



# INTERNATIONAL SOS

## DATA PROTECTION POLICY

### Version 1.02

Ownership of this Policy: Group General Counsel

Any questions or suggestions regarding this Policy may be directed to:  
Andrew da Roza, Group General Counsel

Effective: December 2008

Classification: Level 1

<u>Version No.</u>	<u>Drafted By</u>	<u>Date</u>
Version 1.00	Andrew da Roza	November 2008
Version 1.01	Eric Tsui	February 2009
Version 1.02	Eric Tsui	February 2009

© 2008 All copyright in these materials are reserved to International SOS Pte. Limited. 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 International SOS Pte. Limited.

## Approvers

This document was approved by:

Name	Title	Date
Laurent Sabourin	Group Managing Director	November 2008

## Table of Amendments

This section records the history of significant changes and only the most significant changes are described here. Please refer to the relevant sections in the document for more details.

Version No.	Section	Description of Changes / Updates	By / Date
1.01	1.3 and 2.1.5	From Document Retention Policy to Data Retention Archiving and Destruction Policy; Various spelling mistakes	Eric Tsui/Feb 2009
1.02	2.1.8	Paragraph four regarding medical data disclosure	Eric Tsui/Feb 2009

## **TABLE OF CONTENTS**

- 1 INTRODUCTION
  - 1.1 Introduction
  - 1.2 Purpose of the Policy
  - 1.3 Compliance with Laws, Other Policies and Contracts of Employment
  - 1.4 Questions Regarding the Policy
- 2 THE TEN PRINCIPLES OF DATA PROTECTION
  - 2.1 The Principles
    - 2.1.1 Authority and Accountability
    - 2.1.2 Identify Purposes for Collecting Personal Data
    - 2.1.3 Consent of the Data Subject
    - 2.1.4 Collection Limitations and Accuracy
    - 2.1.5 Limiting Use, Disclosure, Retention and Destruction
    - 2.1.6 Security
    - 2.1.7 Openness
    - 2.1.8 Individual Access and Correction
    - 2.1.9 Challenging Compliance
    - 2.1.10 Transfers to a Third Party and Cross-Border Personal Data Flows
- 3 EXCEPTIONS TO THE POLICY
- 4 ENFORCEMENT, AUDITS AND REPORTING BREACHES
- 5 CONTINUOUS IMPROVEMENTS AND BEST PRACTICES

# 1 INTRODUCTION

## 1.1 Introduction

This Data Protection Policy (the "Policy") has been adopted by International SOS ("Intl.SOS") in order to set out the obligations of 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.

Intl.SOS and our employees shall vigilantly take all appropriate measures to ensure the accuracy, integrity and security of personal data and to permit appropriate access to such data in accordance with: the relevant laws and regulations; the US Safe Harbour Principles and the EU Binding Corporate Rules (as described in paragraph 1.2 below); this Policy; and the standard operating processes and procedures.

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 or deceased 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.

Personal data does not include data concerning a company, a partnership or an association.

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.

Personal data includes both factual information and opinions or judgments.

This Policy applies to the officers and employees of Intl.SOS and all directors appointed by Intl. SOS, throughout the world.

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.

- a. 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 depends on our reputation, this Policy goes beyond the requirements of the law.

- b. 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.
- c. 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 Australian and New Zealand, Japan, Singapore, South Africa and the United Kingdom. This Policy incorporates the broad principles upon which these data protection laws are based.
- d. Intl.SOS also adheres to the "Data Protection Safe Harbour Principles" of the United States and has registered a US operating company with the US Department of Commerce for this purpose (the "US Safe Harbour Principles").
- e. Intl.SOS will adopt Binding Corporate Rules, subject to approval by the data protection authorities of the European Economic Area (the "BCR").

The US Safe Harbour Principles and the BCR permits us to transfer 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.

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.

- f. 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 (HIPPA) in the United States. The relevant operations processes and procedures shall be consistent with and support such laws and regulations.
- g. Failure by Intl.SOS and our employees to abide by the laws, regulations, the Safe Harbour Principles and the BCR will result in sanctions that may include criminal prosecution, fines, compensation and other measures. Employees should be aware that they may be exposed to personal liability.
- h. 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.

### **1.3 Compliance with Laws, Other Policies and Contracts of Employment**

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.

Further, each employee has legal obligations under their contract of employment with Intl.SOS concerning confidentiality and trade secrets.

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.

All employees shall undertake the compulsory on-line training on data protection and managers shall have the responsibility of ensuring that training is completed by the employees in their teams.

### **1.4 Questions Regarding the Policy**

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. 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, the Group General Manager, Compliance or the Group General Counsel.

## 2 THE TEN PRINCIPLES OF DATA PROTECTION

### 2.1 The Principles

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:

#### 2.1.1 Authority and Accountability

The Group General Counsel is the Chief Data Protection Officer with overall responsibility for this Policy and the protection of personal data. Other individuals shall be 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. 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.

#### 2.1.2 Identify Purposes for Collecting Personal Data

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

#### 2.1.3 Consent of the Data Subject

The knowledge and consent of the data subject must be given before their personal data can be collected, used, disclosed, transferred or destroyed. If the data is sensitive, the data subjects' written approval is required.

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.

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.

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.

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.

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 or the Group General Counsel.

#### 2.1.4 **Collection Limitations and Accuracy**

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.

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.

#### 2.1.5 **Limiting Use, Disclosure, Retention and Destruction**

Personal data shall be used and disclosed only for the purposes for which it was collected.

Employees shall comply with the 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.

Personal 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.

### 2.1.6 Security

Intl.SOS and our employees shall have in place, the appropriate technical and organisational measures to protect personal data against the accidental or unlawful damages 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.

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.

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.

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.

Managers shall make employees aware of the importance of maintaining confidentiality of personal data.

### 2.1.7 Openness

Intl.SOS and our employees shall be open about the policies with respect to the management and protection of personal data.

This Policy shall be available on the Intl.SOS website for employees, customers, service providers, partners and the general public.

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.

The Human Resources Department shall inform employees and seek their consent on what personal data Intl.SOS collects and retains how it will be used, who it may be transferred to and how it can be accessed.

### 2.1.8 Individual Access and Correction

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.

The individual requesting the data shall describe it with reasonable specificity before the data is provided.

Intl.SOS and our employees shall verify the identity of the person requesting the data before granting access.

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.

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.

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.

### 2.1.9 Challenging Compliance

Individuals shall be given the responsibility of Data Protection Administrators and they shall receive, record, address and elevating 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.

These individuals shall represent a country or a group of locations.

The country or location General Managers shall be responsible for handling complaints and enquires raised in respect of personal data complaints, enquiries or issues raised by customers, service providers and the general public. The country or location General Managers shall elevate these complaints to the Group Director, Medical Services and Operations as appropriate. Complainants who are unsatisfied with the responses from the Data Protection Administrators may elevate complaints to the Group Director Medical Services and Operations.

The Group General Manager for International Human Resources shall be responsible for handling complaints and enquires raised by expatriate employees. The Group General Manager for International Human Resources shall elevate these complaints to the Group Director, Human Resources as appropriate. Complainants who are unsatisfied with the responses from the Data Protection Administrators may elevate complaints to the Group Director Human Resources.

The country or location Human Resources Managers shall be responsible for handling complaints and enquires raised by employees who are not expatriates. The Human Resources Managers shall elevate these complaints to the Group Director Human Resources as appropriate. Complainants who are unsatisfied with the responses from the Data Protection Administrators may elevate complaints to the Group Director Human Resources.

The Group General Manager, Compliance shall be responsible for handling complaints and enquires raised by Government authorities. The Group General Manager, Compliance shall elevate complaints to the Group General Counsel as appropriate.

If the complainant continues to be unsatisfied, they may elevate the complaint to the Group General Counsel. The Group General Counsel shall promptly address the complaint and record the outcome and provide the record to the Group General Manager, Compliance.

The relevant department shall be responsible for communicating to the data subject, the contact details of the responsible Data Protection Administrator and shall also communicate the opportunity to elevate the matter to the Group General Counsel.

**In respect of Intl.SOS Online services**, complaints shall be directed to the International SOS On-line's Data Privacy officer at:

[privacy@internationalsos.com](mailto:privacy@internationalsos.com).

International SOS Online is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. If the complainant is not satisfied, they can contact TRUSTe at:

[http://www.truste.org/consumers/watchdog\\_complaint.php](http://www.truste.org/consumers/watchdog_complaint.php).

TRUSTe will then serve as a liaison to resolve the complaint.

All complaints shall be addressed expeditiously and an acknowledgement of the identity of the employee addressing the complaint and the approximate length of time that will be taken to review the complaint will be provided 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 Group General Manager, Compliance.

If the complaints prove justified, the Data Protection Administrator, the Group Director, Medical Services and Operations, the Group Director Human Resources, the Group General Manager, Compliance or the Group General Counsel (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.

A complainant is free to raise complaints with the relevant data protection authorities or take court proceedings.

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.

### 2.1.10 Transfers to a Third Party and Cross-Border Personal Data Flows

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. the data subject consents to the transfer.

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, the Group General Manager, Compliance or the Group General Counsel.

### 3 EXCEPTIONS TO THE POLICY

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 Group General Counsel. The Group General Counsel 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

Breaches of this Policy will have serious legal and reputation repercussions and could cause damage and distress to the lives of others. Consequently, breaches will lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.

The Group General Manager, Compliance 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 US Safe Harbour Principles and the BCR and providing reports and recommendations to the Group General Counsel. The Group General Counsel shall elevate such reports to the Data Protection Steering Committee (further described below) as appropriate. The Group General Counsel or the Data Protection Steering Committee may request that specific audits be performed by the Group General Manager, Compliance.

Under the guidance and advice of the Legal department and the General Manager, Compliance, all employees are expected to cooperate with the data protection authorities (including any audits conducted by them).

All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor, the Group General Manager, Compliance or the Group General Counsel. Reports made in good faith by someone who has not breached the 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](mailto:Compliance@internationalsos.com)

## 5 CONTINUOUS IMPROVEMENTS AND BEST PRACTICES

A Data Protection Steering Committee (the “Steering Committee”) shall be formed and Chaired by the Group General Counsel in the capacity of Chief Data Protection Officer. The Vice Chairman shall be the Chief Information Officer and the Secretary shall be the Group General Manager, Compliance. The other members of the Steering Committee shall comprise of:

Chairman of the Information Security Management Committee;

Chief Executive Officer, TSS;

Chief Executive Officer, MedAire;

Group Medical Director, Assistance;

Group General Manager, Assistance Services;

Group General Manager, Assistance Worldwide;

General Manager, Group Finance;

General Manager, Group Projects;

General Manager, HR Services;

Group General Manager Market Strategy & Planning;

Corporate Network Director; and

a representative from SOS Online.

The Steering Committee shall be responsible for reviewing the Data Protection Policy, the Procedures and Operating Standards to ensure that they are in compliance with: the changes in the 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.

The Steering Committee shall also review the reports of the Group General Manager, Compliance and the recommendations of the Group General Counsel and make recommendations to the Group Managing Director. The Group General Counsel shall monitor the implementation of the recommendations.

The Steering Committee shall be responsible for initiating (at the request of its members), reviewing and approving training courses on compliance with personal data protection measures.

The Steering Committee shall meet in person or by telephone no less than once each half year or as the Steering Committee shall decide and the Secretary shall circulate the agenda no less than two calendar weeks before each meeting. The Secretary shall take minutes of the meeting and circulate the minutes for comments by the members of the Steering Committee who attended the meeting not later than two weeks after the meeting. The Chairman shall execute the agreed minutes and they shall be circulated to the members of the Steering Committee, the Chief Executive Officer, the Group Managing Director and the Group Medical Director. 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. The Group General Counsel shall be responsible for monitoring such action items and ensuring that they are carried out.



© 2008 All copyright in these materials are reserved to International SOS Pte. Limited. 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 International SOS Pte. Limited.