



INTERNATIONAL SOS

Data Protection Policy

Version 1.8

Document Owner: **LCIS Division**
Document Manager: **Group General Counsel**
Effective: ***December 2008***
Updated: ***October 2017***

POLICY

**WORLDWIDE REACH.
HUMAN TOUCH.**

© 2017 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.

The only controlled copy of this document is maintained electronically. If this document is printed, the printed version is an uncontrolled copy.

Group	International SOS Data Protection Policy	Policy
--------------	---	---------------

LINK TO STANDARD:	Data Protection Policy	DOCUMENT OWNER:	LCIS
EFFECTIVE DATE:	December 2008	DOCUMENT MANAGER:	Group General Counsel

Revision History

Revision	Rev. Date	Description	Prepared by	Reviewed by	Date	Approved by	Date
1.0		Original Document					Dec 08
1.7	Aug 17	Minor update to terminology	David Cameron	Manoj Tewari	Aug 17	Greg Tanner	Aug 17
1.8	Oct 17	Added change control page, changes for GDPR compliance	David Cameron	Katrin Maeurich Mark Crawford	Oct 17	Greg Tanner	Oct 17

Responsibilities

All employees are to follow the procedures detailed in this document.

Abbreviations / Definitions

Definitions are contained in the body of the document.

References

© 2017 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.

TABLE OF CONTENTS

1	INTRODUCTION.....	4
	1.1 Introduction	4
	1.2 Purpose of the Policy.....	5
	1.3 Compliance with Laws, Other Policies and Contracts of Employment.....	6
	1.4 Questions Regarding the Policy	6
2	THE TEN PRINCIPLES OF DATA PROTECTION	7
	1. Authority and Accountability	7
	2. Identify Purposes for Collecting Personal Data.....	7
	3. Consent of the Data Subject.....	7
	4. Collection Limitations and Accuracy.....	8
	5. Limiting Use, Disclosure, Retention and Destruction	8
	6. Security.....	9
	7. Transparency.....	9
	8. Individual Access and Correction	9
	9. Challenging Compliance.....	10
	10. Transfers to a Third Party and Cross-Border Personal Data Flows.....	12
3	EXCEPTIONS TO THE POLICY	13
4.	ENFORCEMENT, AUDITS AND REPORTING BREACHES	13
5.	CONTINUOUS IMPROVEMENTS AND BEST PRACTICES.....	14

INTERNATIONAL
SOS

1 INTRODUCTION

1.1 Introduction

- 1.1.1. This Data Protection Policy (the "Policy") has been adopted by International SOS ("Intl.SOS") in order to set out the framework for Intl.SOS and our employees in respect of the collection, recording, organisation, storage, adaptation, alteration, retrieval, use, treatment, handling, disclosure, correction, providing access to, blocking, erasure and destruction of personal data.
- 1.1.2. Intl.SOS and our employees shall diligently take appropriate measures to ensure the accuracy, integrity and security of personal data and to only permit appropriate access to such data in accordance with relevant laws and regulations, including, where applicable: the EU GDPR, the US HIPPA legislation; the Group's Binding Corporate Rules (as described in paragraph 1.2 below); this Policy; and standard operating processes and procedures.
- 1.1.3. The words: "personal data" when used in this Policy means data:
 - (a) in electronic, paper or other form and whether oral or in writing; and
 - (b) that relates to living individuals (the "data subject") who can be identified from the data or from other information which is in the possession of or likely to come into the possession of Intl.SOS or our employees
- 1.1.4. Personal data does not include data concerning a company, a partnership or an association. Personal data relating to a person who is deceased shall be treated with these rules in mind, subject however, to applicable laws which may impose lower obligations with respect thereto.
- 1.1.5. Personal data need not be sensitive or secret to require protection under this Policy and it may come from many sources and concern many different data subjects, such as employees, our customers, our customers' employees or their families, our service providers and our partners.
- 1.1.6. Personal data includes both factual information and opinions or judgments which include identifiable personal data.
- 1.1.7. This Policy applies to the employees of all Intl.SOS Group entities, and to all officers and directors appointed to Intl.SOS Group companies throughout the world.
- 1.1.8. Intl.SOS also expects that our service providers will introduce principles in their respective businesses that are substantially similar to the principles set out in this Policy.

1.2 Purpose of the Policy

There are several important reasons why personal data must be carefully protected by Intl.SOS and our employees.

1.2.1. International SOS is the world's leading provider of medical assistance, international healthcare and security services. Our mission is to deliver the highest levels of service and customer care to our clients across the world. Our customers entrust us with sensitive personal data such as medical data. Our reputation and ability to continue serving our customers is dependent on our ability to protect their personal data.

Our excellent reputation is the product of many years work by everyone in our organisation but it can be swiftly damaged unless every day, across the globe, our employees continually assess, improve and adhere to the data protection principles in this Policy.

As our future success depends on our reputation, this Policy goes beyond the requirements of the law.

1.2.2. Intl.SOS and our employees are bound by laws and regulations to protect personal data in the countries in which we do business and to which we transfer personal data.

1.2.3. Intl.SOS adheres to the data protection laws of the countries in which we do business. There are, for example, specific and comprehensive data protection laws in, among other countries, Australia and New Zealand, Japan, Singapore, South Africa, the EU, the United States and the United Kingdom. This Policy incorporates the broad principles upon which these data protection laws are based.

1.2.4. Intl.SOS has adopted Binding Corporate Rules (the "BCR") which have been approved by the data protection authorities of the European Economic Area. The establishment of these BCRs allow for the transfer of personal data from our operating companies in the European Economic Area (the "EEA") to our operating companies in the US and other countries outside the EEA.

1.2.5. Intl.SOS and our employees are subject to audits by the US Department of Commerce, the data protection authorities in the EEA and other Government authorities and agencies and we are required to submit information and reports on our compliance with data protection processes and procedures.

1.2.6. Intl.SOS will continue to monitor data protection legislation and international treaty and comity developments regarding data protection, and will update its policies and procedures accordingly.

1.2.7. Intl.SOS and our employees may be required to adhere to specific data protection and data management laws and regulations in respect of personal medical data. Intl.SOS does, for example, adhere to the

relevant provisions of the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the GDPR in the European Union and applicable legislation of other countries within which we have operations. The relevant operational processes and procedures shall be consistent with and support such laws and regulations.

- 1.2.8. Failure by Intl.SOS and our employees to abide by applicable laws and regulations may result in sanctions that include criminal prosecution, fines, compensation and other measures. Employees should be aware that they may be exposed to personal liability.
- 1.2.9. Data protection is of great importance to our customers and service providers. Intl.SOS has therefore entered into contracts with our customers and service providers that oblige Intl.SOS and our employees to take measures to protect their data and to disclose and otherwise deal with data in a manner that the customers or our service providers direct. Failure by Intl.SOS or our employees to comply with the contract terms may result in the contract being cancelled and damages being awarded against Intl.SOS, as well as administrative and penal sanctions outlined above.

1.3 Compliance with Laws, Other Policies and Contracts of Employment

- 1.3.1. This Policy should be read in the context of applicable laws and in conjunction with other relevant policies and standard operating processes and procedures. The other policies include (but are not limited to): the Code of Conduct and Ethics, the Information Security Policy, the Clean Desk Policy, the Call Recording Policy, the Restricted Data Policy and the Data Retention Archiving and Destruction Policy.
- 1.3.2. Further, each employee has legal obligations under their contract of employment with Intl.SOS concerning confidentiality and trade secrets.
- 1.3.3. Intl.SOS expects employees to comply with applicable laws and regulations and to be familiar with and to fully comply with this Policy and their obligations under their contracts of employment.
- 1.3.4. All employees shall on an annual basis undertake the compulsory on-line training on data protection (or the associated test of knowledge). Managers shall have the responsibility of ensuring that training is completed by the employees in their teams.

1.4 Questions Regarding the Policy

- 1.4.1. This Policy provides clear principles. However, new legal and other considerations arise from time to time and the social, political, commercial and legal environments change rapidly.
- 1.4.2. Employees may therefore have questions from time to time on how this Policy will apply to particular situations. Employees are encouraged to seek guidance from their supervisor, or the Chief Data Protection Officer, or in the EU specifically, the EU Data Protection Officer.

2 THE TEN PRINCIPLES OF DATA PROTECTION

This Policy sets out ten principles of data protection that every employee is required to understand and follow and every manager is required to communicate to their team.

Although described in this Policy separately, the principles are interrelated and they must be understood as a whole.

The ten principles are:

1. Authority and Accountability

- a) The Group General Counsel is the Chief Data Protection Officer with overall responsibility for this Policy and the protection of personal data.
- b) Each employee is the owner of the data they utilize and is accountable to their manager or supervisor for compliance with this Policy. Other individuals are designated as having authority and being accountable for specific aspects of the interpretation, implementation, audit, enforcement and development of personal data protection at Intl.SOS.
- c) To the extent that these individuals and the scope of their responsibilities are not set out in this Policy, this will be clearly set out in relevant standard operating processes and procedures.

2. Identify Purposes for Collecting Personal Data

- a) No personal data shall be collected unless the purpose of collecting the data is made known to and is understood by the data subject.
- b) If the purpose changes, the data subject shall be notified of the new purpose before the data is used for this purpose.

3. Consent of the Data Subject

- a) The knowledge and consent of the data subject is required before a data subject's personal data is processed (i.e. collected, used, disclosed, transferred, etc.). Although there are exceptions which allow emergency use of personal data, or which can be used to obtain deemed consent, the Company's preference is to seek to obtain clear, specific and demonstrable consent wherever reasonably possible.
- b) In the event that information is gathered electronically using the worldwide web, a data subject may give consent by clicking on an appropriate icon but the system shall require that the data subject positively affirms their consent before the data is gathered.
- c) The data subject must understand: why the data is being collected; how it will be used; and who it will be transferred to and why. If requested by the data subject, Intl.SOS will also let the data subject know how the personal data will be stored and kept secure and how long it will be retained.

-
- d) If the data is sensitive personal data, the data subject should be informed about the alternatives to providing the data and the consequences of not providing it.
 - e) An individual shall be permitted to withdraw consent at any time and Intl.SOS and our employees shall promptly honour any such withdrawal and notify the data subject when Intl.SOS has ceased gathering data.
 - f) In the event that circumstances arise in which the law, regulations or contractual commitments require that personal data be collected, used, disclosed or transferred without the consent of the individual, employees shall raise this with their supervisor. If the supervisor is in concurrence, the supervisor shall raise this with the Group General Manager, Legal, the Chief Data Protection Officer, or, in the EU, the EU DPO.

4. Collection Limitations and Accuracy

- a) Personal data shall be collected lawfully and fairly (without deception) and the collection shall be limited only to the purposes identified by Intl.SOS that are lawful, legitimate and necessary for Intl.SOS to perform its business and operations. The personal data collected should be adequate for the purposes identified and shall not be excessive.
- b) Personal data shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is to be used, taking into account the interests of the individual and what is reasonable and practicable. Where practicable, data should be provided or confirmed by the data subject.

5. Limiting Use, Disclosure, Retention and Destruction

- a) Personally Identifiable data shall be used and processed only for the specified, explicit and legitimate purposes for which it was collected.
- b) Employees shall comply with the relevant laws and regulations with regard to data retention and with the Data Retention Archiving and Destruction Policy and relevant standard operating processes and procedures. Subject to relevant laws and regulations, personal data shall be retained no longer than is necessary for the purposes identified.
- c) Personally Identifiable data should be destroyed in a manner that prevents its recreation and care shall be taken to ensure that there is no unauthorised access during the destruction of data.

6. Security

- a) Intl.SOS and our employees shall have in place, the appropriate technical and organisational measures to protect personal data against accidental or unlawful damage or destruction or accidental loss, theft, alteration, unauthorised disclosure, access or use and which provide a level of security appropriate to the risk represented by the nature of the personal data being protected and purposes for which it is being collected.
- b) Employees shall comply with the Information Security Policy, Laptop Policy, Clean Desk Policy and other policies, procedures and operating standards to protect the security of personal data.
- c) Security precautions shall correspond to the sensitivity of the personal data (the higher the sensitivity, the more security is appropriate) and they shall be improved in accordance with the state of technological development.
- d) Personal data shall be accessed by employees strictly on a need-to-know basis to perform their duties and only in support of legitimate business purposes.
- e) Managers shall make employees aware of the importance of maintaining confidentiality of personal data.

7. Transparency

- a) Intl.SOS and our employees shall be open about our policies with respect to the management and protection of personally identifiable data.
- b) This Policy shall be available on the Intl.SOS website for employees, customers, service providers, partners and the general public.
- c) The Intl.SOS website shall set out a Personal Data Privacy Statement describing what personal data from customers and service providers is held by Intl.SOS, the purpose for which it is held, how it can be accessed, and who the data may be transferred to. The Personal Data Privacy Statement shall make it clear that the Group General Counsel as the Chief Data Protection Officer has overall responsibility for this Policy and it shall provide the contact details where complaints in respect of data protection can be sent.
- d) The Human Resources Department shall inform employees and seek their consent on what personally identifiable data Intl.SOS collects and retains how it will be used, who it may be transferred to and how it can be accessed.

8. Individual Access and Correction

- a) Intl.SOS and our employees shall give individuals: confirmation of what personal data has been collected and is being stored; and access to their personal data; within a reasonable time after receiving their request and for a reasonable cost.
- b) The individual requesting the data shall describe it with reasonable specificity before the data is provided, in order to facilitate timely identification.

- c) Intl.SOS and our employees shall verify the identity of the person requesting the data before granting access.
- d) In certain cases personal medical data may be disclosed directly to a medical practitioner who is treating the data subject without being disclosed at the same time to the data subject.
- e) If the data subject has successfully demonstrated that the data is inaccurate or incomplete and has provided alternative or additional personal data that is verifiably accurate, Intl.SOS and our employees shall promptly correct the data at Intl.SOS's sole cost.
- f) If the data subject has successfully demonstrated that the data is unnecessary or illegitimate for our purposes, Intl.SOS and our employees shall promptly destroy it at Intl.SOS's sole cost.
- g) The process for subject access requests is detailed in the Data Subject Access Request Procedure.

9. Challenging Compliance

- a) Individuals shall be given the responsibility of Data Protection Officers and Data Protection Administrators. They shall ensure that data is managed, protected and utilized in compliance with this policy. Data Protection Officers and by escalation, Data Protection Administrators, shall receive, record, address and elevate complaints concerning the handling of personal data from customers, employees, service providers and the general public. This role may be in addition to other roles that they have.
- b) These individuals shall represent a country or a group of locations.
- c) The Regional Managing Director or its equivalent of each Regional Operating unit shall serve as the Data Protection Administrator for that unit. The Data Protection Administrator shall assign the country or location General Managers or a designated staff member to serve as Data Protection Officers responsible for ensuring compliance with this policy throughout their country or location, handling complaints and enquires raised in respect of personal data complaints, enquiries or issues raised by customers, service providers, employees and the general public. The Data Protection Officers shall ensure that the Data Protection Policy is properly implemented in their location and elevate any complaints to the Data Protection Administrators appropriate. Complainants who are unsatisfied with the responses from the Data Protection Administrator may elevate complaints to the Chief Data Protection Officer.
- d) The Group Directors of each Corporate Headquarters Division shall be the Data Protection Administrator for that Division. The functional Data Protection Administrator shall assign the Group General Managers of their function to serve as Data Protection Officers responsible for ensuring implementation and compliance with this policy throughout each Corporate Headquarters division. They shall also designate functional Data Protection Administrators in each

region and in major countries. Such functional Data Protection Officers shall elevate these complaints to the appropriate Data Protection Administrators. Complainants who are unsatisfied with the responses from the Data Protection Administrator may elevate complaints to the Chief Data Protection Officer.

- e) The head of each Business Line shall be the Data Protection Administrator for that Division. The Data Protection Administrator shall assign the General Managers to serve as Data Protection Officers responsible for ensuring implementation and compliance with this policy throughout each Business Line, handling complaints and enquires raised by customers, service providers, employees and the general public. Such Data Protection Officers shall elevate these complaints to the Data Protection Administrators appropriate. Complainants who are unsatisfied with the responses from the Data Protection Administrator may elevate complaints to the Chief Data Protection Officer.
- f) The Chief Data Protection Officer shall be responsible for advising the Data Protection Administrators, Data Protection Committee, Information Security Management Subcommittee, and Group Executive Committee with respect to this policy. The Chief Data Protection Officer or his/her delegate shall handle complaints and enquires raised by Government authorities. With respect to enquiries received by the business from EU based data protection authorities, these will be handled initially by the EU DPO, who shall keep the Chief Data Protection Officer apprised of all developments.
- g) The relevant department shall be responsible for communicating to the data subject, the contact details of the responsible Data Protection Officer and shall also communicate the opportunity to elevate the matter to the Chief Data Protection Officer.
- h) In respect of Intl.SOS Information Security and Tracking services and external websites, complaints shall be directed to the International SOS On-line's Data Privacy officer using the format available on our Privacy page <https://www.internationalsos.com/privacy>.
- i) The Privacy Feedback button displayed on the Intl.SOS privacy page provides users a means to ask questions or provide feedback regarding our privacy practices through TRUSTe's Dispute Resolution System. TRUSTe is an independent organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. TRUSTe's Dispute Resolution System is an online tool that lets individuals report violations of posted privacy statements and specific privacy issues that pertain to TRUSTe clients. TRUSTe investigates all eligible complaints and mediates solutions between users and clients. If the complainant is not satisfied with Intl.SOS's response to a complaint they can register their complaint to TRUSTe at: <https://feedback-form.truste.com/watchdog/request>. TRUSTe will serve as a liaison to resolve the complaint where applicable.

-
- j) All complaints shall be addressed expeditiously. An acknowledgement that the complaint is being addressed, and the approximate length of time that will be taken to review the complaint will be provided to the complainant no later than five (5) business days from the date the complaint was received. Regular updates shall be given to the complainant on the progress of the review if the review is likely to take longer than seven (7) business days. The complaint and outcome shall be recorded and made available for review by the Chief Data Protection Officer.
 - k) If the complaints prove justified, the appropriate Data Protection Officer, Data Protection Administrator, the Chief Data Protection Officer (as the case may be) shall promptly take measures to rectify the issue, including providing fair and reasonable compensation if that is justified and appropriate.
 - l) A complainant is free to raise complaints with the relevant data protection authorities or take court proceedings.
 - m) It is Intl.SOS's intention to promptly resolve complaints such that the complainant has no desire to seek assistance from data protection authorities or the courts.

10. Transfers to a Third Party and Cross-Border Personal Data Flows

- a) Intl.SOS and our employees may transfer personal data to a third party, including a third party in another country, if it is lawful, accurate, not excessive for the purpose, legitimate and necessary for the purpose communicated to the data subject and only if one or more of the following apply :
 - (a) the recipient of the data is subject to a law, binding scheme, contract, or policy that upholds the principles of fair handling of information of personal data that are similar to the principles in this Policy; or
 - (b) Consent of the data subject to the transfer has been obtained (in accordance with applicable criteria).
- b) In the event that personal data is transferred by Intl.SOS from the EEA to a third party (not being an Intl.SOS employee) in a country outside the EEA that does not provide adequate data protection safeguards, the Intl.SOS employees shall also comply with the provisions of the BCR. If an employee has any questions regarding the application of the provisions of the BCR, they should promptly raise them with the Group General Manager, Legal, or the Chief Data Protection Officer.

3 EXCEPTIONS TO THE POLICY

- 3.1. In the event that circumstances arise in which it is not in the interests of the data subject, Intl.SOS or third parties to comply with any of these principles or if there is a good reason for standard operating processes to deviate from these principles, employees shall raise this with their supervisor. If the supervisor is in concurrence, the supervisor shall raise this with the Chief Data Protection Officer. The Chief Data Protection Officer shall elevate this to the Group Managing Director as appropriate and provide a report to the Data Protection Steering Committee (further described below).

4. ENFORCEMENT, AUDITS AND REPORTING BREACHES

- 4.1. Breaches of this Policy may have serious legal and reputation repercussions and could cause material damage to International SOS. Consequently, breaches can potentially lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.
- 4.2. The Chief Data Protection Officer shall be responsible for reviewing the reports of unsatisfied complaints in respect of the management of personal data, regularly auditing compliance with this Policy, the BCR and providing reports and recommendations to the Data Protection Steering Committee (further described below) as appropriate. The Chief Data Protection Officer or the Data Protection Steering Committee may request that specific audits be performed by the Compliance Department.
- 4.3. Under the guidance and advice of the Legal department and the Chief Data Protection Officer, all employees are expected to cooperate with the data protection authorities (including any audits conducted by them).
- 4.4. All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor or the Group General Counsel. Reports made in good faith by someone who has not breached this Policy will not reflect badly on that person or their career at Intl.SOS. Reports may be made using the following e-mail address: Compliance@internationalsos.com.

5. CONTINUOUS IMPROVEMENTS AND BEST PRACTICES

- 5.1. A Data Protection Steering Committee (the “DPC”) shall be formed and Chaired by the Group General Counsel in the capacity of Chief Data Protection Officer. The other members of the DPC shall comprise of:
- (a) Group Managing Director;
 - (b) Group Chief Financial Officer;
 - (c) Group Director, Medical Services;
 - (d) Group Director, Assistance;
 - (e) Group Chief Information Officer;
 - (f) Group Medical Director, Assistance;
 - (g) Chief Executive Officer, Government Services;
 - (h) Chief Executive Officer, Aspire Lifestyles;
 - (i) Chief Operating Officer, TRICARE;
 - (j) Group Director, Human Resources;
 - (k) Chief Security Officer;
 - (l) Director Information Security and Compliance;
 - (m) Group Director, Sales;
 - (n) Chief Digital Officer, Information and Tracking Group;
 - (o) Chief Privacy Officer; and
 - (p) Data Protection Officer, Europe (by invitation).
- 5.2. The DPC shall be responsible for reviewing the Data Protection Policy, the Procedures and Operating Standards to ensure that they are in compliance with: relevant law; best practices among multinationals; recommendations published by internationally respected institutions or Government bodies; and the expectations of data subjects; and that they are aligned with the state of technological development.
- 5.3. The DPC shall form an Information Security Management Subcommittee. The Subcommittee shall monitor information security and privacy risks and conduct projects at the direction of the DPC.
- 5.4. The DPC shall review the reports of the Compliance Department, the Information Security Management Subcommittee, the recommendations of the Chief Data Protection Officer and make recommendations to the Group Managing Director. The Chief Data Protection Officer shall monitor the implementation of the recommendations.
- 5.5. The DPC shall be responsible for initiating (at the request of its members), reviewing and approving training courses on compliance with personal data protection measures.

- 5.6. The DPC shall meet in person or by telephone no less than once each half year or as the DPC shall decide and the Secretary shall circulate the agenda prior to each meeting.
- 5.7. The Secretary shall take minutes of the meeting and circulate the minutes for comments by the members of the DPC who attended the meeting not later than one week after the meeting.
- 5.8. The Chairman shall execute the agreed minutes and they shall be circulated to the members of the DPC, the Chief Executive Officer, the Group Managing Director and the Group Medical Director.
- 5.9. The minutes of the meeting shall be read out by the Chairman at the next subsequent meeting and the relevant members shall report on the status of any action items set out in the minutes.
- 5.10. The Chief Data Protection Officer shall be responsible for monitoring such action items and ensuring that they are carried out.



© 2017 All copyright in these materials are reserved to AEA International Holdings Pte. Ltd. No text contained in these materials may be reproduced, duplicated or copied by any means or in any form, in whole or in part, without the prior written permission of AEA International Holdings Pte. Ltd.