INTERNATIONAL SOS

UK Binding Corporate Rules for Controllers

Version 1.0

UK-BCR-C

Document Owner:	**LCIS Division**
Document Manager:	**Data Protection Officer, UK**
Effective Date:	2021
Last Updated:	March 2021

WORLDWIDE REACH.
HUMAN TOUCH.

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.

It is particularly important that data subjects whose personal data are covered by the United Kingdom's Data Protection Act 2018 and the UK GDPR, continue to be able to exercise their rights, whether their data is being processed in the UK or has been transferred to countries that have not been deemed to ensure an adequate level of data protection ("Third Countries") by the European Commission ("EC") prior to the UK's exit from the European Union (and upheld under the UK's own regime), or by UK adequacy regulations after the UK's exit from the European Union.

These UK Binding Corporate Rules ("UK-BCR" or "Rules") are part of the International SOS Data Protection Management Program and function as a legal instrument in accordance with UK GDPR Article 47, safeguarding personal data transferred from International SOS Group entities in the UK acting as Controllers ("Data Exporters"), to other International SOS Group entities in Third Countries, acting as Controllers or Processors ("Data Importers").

The UK-BCR are legally binding and apply to every signatory entity and their employees. They also establish the Data Exporters' liability for breaches caused by Data Importers and confer enforceable rights on all data subjects whose personal data is processed by the UK-BCR Members.

1.1 Definitions

The terms used in this document have the following meaning and must be interpreted in accordance with the UK GDPR. Any terms not specifically defined here shall have the meaning provided by the UK GDPR.

AEA: AEA International Holdings, Pte. Ltd, parent holding company of the International SOS Group;

UK Binding Corporate Rules or "UK-BCR": the personal data protection policies set out in this document, including those referenced and listed in 10 APPENDIX 1: POLICIES, STANDARDS AND PROCEDURES;

Commissioner: Information Commissioner's Office (ICO); the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Controller: the natural or legal person, the department or any other organisation who determines the purposes and means of the processing of personal data;

Data Exporters: International SOS Group entities established in the UK having endorsed these Rules and transferring personal data to another International SOS Group entity, established in a Third Country;

Data Importers: International SOS Group entities established in a Third Country, having endorsed these Rules;

data subject: an identified or identifiable natural person to whom the UK personal data relates;

entity: a company belonging to the International SOS Group or an establishment of a company belonging to the International SOS Group or any other company in which the International SOS Group has a share of the registered capital regardless the amount of such share;

UK personal data: personal data which is processed by a Member and to which the UK GDPR applies;

UK GDPR: UK General Data Protection Regulation;

Inter Group Agreement (IGA): contract between a group of associated companies, such as the International SOS Group; the IGA binds UK Members to follow these Rules;

International SOS Group: group of companies operating under the International SOS trademark umbrella. The parent holding company is AEA International Holdings, Pte. Ltd ("AEA");

International SOS Group Privacy Notice: notice provided at www.internationalsos.com/privacy

(UK-BCR) Member: International SOS Group entity, signatory to the Inter Group Agreement ("IGA") which incorporates these Rules;

personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processor: any person or organisation who processes personal data on behalf of the Controller;

processing (of personal data): any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction of personal data;

Responsible Member (UK): International SOS Group entity established in the UK, to which the Group has delegated responsible for data protection and acceptance of ultimate liability for any breaches of these Rules by Members (see 1.4);

Special Category Data: personal data that is particularly sensitive and, as such, requires additional safeguards to ensure its protection. It includes details that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; is genetic data, is biometric data for the purposes of uniquely identifying a natural person, is concerning an individual's health, or is concerning an individual's sexual orientation or activity;

Third Countries: countries that have not been deemed to ensure an adequate level of data protection ("Third Countries") by the European Commission ("EC") prior to the UK's exit from the European Union (and upheld under the UK's own regime), or by UK adequacy regulations after the UK's exit from the European Union.;

Third Party: the natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data;

Third Party Beneficiary: a person who benefits from a contract that is made between two other parties. Data Subjects are Third Party Beneficiaries of the UK-BCR without being parties to the agreement.

(UK data) transfer: communicating, copying, moving or allowing access to personal data via a network (including remotely), or communicating, copying or moving these data from one media to another, to the extent that the data are subject to processing in the recipient country.

1.2 Scope

These Rules apply to all Members regardless of their location and competent jurisdiction. The Members, their locations and representatives are listed in 11.

These Rules apply to all personal data processing activities carried out by the Members where UK personal data is transferred by a Data Exporter acting as Controller in the UK, to a Data Importer acting as Controller or Processor and any further transfer to another Member or Third Party established in a Third Country.

A list of the processing activities concerned is provided in 10.

1.3 Endorsement, Duty to Comply and Prevailing Obligations

By endorsing these Rules via signature of the separate Inter Group Agreement (IGA), Members irrevocably agree to comply, and ensure that their employees comply, with these Rules.

The Members agree to take such measure as may be necessary to ensure that each of them will adjust its processing activities to meet the requirements of these Rules.

In the event these Rules are not complied with, data subjects shall have recourse to the Commissioner.

The provisions in these Rules are in addition to any other obligations relating to personal data under applicable data protection and privacy laws. Where such laws provide a higher protection for data subjects, they will prevail over these Rules.

1.4 Member with Delegated Responsibility ("Responsible Member (UK)")

1.4.1 To the extent that the International SOS Group's parent company AEA International Holdings, Pte. Ltd. ("AEA") is incorporated in Singapore, thus established outside the UK, responsibility for data protection is accepted by **International SOS (Assistance) UK** ("Responsible Member (UK)").

1.4.2 Further details about how the governance structure implemented by AEA supports the Responsible Member (UK) in carrying out its duties and the nature and extend of liability and indemnification are provided in 5 GOVERNANCE, 6 LIABILITY and the IGA.

1.4.3 The Responsible Member (UK) shall ensure

- the proper implementation of the Rules;
- monitoring and enforcing compliance of each Member (5.2 Monitoring Compliance and 7 SANCTIONS) and management of any breaches in accordance with the applicable International SOS Policies and Procedure;
- review of the Rules at least annually, keeping them updated, and communicate updates to the Members and the Commissioner (5.3);

- that it provides general information on any requests to share personal data received from law enforcement or other state security bodies to the Commissioner (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.) where it was prohibited to notify the Commissioner of such requests at the time;
- that transfers of personal data to any public authority are limited and proportionate and never indiscriminate;
- that the Rules, or a public version of the Rules, are easily accessible to the data subjects whose personal data are processed by Members by publishing them alongside the International SOS Group Privacy Notice.

1.4.4 A Data Protection Officer (DPO), Europe (11.3.2), shall be appointed by AEA in accordance with UK GDPR Art.37 to represent the Responsible Member (UK) and with responsibility to monitor compliance with the Rules.

1.4.5 The Responsible Member (UK) shall be the prime contact for other Members and the Commissioner in relation to the UK-BCR.

1.4.6 If the legislation of a Third Country would prevent a Member from fulfilling its obligations under these Rules and the IGA, the Responsible Member (UK) shall undertake a risk assessment considering the nature and context of the processing, as well as the categories of data subjects and personal data processed and provide recommendations accordingly. If the risk cannot be reduced to an acceptable level, the Responsible Member (UK) shall notify the Commissioner.

1.4.7 Should a Member receive a request to disclose UK personal data from a law enforcement agency or other state security bodies, they should immediately inform the Data Exporter and the Responsible Member (UK). The Responsible Member (UK) should notify the Commissioner and, where applicable, the Controller about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure. Should such a notification be prohibited by law, to preserve the confidentiality of an investigation, the Responsible Member (UK) or the applicable Member, in concert with the International SOS Chief Data Protection Officer and Privacy Team, shall use their best efforts to obtain the right to waive this prohibition, fully or partially, so as to be able to share as much information as possible with the Commissioner and if requested by the Commissioner, provide information to demonstrate what actions it has taken under this section (unless this would also be prohibited by law).

2 UNDERTAKINGS

2.1 Undertakings Given by All Members

2.1.1 **Data Protection Policy**

All Members shall process personal data only in accordance with International SOS Group Policies, adopted Standards and Procedures listed in 8. In particular, they must adhere to the principles and meet the obligations set out in the International SOS Data Protection Policy:

- Accountability
- Purpose Limitation

- Lawfulness, Transparency and Fairness
- Data Minimisation and Accuracy
- Retention and Destruction
- Security
- Data Subject Rights
- Challenging Compliance and Complaints
- "Data Protection by Design and Default" – Data Protection Impact Assessments.

2.1.2 **Accountable Manager**

Each Member shall appoint an individual, usually the General Manager, in charge of ensuring adherence with these Rules, and a Data Protection Expert, supporting the administrative aspects of monitoring compliance, and communicate this information to the Responsible Member (UK).

In countries where the law requires the appointment of a Data Protection Officer with specific responsibilities, the Accountable Manager shall appoint a suitable person to the role in concert with the Chief Data Protection Officer and Privacy Team.

2.1.3 **Security**

Members shall implement appropriate technical and organisational measures, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised parties. This shall include the conclusion of contracts between Data Exporters and Importers that include International SOS standard Information Security clauses and, where the Importer acts as Data Processor, Data Processing Agreement. Members shall implement such measures in compliance with the International SOS Data Protection Policy, Information Security Policy, Contracts Policy, Data Retention, Archiving and Destruction Policy and any other applicable Group Policies.

2.1.4 **Data Breaches**

Members shall notify all personal data breaches without undue delay in accordance with the International SOS Data Breach Contingency Plan to ensure timely risk assessment by the responsible legal team and notification to the Commissioner and the data subject(s) where required. Records stating basic facts about personal data breaches, associated risk assessments and mitigating and remedial actions taken shall be maintained in the International SOS incident reporting system and made available to the Commissioner if requested.

2.1.5 **Data Subject Complaints, Claims and Requests**

The Member receiving any data subject complaint or claim is in principle responsible for handling any communication with the data subject unless in a specific case the affected Member and the responsible Data Protection Officer or the Privacy Team agree otherwise.

Data subject rights requests are managed by the Privacy Team in accordance with the Data Subject Rights Requests Procedure. Members shall direct such requests in accordance with the procedure and, where required, support the fulfilment in a timely and proactive manner.

2.1.6 Records of Processing

Members shall at all times maintain complete and accurate records of their personal data processing activities within the processing register provided by the International SOS Group. Such records must include the following information:

- the name of the Member and of the employee tasked with overseeing the processing activity and who is responsible to keep the record updated,
- the name and contact details of the responsible data protection officer;
- the categories of data subjects and of types of personal data concerned;
- the purposes of the processing;
- the data retention limits;
- a general description of the technical and organisational security measures implemented.
- the categories of recipients to whom the personal data is transferred or who have access to the personal data;
- description of the data asset(s) used to receive, store, transfer and otherwise process the personal data
- identification of any vendor(s) undertaking part or all of the personal data processing on behalf of the Member, the Third-Party risk assessments completed in relation to the processing and the agreements entered into with such vendors;
- identification of all countries that the personal data may be transferred to and what safeguards have been implemented.

2.1.7 Data Protection Impact Assessment

Members shall undertake Data Protection Impact Assessments in relation to any new “High Risk” personal data processing they intend to implement or when an intended change to an existing processing activity, may lead to a high risk to data subjects’ rights and freedoms.

Transfers of UK personal data to Third Countries shall automatically trigger a Data Protection Impact Assessment.

Members shall develop treatment plans and carry out actions to address any risks identified in the process, as well as undertaking annual reviews of the continued appropriateness and efficacy of the risk treatment.

2.1.8 Training and Awareness

Members shall ensure that their employees and processors that have permanent or regular access to personal data, are involved in the collection of personal data or in the development of tools used to process personal data, complete appropriate general and role-specific training and, at a minimum, the International SOS Group mandatory annual Compliance E-Learning.

Members shall inform their staff of the binding nature of the content of these Rules, of the means to comply by providing relevant procedures, and of the disciplinary measures that may be taken in case of failure to comply. This can be accomplished via the completion of the Compliance E-Learning which requires acknowledgement that the Data Protection Policy and UK-BCR have been read and consequences of non-adherence understood.

2.1.9 **Participation in Audits**

Members shall actively participate in the internal and external audits undertaken to ascertain compliance with these Rules in accordance with 5.2 Monitoring Compliance. They shall develop Non-Compliance Corrective Action (NCCA) plans in response to any findings, take action accordingly and confirm their effectiveness in addressing the non-conformities. The current status of NCCA shall be made available to the Responsible Member (UK), DPO, UK and Privacy Team on request.

2.1.10 **Mutual Cooperation**

Members shall co-operate and support each other to provide timely and comprehensive privacy notices to data subjects and to appropriately manage any request, complaint or claim from data subjects in accordance with 3 RIGHTS OF DATA SUBJECTS and 4 COMPLAINTS and any investigations or other actions by the Commissioner.

2.1.11 **Cooperation with the Commissioner**

Members shall co-operate with, provide their processing records to, and submit their personal data processing activities and risk assessments to audits on request from the Commissioner. They shall collaborate with the Responsible Member (UK), DPO, UK and Privacy Team to comply with advice received from the Commissioner in relation to the Rules.

2.1.12 **Regulatory Obligation Impacting Compliance / Requests for Disclosure**

If a Member considers that the legislation applicable to it would prevent it from complying with the Rules or the IGA or have a substantial adverse effect on the protections provided by these Rules or the IGA, the Member shall notify the Responsible Member (UK), DPO, UK and the Chief DPO, unless this would be prohibited by a law enforcement authority or state security body, for example where secrecy is required to preserve the confidentiality of a law enforcement investigation (a “secrecy requirement").

2.2 Undertakings Given by Members as Data Exporters

2.2.1 **Continuous Compliance with UK GDPR and UK-BCR**

The Data Exporters warrant that their processing, including the transfer itself, of the personal data has been, is and will continue to be carried out in compliance with the International SOS Data Protection Policy and these Rules, thus continuing to assure the adequate level of protection of rights and freedoms afforded to data subjects under the UK GDPR.

2.2.2 **Assessment of Third Country Regulations**

In particular, they shall transfer personal data to a Data Importer only if, having taken due account of the specific context of the transfer and intended processing, the laws to which the Data Importer is subject, and considering any supplemental safeguards to those specified in these Rules (including technical and organisational measures), they have deemed that the laws of the Third Country in which the Importer is established and/or processes the personal data do not prevent their compliance with the Rules.

2.2.3 **Informing Data Subjects of Transfers**

The Data Exporters shall ensure that data subjects are made aware of the transfer of their data to a Third Country, and of these Rules safeguarding such transfer, by way of providing a

privacy notice and/or linking to the International SOS Group Privacy Notice and including this information there.

2.3 Undertakings Given by Members as Data Importers

2.3.1 Absence of Regulatory Obligation Impacting Compliance

Data Importers warrant that at the time of their endorsement of these Rules, having taken due account of the specific context of the processing, the laws to which they are subject in the country in which they are established and/or process the personal data, and considering any supplemental safeguards to those specified in these Rules (including technical and organisational measures), they have no reason to believe that the applicable laws prevent them from fulfilling their obligations under the Rules.

2.3.2 Purpose Limitation

Data Importers undertake to process the personal data transferred in accordance with the intended purpose at the time of collection and consequently to process personal data only in a manner compatible with the purpose of the transfer.

2.3.3 Meeting Conditions for Further Transfers

Data Importers shall only process and transfer personal data to another Importer if the conditions set out in 2.2 are fulfilled.

Prior to any onward transfers to recipients that are not Members, Data Importers shall ensure that

- by way of the International SOS Group's third-party risk assessment process it has been ascertained that the recipient will have in place appropriate technical and organisational measures, equivalent to those provided by the Members;
- they conclude a contract with the recipient that include the standard International SOS Information Security clauses or equivalent, specifying the security measures taken by the entity to which the transfer is made;

2.3.4 Safeguarding Transfers to Third Countries

When a further transfer is made, so that processing of the personal data will take place in a Third Country, the Data Importer shall ensure that the personal data is adequately protected in accordance with Art. 45 of UK GDPR or where appropriate, implement appropriate safeguards with the recipient in accordance with UK GDPR Art. 46, such as Standard Contractual Clauses. Any exemption to this, applying one of the derogations set out in UK GDPR Art. 49, must be exceptional and ad hoc in nature and shall require prior approval on a case-by-case basis by the Responsible Member (UK).

2.4 Additional Undertakings Given by Members as Data Importers and Processors

2.4.1 Data Processing Agreements

Any sub-processing approved by the Data Exporter shall be carried out only in accordance with the standard terms provided in the International SOS Data Processing Agreement.

2.4.2 Conditions for Engaging Sub-Processors

The Data Importer acting as Processor may transfer the personal data to any sub-processor, on the condition that the Data Exporter has been informed and consents to this. The Data Exporter's consent to this sub-processing shall be recorded in the service agreement or Data Processing Agreement between the Data Exporter and Importer. The agreement shall specify that any sub-processor must be bound by an obligation to comply with these Rules. The Rules shall either be attached to or linked to in the agreement.

2.4.3 Change of Sub-Processors or Processing Locations

The Processor must inform the Data Exporter of any planned change involving the use of sub-Processors, prior to the transfer of personal data to any new sub-Processor and/or location. The Data Exporter may oppose the planned change and/or terminate the Service Agreement entered into with the Processor, in accordance with the provisions of the agreement.

3 RIGHTS OF DATA SUBJECTS

3.1.1 Accessibility of UK-BCR and Information about Transfers

The UK-BCR or a public version of the UK-BCR shall be published alongside the International SOS Group Privacy Notice so as to be easily accessible to data subjects.

The International SOS Group Privacy Notice shall include information about the purpose of any transfer of personal data to Third Countries, identity of the recipient(s), and the nature and location of the processing carried out by the recipient.

3.1.2 Enforcement and Recourse for Third Party Beneficiaries (Data Subjects)

As Third Party Beneficiaries, data subjects can enforce their rights in relation to any breaches of these Rules.

Specifically, data subjects have the right to:

- be informed, access their personal data, ask for rectification or erasure, restrict or object to processing and data portability.
- claim enforcement of

- Data Protection Principles as set out in the International SOS Data Protection Policy (2.1.1)
- the security and confidentiality obligation (2.1.3);
- the obligation for the Members to immediately inform the Responsible Member (UK) if the legislation applicable to it may prevent it from fulfilling its obligations under these Rules (2.1.7);
- Members' duty to cooperate with each other (2.1.5) and/or with the Commissioner (2.1.8);
- the Obligation not to make onward transfers outside the group without informing the data subjects and without entering into an appropriate agreement with the entity (2.2.3 and 2.3.4);
- accessibility of the UK-BCR (3.1.1)
- their right to complain (4)
- their right to seek other means of recourse and compensation (4.5)

- obtain, when they have suffered damage as a result of unlawful processing or any act incompatible with these Rules a correction of the actions or inactions that violated the Rules and, if appropriate, compensation for damage suffered.
- apply to the Commissioner and/or refer the matter to the competent courts, in accordance with 4.6 for all violations of these Rules and their rights as specified herein.

4 COMPLAINTS

4.1 Procedure

4.1.1 Data subjects may lodge a complaint about unlawful processing or an act relating to them that is incompatible with these Rules, by following the guidance provided in the International SOS Group Privacy Notice.

4.1.2 If a complaint is received by a Member through any other means, they shall acknowledge receipt of the complaint, follow their usual complaints procedure, and involve the responsible Data Protection Officer, Legal Team or Privacy Team to investigate and resolve any dispute within a reasonable timeframe as set out below.

4.1.3 If a complaint relates to a previously unidentified data breach or a breach of these Rules, it shall also be managed in accordance with the Data Breach Contingency Plan and applicable incident management procedures as described in 2.1.4.

4.2 Directing Complaints

4.2.1 Before any personal data is released to the complainant, their identity or their authorisation to act on the data subject's behalf must be confirmed.

4.2.2 All complaints shall be sent in a timely manner to the Member responsible for the processing in question, who shall be responsible for handling them in accordance with these Rules.

4.2.3 In the event that the data subject is unable to receive a satisfactory response from the Member because it is no longer an operating entity, ceased to legally exist or has become insolvent, without all of its obligations having been transferred by contract or by the effects of the law, to its legal successor, the entity in claim shall handle the data subject's claim or complaint in accordance with these Rules.

4.3 Timely Resolution of Complaints

4.3.1 Upon receipt of a complaint, and no later than within five business days, the data subject should receive an acknowledgement of receipt together with the following:

- the identity of the entity and/or employee in charge of handling the complaint;
- the approximate length of time required to handle the complaint, or an immediate answer, or a request for additional documents.

4.3.2 The data subject shall be kept informed of the progress of the review of the complaint.

4.3.3 Complaints should be fully addressed without undue delay and a response sent to the data subject within 30 calendar days of the date of receipt or from when the identity of the data subject has been verified. In some cases of greater complexity, this period may be extended by a further two months. The data subject shall be informed if an extension is required before the initial 30 days have elapsed.

4.3.4 At the end of the review, the data subject shall be informed:

- whether the complaint has been found to be justified or is dismissed;
- of the proposed solution and available remedies;
- of other means of recourse as described in 4.5 and 4.6.

4.4 Role and Autonomy of the Person in Charge of the Investigation

4.4.1 The designated individual is responsible for:

- managing complaints lodged by data subjects;
- where applicable, opening an investigation to gather and review the facts.

4.4.2 The individual designated to manage the complaint and find a solution to the dispute shall act with independence, neutrality and impartiality in the exercise of his or her mission. They must help the data subject and the Member concerned to find a solution.

4.5 Other Means of Recourse

4.5.1 If a data subject is not satisfied with the manner in which their request, complaint or claim has been processed or if no answer is given within the time limits stated, they may contact the DPO, UK at dpo.europe@internationalsos.com or Chief DPO at dpo@internationalsos.com.

4.5.2 The data subject may also raise the issue before the Commissioner or bring a claim before a competent court as set out in 4.6.

4.6 Competent Jurisdiction

4.6.1 If no amicable settlement can be found between the data subject and the entity concerned pursuant to the internal complaint process described in 4, the data subject may refer the matter to a competent UK court in order to obtain a judicial remedy, the right to redress or, where appropriate, compensation for the damage suffered as a result of a violation of the Rules.

5 GOVERNANCE

5.1 Governance Structure

5.1.1 The International SOS Data Protection Policy provides detailed information in section "5. GOVERNANCE: AUDIT, MANAGEMENT REVIEW AND CONTINUOUS IMPROVEMENT".

5.1.2 The AEA Executive Committee shall appoint a DPO, UK (in accordance with UK-GDPR Art. 38-3) to represent the Responsible Member (UK) and ensure that they are sufficiently resourced and supported to carry out their duties. Details of the DPO, UK are available at 11.3.2.

5.1.3 The DPO, UK advises the AEA Executive Committee via the Chief DPO, who is also the Group General Counsel and member of the AEA Executive Committee (11.3.1).

5.1.4 In accordance with UK-GDPR Art.39, and specifically in relation to these Rules, the DPO, UK is responsible to

- maintain accuracy and completeness of the UK-BCR, keeping records of the modifications of the Rules and up to date list of Members;
- stay up to date with any changes or additions to the
- deal with audit requests from the Commissioner or any competent Authority;
- monitor and report to the AEA Executive Committee on compliance with the UK-BCR, with support from the Privacy Team and leveraging the International SOS internal audit program (5.2);
- ascertain any new Members ability to comply with these Rules through independent audit and/or data protection risk assessment in relation to their personal data processing activities (5.3.7)

5.1.5 The International SOS Privacy Team shall be responsible to

- ensure that the compliance obligations under these Rules are communicated for the organisation at board level and to stakeholders in all business lines and functions;
- escalate residual privacy and data protection related risks to the AEA Risk Management Committee;
- work closely with Information Security, Security, legal teams and the DPO, UK to respond effectively to data breaches and meet regulatory notification requirements;

- ensure adherence to these Rules during procurement process and/or product development process including information security review, privacy impact assessment, legal review.
- hold Members accountable for maintenance of Data Asset and personal data Processing Inventory records;
- respond to data subject rights requests;
- advise on responses to complaints from data subjects;
- support Members with the development of compliance measures / remedial action plans;
- enforce the requirement for and support Members with Data Protection Impact Assessments.

5.1.6 Compliance with training requirements shall be monitored by local HR teams and regularly reported to the responsible General Manager by the local Data Protection Expert or DPO (where appointed).

5.1.7 Complaints and data breaches shall be dealt with by the persons nominated for such tasks by each Member in accordance with the relevant procedures. When such incidents are escalated to the responsible legal team, they may involve the DPO, UK and/or Privacy Team if required to resolve a dispute, substantiate applicability or liability in the context of these Rules and provide advice on notification obligations.

5.2 Monitoring Compliance

5.2.1 The International SOS Group shall conduct internal and/or external audits at least annually, covering all requirements of these Rules and processing carried out by Members, as well as any additional ad-hoc audits and risk assessments as specified and requested by the DPO, UK and Responsible Member (UK).

5.2.2 The International SOS Group may adopt a standard providing controls gleaned from the provisions of the GDPR and undertake to maintain independent certification to such a standard. Such certificate should be made available to the data subjects alongside these Rules.

5.2.3 The scope and frequency of the audits shall take into consideration the risks to personal data processes and activities and previous audit performance, in accordance with the International SOS Internal Audit Policy, ensuring that:

- audit scope includes all compliance obligations and relevant activities of Members in accordance with these Rules;
- audits are carried out by appropriately trained, competent auditors;
- impartiality of auditors is ensured;
- audit reports detail any significant deviation from requirements of the requirements set out in these Rules.

5.2.4 Audit reports shall be shared following the conclusion of each audit to the Privacy Team, Member's top management and Group Executive Committee. Each audit report shall include actions related to the specific observations and recommendations. The AEA Executive Committee member responsible for the audited business line or function is responsible for ensuring that recommended actions be addressed and for reporting to the AEA Risk

Management Committee as to the open remedial actions. with International SOS Internal Audit Policy

5.2.5 Management reviews attended by each Member's top management shall be performed at appropriate planned intervals, annually as a minimum, to review compliance with these Rules.

5.2.6 The management review shall include the following topics:

- status of previous management review action plans;
- results of internal and external audits;
- customer satisfaction and feedback from interested parties including complaints;
- incidents, breaches, nonconformities and associated corrective actions;
- the effectiveness of actions taken to address the Data Protection Impact Assessment; monitoring and surveillance results;
- performance of suppliers and service providers;
- any change related to the Data Protection Impact Assessment;
- any changes of the Rules.

5.2.7 Members shall determine opportunities for improvement and implement necessary actions to meet their compliance obligations in relation to these Rules.

5.2.8 When a non-compliance is identified, the Member shall:

- take action to address the immediate issue;
- evaluate actions through the identification of a root cause of a nonconformity to prevent recurrence elsewhere;
- implement the action plan, verify that the corrections have been effectively implemented.

5.2.9 Members shall retain documented information as evidence of the nature of the nonconformities and the related corrective actions.

5.2.10 Members will provide copies of the result of any audit to the Commissioner and will agree to audits by the Commissioner in accordance with the UK GDPR and Data Protection Act.

5.3 Changes to the Rules

5.3.1 Changes in regulations, guidance from the Commissioner or the company structure may necessitate an update of the Rules.

5.3.2 The content of the UK-BCR may be modified by AEA, with the support of the DPO, UK and Legal Manager Europe acting in concert with the Privacy Team.

5.3.3 The modified text of the Rules shall be shared with all Members and made available to data subjects without undue delay.

5.3.4 Any changes to the Rules should be reported at least annually to the Commissioner with a brief summary of changes and the reasons for the update.

5.3.5 The DPO, UK shall be responsible for keeping records of the modifications of the Rules and up to date list of Members on a reliable and durable medium.

5.3.6 **Updating the Rules Without Requiring New Approval**

Modification of the Rules should not affect the level of the protection offered or significantly affect them in other ways such as changing their binding character. Should such substantial change nevertheless be deemed necessary, it must be promptly communicated to the relevant data protection authorities via the lead authority who may decide that re-approval of the UK-BCR has to be sought.

5.3.7 **New Members**

Any UK data transfer to a new Member will require the implementation of another legal instrument in accordance with UK GDPR Article 47 to safeguard personal data until the Member is effectively bound by the Rules and the Responsible Member (UK) and DPO, UK has ascertained their ability to comply through independent audit and/or data protection risk assessment in relation to their personal data processing activities.

6 LIABILITY

6.1.1 The Responsible Member (UK) shall be ultimately liable for any breaches of these Rules by a Member. AEA shall indemnify the Responsible Member (UK) for any cost incurred (an indemnity clause is included in the IGA accordingly).

6.1.2 AEA shall take necessary action to adequately support the Responsible Member (UK) to remedy any breaches of the Rules and pay compensation to data subject(s) for any material or non-material damages resulting from such violations.

6.1.3 AEA shall ensure that sufficient resources are available to cover the payment of compensation for breaches of these Rules.

6.1.4 If the Responsible Member (UK) can prove that a Member is not responsible for the act resulting in the damage claimed by the data subject(s), they may discharge themselves from any responsibility.

6.1.5 The Responsible Member (UK) accepts that a data subject may bring a complaint against it, to enforce their rights, before the Commissioner or before a competent UK court. While it is not required, data subjects are encouraged first to report their concerns directly to a Member rather than the Commissioner or a UK court.

7 SANCTIONS

7.1.1 Sanctions may be taken by AEA in the event of:

- breach of the provisions of these Rules;
- non-compliance with the recommendations and advice made after an audit;
- breach of the duty of co-operation with the relevant data protection authorities.

7.1.2 In accordance with the applicable employment legislation, internal corporate rules and employment agreements, sanctions may consist of disciplinary measures taken against the employees who breach the law in processing personal data or who breach these Rules.

7.1.3 Furthermore, these sanctions may be accompanied by other measures, if ordered by the competent independent administrative or judicial local authorities.

8 APPENDIX 1: POLICIES, STANDARDS AND PROCEDURES

The International SOS Group has implemented Policies and Procedures and adopted Standards to establish a Management System that ensures Members' compliance with these Rules. The below list is not exhaustive, and Members and their staff shall comply with all relevant Policies and Procedures unless a well-founded exception request has been duly approved by the Responsible Member (UK) in concert with the Group Heads of Compliance and Security and the Information Security Management Committee (as appropriate).

8.1.1	Data Protection Policy	**Public**
8.1.2	Data Retention, Archiving and Destruction Policy	**Public**
8.1.3	Information Security Policy	**Public**
8.1.4	Code of Conduct and Ethics	**Public**
8.1.5	Group General Affairs Policies and Procedures	Internal
8.1.6	Contracts Policy	Internal
8.1.7	Internal Audit Policy	Internal
8.1.8	Call Recording Policy	Internal
8.1.9	Access Control Policy	Internal
8.1.10	Bureau Veritas Data Protection Technical Standard	**Public**
8.1.11	Data Subject Rights Requests Procedure	Internal
8.1.12	Incident Reporting and Management	Internal
8.1.13	Security Procedure	Internal
8.1.14	Information Security Reporting Procedures	Internal
8.1.15	Data Breach Contingency Plan	Internal
8.1.16	Data Protection Impact Assessment (DPIA) Procedure	Internal
8.1.17	Data Protection Rules for Application Design	Internal
8.1.18	Legal and Regulatory Requirements Procedures	Internal
8.1.19	Guidelines for Obtaining Consent to Share Personal and Medical Information	Internal
8.1.20	Audit or Investigation Request Response Process and Procedure	Internal
8.1.21	IT Demand Management Process and Procure to Pay Procedures	Internal
8.1.22	Data Breach Assessment Tools	Internal

9 APPENDIX 2: PROCESSING ACTIVITIES

A comprehensive record of all processing activities carried out by Members shall be maintained in the Processing Register provided by the International SOS Group and made available to the data subjects concerned via the International SOS Group Privacy Notice and additional privacy notices provided to International SOS employees.

9.1 Medical and Security Assistance Service Delivery

Purpose	cross-border delivery of medical and security advisory and assistance services and client reporting
Data Subjects	Employees of subscribing organisations and individuals; International SOS employees; Healthcare and other professionals and consultants supporting the delivery of the services
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☐ Identification or access data (e.g. username, password, customer number) ☑ Data relating to financial information (e.g. income, credit card, bank details) ☑ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☑ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☑ Racial or ethnic origin ☐ Political Views ☑ Philosophical or religious opinions ☐ Union membership ☑ Sexual orientation ☑ Health data ☐ Biometric data ☐ Genetic data
Processing	capture, access, use, update, storage, transfer, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

9.2 Global Assistance Network Management

Purpose	managing a network of credentialled medical, security and logistics providers
Data Subjects	Individual providers and representatives or employees of providers
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☐ Identification or access data (e.g. username, password, customer number) ☑ Data relating to financial information (e.g. income, credit card, bank details)

	☑ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)
	☑ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin
	☐ Political Views
	☑ Philosophical or religious opinions
	☐ Union membership
	☐ Sexual orientation
	☐ Health data
	☐ Biometric data
	☐ Genetic data
Processing	capture, access, use, update, storage, transfer, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam

9.3 Medical Services

Purpose	provision or administration of clinical services including occupational health assessments
Data Subjects	Employees of subscribing organisations, including International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age)
	☑ Contact details
	☑ Identification or access data (e.g. username, password, customer number)
	☐ Data relating to financial information (e.g. income, credit card, bank details)
	☑ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)
	☐ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☑ Racial or ethnic origin
	☐ Political Views
	☐ Philosophical or religious opinions
	☐ Union membership
	☑ Sexual orientation
	☑ Health data
	☐ Biometric data
	☐ Genetic data
Processing	capture, access, use, transfer, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New

	Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Congo, Republic of Korea, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United States, Venezuela, Vietnam.

9.4 IT Service Desk and User Support

Purpose	Global IT User Support
Data Subjects	International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☑ Identification or access data (e.g. username, password, customer number) ☐ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐ Union membership ☐ Sexual orientation ☐ Health data ☐ Biometric data ☐ Genetic data
Processing	capture, access, use, deletion
Third Countries	India, Malaysia, United States

9.5 IT Application Support

Purpose	development and administrative support for a range of internally and externally facing IT applications
Data Subjects	International SOS employees; representatives of client and prospective client organisations; individual providers and representatives or employees of providers
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☑ Identification or access data (e.g. username, password, customer number) ☑ Data relating to financial information (e.g. income, credit card, bank details) ☑ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☑ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☑ Data relating to offenses, convictions, security measures
Special Category Personal Data	☑ Racial or ethnic origin ☐ Political Views

	☐ Philosophical or religious opinions
	☑ Union membership
	☑ Sexual orientation
	☑ Health data
	☐ Biometric data
	☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam

9.6 Business Travel Booking

Purpose	business travel management
Data Subjects	International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age)
	☑ Contact details
	☑ Identification or access data (e.g. username, password, customer number)
	☑ Data relating to financial information (e.g. income, credit card, bank details)
	☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)
	☑ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin
	☐ Political Views
	☐ Philosophical or religious opinions
	☐ Union membership
	☐ Sexual orientation
	☐ Health data
	☐ Biometric data
	☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam

9.7 Employee Travel Risk Management

Purpose	travel risk management in relation to employees
Data Subjects	International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☑ Identification or access data (e.g. username, password, customer number) ☐ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐ Union membership ☐ Sexual orientation ☐ Health data ☐ Biometric data ☐ Genetic data
Processing	capture, access, use, update, storage, deletion
Third Countries	Australia, China, Hong Kong, India, Indonesia, Malaysia, Philippines, Russia, Singapore, South Africa, Taiwan, Thailand, United Arab Emirates, United States, Vietnam.

9.8 Assistance App

Purpose	allowing users to share their location, receive automated alerts and access advice and assistance services
Data Subjects	Employees of subscribing organisations, including International SOS employees and individual users
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☑ Contact details ☑ Identification or access data (e.g. username, password, customer number) ☐ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐ Union membership ☐ Sexual orientation ☐ Health data ☐ Biometric data

	☐ Genetic data
Processing	access, use, update, storage, transfer, deletion
Third Countries	Australia, China, Hong Kong, India, Indonesia, Malaysia, Philippines, Russia, Singapore, South Africa, Taiwan, Thailand, United Arab Emirates, United States, Vietnam.

9.9 Enterprise Resource Management

Purpose	internal and external recruitment; compensation, benefits and reimbursements; human resources administration and management; career development
Data Subjects	internal and external candidates / applicants; International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age)
	☑ Contact details
	☑ Identification or access data (e.g. username, password, customer number)
	☑ Data relating to financial information (e.g. income, credit card, bank details)
	☑ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)
	☑ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin
	☐ Political Views
	☐ Philosophical or religious opinions
	☑ Union membership
	☐ Sexual orientation
	☑ Health data
	☐ Biometric data
	☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

9.10 Sales

Purpose	statistical analysis on client's database; management of prospects' contacts; general customer relationship management; creation/deletion of client's general and financial information.
Data Subjects	representatives of client and prospective client organisations
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age)
	☑ Contact details
	☐ Identification or access data (e.g. username, password, customer number)
	☐ Data relating to financial information (e.g. income, credit card, bank details)
	☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)

	☐ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin
	☐ Political Views
	☐ Philosophical or religious opinions
	☐ Union membership
	☐ Sexual orientation
	☐ Health data
	☐ Biometric data
	☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

9.11 Marketing

Purpose	business-to-business marketing of products and services.
Data Subjects	representatives of client and prospective client organisations
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age)
	☑ Contact details
	☑ Identification or access data (e.g. username, password, customer number)
	☐ Data relating to financial information (e.g. income, credit card, bank details)
	☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code)
	☐ Official documents (Passports, identity documents, etc.)
	☑ Location data (incl. IP Address)
	☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin
	☐ Political Views
	☐ Philosophical or religious opinions
	☐ Union membership
	☐ Sexual orientation
	☐ Health data
	☐ Biometric data
	☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian

	Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

9.12 Claims and Accounting

Purpose	Processing of claims and settlement of invoices.
Data Subjects	Individual providers and representatives or employees of providers; representatives and employees of subscribing organisations; International SOS employees; individual beneficiaries of services.
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☐ Contact details ☐ Identification or access data (e.g. username, password, customer number) ☑ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐☑ Union membership ☐ Sexual orientation ☐ Health data ☐ Biometric data ☐ Genetic data
Processing	capture, access, use, update, storage, transfer, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam

9.13 Billing

Purpose	Invoicing for services rendered
Data Subjects	Employees of subscribing organisations, including International SOS employees and individual users
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☐ Contact details ☐ Identification or access data (e.g. username, password, customer number) ☐ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures

Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐ Union membership ☐ Sexual orientation ☑ Health data ☐ Biometric data ☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

9.14 Reporting and Analysis

Purpose	Understand performance and improve business processes. Forecasting and budget planning.
Data Subjects	Employees of subscribing organisations and individuals; International SOS employees
Personal Data	☑ Civil status (e.g. name, gender, date of birth, age) ☐ Contact details ☑ Identification or access data (e.g. username, password, customer number) ☑ Data relating to financial information (e.g. income, credit card, bank details) ☐ Government Identifier (e.g. Social Security or Civil Reg. Number, Tax Code) ☐ Official documents (Passports, identity documents, etc.) ☑ Location data (incl. IP Address) ☐ Data relating to offenses, convictions, security measures
Special Category Personal Data	☐ Racial or ethnic origin ☐ Political Views ☐ Philosophical or religious opinions ☐ Union membership ☐ Sexual orientation ☐ Health data ☐ Biometric data ☐ Genetic data
Processing	access, use, update, storage, deletion
Third Countries	Afghanistan, Algeria, Angola, Australia, Azerbaijan, Bahrain, Brazil, British Virgin Islands, Cambodia, Cameroon, Chad, China, Colombia, Equatorial Guinea, Fiji, Gabon, Ghana, Guinea, Guyana, Hong Kong, India, Indonesia, Iraq, Kazakhstan, Kenya, Lesotho, Madagascar, Malaysia, Mali, Mauritania, Mauritius, Mexico, Mongolia, Mozambique, Myanmar, Namibia, Nauru, Niger, Nigeria, Papua New Guinea, Peru, Philippines, Puerto Rico, Qatar, Republic of Korea, Republic of the Congo, Russian Federation, Senegal, Singapore, South Africa, Sultanate of Oman, Suriname, Taiwan, Thailand, Turkey, Uganda, United Arab Emirates, United Republic of Tanzania, United States, Venezuela, Vietnam.

10 APPENDIX 3: MEMBERS (AND THEIR REPRESENTATIVES)

10.1 Company Structure

International SOS is the worldwide registered trademark for the diverse group of companies operating under the International SOS trademark umbrella. The parent holding company is **AEA International Holdings, Pte. Ltd.** (331 north Bridge Road, 17-00 Odeon Towers, 188720 Singapore) which is incorporated in Singapore and operates under Singapore law.

AEA International Holdings Pte. Ltd. has subsidiary companies around the globe. These operating companies provide medical assistance, security, evacuation, travel and consulting services. In order to comply with applicable local laws, these services are provided through many locally incorporated subsidiary companies and subcontracted affiliates and partners, including hospitals and clinics, serving the needs of International SOS customers in 90 countries.

10.2 Responsible Member (UK)

International SOS Assistance UK Limited
Chiswick Park (Building 4), 566 Chiswick High Road, London, W4 5YE, United Kingdom
Company number 01908770

10.3 Data Protection Officers

10.3.1	Group Chief Data Protection Officer	Greg Tanner, dpo@internationalsos.com (AEA International Holdings Pte. Ltd., Singapore)
10.3.2	Data Protection Officer, Europe	Katrin Maeurich, dpo.europe@internationalsos.com (International SOS Assistance UK Limited)

10.4 Exporters

Legal Entity	Country	Representative
To obtain details of a specific legal entity, please email dpo@internationalsos.com	United Kingdom	To obtain details of representative for a legal entity and how to contact them, please email dpo@internationalsos.com

10.5 Importers

Legal Entity	Country	Representative
To obtain details of a specific legal entity, please email dpo@internationalsos.com	Afghanistan Algeria Angola	To obtain details of representative for a legal entity and how to contact them please email dpo@internationalsos.com

Australia

Azerbaijan

Bahrain

Brazil

Cambodia

Canada

China

Equatorial Guinea

Ghana

Hong Kong

India

Indonesia

Iraq

Japan

Kazakhstan

Korea

Malaysia

Mauritius

Mongolia

Mozambique

Myanmar

New Zealand

Nigeria

Peru

Philippines

Qatar

Russian Federation

Singapore

South Africa

Switzerland

Taiwan

Thailand

United Arab Emirates

United States