Stratogen Inc. Privacy Policy

Tier 1

Document Control
Reference: ISMS DOC 18.6_STR
Issue No 2.0
Issue Date: 30/04/2018

Contents

1. Our Commitment

The Board of Directors and management of Stratogen Inc (Alto Hosting) part of the Access Group, are committed to compliance with all relevant laws in respect of personal data, and specifically where required for the EU and Member States and the Privacy Shield Framework for the USA

Stratogen Inc – part of the Access Group complies with the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and/or Switzerland to the United States.

Stratogen Inc has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

Stratogen Inc – has committed to adhering to EU General Data Protection Regulation and is certified to ISO27001:2013

For further information relating to how Access Stratogen manage and process date – please contact Information.Security@theaccessgroup.com

The current version of our Privacy Policy and contact information can be obtained from our website

https://www.theaccessgroup.com/hosting-us/privacy-and-legal/

2. Scope

Data

This policy applies to all Data held or processed by the Stratogen, for customers', clients', employees, suppliers' and partners'. Whether managed on premise or remotely via client connections.

This includes personal data, the organisation processes from any source, and held by the company in either electronic or paper format that has been classified as Confidential or Restricted [ISMS DOC 8.6 Information Classification Policy], particularly Personally Identifiable Information held or processed by Stratogen on any of the following (but not limited to):

- Desktops
- Laptops
- Phones
- Tablets
- Email
- External Media
- Websites
- Networks
- Hosting infrastructure
- Hard copy media

3. Third Parties

Partners and any third parties working with, or for Stratogen and who have, or may have access to personal data, will be expected to have read, understood and to comply with this policy (see section on Third Party/Suppliers)

4. Definitions

Personal Information/ PII

Personal Information or Personally Identifiable information is any information related to a natural person or 'Data Subject' that can be used to "directly or indirectly identify" a person. It can be anything from a name, a photo, an email address (personal or business), bank details, and posts on social networking websites, medical information, or a computer IP address. See Annex B for more information related to PII

Special categories of personal data (EU)

Personal data revealing any of the following categories cannot be processed without affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorised by the individuals through the exercise of opt-in choice. In addition, Access Stratogen will treat as sensitive, any personal information received from a third party where the third party identifies and treats it as sensitive.

- The racial or ethnic origin of the data subject,
- Religious beliefs or other philosophical beliefs of a similar nature,
- Trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- Physical or mental health or condition,
- Genetic or biometric data
- Sexual orientation or data concerning a natural person's sex life
- There are also separate safeguards for alleged or criminal convictions

Legal Basis for Processing Data (EU)

- The data subject has given explicit consent;
- It is necessary to fulfil the obligations of controller or of data subject;
- It is necessary to protect the vital interests of the data subject;
- Processing is carried out by a foundation or not-for-profit organisation [only those in blue text]
- The personal data has manifestly been made public by the data subject (Press leaks excluded)
- Establishment, exercise or defence of legal claims;
- Reasons of public interest in the area of public health; (NHS for instance)
- Archiving purposes in the public interest; (Census)
- A Member State has varied the definition of a special category. (if UK excludes anything)

Data subject

Any living individual who is the subject of personal data held by an organisation.

Data controller /Controller / Co-Controller

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

Data Processor / Processor

A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach

A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Third party

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system

Any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Pseudonymisation

The technique of processing personal data in such a way that it can no longer be attributed to a specific “data subject” without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution

5. Categories of Data

Employees

Access Stratogen commits to cooperate with EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU in the context of the employment relationship.

- Name/s
- Partner / Spouse
- DOB
- Address
- Contact Numbers
- Social Security ID
- Tax Details
- Next of Kin
- Medical Information / History
- Employment records
- Qualifications and Official Memberships relating to employment
- Gender
- Sexual orientation if provided
- Right to work information
- Passport details where travel is offered

Use and disclosure

Personal information for employees is used for contractual employment purposes, to facilitate salary payments, provide support and care, travel and staff benefits. Access Stratogen ensures that all partners providing services to employees are compliant with GDPR and the Privacy Shield Framework and that information is provided to staff in the form of freely available Privacy Notices.

Clients

Use and data Disclosure

Where Access Stratogen provides VMWare Private and Cloud hosting – the client is responsible for the data. Access Stratogen do not have access to any data.

Access Stratogen collects information from clients in order to provide hosting services and technical support where the client takes an “infrastructure only” solution – this is limited to business email address and contact information.

Where Access Stratogen collects information in order to provide SaaS services, data collected will be dependent on the nature of the software as detailed in Appendix A

Access Stratogen does not share any client data with third parties

6. General Disclosures

Certain disclosures without consent so long as the information is requested for one or more of the following purposes:-

Privacy Shield

- the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements

GDPR

- To safeguard national security;
- Prevention or detection of crime including the apprehension or prosecution of offenders;
- Assessment or collection of tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party; and to protect the vital interests of the individual, this refers to life and death situation

POLICY

Compliance with the GDPR is described by this relates to all connected processes. Any breach of this Policy must be reported to the Information Security Manager (where it involves Personal Information and presents a risk to the rights and freedoms of an individual).

7. Roles & Responsibilities

People

This Policy applies to all permanent, temporary or contract staff, third party suppliers or affiliates and visitors to Stratogen premises.

The Information Security Manager will be responsible for

- Development and implementation of Privacy required by this policy
- Security and risk management in relation to compliance with ISMS DOC 4.4 Risk assessment process & Methodology
- Ensuring that the Access Group including Stratogen Inc. complies with the Privacy Shield Framework and GDPR as referenced in Section 1
- Being the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.
- Being an initial point of contact for complaints and disputes.

The Information Security Manager will also review the retention dates of all the personal data processed by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose

8. Consent (EU)

Stratogen understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

Stratogen understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement

Consent will not be inferred from non-response to a communication.

For sensitive data, explicit written consent must be obtained, unless an alternative legitimate basis for processing exists.

.

9. The GDPR Principles (EU)

Data shall be

1	Processed lawfully, fairly and in a transparent manner		
2	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes		further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3	Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed		
4	Accurate and, where necessary, kept up to date		every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay:
5	Personal data shall not be kept for longer than is necessary for that purpose or those purposes for which it was originally collected		**P**ersonal 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 organisational measures Data must be deleted in line with ISMS DOC 18.2 Records Management Policy/Schedule Where data retention that exceeds the retention periods defined in ISMS DOC 18.2 Records Management Policy/Schedule, justification must be subject to written approval from the CISO and clearly identified and in line with the requirements legislation
6	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 organisational measures incorporating “Privacy by Design / Privacy by Default” in line with ISMS DOC 14.1 Secure Development Policy

.

10. Technical measures

Can include but are not limited to:-

- Password protection
- Acceptable Use
- Automatic locking of idle terminals
- Virus checking software and firewalls
- Role-based access rights
- Encryption of devices
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Identifying appropriate international security standards relevant to Stratogen Inc
- All personal data should be accessible only to those who need to use it, and access may only be granted in line with ISMS DOC 9.1 Access Control Policy

Non-Technical Measures

Applying appropriate training levels throughout Stratogen Inc - All Employees/Staff will be provided with training to ensure that they understand Access UK's policy and the procedures it has put into place to implement that policy. This will take place within 1 week of joining and annually thereafter.

- Ensuring awareness programme in place
- Measures that consider the reliability of employees
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Implementing a BYOD and Mobile Policy for portable devices
- Restricting the use of employee's own personal devices being used in the workplace using and MDM solution
- Making regular, secure backups of personal data and storing the media off collection site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when personal information

11. The Rights & Choices of the Individual (Privacy Shield & EU)

Access Stratogen Inc ensures that data subjects may exercise the following rights and in all cases please contact Information.Security@theaccessgroup.com . Your request will be acknowledged, registered and processed in line with the mandated time frames available on the Information Commissioners Website

The Rights	
The Right to be Informed *(in the form of a privacy notice at the time the data is collected – or within 30 days if not collected directly)*	○ In the form of a Privacy Notice provided to the data subject
The Right of Access *Response without undue delay but provided within one month at no cost*	○ Information about how data is being processed ○ Access to that data in a commonly used electronic format if requested ○ Any other supplementary information (as per privacy notice)
The Right to Rectification *Response without undue delay but provided within one month at no cost*	
The Right to Erasure /Right to be Forgotten *Response without undue delay but there is no specific timeline mandated for completion (again no cost)*	○ Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed. ○ When the individual withdraws consent. ○ When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. ○ The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR). ○ The personal data must be erased in order to comply with a legal obligation.
Right to Restrict Processing	
The Right to Data Portability *Response without undue delay but provided within one month at no cost*	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, It must be provided in a structured, commonly used and machine-readable form. Open formats include CSV files. (this does not include PDF files) Note: If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual
The Right to Object	
Rights in relation to automated decision making and profiling	This is automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict :- ○ performance at work; ○ economic situation; ○ health; ○ personal preferences; ○ reliability; ○ behaviour; ○ location; or ○ Movements. When it has a legal or similarly significant effect on the individual. In this case, it is necessary to obtain human intervention, permit the data subject to express their point of view; and obtain an explanation of the decision and challenge it.

Privacy Notice

Privacy notices must be issued at the time of Data collection or within 30 days if data is not obtained directly from the data subject.

- The identity and contact details of the controller and where applicable, the controller's representative and the data protection officer (Information Security Manager)
- Purpose and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data (where not obtained directly from the data subject)
- Who the data was obtained from (where not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data and safeguards
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- Description of technical and organisational security measures
- The Rights
- The Principles
- How to complain to the company and supervisory authority
- How to withdraw consent

12. Data Inventory (EU)

Stratogen Inc has established a data inventory and data flow process as part of its approach to address risks and opportunities

- Business processes that use personal data;
- Source of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- Recipients, and potential recipients, of the personal data;
- The role of the Stratogen Inc throughout the data flow;
- Key systems and repositories;
- Any data transfers; and
- All retention and disposal requirements.

13. Breach Reporting

All Employees/Staff, contractors or temporary personnel are responsible for reporting any and all personal data breaches (including those that appear to be insignificant) to the Information Security Manager in line with the ISMS DOC 16.1 Incident Management Policy & Process and using the ISMS REC16.2R Incident Report

Where EEA data is involved it must be reported to Access information security immediate in order to adhere to the EEA reporting requirements

14. Supplier & Third Parties Management

In addition to the requirement that Partners and any third parties working with or for Access and who have access to personal data will be expected to have read, understood and to comply with this policy, no third parties or suppliers may be engaged without a Supplier Assessment being undertaken. This determines any data sharing arrangements in which data subjects should be notified and appropriate undertakings from the supplier in relation to the Privacy Shield Principles

Stratogen Inc must ensure that personal data is not disclosed to unauthorised third parties. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party and if unsure, should refer to the Access Information Security Manager or CISO.

No third party may access personal data without having first entered into a data confidentiality agreement in line with ISMS DOC 15.1 Supplier Relationships, which imposes on the third party, obligations no less onerous than those to which Stratogen Inc. is committed, and which gives Stratogen the right to audit compliance with the agreement.

Access Stratogen will offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorised by the individuals. Note: it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of Access Stratogen. However, Access Stratogen shall always enter into a contract with the agent.

Individuals will be provided with clear, conspicuous, and readily available mechanisms to exercise choice

In the context of an onward transfer, Access Stratogen is responsible for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. We shall remain liable under the Principles if our agent processes such personal information in a manner inconsistent with the Principles, unless Access Stratogen proves that it is not responsible for the event giving rise to the damage.

Suppliers in use

Data Centres

- Denver CO - Fortrust
- Edison New Jersey - IO
- Coresite – under construction

All data centres are ISO27001/SSAE-16 certified

Other services utilised
Transit circuits
Fiber network services
Hardware support and maintenance
Data Centre Internet Connectivity
Internet cross connect services
Network monitoring software
Remote Hand support (rebooting servers)
Office internet services
Office telephones
Office Wifi services (none in the data centre)
Legal Services

15. Retention and disposal of Data

Stratogen Inc shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

The Access group data retention and data disposal procedures in line with ISMS DOC 18.2 Records Management Policy/Schedule will apply in all cases.

All data received or databases created, processed, stored or received for clients must be recorded on the data Register

Personal data must be disposed of securely and must be done in accordance with the secure disposal procedure included in ISMS DOC 8.6 Information Classification Policy

16. Disputes & Complaints

In compliance with both the Privacy Shield Principles and GDPR Stratogen Inc. commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Access Stratogen at: Information.Security@theaccessgroup.com

The complaint/issue will be immediately acknowledged, recorded, a reference provided and all efforts to resolve will be undertaken at that point

Access Stratogen has further committed to refer unresolved Privacy Shield complaints to **JAMS** - https://www.jamsadr.com/global/, being a Dispute Resolution (ADR) Provider under the EU–U.S. Privacy Shield Program and/or the Swiss–U.S. Privacy Shield Program for non HR disputes.

All Dispute, Complaint and arbitration services are provided at no cost to you.

EU citizen Complaints and Arbitration service

USCIB – https://www.uscib.org/

EU DPAs dispute resolution services (HR disputes)

Information Commissioners Office - https://ico.org.uk/

Additional Information

- Access Stratogen is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- There is also the possibility, under certain conditions, for the individual to invoke binding arbitration under the Privacy Shield Framework (ICDR-AAA - https://www.icdr.org/)

17. Annex A – Data processing for SaaS products

Nature of Processing	We receive data uploaded to the service by users where it is stored in a cloud environment or on premise in accordance with the options selected by the client.
Categories of Data Subject	The data may relate to the following categories of data subject: For example Prospects, customers, business partners and vendors of Customer (who are natural persons) Employees or contact persons of Customer's prospects, customers, business partners and vendors Employees, agents, advisors, freelancers of Customer (who are natural persons) Customer's Users authorised by Customer to use the Services Supporters of organisations
Processing purpose	It will vary by clients and software – Full Software Fact sheets can be requested from Information.Security@theaccessgroup.com Processing is dependent on the type of software but in all cases, the client remains the data controller and determines how the software is used.
Personal information, that on its own or with any other data in the system, can identify an individual	Depending on the SaaS software in use – it can include bit is not following – Email Address Name Gender Usernames Birth Date Address Photographs Place of birth Employment History Salary Vehicle registration plate number National ID numbers/Social security number/ NI Numbers Organisation Memberships Passport Number Passwords Marital Status Mobile phone number or house phone Bank Details Driver's license number Education History
Special categories of Data stored ○ Race / Ethnic origin	Gender whether different to that of birth Region of birth Ethnic Origin Religion Sexual Orientation Disability

○ Political opinions /Religion / Philosophical beliefs ○ Trade union membership ○ Genetic data /Biometric data / Health Sexual Orientation / Concerning a natural person's sex life	Absence reasons (could be health related) *Note- Fields are classified according to type*

18. Annex B PII Summary

Category of Information	Comments
A letter written in a person's official capacity	
Bank Details	
Business Cards	
Business Telephone number	Direct line
Bio-metric data – Retina, face, fingerprints, handwriting	Sensitive Personal
Car VIN Number or number plate (where registered to an individual)	
Cookies	
Credit cards / Bank Cards / Store Cards	
Credit score / Record	
Criminal record	carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects
Date of Birth	When used in conjunction with other information
Details about a person's land ownership or disputes to do with their land	
Digital identity	
Disability information	Sensitive Personal
Driver's license number	
Education and employment history	
Email address (personal and business)	
Ethnicity / Race	Sensitive Personal
Events attended	
Fingerprints	
Full Name	
Gender	
Genetic information	Sensitive Personal
History / background	
Home address	
Insurance details	
IP Address	(not PII by itself in USA)
Job position / title (with Company)	
Location information	
MAC Address	
Maiden name	
Medical/ Health information	Sensitive Personal
Mother maiden name	
National ID numbers / Social security number	
Next of Kin information	
NI Numbers	
Opinions given as part of a person's employment	
Organisation Memberships	
Patient ID	

Category of Information	Comments
Passport number	
Passwords	
Photographic Passes (train / business)	
Photos	
Place of birth	When used in conjunction with other information
Political and religious leanings and affiliation	Sensitive Personal
Salary	
Security tokens	
Session information and tokens	
Sexual orientation	Sensitive Personal
Status	
Mobile phone number or house phone	
Trade Union Membership	Sensitive Personal
Usernames / Screen names / aliases	
Vehicle registration plate number (where vehicle registered to individual)	
Video Recording	
Views on controversial issues / Philosophical beliefs	Sensitive Personal
Visas	
What you are doing when / status (Social Network Sites)	
Where the information is so unique that it cannot be anyone else	