INTERNATIONAL SOS GDPR COMPLIANCE

**this is a redacted version of the GDPR Narrative for publication. To receive the full version, please get in touch with your International SOS point of contact.*

1. COMPLIANCE REQUIREMENTS

1.1. Data Protection Officer (DPO)

DPO (Group): Greg Tanner (Singapore); dpo@internationalsos.com
DPO (Europe): Katrin Mäurich (UK); dpo.europe@internationalsos.com

1.2. Controller-Processor Responsibilities

When processing Personal Data in the context of providing our Traveller Tracking services, we regard ourselves as the Processor. All other services, with some minor exceptions, see us acting as the Controller. Where we are Processor, we provide a standard Data Processing Agreement as an addendum to our contract with clients. Please see 2 KEY SERVICES for detail on data collection and flow.

1.3. Data Processing Records

We maintain a Data Asset Register including records of Information Security and Privacy Impact Assessments, lawful bases for processing, and Data Flow Maps.

1.4. Conditions For Lawful Basis For Processing

We have established the lawful bases for all Personal Data processing activities and they have been documented as part of our processing records.
Consent procedures have been implemented where required and records of consent are maintained.

1.5. Privacy Policy & Notice

We provide a transparent and concise Privacy Notice and have published our Data Protection Policy, both at www.internationalsos.com/privacy. Our apps and other digital platforms provide a direct link to this information and we refer callers to our Assistance Centres to it in a pre-recorded message. During the provision of services, where International SOS act as Controller, notice of purpose is also provided at the time data is collected directly from the data subject.

1.6. Data Subject Rights

We have implemented a Data Subject Rights Procedure which allows Data Subjects to exercise their rights to access, rectify and delete their Personal Data in accordance with GDPR. We carry out identity checks to ensure that access to data is not provided to unauthorised persons acting as or on behalf of the Data Subject. If requested, we provide data in common, portable formats, such as .csv or .doc. Where we act as Processor of Personal Data on behalf of a client, we will contact the client for instructions if a request is received directly from a Data Subject.

1.7. Privacy and Data Protection Impact Assessments

Privacy by Design has been embedded in all change management processes and in particular for procurements activities. Privacy Impact Assessments are undertaken and where significant impact on the way we process Personal Data has been identified, there is a requirement to complete a comprehensive Data Protection Impact Assessment and put in place appropriate Technical and Organisational Measures (TOM) to address any risk to Privacy. Assessment outcomes must be signed off by our Data Protection Officers before a project can be approved.

1.8. Information Security

Our Information Security Management System (ISMS) is certified to ISO/IEC 27001 standard. We commission annual vulnerability assessment and penetration testing and independent assessment and attestation (SOC 2 Type II) of the design and effectiveness of the measures we have implemented to

protect data. A detailed description of these Technical and Organisational Measures (TOM) is available in our ISMS Narrative document and we will also share independent verification reports on request.

1.9. Breach Management

In addition to our Incident Management Procedures which ensure proper escalation and management of information security incidents, we have established a Data Breach Contingency Plan to deal with high risk data breaches. Governance is in place to ensure that all incidents are investigated and appropriate action plans are developed to address any risks identified and prevent recurrence.

1.10. Data Transfers

In the course of service delivery, we are required to transfer Personal Data worldwide, between International SOS companies, clients, members and third parties such as medical, security, technical and logistics providers. Where we transfer Personal Data from the EEA to another country which does not have adequacy status, we rely on Binding Corporate Rules (International SOS entities), Privacy Shield certification (US) or Standard Contractual Clauses (Rest of the World) for Third-Party Service Providers as appropriate.

1.11. Special Categories Of Data

We process Special Category Personal Data when providing Medical and Security Assistance, Occupational Health and other Medical Services. We do so based on contract or legitimate interest and if such information needs to be shared, we do so only with the Data Subject's explicit consent. We only collect as much information as is required to fulfil the request for assistance, for example health information when providing a medical referral and religious believes or sexual orientation when providing Travel Security advice.

1.12. Accountability

We have been commissioning third party audits against GDPR compliance criteria with internationally well-established Testing, Inspection and Certification Services Companies such as the British Standards Institute (BSI). Quality indicators have been defined in relation to our Information Security System and Privacy Programme and we audit these at a local level annually as part of our internal standards audits. Regular functional reporting on GDPR compliance levels and Information Security to board level informs our Information Security and Privacy Strategies.

1.13. Data Retention And Deletion

Our Data Retention, Archiving and Destruction Policy is published at www.internationalsos.com/privacy. Retention periods have been defined based on the purpose of processing. At the end of the defined period, Personal Data is destroyed, either by deletion of all data or by anonymisation of particular datasets. Where we act as Processor, clients may instruct us to destroy or return data sooner or later than our standard retention period.

2. KEY SERVICES

2.1. TravelTracker

International SOS acts as Processor.

Personal Data is received via data feed (GDS) from Travel Agencies or directly from client. The lawful basis has been determined by the Controller (the client). Personal Data is shared with subsidiary companies and sub-contractors who provide the same technical and organisational controls as International SOS to protect the security and confidentiality of the data. Such data transfers are lawful based on Binding Corporate Rules (International SOS entities), Privacy Shield certification (sub-processors in the US) and Standard Contractual Clauses (sub-processors based in the Rest of the World).

Our Online Support Teams have access to Personal Data in Singapore, Australia, UK, Spain, France, US, China and Japan. In addition, authorised International SOS employees can access Personal Data

(for crisis reporting) from our Assistance Centres in Australia, China, Czech Republic, France, Germany, Hong Kong, India, Indonesia, Japan, Malaysia , Philippines, Russia, Singapore, South Africa, South Korea, Spain, Switzerland, Taiwan, Thailand, United Arab Emirates, United Kingdom, United States and Vietnam.

Sub-processors can access Personal Data in the following countries[1]:

#		Location	Service(s)
1a	*	USA	Hosting; Data Aggregation/Transformation and Storage
1b	**	France	Hosting
2		India	Maintenance, Administration, Development and Support
3		USA	Administration and Support
4		USA	Administration and Support
5	***	UK	Data Aggregation/Transformation

*Aggregation/Transformation only for most EU clients (no hosting)
**Hosting only for EU clients or by individual agreement
***only used by small group of clients with technical restrictions

We retain the personal data only for as long as is necessary for the specified legal or contractual purposes. Requests from data subject who wish to exercise their legal rights are referred to the respective client who is the Controller.

2.2. Medical and Security Assistance

International SOS acts as Controller.

Personal Data is collected when data subject contacts one of our Assistance Centres by phone or email. The lawful basis for collecting and processing the Personal Data is legitimate interest and contract. Where we transfer sensitive data we rely on explicit consent (verbal or written depending on circumstance). We collect no more data than is required to fulfil the request for assistance. Personal Data is stored in our Case Management System, in our Assistance Centres, with the central hub hosted in a US Data Centre. Authorised personnel in our Assistance Centres have access to the Personal Data. Personal Data is shared with subsidiary companies and sub-contractors who provide the same technical and organisational controls as International SOS to protect the security and confidentiality of the data. In some cases Personal Data needs to be shared with third parties who may not provide the same safeguards; this will only be done with the express consent of the data subject. We retain the Personal Data only for as long as is necessary for specified legal or legitimate organisational purposes.

2.3. Occupational Health Services

International SOS acts as Controller.

Personal Data is received from the client via online portal submission and stored and processed in a Case Management System, hosted either at our Data Centre in the US or in France. Authorised personnel in our Paris and Johannesburg Assistance Centres have access to the personal data.

Occupational Health Providers are either third party service providers or International SOS owned clinics. Both are regularly assessed to ensure consistent standard of services. We have contracts in place with all 1st Choice Providers. Where we have contracts in place, we have data protection clauses as an addendum which include key principles for management and processes related to personal data. We assess. Where there is no contract, the Guarantee of Payment acts as T&Cs and includes data protection requirements for the case concerned. During our provider visits (provider evaluation which is

[1] Exceptions are made based on individual client requirements. Some EU clients do not use GDS so there is no processing in the USA. ETL Solutions (UK) is used for aggregation/transformation for a small number of clients due to technical restrictions on their side. Some non-EU clients prefer to use the French server and some EU clients' Personal Data is hosted on the US server based by agreement.

part of regular network quality assessments) one of the criteria checked are secure patient file storage – paper files must be locked with controlled access and servers need to be in the EU.

After an Occupational Health Assessment, the results are sent by the occupational health provider to International SOS as email attachment. Some providers use a secure internet site to upload the medical results. Where escalation is required, we send results to the client's Medical Director by email attachment. The Health Summary is available to employees via an online portal and can be sent to them via email attachment on request. We use TLS (Transport Layer Security) to encrypt our emails in transit.