.
You can enable or disable location services when you use our Service at any time, through your device settings.

**Tracking Cookies Data**
We may use cookies and similar tracking technologies to track the activity on our Service and hold certain information.
Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies that may also be used are beacons, tags, and scripts to collect and track information and to improve and analyse our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

**Examples of Cookies we may use:**
Session Cookies. We use Session Cookies to operate our Service.
Preference Cookies. We use Preference Cookies to remember your preferences and various settings.
Security Cookies. We use Security Cookies for security purposes.

**Use of Data**
SASE uses the collected data for various purposes:
– To provide and maintain our Service, including articles and discussion points and maintaining a community
– To notify you about changes to our Service
– To allow you to participate in interactive features of our Service when you choose to do so
– To provide customer support
– To gather analysis or valuable information so that we can improve our Service
– To monitor the usage of our Service
– To detect, prevent and address technical issues
– To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information

**Legitimate Interest**
We sometimes process data under a basis of legitimate interest. This is most likely when the processing is not deemed to be unexpected or high risk. In this instance we will ensure that our processing is proportionate and has a minimal privacy impact. We will always review our Legitimate Interest Assessment if we intend to use data for a new purpose to ensure that this purpose is compatible with it original use. We will always ensure that we stop the processing of your data if you object to us doing so and we will always offer an opt out option.

* We have checked that legitimate interests is the most appropriate basis.
* We understand our responsibility to protect the individual’s interests.
* We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
* We have identified the relevant legitimate interests.
* We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
* We have done a balancing test, and are confident that the individual’s interests do not override those legitimate interests.
* We only use individuals’ data in ways they would reasonably expect, unless we have a very good reason.
* We are not using people’s data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
* If we process children’s data, we take extra care to make sure we protect their interests.
* We have considered safeguards to reduce the impact where possible.
* We offer an opt out.
* If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
* We keep our LIA under review and repeat it if circumstances change.
* We will continue to include information about our legitimate interests in this privacy notice.

**Retention of Data**
SASE will retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.
SASE will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer time periods.

**Transfer Of Data**
Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside United Kingdom and choose to provide information to us, please note that we transfer the data, including Personal Data, to United Kingdom and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.
SASE will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organisation or a country unless there are adequate controls in place including the security of your data and other personal information.

**Disclosure Of Data**
**Disclosure for Law Enforcement**
Under certain circumstances, SASE may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

**Legal Requirements**
SASE may disclose your Personal Data in the good faith belief that such action is necessary to:

* To comply with a legal obligation
* To protect and defend the rights or property of SASE
* To prevent or investigate possible wrongdoing in connection with the Service
* To protect the personal safety of users of the Service or the public
* To protect against legal liability
* Security Of Data
* The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

**Your Rights**
SASE aims to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data. Please contact us to make the required changes.

If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please contact us.

In certain circumstances, you have the right:

* To access and receive a copy of the Personal Data we hold about you
* To rectify any Personal Data held about you that is inaccurate
* To request the deletion of Personal Data held about you
* You have the right to data portability for the information you provide to SASE. You can request to obtain a copy of your Personal Data in a commonly used electronic format so that you can manage and move it.
* Please note that we may ask you to verify your identity before responding to such requests.

**Service Providers**
We may employ third party companies and individuals to facilitate our Service (“Service Providers”), to provide the Service on our behalf, to perform Service-related services or to assist us in analysing how our Service is used.
These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

**Analytics**
We may use third-party Service Providers to monitor and analyse the use of our Service.

**Google Analytics**
Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualise and personalise the ads of its own advertising network.

You can opt-out of having made your activity on the Service available to Google Analytics by installing the Google Analytics opt-out browser add-on. The add-on prevents the Google Analytics JavaScript (ga.js, analytics.js, and dc.js) from sharing information with Google Analytics about visits activity.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: <http://www.google.com/intl/en/policies/privacy/>

**Google AdWords**
Google AdWords remarketing service is provided by Google Inc.
You can opt-out of Google Analytics for Display Advertising and customize the Google Display Network ads by visiting the Google Ads Settings page: <http://www.google.com/settings/ads>
Google also recommends installing the Google Analytics Opt-out Browser Add-on – <https://tools.google.com/dlpage/gaoptout> – for your web browser. Google Analytics Opt-out Browser Add-on provides visitors with the ability to prevent their data from being collected and used by Google Analytics.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: <http://www.google.com/intl/en/policies/privacy/>

**Facebook**
Facebook remarketing service is provided by Facebook Inc.

You can learn more about interest-based advertising from Facebook by visiting this page: <https://www.facebook.com/help/164968693837950>

To opt-out from Facebook’s interest-based ads follow these instructions from Facebook: <https://www.facebook.com/help/568137493302217>

Facebook adheres to the Self-Regulatory Principles for Online Behavioural Advertising established by the Digital Advertising Alliance. You can also opt-out from Facebook and other participating companies through the Digital Advertising Alliance in the USA <http://www.aboutads.info/choices/>, the Digital Advertising Alliance of Canada in Canada <http://youradchoices.ca/> or the European Interactive Digital Advertising Alliance in Europe [http://www.youronlinechoices.eu](http://www.youronlinechoices.eu/), or opt-out using your mobile device settings.

For more information on the privacy practices of Facebook, please visit Facebook’s Data Policy: https://www.facebook.com/privacy/explanation

**Mailchimp**
Mailchimp is a customer management system in which we sometimes store customers contact details in order to send you marketing that we believe will be useful to you.

To opt out of any emails received from SASE via Maichimp, please click the link at the bottom of the email you receive.
For more information on the privacy practices of Mail Chimp, please visit their data policy: <https://mailchimp.com/legal/privacy>

**Links To Other Sites**
Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party’s site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

**Children’s Privacy**
Our website services do not address anyone under the age of 16 (“Children”) without parental consent.

We do not knowingly collect personally identifiable information from anyone under the age of 16 on our website. If you are a parent or guardian and you are aware that your child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

**Changes To This Privacy Policy**
We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the “effective date” at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

**Data Protection Policy**

1.         Policy statement
As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities SASE will collect, store and process personal data, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations in accordance with our operational and legal obligations.

The types of personal data that we may be required to handle include information about current, past and prospective employees, suppliers, licensees, customers, students, contractors and others with whom we communicate. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations, including GDPR. The Act imposes restrictions on how we may process personal data.

2.         Status of the policy
This policy has been in place since 23rd May 2018 and approved by Helen Johnson (Managing Director). It sets out our rules on data protection, the eight data protection principles contained in it and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Helen Johnson (helen@goddessacumen.com). Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Manager.

This policy does not form part of any employee’s contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Compliance Manager.

3.         Definition of data protection terms
Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual’s privacy in some way. Mere mention of someone’s name in a document does not constitute personal data, but personal details such as someone’s contact details or salary would still fall within the scope of the Act.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed.  They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

Data users include employees whose work involves using personal data.  Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data.  It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it.  Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.  Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4.         Data protection principles
Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

* Processed fairly and lawfully
* Processed for limited purposes and in an appropriate way
* Adequate, relevant and not excessive for the purpose
* Accurate
* Not kept longer than necessary for the purpose
* Processed in line with data subjects’ rights
* Secure
* Not transferred to people or organisations situated in countries without adequate protection
* Fair and lawful processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case SASE), who the data controller’s representative is (in this case the Data Protection Compliance Manager), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject’s explicit consent to the processing of such data will be required in order that (eg.) we may operate our policies, such as health and safety and equal opportunities.

**Processing for limited purposes**
Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

**Adequate, relevant and non-excessive processing**
Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

**Accurate data**
Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

**Timely processing**
Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Data Protection Compliance Manager.  Processing in line with data subject’s rights Data must be processed in line with data subjects’ rights.

Data subjects have a right to:

* Request access to any data held about them by a data controller (data subjects are entitled to ask what Personal data we hold about them and why)
* Prevent the processing of their data for direct-marketing purposes
* Ask to have inaccurate data amended
* Prevent processing that is likely to cause damage or distress to themselves or anyone else

You are responsible for:

* Checking that any Personal data provided to us is accurate and up to date
* Informing us of any changes to Personal data which is provided to you (eg. change of  address)
* Ensuring that if you work with SASE and collect Personal data about other people as part of your responsibilities, you do so in compliance with this policy.

**Data security**
We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. Further, you should not disclose (orally, in writing or otherwise) any personal data or information to any unauthorised third party and only the Data Protection Manager, a Trustee, or the Chief Executive may authorise such disclosure.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

* Confidentiality means that only people who are authorised to use the data can access it
* Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
* Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs

**Security procedures include:**

* Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
* Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required
* Password protection. Information stored on computers and cloud data services should be password protected.

**Equipment**

* Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended and/or that each individual requires unique password access to their specific computer, with such passwords not being passed on to another person with the exception of our IT team and only passed on to another person with the prior written consent of the Data Protection Compliance Manager. Data users should ensure that no programmes or equivalent are downloaded, otherwise read, displayed and/or saved onto any PC and/or our central computer system without obtaining the prior written consent of the Data Protection Compliance Manager
* Contractors and other third party, non-employee data processors. Data users should ensure that only personal data necessary for data processors’ carrying out of their tasks on behalf of us are passed to the data processor
* Data breaches or potential data breaches. All Data users must immediately report (together with details (if known)) any known or suspected data breaches to the Data Protection Compliance Manager in order that appropriate action to rectify the potential or known breach may be taken and appropriate actions to prevent a repeat occurrence may be considered and implemented in due course

**Dealing with subject access requests**
Data subjects whose personal data is held by us have the conditional right to access any personal data that is being held by us about them on computer and also have access to paper-based personal data held in manual filing systems. This right is subject to certain exemptions which are set out in the Act.

A formal request from a data subject for information that we hold about them must be made in writing. Any member of staff or licensee who receives a written request should forward it to the Data Protection Compliance Manager immediately at our usual SASE address.

We aim to comply with requests for access to personal data as quickly as possible, but we will ensure that it is provided within 30 days of receipt of a request unless there is a good reason for delay (eg. the requester as failed to provide all of the necessary information to the Data Protection Compliance Manager’s satisfaction).

**Providing information over the telephone**
Any member of staff, volunteer, or Trustee dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

* Check the caller’s identity to make sure that information is only given to a person who is entitled to it
* Suggest that the caller put their request in writing if they are not sure about the caller’s identity and where their identity cannot be checked
* Refer to the Data Protection Compliance Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information

**Disclosure of Personal Data**
No personal data may be disclosed to or shared with any person or entity not employed by us (and sub-contractors are not employed by us) without the prior written consent of our Data Protection Compliance Manager. All queries regarding disclosure or Data sharing must be raised with our Data Protection Compliance Manager prior to making any such Data disclosure sharing. If any doubt exists as to whether or not any individual should be processing Data, it is our policy that no processing should take place by that or any other individual until it has been authorised by the Data Protection Compliance Manager.

Accordingly, SASE may share client data for the sole purpose of arranging the provision of services. SASE will only disclose this information for this sole purpose with the consent of the client.

**Monitoring and review of the policy**
This policy is reviewed annually by the Data Protection Compliance Manager. Any necessary amendments discovered will be implemented as soon as is reasonably practicable.

SASE will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

**Photography Consent Form**

SASE will only use and reuse photographs of employees/licensees and customers if they freely and willingly sign and date the latest version of our Photography Consent Form in advance and accordingly agree to the purposes for which we wish to use and reuse their photographs as detailed in the form. If anyone does not wish us use photographs featuring them, they should simply decline to complete the Form.

**Contact Us**
If you have any questions about these policies, please contact us:
By email: info@sase.org.uk By phone: 07984 348 646