GDPR-Compliant by May 25, 2018 – Are You Ready?

The European Union’s General Data Protection Regulation (GDPR or regulation) was adopted in 2016 and becomes effective May 25, 2018. This regulation is the EU’s attempt to provide better data security and privacy protection for EU citizens and to allow them greater control over their personal data.

This regulation will affect any association or organization that collects or processes personal data of an EU citizen, who is residing in the EU, regardless of the location of the association or where the personal data is stored. The full GDPR text may be viewed at: https://gdpr-info.eu.

“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier (e.g., email address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

An association that owns or manages personal data of EU citizens residing in the EU is defined by the GDPR as the Data Controller. A vendor that the Data Controller utilizes to process or store the Controller’s personal data is generally defined as a Data Processor.

Under the GDPR, Data Controllers are responsible for, and must be able to demonstrate compliance with the principles relating to the processing of personal data. Data Processors are responsible for implementing technical and organizational measures that allow Data Controllers to comply with the regulation.

According to the regulation, the Data Controller must select Data Processors who can provide “sufficient guarantees” that the GDPR requirements will be met. In addition, there must be a written contract between the parties that contains minimum criteria specified in the regulation.
Data Controllers and Data Processors are required to understand and follow the requirements of the regulation. In brief, the major requirements include:

- EU citizens residing in the EU ("EU citizens/residents") must consent to the storage and use their personal data. This requires the affirmative action by the individual to give consent. For example, pre-checked opt-outs are not compliant.

- Individuals who are EU citizens/residents and EU authorities must be notified within 72 hours of discovering a security breach impacting the personal data of such individuals.

- EU citizens/residents must be able to receive copies of their digital personal data when requested, as well as a description of where they are stored, their use, and the opportunity to correct them.

- EU citizens/residents have the right to have their personal data deleted and not used or shared.

- GDPR requires that organizations have data privacy controls and security built into products and systems. It is expected that this requires the use of commercial best practices for data security.

The maximum fine for infringements is the greater of 20 million Euros or 4 percent of the offender's worldwide turnover (sales) for the prior financial year.

An informative GDPR handbook prepared by White & Case can be viewed at: https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation
This draft is not to be taken as legal advice or suitable for use without review and guidance from a company or organization's legal counsel and other professional advisors.

DRAFT
Data Processing Addendum

This Data Processing Addendum, including Annex I attached hereto and made a part hereof (the "DPA") is executed between

Name/Address
("Client" or the "Controller")

and

Name/Address
("Processor").

Processor and Client are hereinafter referred to jointly as the "Parties" and each individually as a "Party."

Background:

Processor and Client have entered into this DPA further to the underlying Master Services Agreement dated ___________ (the "Agreement") relevant to Processor's provision of the Services. The Parties have agreed to enter into this DPA for purposes of compliance with applicable Data Protection Law.

The DPA shall form an integral part of the Agreement. References in this DPA to the Agreement are to the Agreement as amended by this DPA.

The DPA is effective as of ___________ (the "Effective Date").

Agreed Terms:

1. Definitions

The following definitions shall apply for this DPA:

"Data Protection Law" means the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and any European Union Member State data protection laws and regulations implementing or supplementing the GDPR applicable to Processor.

"Data processor" or "processor", "data controller" or "controller", "data subject", "personal data", "personal data breach", "processing" and "supervisory authority" shall have the meanings given to such terms in the GDPR. Personal data includes all personal data subject to Data Protection Law that Processor processes on behalf of Client in accordance with the Agreement.

"Services" means the services and other activities that Processor shall provide or carry out for Client as set forth in the Agreement and any Statement of Work.
“Subprocessor” means another processor engaged by Processor to process personal data on behalf of Client in accordance with Client’s instructions.

2. Scope and operation

2.1 This DPA applies to Processor’s processing of personal data that is subject to Data Protection Law in providing Services to Client in accordance with the Agreement. Annex 1 to this DPA sets out certain details regarding Processor’s personal data processing activities as required by Article 28(3) of the GDPR.

2.2 The Parties agree that for this DPA, Client is the data controller of the personal data and Processor is the data processor, except when Client acts as a data processor of personal data, in which case Processor is a subprocessor.

2.3 In accordance with GDPR Article 28(3)(a), Processor and any person acting under its authority shall only process personal data upon Client’s documented instructions, unless required to do so by EU or EU Member State law to which Processor is subject. In this case, Processor shall inform Client of the relevant legal requirement before processing, unless Processor is legally prohibited from informing Client of the requirement.

3. Security Measures

When Processor processes personal data on Client’s behalf, Processor shall:

3.1 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with the processing activity, including, as required, the measures referred to in Article 32(1) of the GDPR.

3.2 Take 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.

3.3 Ensure that persons authorized by Processor to process Client personal data have committed themselves to confidentiality, are under appropriate statutory confidentiality obligations and have received adequate training on data protection laws relating to personal data.

4. Subprocessing

4.1 Client hereby grants general written authorization for Processor to engage another processor (a “Subprocessor”) with Client’s prior specific written authorization. Processor shall inform Client in advance of its intention to add or replace Subprocessors.

4.2 Processor may continue to use Subprocessors engaged as of the Effective Date of this DPA, subject to compliance with Processor’s obligations under the Agreement and Data Protection Law. These Subprocessors are: LIST.

4.3 Processor shall ensure that Subprocessors are bound by a written agreement requiring the Subprocessor to adhere to the same data protection obligations as those applicable to Processor under this DPA and applicable Data Protection Law. Processor shall be responsible for a Subprocessor’s failure to adhere to its data protection obligations in such written agreement.
5. **Data Subject Rights**

5.1 Insofar as is possible, Processor shall provide Client appropriate assistance in responding to requests from data subjects seeking to exercise their rights as set forth in the GDPR.

5.2 Processor shall promptly notify Client in writing if it receives a request to exercise a data subject right from a data subject whose personal data is processed by Processor in connection with its provision of the Services.

5.3 Processor shall not be obligated to respond directly to a data subject regarding a data subject request except as required by applicable laws to which Processor is subject.

6. **Personal Data Breach.** Processor shall notify Client without undue delay after becoming aware of a personal data breach affecting Client personal data that Processor processes in accordance with the Agreement. Upon Client’s written request, Processor shall provide commercially reasonable assistance to Client in meeting Client’s obligations under the GDPR regarding such personal data breach.

7. **Audits and Inspections.** Processor shall make available to Client such information as is necessary to demonstrate compliance with Processor’s obligations in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client.

8. **Data Protection Impact Assessment and Prior Consultation.** Upon written request from Client, Processor shall provide commercially reasonable assistance to Client with data protection impact assessments and prior consultations with supervising authorities in accordance with Articles 35 and 36 of the GDPR. The requirements of the prior sentence apply solely to the processing of Client personal data in accordance with the Agreement and taking into account the nature of the processing and information available to Processor.

9. **Deletion or Return of Client Personal Data.** Unless otherwise prohibited by applicable law, Processor shall, upon Client’s written request, delete or return Client’s personal data to Client after the end of the provision of Services and delete existing copies unless EU law or EU Member State law requires storage of the personal data.

10. **Recordkeeping.** Both Parties agree that this DPA constitutes a complete record of the processing activities that Processor is required to maintain under Article 30(2) of the GDPR with regard to processing activities carried out on behalf of Client.

11. **Amendment.** Upon written agreement by both Parties, this DPA may be amended as required to comply with updates to Data Protection Law.

12. **Governing Law.** This DPA and all obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

13. **Order of Precedence.** In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement, the provisions of this DPA shall prevail.

14. **Severability.** If any provision of this DPA is invalid or unenforceable, the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be amended as needed to ensure its validity or enforceability, preserving the intentions of the Parties as far as possible, or if not possible, construed in a manner as if the invalid or unenforceable provision had never formed part of the DPA.
IN WITNESS WHEREOF, Client and Processor have executed this DPA as of the Effective Date.

Client Name: ___________________________  Processor Name: ___________________________
Signed: ________________________________  Signed: ________________________________
Printed Name/Title: ______________________  Printed Name/Title: ______________________
Date: _________________________________  Date: _________________________________

ANNEX 1: DESCRIPTION OF PERSONAL DATA PROCESSING

Annex 1 describes Processor’s processing of Client personal data in the course of its performance of the Services, in accordance with Section 2.1 of this DPA and applicable Data Protection Law.

- **Subject matter, duration, nature, and purposes of personal data processing**

  The subject matter of the personal data processing is Processor’s provision of the Services in accordance with the Agreement. The duration of the personal data processing is limited to the term of the Agreement. The nature and purpose of Processor’s processing activities is to provide Services to Client in accordance with the Agreement.

- **Categories of personal data**

  Processor may process the following types of personal data:

  LIST

- **Data subjects**

  Processor may process personal data concerning the following categories of data subjects:

  LIST