INTERNATIONAL SOS

Data Protection Policy

Version 2.00

POLICY

Document Owner: **Legal**

Document Manager: **Chief Privacy Officers**

Effective: ***December 2008***

Updated: ***September 2020***

WORLDWIDE REACH.
HUMAN TOUCH.

Group	INTERNATIONAL SOS Data Protection Policy	Policy

		DOCUMENT OWNER:	**Legal**
EFFECTIVE DATE:	December 2008	**DOCUMENT MANAGER**:	Chief Privacy Officers

Revision History

Revision	Rev. Date	Description	Prepared by	Reviewed by	Date	Approved by	Date
1.0		**Original Document**					Dec 2008
1.7	Aug 2017	Minor update to terminology	David Cameron	Manoj Tewari	Aug 2017	Greg Tanner	Aug 2017
1.8	Oct 2017	Added change control page, changes for GDPR compliance	David Cameron	Katrin Maeurich Mark Crawford	Oct 2017	Greg Tanner	Oct 2017
1.9	Aug 2018	Removed section 9 (i) relating to TRUSTe as Intl.SOS no longer subscribe to Truste	Lim Thau Khuan	Richard Wee	Aug 2018	Greg Tanner	Aug 2018
1.10	December 2019	Annual review of Intl.SOS Public Group Policies	Lim Thau Khuan	Richard Wee	December 2019	Greg Tanner	December 2019
2.00	May 2020	DPIA, Data Subject Rights; Governance; restructuring; transferred to L1 document template	Katrin Maeurich	Richard Wee, David Cameron, Greg Tanner,	May 2020	Shireen A Lee, Lorraine Lee	September 2020

Responsibilities

Chief Privacy Officers are responsible for keeping this Policy up to date and fit for purpose. Information Security and Chief Security Officers should review and contribute to the content of this policy. All International SOS employees and agents are responsible to know and understand this policy and follow the principles set out within it to protect Personal Data they handle in the course of their work.

TABLE OF CONTENTS

1. INTRODUCTION

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 and payment card data. Our reputation and ability to continue serving our customers and comply with applicable regulations is dependent on our ability to ensure the confidentiality, integrity and availability of Personal Data on one hand, and our commitment to the protection of data subjects' rights on the other.

To ensure data protection, Intl.SOS and our employees shall take appropriate technical and organisational measures in accordance with applicable laws and regulations, relevant adopted codes of conduct and standards, and contractual obligations.

This Policy sets out the guiding principles for the processing of Personal Data (broadly aligned with the European General Data Protection Regulation) and describes the management system Intl.SOS has implemented to effectively achieve its data protection objectives.

1.1. Objectives

1.1.1. The Policy sets out our Compliance Obligations and how Intl.SOS has established accountability to customers and data subjects.

1.1.2. The Policy is a commitment by Intl.SOS to deliver products and services involving Personal Data processing in compliance with all applicable regulations, relevant adopted codes of conduct and standards (see 1.4 Compliance Obligations).

1.1.3. It is a commitment to the protection of the Personal Data we process, including prevention of Personal Data breaches, and the upholding of the rights of data subjects.

1.2. References

1.2.1. This Policy should be read in the context of applicable data protection laws and in conjunction with other relevant policies, standards, and codes of conduct such as the International SOS 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; International SOS Binding Corporate Rules; International SOS Inter-Company Standard Contractual Clauses; and various data protection laws including, but not limited to, the Privacy Act (1988) [Australia], the Personal Information and Electronic Documents Act [Canada], The General Data Protection Regulation (GDPR) 2016 [European Union]; the Personal Data Protection Act [Singapore], Health Insurance Portability and Accountability Act 1996 (HIPAA) [United States]; Health Information Technology for Economic and Clinical Health (HITECH) Act 2009 [United States]; California Consumer Privacy Act (CCPA) [United States].

1.3. Questions Regarding the Policy

1.3.1. This Policy provides essential principles for the protection of Personal Data. However, new legal and other considerations regularly arise and the social, political, commercial and legal environments change rapidly.

1.3.2. 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, Chief Privacy Officers, Privacy Programme Manager, or their country Data Protection Officer where one has been appointed.

1.4. Definitions

1.4.1. **Personal Data** is any information that relates to an identified or identifiable individual (the "data subject").

(a) Another term for this is Personally Identifiable Information (PII).
(b) This may be data in electronic, paper or other form such as audio recording, images or finger prints.
(c) Personal Data does not include data concerning a company, a partnership or an association.
(d) Personal Data need not be sensitive or secret to require protection under this Policy and it may come from many sources and concern a variety of data subject types, such as employees, our customers, our customers' employees or their families, our service providers and our partners.
(e) Personal Data includes both factual information and opinions or judgments.
(f) 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.

1.4.2. **Special Category Personal Data** is data that requires additional protection because use of this data could create significant risks to the Data Subject's fundamental rights and freedoms such as freedom of thought, conscience and religion; freedom of expression; freedom from discrimination; the right to respect for private and family life; or freedom from discrimination.

(a) Another term for this is Sensitive Data.

(b) Examples of Special Category Data:

(i) Personal Data revealing racial or ethnic origin;
(ii) Personal Data revealing political opinions;
(iii) Personal Data revealing religious or philosophical beliefs;
(iv) Personal Data revealing trade union membership;
(v) Genetic data;
(vi) Biometric data (where used for identification purposes);
(vii) Data concerning health;
(viii) Data concerning a person's sex life or their sexual orientation.
(ix) Data concerning criminal conviction history.

1.4.3. **Data Subject** is the individual to whom the Personal Data pertains. Another term for this is PII Principal.

1.4.4. **Data Asset** is something that supports information-related activities and Personal Data Processing Activities. This can be a system, application, database, back-up disk or even a file cabinet.

1.4.5. **Data Protection / Privacy Impact Assessment** is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects.

1.4.6. **Processing** means any operation which is performed on 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.

1.4.7. **Data Controller** is a person or organisation who (either alone or jointly or in common with other persons or organisations) determines the purposes for which and the manner in which any Personal Data are processed.

1.4.8. **Data Processor** means any person (other than an employee of the Data Controller) or organisation who processes the data on behalf of the Data Controller.

2. COMPLIANCE OBLIGATIONS

Intl.SOS has various compliance obligations in relation to Data Protection which are derived from regulation, contracts, adopted codes of conduct and standards.

Failure by Intl.SOS and our employees to fulfil our compliance obligations, especially those derived from contracts and applicable regulations, may result in significant detrimental impact on data subjects and clients, damage to our business reputation and resources and sanctions including criminal prosecution, fines, compensation and other measures.

2.1. Data Protection Regulations

Most countries in which Intl.SOS operates have Data Protection regulations that must be complied with. Some regulations are generally applicable to all Personal Data processing, others are sector specific (such as healthcare or financial transactions). This Policy is revised annually to ensure that changes in Data Protection regulations are addressed.

2.1.1. Our Privacy and Legal Teams continuously monitor developments of general and sector-specific data protection regulation and international treaty and comity and update our management system accordingly.

2.1.2. Intl.SOS is 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 by many contracts to submit information and reports on our compliance with data protection processes and procedures to our clients.

2.2. Codes of Conduct and Standards

We continuously monitor developments of general and sector-specific evolution of standards and codes of conduct regarding data protection and update our management system accordingly.

In addition to Data Protection regulation in the countries where Intl.SOS operates, we are subject to the following:

2.2.1. Intl.SOS has adopted **Binding Corporate Rules - Controller** (BCR-C) which have been approved by the Commission Nationale de l'Informatique et des Libertés (CNIL) in accordance with GDPR Art. 46-2(b) & 47.

2.2.2. BCR are a voluntary code of conduct providing a comprehensive set of compliance obligations that are similar to those imposed by the GDPR. 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 outside the EEA where Intl.SOS acts as Data Controller.

2.2.3. All Intl.SOS operating companies acting as Data Controller have signed the BCR-C and shall maintain compliant. Annual audit shall be required to evidence continuous compliance.

2.2.4. All Intl.SOS operating companies acting as Data Processor on behalf of our customers have signed **Standard Contractual Clauses** with International SOS (Assistance) S.A., our operating company in France, in accordance with GDPR Art. 46 2(c) & 93-2. This provides the necessary safeguards for the transfer of Personal Data from our operating companies in the EEA to our operating companies outside the EEA **where Intl.SOS acts as Data Processor**.

2.2.5. Intl.SOS has adopted ISO 27001 – Information Security Management and Bureau Veritas Data Protection Standard (GDPR) and shall maintain global certification via third party audit.

2.3. Commercial Contracts

2.3.1. Intl.SOS has entered into contracts, including Data Processing Agreements, with our customers, service providers and partners that set data protection obligations specific to the Personal Data processing activities undertaken with them or on their behalf us to take measures to protect personal data and to disclose and otherwise deal with data in a manner that the customers or our service providers direct.

2.3.2. 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.

2.4. Employment Contracts

2.4.1. Each employee has legal obligations under their contract of employment with Intl.SOS concerning confidentiality and trade secrets.

2.4.2. 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.

2.4.3. All employees are required to complete on-line training on data protection (or the associated test of knowledge). Managers shall be responsible for ensuring that training is completed by the employees in their teams.

2.5. Other Policies

2.5.1. This Policy should be read 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.

3. PRINCIPLES OF DATA PROTECTION

3.1. Accountability

3.1.1. Intl.SOS shall establish, implement, maintain and continually improve an Information Security Management System and Privacy Management Program to:

(a) Systematically identify and assess Data Protection risks, taking account compliance obligations, threats, vulnerabilities, and impacts;

(b) Design and implement a coherent and comprehensive suite of Data Protection controls and other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

(c) Ensure that the Data Protection controls evolve to meet Data Protection compliance obligations.

3.1.2. As part of these Management Systems, Information Security and Data Protection Policies shall be established. A Description of the International SOS Management System is set out in 5. PRIVACY MANAGEMENT PROGRAM: AUDIT, MANAGEMENT REVIEW AND CONTINUOUS IMPROVEMENT.

3.1.3. The Group General Counsel is the Chief Data Protection Officer with overall responsibility for the Information Security Management System and Privacy Management Program, including this Policy, and for the protection of Personal Data by Intl.SOS in general.

3.1.4. Each Intl.SOS employee 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. 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.

3.2. Purpose Limitation

3.2.1. Personal Data shall be collected only for specific, explicit and legitimate business purposes and shall not be further processed in a manner incompatible with those purposes unless required or permitted by law or after consent has been obtained from the Data Subject (see 3.3 Lawfulness, Transparency and Fairness).

3.3. Lawfulness, Transparency and Fairness

3.3.1. Personal Data shall be collected by fair and lawful means.

3.3.2. Each Processing activity shall have a lawful basis. Certain Processing activities also will require consent of the Data Subject to establish a lawful basis. Employees responsible for Personal Data Processing are required to record existing Processing activities in the Personal Data Processing Inventory and submit a request for a privacy assessment for new or amended Processing activities. Privacy Programme Managers and Data Protection Officers will determine the lawful basis for the proposed Processing.

3.3.3. Privacy Notices shall be provided to Data Subjects before or at the time of data collection, describing the types of Personal Data processed by Intl.SOS, the purpose and lawful basis of processing, other parties the data may be transferred to and how Data Subjects can exercise their rights or make a complaint.

3.3.4. If the purpose of processing changes, the data subject shall be notified of the new purpose before the data is used for this purpose and their prior consent shall be obtained where required.

3.3.5. Intl.SOS shall be open about our 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.

3.4. Data Minimisation and Accuracy

3.4.1. Personal Data processed shall be adequate, relevant and proportionate to the purposes for which it is collected. Intl.SOS shall not collect Personal Data “or in excess of what is necessary.

3.4.2. Personal Data processed shall be as accurate, complete, and as up-to-date as possible in order to properly satisfy the purposes for which it is used. Intl.SOS shall implement appropriate technical and organisational measures to assure that inaccuracies in Personal Data can be rectified.

3.5. Retention and Destruction

3.5.1. Personal Data processed shall be kept in a form which permits identification of data subjects for no longer than necessary to fulfil to the purposes for which it was collected.). Appropriate technical and organisational measures shall be implemented to ensure that Personal Data is destroyed or anonymised in a manner that prevents its recreation or the re-identification of individuals.

3.5.2. Intl.SOS shall establish and implement a Data Retention Archiving and Destruction Policy that provides rules and principles for the lawful retention and secure destruction of the main types of Personal Data it processes. Furthermore, and in compliance with this retention policy, purpose-bound retention limits and appropriate destruction or transfer procedures shall be specified, implemented and documented in relation to each Personal Data Processing activity recorded in the Processing Inventory.

3.6. Security

3.6.1. Personal Data shall be Processed with appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, theft, alteration, destruction or damage to ensure Personal Data security, confidentiality and integrity.

3.6.2. Security precautions shall correspond to the sensitivity of the Personal Data (the higher the sensitivity, the more security is appropriate), vulnerability of the Data Subjects, context of processing and they shall be improved in accordance with the state of technological development.

3.6.3. Employees shall comply with the Information Security Policy, Laptop Policy, Clean Desk Policy and other policies, procedures and operating standards to ensure the security of Personal Data.

3.6.4. 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.

3.6.5. Managers shall make employees aware of the importance of maintaining confidentiality of Personal Data.

3.7. Data Subject Rights

3.7.1. Upon request, Intl.SOS must inform a Data Subject of the existence, use, and disclosure of their Personal Data and be given access to it or provide them with a copy in a portable format. Individuals have the right to challenge the accuracy and completeness of that information and have it amended as appropriate. They may in some circumstances request for their Personal Data to be deleted or for Intl.SOS to restrict the processing of their data.

3.7.2. Intl.SOS shall respond to all Data Subject Rights requests in a timely manner.

3.7.3. Intl.SOS shall verify the identity of the person requesting the data before granting access and ensure that any information which is provided to the individual requesting the data pertains only to such individual, and does not include Personal Data of other individuals.

3.7.4. If the Data Subject has demonstrated that the data is inaccurate or incomplete and has provided alternative or additional Personal Data that is verifiably accurate, Intl.SOS shall promptly correct the data.

3.7.5. If the Data Subject has successfully demonstrated that the data is unnecessary or not reasonably required for our purposes, Intl.SOS shall promptly destroy it.

3.7.6. Intl.SOS shall only refuse a Data Subject Rights request for a legitimate, lawful business reason, e.g. if the Personal Data is subject to solicitor-client or litigation privilege or if a request is manifestly unfounded or excessive.

3.8. Challenging Compliance and Complaints

3.8.1. An individual must be able to challenge Intl.SOS' compliance with the data protection principles set out in this Policy. Intl.SOS shall publicly communicate how to make a complaint about how it processes Personal Data and ensure that complaints from Data Subjects, customers and other interested parties are effectively managed.

3.8.2. 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 shall 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 or the relevant Chief Privacy Officer.

3.8.3. If the complaints prove justified, the appropriate Chief Privacy Officer, Data Protection Officer, or 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.

3.8.4. Individuals are free to raise complaints with the relevant data protection authorities or take court proceedings.

3.8.5. It is Intl.SOS' intention to promptly resolve complaints such that the complainant has no desire to seek assistance from data protection authorities or the courts.

3.9. "Data Protection by Design and Default" – Data Protection Impact Assessments

3.9.1. Risk assessments shall be conducted to assess any new or revised Processing activity . Risks shall be identified and managed through the process of PIA Threshold Assessment.

3.9.2. Where a business activity may lead to a High Risk to Personal Data, a more detailed Data Protection Impact Assessment (DPIA) shall be carried out.

3.9.3. Such Risk Assessment shall be integrated into Intl.SOS procurement, project and change management processes, thus ensuring that Data Protection principles are applied to all business activities by design and default.

4. 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 Chief Privacy Officer or Chief Data Protection Officer. The Chief Privacy Officer or 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).

5. GOVERNANCE: AUDIT, MANAGEMENT REVIEW AND CONTINUOUS IMPROVEMENT

5.1. The Chief Data Protection Officer shall be responsible for reviewing 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.

5.2. The Chief Data Protection Officer or the Data Protection Steering Committee may request that specific audits be performed by the Compliance Department.

5.3. Two Chief Privacy Officers set the strategic direction for the Privacy Management Program, communicate its values, objectives and structure internally and externally and create, revise and implement policies, procedures, training and tools that comprise and support the it.

5.4. The Chief Privacy Officers ensure that Data Protection Compliance Obligations are identified and communicated for the organisation at board level and to stakeholders in all business lines and functions. They ensure adherence by Group Technology, Assistance Business Line, Medical Services Business Line, Aspire, MedAire to GAPP requirements during procurement process and/or product development process including information security review, privacy impact assessment and legal review.

5.5. The Chief Privacy Officers chair the Data Protection Steering Committee. The Privacy Program Managers chair its Data Privacy Management sub-committee (DPMC) and its sub-committee, the Information Security Management Committee (ISMC) (see 5. AUDIT, MANAGEMENT REVIEW AND CONTINUOUS IMPROVEMENT).

5.6. Two Privacy Program Managers are appointed to advise business lines and functions on privacy risk and risk mitigation and escalate residual data protection related risks to the Chief Privacy Officers and the AEA Risk Management Committee. They work closely with InfoSec, Security and country/regional DPO to respond effectively to data breaches and meet regulatory notification requirements.

5.7. 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).

5.8. A Data Protection Steering Committee (the “DPC”) shall be formed and Chaired by Chief Privacy Officers at the request of the Chief Data Protection Officer. The other members of the DPC shall include the staff listed below and invite participation on a rotating basis from the senior management of each International SOS Group business line or function.

5.9. 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.

5.10. The DPC shall form a Data Privacy Management Subcommittee (“DPMC”) and Information Security Management Subcommittee (“ISMC"). These Subcommittees shall monitor information privacy and security risks and conduct projects at the direction of the DPC.

5.11. The DPC shall review the reports of the Compliance Department, the DPMC, ISMC, the recommendations of the Chief Privacy Officers, and 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.

5.12. 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.

5.13. 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.

5.14. 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.

5.15. The Chairpersons 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.

5.16. The minutes of the meeting shall be read out by the Chairperson at the next subsequent meeting and the relevant members shall report on the status of any action items set out in the minutes.

5.17. The Chief Data Protection Officer shall be responsible for monitoring such action items and ensuring that they are carried out.

6. ENFORCEMENT AND REPORTING BREACHES

6.1. 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.

6.2. 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.