APPENDIX 1: SUPPLIER INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

Purpose

SOS International has legal and contractual obligations on the matters of data protection and IT security. As a part of these obligations we are required to ensure that our suppliers that process personal data on behalf of SOS International implement appropriate technical and organisational security measures and act according to the instructions of SOS International.

The supplier shall thus comply with these Supplier Instructions for processing of Personal Data (hereafter "Instructions") to ensure that the processing of personal data on behalf of SOS International takes place in accordance with our obligations.

Scope

The provisions in the Instructions establish minimum requirements to the supplier to the extent that the supplier is acting as data processor on behalf of SOS International according to the agreement between the parties. In addition to meeting the requirements in the Instructions, the supplier shall comply with all applicable privacy and data protection laws. Should any differences exist between the provisions of the Instructions and applicable laws, the supplier shall adhere to the higher requirements.

The Instructions apply to all kinds of automatic data processing as well as manual filing systems and other forms of systematic manual processing of personal data.

The supplier shall ensure that its employees and sub-suppliers, including consultants, advisors, temporary employees, etc., are subject to similar requirements regarding processing of personal data on behalf of SOS International.

Definitions

'Data Subject' is defined as an individual whose Personal Data are being processed by the supplier.

'disclosure' or 'disclose' is defined as revealing or informing any third party of Personal Data.

'Personal Data' is defined as any information relating to an identified or identifiable individual, e.g. name, personal identification number, address and e-mail.

'processing' or 'process' is defined as any operations or set of operations which is performed upon Personal Data or sets of Personal Data. The definition includes collection, recording, organisation, storage, alteration, use, disclosure and deletion.

'Sensitive Data' is defined as Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life.

‘transfer’ is defined as handing over or giving any third party access to Personal Data.

Data Governance

The supplier shall have appropriate policies and procedures in place to ensure compliance with

- The requirements in these Instructions
- The contractual requirements between the supplier and SOS International
- Applicable privacy and data protection laws

The policies and procedures shall take into account the category of Personal Data in question (e.g. regular, Sensitive, etc.) as well as all the different systems where processing takes place. Furthermore, procedures shall be in place in the event of an incident (e.g. a hacker attack or security breach).

All employees (including temporary employees) and sub-suppliers shall be informed of and trained in these Instructions. Only trained employees and sub-suppliers shall have access to Personal Data processed on behalf of SOS International.

Principles

All Personal Data processed on behalf of SOS International shall be processed in accordance with these principles.

As a minimum SOS International expects our suppliers to:

- Exclusively process Personal Data in accordance with the agreement between the supplier and SOS International
- Exclusively process Personal Data for the purposes intended
- Never process more Personal Data than necessary to fulfil the obligations arising from the agreement between the supplier and SOS International
- Ensure, as far as possible, that the Personal Data processed is accurate and kept up to date. Misinformation and deficient information compose a significant risk for patients and travellers especially
- Follow general advise and rulings from relevant data protection authorities

Disclosure

The supplier shall only disclose Personal Data processed on behalf of SOS International on a need to know basis and only in accordance with the agreement between the supplier and SOS International.

Personal identification numbers shall only be disclosed if it is necessary for securing a precise identification of the Data Subject or if it is a demand from a public authority.

Transfers

Transfers of Personal Data processed on behalf of SOS International must be agreed upon in a signed agreement and transfers may only be made to the extent necessary to fulfil the purposes for which the Personal Data is being processed.

Rights of the Data Subject

As a minimum, SOS International expects our suppliers to:

- When collecting Personal Data, provide the Data Subject with information regarding the purposes of the collection and the identity of SOS International and the supplier
- Provide the Data Subject with access to Personal Data held by the supplier regarding the Data Subject. Access to Personal Data held by SOS International must be granted through our website - please refer any such request to our website
- Delete or rectify inaccurate or incomplete Personal Data when requested to do so by the Data Subject or SOS International

Processing Personal Data for Marketing Purposes

The supplier shall not process Personal Data on behalf of SOS International for marketing purposes unless it is agreed upon in a signed agreement.

Data Retention

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than necessary to fulfil the contractual requirements. Personal Data must subsequently be anonymised or deleted. Suppliers shall observe the applicable statutory record-keeping period unless another period is agreed with SOS International. All records containing Personal Data are affected by these requirements regardless of the medium used,

Statistics, Business Intelligence and Big Data

Processing of Personal Data on behalf of SOS International for statistical purposes is only allowed if agreed upon in a signed agreement. All Personal Data, which are processed for statistical purposes, shall not later be processed for any other purpose. The supplier shall always anonymise Personal Data as soon as possible and at the latest before publishing any outcome of the statistical processing.

Security measures

SOS International requires suppliers to implement appropriate technical and organisational security measures to protect Personal Data which are processed on behalf of SOS International against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the agreement between the supplier and SOS International. The following non-exhaustive list contains examples of the required measures:

Organisational measures:

- The supplier shall identify all information flows to ensure secure processing

- The supplier shall regularly modify the organisational measures in accordance with technical progress
- For each program and back-up containing Personal Data, procedures shall be in place, which outline the media, frequency and retention period
- For each IT-system and any manual filing system containing Personal Data there shall be an instruction stating which personnel is authorised to access which type of data
- Users shall be set up to access Personal Data on a need to know basis
- The supplier shall keep a log on all authorisations, transfers and other processing

Technical measures:

- The supplier shall ensure that no private hard- or software is used to process Personal Data
- The supplier shall have updated anti-virus programs installed on all workstations, computers, laptops, etc.
- When any IT component containing Personal Data is being returned or passed on to others, it shall be ensured that the Personal Data have been deleted
- The supplier shall have a firewall system in place
- The supplier's premises shall be protected by adequate alarm equipment for fire, water damage, intrusion, etc.
- Access to systems where processing takes place shall be protected with adequate password

Data Breach Notification

In the event of suspected or actual material incidents affecting the Personal Data processed on behalf of SOS International, including loss or unauthorised disclosure of Personal Data, the supplier shall inform SOS International without undue delay. Incidents concerning Sensitive Data such as a patient record or Personal Data on more than 20 individual Data Subjects are always regarded as material. The supplier shall provide SOS International with a data breach notification containing information regarding:

- The series of events which led to the data breach
- How many Data Subjects are or could be affected by the data breach
- The categories of Personal Data involved in the data breach (regular, sensitive etc.)
- Availability: Whether the Personal Data have been lost
- Integrity: Whether the Personal Data have been altered
- Confidentiality: Whether the breach has resulted in unauthorised disclosure of or access to Personal Data
- A remedy plan to prevent reoccurring data breaches

The data breach notification shall be sent to groupGRC@sos.eu

Contact Information:
If you have any questions in relation to these Instructions please contact SOS International at:

Compliance@sos.eu
SOS International a/s
Nitivej 6

2000 Frederiksberg
Denmark