MSH INTERNATIONAL
SIACI SAINT HONORE GROUP
Season
39 rue Mstislav Rostropovitch
75 815 Paris cedex 17
Tel: +33 (0)1 44 20 99 99



To the attention of the Legal Department,

**Your contact:** Dominique Ternet-Benard Dominique.ternetbenard@msh-intl.com

**RE: General Data Protection Regulation – Legal Act**

Dear Sir, dear Madam,

On 25 May 2018, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation or GDPR), repealing Directive 95/46/EC, entered into force.

In view of this, the Siaci Saint Honoré Group has launched a program to achieve compliance with the GDPR as stated in our Data Protection Policy (available on this page https://www.msh-intl.com/uploads/ckfinder/Politique_de_Protection_des_Donnees_S2H_EN.pdf) and requires its suppliers and partners to comply with the regulatory provisions on personal data protection.

In the event that, as part of our contractual relations, you should be obliged to process personal data, you will only do so on the basis of our instructions. Under the GDPR, we would be the “data controller” and your company would be the “data processor”.

For this purpose, you will find enclosed a Legal Act stating our respective commitments regarding GDPR. This legal act will govern all personal data processing under our contractual relations. It will be applicable from 25 May 2018 and will cover all the agreements between our two companies and replace all pre-existing contractual provisions on data protection in our agreements.

Please contact us for further information on the GDPR compliance of our contractual relations.

Thanking you in advance for your reply,
Yours faithfully,

Gabrielle Pétillon
Legal Director

*Attached:*

*-Legal act personal data protection*

# PERSONAL DATA PROTECTION

## I. DEFINITIONS

The terms used in this Document that are not defined in this document will have the meaning given to them in the Applicable Regulation.

"**Applicable Regulation**" means:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (known as the General Data Protection Regulation or "GDPR").
- any other local legislation or regulation applicable in respect of personal data protection.

"**Client**" means MSH International which is a party to a Contract with the Service Provider.

"**Contract**" means any signed contract between the Parties or business relationship, resulting in the Processing of Personal Data and for which MSHI is the Controller and the Service Provider is the Processor as defined in the Applicable Regulation. This document shall form an integral part of the Contract.

"**Document**" means the present document.

"**Parties**" means together the Client and the Service Provider.

"**Second-tier processor**" means any subcontractor recruited by the Service Provider to carry out any Processing of Personal Data in the context of the Contract.

"**Service Provider**" means the entity providing services to MSHI according to the Contract and which is a party to said Contract.

## II. GENERAL REMARKS

### II. 1 PURPOSE

The purpose of this Document is to determine the conditions applicable to any Processing of Personal Data to ensure that the Processing complies with the Applicable Regulation.

### II.2 ROLES

The Parties acknowledge that in the context of the performance of the Contract:

- The Client is the Controller and the terms "Client" and "Controller" may be used interchangeably in this Document.
- The Service Provider is the Processor and the terms "Service Provider" and "Processor" may be used interchangeably in this Document.

### II.3 MATERIAL SCOPE

The provisions of this Document shall apply whenever any Processing of Personal Data is carried out for the performance of the Contract. The Parties therefore undertake unreservedly to comply with said provisions and those laid down in the Applicable Regulation.

**II.4 TERRITORIAL SCOPE**

The provisions of this Document shall apply in the situations laid down in Article 3 of the GDPR. If the Service Provider is not based in the European Union but processes Personal Data related to people located in the European Union, the Service Provider undertakes to appoint a Representative based in the European Union.

**II.5 CONTRACTUAL DOCUMENTS**

This Document and the Contract form an indivisible whole, which prevails over any proposal and/or exchange of correspondence prior to its signature, and over any other stipulation set out in the documents exchanged between the Parties and in particular, over any General Conditions of Sale established by the Service Provider. Nonetheless, the Parties acknowledge that for particular Processing purposes, the organisational and technical measures taken to ensure the security of said Processing, as mentioned in the Document, may be supplemented with more specific instructions, provided to the Service Provider by the Client as the Processing proceeds.

In the case of any contradiction or discrepancy between the provisions contained in the body of the Contract or any other associated agreement and this Document, the provisions of this Document will apply, unless otherwise agreed by the Parties.

# III. DATA PROCESSING

The Service Provider undertakes only to carry out Processing on the Personal Data in the context of the performance of the Contract on the Client's instructions.

Each type of processing carried out must be described in written or electronic form. Each of the Parties must provide information on the following points, as applicable:

- subject of the Processing
- duration of the Processing:
- nature and purpose of the Processing:
- type of Personal Data.
- categories of Data Subjects.
- As far as possible, the time frames established for the erasure of Personal Data.
- the category of Recipients receiving Personal Data, including international Recipients, where this has been authorised by the Controller.
- Any international Transfers carried out by the Processor identifying the third country and, if applicable, documents attesting to the existence of appropriate guarantees in relation to said Transfers.
- the name and contact details of any Processor. The same information will be provided once the Parties have appointed a Representative.

- As far as possible, and unless it has already been provided in the Contract or any other agreement associated with it, a description of the technical and organisational measures taken to ensure the security of the Processing.

Should the Service Provider be required to carry out any operation that would diverge from or exceed the instructions given by the Controller, it undertakes to notify the latter of said change in writing, ten (10) days prior to its implementation. The Controller reserves the right to reject said change if it considers that it presents a risk for the Processing. If the change is accepted, the Parties will agree to amend the Contract, this Document or the description of the aforementioned Processing as required.

# IV. SECURITY OF PROCESSING

### IV.1 CONFIDENTIALITY

For each Processing operation carried out, the Service Provider and any second-tier Processor, as well as anyone authorised by it to process Personal Data, are bound by a duty of strict confidentiality and in particular, undertake to:

- Not disseminate in full or in part, any of the Personal Data entrusted to them to any Recipient, either private or public, without the express, prior consent of the Controller.
- Commit the necessary resources to ensure the confidentiality of any Processing carried out at a technical level.
- Carry out regular checks on any second-tier Processors and anyone authorised by it to process Personal Data to ensure compliance with said duty of confidentiality.

### IV.2 MEASURES TO ENSURE SECURITY OF PROCESSING

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

### IV.3 NOTIFICATION OF BREACHES AND RISKS OF BREACH

The Processor undertakes to notify the Controller as soon as possible after it becomes aware of any security breach resulting, either accidentally or unlawfully, in the destruction, loss, alteration, disclosure of or unauthorised access to the Personal Data (hereinafter, “the Breaches”).

It also undertakes to notify the Client of any vulnerability in its IT security system that might result in a Breach or a risk of a Breach.

The notification will be sent to the Data Protection Officer referred to in Article XI Contacts of this Document.

The notification of the Breach must contain the following information, as a minimum:

- A description of the nature of the Breach including, if possible, the categories and approximate number of Data Subjects affected by the Breach and the categories and approximate number of Personal Data records concerned, along with any information that might help to identify them;
- The name and contact details of the Data Protection Officer or other point of contact, from whom additional information may be obtained;
- A description of the probable consequences of the Breach;
- A description of the measures already taken or to be taken to remedy the Breach and, if applicable, measures to mitigate the negative consequences of said Breach.

The Processor undertakes to ensure that any second-tier Processors and any person authorised by it to process Personal Data in the context of the Contract are informed and apply the notification procedure described in this Article.

**IV.4 MANAGEMENT OF BREACHES AND RISKS OF BREACH**

In general terms, the Service Provider undertakes to cooperate actively with the Controller in managing Breaches and risks of Breaches of Personal Data.

Any Breach or risk of a Breach detected will be swiftly evaluated by the Service Provider and an appropriate mechanism implemented to identify the root cause of the Breach or risk of a Breach, with the aim of preventing or mitigating the effects of the Breach or the risk of a Breach.

Once a Breach or the risk of a Breach has been detected, the Service Provider will take all the necessary measures to prevent such incidents recurring in future.

The Service Provider shall keep the Client informed of its actions in respect of this Article on a regular basis.

For Breaches reported to the competent Supervisory Authority, the Parties undertake to consult with each other before issuing any public communications concerning said Breach.

The Processor undertakes to ensure that any second-tier Processors and any person authorised by it to process Personal Data in the context of the Contract are informed and apply the management procedure for Breaches and risks of Breaches described in this Article.

## V. RULES APPLICABLE TO TRANSFERS

In general terms, the Service Provider undertakes not to transfer Personal Data processed under the terms of the Contract outside the European Economic Area (EEA) to a third country or international organisation, unless the transfer has been specifically authorised in the instructions communicated by the Client.

If applicable, the Service Provider undertakes only to transfer Personal Data outside the EEA in accordance with the conditions set out below. It is stipulated that the following conditions relating to transfers shall also apply to subsequent transfers of Personal Data from the third country or International Organisation concerned to another third country or another International Organisation.

- The transfer is made outside the EEA to a country or International Organisation providing an adequate level of protection confirmed by a decision of the European Commission.

Or

- The transfer is made outside the EEA to a country or International Organisation subject to the provision of appropriate guarantees by the Processor, as listed in Article 46 of the GDPR and in particular:

  - The implementation of binding corporate rules;
  - The signature of standard Personal Data protection clauses adopted by the European Commission.

The Processor undertakes to ensure that any second-tier Processors and any person authorised by it to process Personal Data in the context of the Contract are informed and apply the rules relating to transfers described in this Article.

## VI. RESTITUTION

Once a service related to Processing is complete, the Processor undertakes, at the Controller's discretion and on its request, without delay, to:

- erase or return all Personal Data processed in respect of the Contract to the Controller. The data will be returned in a readable, usable format that meets the security standards for Processing described in this Document.

And to:

- destroy the Personal Data processed in the context of the Contract unless European Union law or the law of the member state concerned requires said Personal Data to be retained, in which case, the Processor shall inform the Controller promptly of its statutory obligation. Once the destruction of the Personal Data is complete, the Processor shall provide the Controller with a certificate of destruction of said data, without delay.

The Processor undertakes to ensure that any second-tier Processors and any person authorised by it to process Personal Data in the context of the Contract are informed and apply the rules relating to reversibility described in this Article.

## VII. AUDIT

The Controller reserves the right to audit the Processor and any second-tier Processors and any other person authorised by it to process Personal Data in the context of the Contract, to ensure that the latter are compliant with the provisions of this Document and the Applicable Regulation.

The Controller will appoint an independent auditor, which is not a competitor of the Processor and will be subject to a prior confidentiality agreement and must comply with the internal regulations of the entities being audited. The audit will be carried out during the working days and times of the entities being audited and may be carried out at any site where Personal Data are processed in the context of the Contract.

The Processor undertakes to cooperate actively with the auditor by making all resources and information necessary for it to carry out its duties available to it.

A copy of the audit report written by the auditor will be given to each Party and examined jointly by the Parties, who undertake to meet for this purpose.

Should the audit reveal the existence of failures to fulfil their obligations by the entities audited, the Controller may ask the entities concerned to implement corrective measures at their own expense, without delay.

The audit ordered by the Controller will be at its own expense, except in the event of a failure by the Processor to fulfil its obligations under this document or the Applicable Regulation being revealed in the audit report. In this case, the costs of the audit will be payable exclusively by the Processor.

The Processor undertakes to inform any second-tier Processors and any person authorised by it to process Personal Data in the context of the Contract about the rules applicable to the audit, and to audit the aforementioned entities based on the same scope as the audit ordered by the Client. The Processor will then send the reports for the audits it has undertaken to the Client.

## VIII. DUTY TO ASSIST AND COOPERATE

The Processor will help the Controller to fulfil its obligation to respond to requests from Data Subjects in exercising their rights, as outlined in Chapter III of the GDPR and in particular, requests relating to rights of access, rectification, erasure or objection to the Processing of Personal Data. If a Data Subject sends a request directly to the Processor, the latter undertakes to notify the Controller within three (3) days of receiving said request. The Processor undertakes not to respond directly to the request received unless it has been authorised to do so by the Controller.

The Processor undertakes to cooperate actively with the Controller by making all the necessary information available, so that it can demonstrate its compliance with the Applicable Regulation, notably in respect of the Supervisory Authority concerned.

The Processor undertakes to cooperate actively with the Client to carry out the impact assessment previously conducted, prior to any Processing likely to create a high risk for the rights and persons of the Data Subjects concerned by the Processing.

In general terms, the Parties undertake to cooperate in respect of any inspection and investigation conducted by the competent Supervisory Authority concerning any Processing carried out in relation to the performance of the Contract.

## IX. SUBCONTRACTING

Notwithstanding the provisions of the Contract in respect of subcontracting, in general terms, the Service Provider shall not recruit a second-tier Processor without the Client's express prior consent.

If necessary, the Service Provider shall only use the services of second-tier Processors that present adequate guarantees as to the implementation of appropriate technical and organisational measures, so that the Processing carried out in relation to the Contract and on behalf of the Client complies with this Document and the Applicable Regulation.

The Client reserves the right to object to the addition of any second-tier Processor, without having to state reasons for its objection.

If, in accordance with the conditions set out in this Article, the Service Provider recruits a second-tier Processor, said Service Provider will require it to meet the same obligations in respect of Personal Data protection as those set out in this Document, in a dedicated written agreement.

At the Client's request, the Service Provider shall provide a copy of the dedicated agreement by which the Service Provider's commitments in respect of this Document and its compliance with the Applicable Regulation are passed on to the second-tier Processor.

The Service Provider undertakes to audit its second-tier Processors at its own expense, at regular intervals, to ensure they are compliant with the Applicable Regulation and this Document, and in particular, with regard to the implementation of appropriate technical and organisational measures to ensure the security of the Processing. The Service Provider shall send the audit reports to the Client without delay, for it to use at its discretion.

The Service Provider shall retain sole responsibility for any failure by its second-tier Processors to comply with the Applicable Regulation and this Document.

## X. LIABILITY

Notwithstanding any clause to the contrary in the Contract, the Service Provider's liability in respect of the Client shall be unlimited in respect of the compensation due according to the terms of this Document.

Any failure to comply with this Document and the Applicable Regulation may result in the automatic termination of the Contract by the Client, without penalty.

Each of the Parties shall remain fully liable, as applicable, for the payment of any administrative fines and damages imposed on them by a Supervisory Authority or court.

If the Processor is not based in the EEA and appoints a Representative, the latter will deal with the payment of any administrative fines and damages imposed on them by a Supervisory Authority or court in the event of a failure to pay by the Service Provider.

The Service Provider undertakes to impose the obligation referred to above on its appointed Representative in a dedicated written agreement and to provide the Client with a copy of said agreement on request.

## XI. CONTACTS

The Client has appointed the following, in relation to the performance of this Document:

Data Protection Officer:

Ms Samanta Le Pont – Data Protection Officer

dpo@s2hgroup.com

39, rue Mstislav Rostropovitch 75815 PARIS France

Paris, May 25 of 2018,

Gabrielle Pétillon, Head, of Legal