DATA PROTECTION POLICY

Introduction

1 In undertaking the business of STUDYSMART KONSTANTINOS KIRITSIS & SIA EE, we all create, gather, store and process limited amounts of data on a variety of data subjects such as on students (potential, current and former), staff, customers/suppliers and members of the public. Our use of personal data ranges from financial transactions with commercial customers through to the processing a student's details throughout their journey, from application through to their accreditation by a professional body.

2 Some of the data we create/collect and process will be other people's personal data but **we do not** collect sensitive data, i.e. data concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sexual life

3 As our recording and use of data continues to increase, it is more important than ever that every member of our staff and associates understand the law that exists in relation to data protection and their responsibilities in ensuring that data is secured and protected in line with the law.

4 Data protection is an important part of the StudySmart's overall information security arrangements. All information must be handled safely and securely according to agreed policy. In addition to good practice, some data sets are subject to external legislation and it is vital that staff and associates recognise both categories in their handling of StudySmart's information and data.

5 Data protection legislation has existed in Greece for many years with the Data Protection Act (Article 2472/1997) being the current iteration. However in May 2018, new EU legislation will come into force - the General Data Protection Regulations (GDPR).

6 As StudySmart processes 'personal data' of staff, associates, students and other individuals, it is defined as a Data Controller for the purposes of the GDPR. StudySmart currently processes personal data strictly in accordance with Data Protection legislation and this will continue to be the case in relation to the GDPR.

7 The GDPR applies to all data relating to, and descriptive of, living individuals defined in the Regulations as 'personal data'. Individuals are referred to as 'data subjects'. For further definitions of terms used please see the glossary in section 1 of the Data Protection Guidance Handbook.

8 The GDPR places obligations on StudySmart and the way it handles personal data. In turn the staff, associates and students of StudySmart have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a valid condition of processing (e.g. consent obtained from the data subject, legitimate interest or a contract with them) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). There are restrictions on what we are allowed to do with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

9 StudySmart is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

Purpose of Policy

10 This policy sets out the responsibilities of StudySmart, its staff, its associates and its students to comply fully with the provisions of the GDPR. It is accompanied by a list and

links to other, associated policies and a Data Protection Guidance Handbook with provides information and guidance on different aspects of data protection and data security. This policy, its associated policies and the Guidance Handbook form the framework from which staff, associates and students should operate to ensure compliance with data protection legislation.

Scope

11 The policy applies to all staff, associates and students, and all items of personal data that are created, collected, stored and/or processed through any activity of StudySmart across all areas including seminars, masterclasses, and professional services.

Background

Data Protection principles

12 StudySmart is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation').
c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
d) Personal data shall be accurate and where necessary kept up to date ('accuracy').
e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').
f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Personal Data

13 Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which StudySmart either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious believes. Despite StudySmart does not collect such information, further information and guidance on personal data, including a full list of 'special categories' of personal data, is provided in section 3 of the Data Protection Guidance Handbook.

14 The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

15 StudySmart, as data controller, remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

16 Staff and associates developing new projects or processes or revising existing processes need to take data protection into account as part of this process and may need to carry out a data protection impact assessment.

17 In the event that there is a data protection breach this will have to be reported to the Managing Director's Office no later than 72 hours after the breach is discovered.

Associated Policies

18 The following associated policies should be consulted in conjunction with the Data Protection Policy as appropriate.

- Information Technology Use Policy (*to be developed when required*)
- Data Classification and Handling Policy (*to be developed when required*)
- Data Security Policy (*to be developed when required*)
- Mobile Working Policy (*to be developed when required*)

Policy

The Policy is set out in the following sections:

i. **General**
ii. **Data Security**
iii. **Data Retention**
iv. **Conditions of Processing and Consent**
v. **Privacy Notices**
vi. **Record of Processing Activities**
vii. **Children**
viii. **Research**
ix. **Subject Access Requests and Data Subject Rights**
x. **Data Sharing**
xi. **Transfers of Personal Data Outside the EU**
xii. **Data Protection Impact Assessments and Data Protection by Design**
xiii. **Direct Marketing**
xiv. **Personal Data Breach**
xv. **Impact of Non-compliance**

i. General

19 StudySmart is responsible for demonstrating compliance with the six data protection principles (see paragraph 12).

20 Compliance with the GDPR, and adhering to these principles is the responsibility of all members of StudySmart (including associates). Any deliberate breach of this policy may lead to disciplinary action being taken, tutor contract immediate cancellation, access to StudySmart facilities being withdrawn, or even criminal prosecution.

21 StudySmart is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. For more information about these records see section vi Records of Processing Activities.

ii. Data Security

22 All StudySmart users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. More information is included in section 4 of the Data Protection Guidance Handbook.

iii. Data Retention

23 Individual areas within StudySmart are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on StudySmart's

guidance. Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.

24 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed is should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.

25 If data is fully anonymised then there are no time limits on storage from a data protection point of view (see paragraph 57).

iv. Conditions of Processing and Consent

26 In order for it to be legal and appropriate for StudySmart to process personal data at least one of the following conditions must be met:

a) The data subject has given his or her consent
b) The processing is required due to a contract
c) It is necessary due to a legal obligation
d) It is necessary to protect someone's vital interests (i.e. life or death situation)
e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by public authorities in performance of their public tasks).

27 All processing of personal data carried out by StudySmart must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

28 Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent.

29 Anyone who has provided consent has the right to revoke their consent at any time.

30 Further information about obtaining consent can be found in section 5 of the Data Protection Guidance Handbook.

v. Privacy Notices

31 Under the 'fair and transparent' requirements of the first data protection principle, StudySmart is required to provide data subjects with a 'privacy notice' to let them know what it does with their personal data. (the main privacy notices for StudySmart can be viewed at: www.studysmart.gr/dataprotection.

32 Privacy notices are published on the StudySmart website and are therefore available to staff, associates and students from their first point of contact with StudySmart. Any processing of staff or tutor or student data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided.

33 Further information on what information should be included in a privacy notice is provided in section 5 of the Data Protection Guidance Handbook.

vi. Records of Processing Activities

34 As a data controller StudySmart is required to maintain a record of processing activities which covers all the processing of personal data carried out by StudySmart. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. StudySmart has the following Records of Processing activities:

- Staff data (including job applicants, previous staff, honorary, emeritus and visiting staff)
- Tutor data (including cv, tax numbers, IKA numbers, Bank account numbers, photos, videos)
- Student data (including potential, existing, and past)
- Data subjects other than staff, associates, students, applicants, and past employees

35 Copies of these records can be found at StudySmart's premises at 54 Aigialeias Street, Marousi, Athens, Greece.

36 Staff and associates embarking on new activities involving the use of personal data and that is not covered by one of the existing records of processing activities should inform the Data Protection Officer which is the Managing Director (data.protection@studysmart.gr) before starting the new activity.

vii. Children

37 Under GDPR the following restrictions apply to the processing of personal information relating to children:

- Online services offered directly to children require parental consent.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

38 StudySmart does not possess or collect such data. The Data Protection Officer which is the Managing Director (data.protection@studysmart.gr) should be informed if any of the above activities are being contemplated.

viii. Research

39 Data collected for the purposes of research are covered by the GDPR. It is important that staff and associates collecting data for the purpose of research or consultancy incorporate an appropriate form of consent on any data collection form.

40 Further information and guidance on data protection and research is provided in section 6 of the Data Protection Guidance Handbook.

ix. Subject Access Requests and Data Subject Rights

41 The GDPR gives data subjects the right to access personal information held about them by StudySmart. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that StudySmart holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

42 StudySmart must respond to all requests for personal information and information will normally be provided free of charge.

43 References are disclosable to the person about whom they are written under the subject access provisions of the GDPR. This includes references received by StudySmart from external sources and confidential references given and received internally e.g. as part of advancement and promotions procedures. There is an exemption from disclosure for references written by StudySmart staff and associates and sent externally, however these references would still be accessible to the applicant from the organisation to which the reference was sent. In order to maintain confidentiality and to prevent the unauthorised disclosure of information, staff and associates should not provide references without a prior request from the student concerned.

44 StudySmart is not required to disclose examinations and mock-test scripts, however students are entitled to access any marks or comments annotated on the script. Students are entitled to their marks. Unpublished marks must be disclosed within 5 months of a subject access request.

45 Further information and guidance about handling subject access requests can be found in section 7 of the Data Protection Guidance Handbook.

46 Data subjects have a number of other rights under the GDPR. These include:

- **Right to Object –** Data subjects have the right to object to specific types of processing which includes processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right (see section xiii on direct marketing). Online services must offer an automated method of objecting. In some cases there may be an exemption to this right for research or statistical purposes done in the public interest.
- **Right to be forgotten (erasure) –** Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.
- **Rights in relation to automated decision making and profiling** – The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.
- **Right to Rectification -** The right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.
- **Right to Portability –** the data subject has the right to request information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

47 The availability of rights largely depends on the legal justification for processing. The table below summarises when rights are available.

Legal Justification	Right to:				
	Object	Erasure	Automated Decision making	Rectification	Portability
Consent	**X** but can withdraw consent	√	**X** but can withdraw consent	√	√
Contract	**X**	√	**X**	√	√
Legal Obligation	**X**	**X**	**X**	√	**X**
Vital Interest	**X**	√	**X**	√	**X**
Public Task	√	**X**	√	√	**X**
Legitimate Interests	√	√	√	√	**X**

48 Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month or receiving the request. Members of staff should consult the Data Protection Officer which is the Managing Director (data.protection@studysmart.gr) if any requests like these are received.

x. Data Sharing

49 Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of StudySmart.

50 As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.

- Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned (see paragraph 12)
- It must meet one of the conditions of processing (see section iv). Legitimate reasons for transferring data would include:
  - That is was a legal requirement
  - It is **necessary** for the official core business of StudySmart
- If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided (see section 5 on Consent & Privacy Notices in the Data Protection Guidance Handbook).
- StudySmart is satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.
- Where a third party is processing personal data on behalf of StudySmart a written contract **must** be in place. A contract is also advisable when data is being shared for reasons other than data processing so StudySmart has assurances that GDPR requirements are being met.

51 Staff should consult with the Data Protection Officer which is the Managing Director (data.protection@studysmart.gr) if they are entering into a new contract that involves the sharing or processing of personal data.

52 Staff and associates who receive requests for personal information from third parties such as relatives, police, local councils etc. should consult the section 9 of the Data Protection Guidance Handbook on Requests for Personal Information from Third Parties.

xi. Transfers of Personal Data Outside the EU

53 Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate

level of protection for the data and some exemptions under which the data can be exported. In many cases StudySmart will require consent of the data subjects before personal information can be transferred out of the EU.

54 Information published on the internet must be considered to be an export of data outside the EU. This covers data stored in the cloud unless the service provider explicitly guarantees data storage only takes place within the EU. Currently StudySmart does not possess data stored on cloud other than Mailchimp for email marketing purposes in which Mailchimp data policy consents with GDPR policies and a copy of that agreement is available at StudySmart premises.

55 The Data Protection Authority (www.dpa.gr) on the use of Cloud Computing should be consulted before any use of external computing resources or services via a network which may involve personal data.

56 Staff involved in transferring personal data to other countries should consult section 10 of the Data Protection Guidance Handbook.

xii. Data Protection Impact Assessments and Data Protection by Design

57 Under the GDPR StudySmart has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

58 It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a specify 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

59 Further information about techniques that can be used to reduce the risks associated with handling personal data including Anonymisation and Pseudonymisation see section 12 of the Data Protection Guidance Handbook on Data Protection by Design and Default.

60 For some projects the GDPR ***requires*** that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include: those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV). The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. Information about when and how to carry out a DPIA can be found in section 11 of the Data Protection Guidance Handbook on Data Protection Impact Assessments.

xiii. Direct Marketing

61 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots for fund raising, advertising courses etc. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. StudySmart must cease direct marketing activity if an individual requests the marketing to stop.

62 Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[2] which covers marketing via telephone, text and email. For more information about direct marketing and PECR please see section 13 of the Data Protection Guidance Handbook.

[2] *The Privacy and Electronic Communications (EC Directive) Regulations 2003 is due to be replace by a new ePrivacy Regulation probably in 2018*

xiv. Personal Data Breach

63 StudySmart is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. StudySmart makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

64 If a data protection breach occurs StudySmart is **required** in most circumstances to report this as soon as possible to the Data Protection Authority, and not later than 72 hours after becoming aware of it.

65 If you become aware of a data protection breach you must report it immediately. Details of how to report a breach and the information that will be required are included in section 14 of the Data Protection Guidance Handbook on Personal Data Breaches.

xv. Impact of Non-compliance

66 All staff, associates and students of StudySmart are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff or tutor or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff or associates may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of StudySmart i.e. for their own purposes, which are outside the legitimate purposes of StudySmart.

67 StudySmart could be fined for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement. Further information about the fines are in section 15 of the Data Protection Guidance Handbook.

StudySmart Contacts

68 The University's named Data Protection Officer which is the Managing Director is Dr. Demetrios Kiritsis.

69 In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Officer, email: data.protection@studysmart.gr, tel: +30 211 411 3235.