

# Data Processing Addendum

*Last Revised: August 7, 2018*

This Mark Business Intelligence Systems LLC ("MarkBIS") Data Processing Addendum ("DPA") forms part of, and is subject to the provisions of, our Terms of Service, and the terms of any duly executed Statement of Work ("SOW") and/or Master Services Agreement ("MSA") between you and us (collectively, the "Agreement"). Capitalized terms that are not defined in this DPA have the meanings set forth in the Agreement.

## 1. Additional Definitions

---

The following definitions apply solely to this DPA:

- (a) the terms "controller", "data subject", "personal data", "process", "processing" and "processor" have the meanings given to these terms in EU Data Protection Law.
- (b) "Breach" means a breach of the Security Measures resulting in access to MarkBIS's Vendor Systems storing Your Controlled Data and the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Controlled Data transmitted, stored or processed by MarkBIS on your behalf and instructions through the Services.
- (c) "Content" means your Client Content and any content provided to us from your Users, including without limitation text, documents, files, photos, images, audio, video, code, and any other materials.
- (d) "EU Data Protection Law" means any data protection or data privacy law or regulation of Switzerland or any European Economic Area ("EEA") country applicable to Your Controlled Data, including, as applicable, the GDPR and the e-Privacy Directive 2002/58/EC.
- (e) "Files" is a sub-set of Content that includes any Content processed by you or your Users in the form of files or documents, regardless of the type of Content or file processed (e.g. Excel, Word, PDF, etc). Within the Application, Files may be referred to as "Attachments" or "Attached Files".
- (f) "GDPR" means the EU General Data Protection Regulation 2016/679.
- (g) "Data Concerning Health" means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual.
- (h) "Genetic Data" means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development.
- (i) "Security Measures" means the technical and organizational security measures described in the Service Level Agreements in the Agreement.
- (j) "Sub-Processor" means an entity engaged by MarkBIS to process Your Controlled Data.

- (k) "Your Controlled Data" means the personal data in the Content we process on your behalf, and instructions as part of the Services, but only to the extent that you are subject to EU Data Protection Law in respect of such personal data. Your Controlled Data does not include (a) personal data when controlled by us, including without limitation data we collect (including IP address, device/browser details and web pages visited prior to coming to Your Site) with respect to your Users' interactions with the Services through their browser and technologies like cookies, or (b) Prohibited Data.

## 2. Applicability

---

This DPA only applies to you if you or your Users are data subjects located within the EEA or Switzerland and only applies in respect of Your Controlled Data. If you or your Users are non-EEA or non-Switzerland data subjects, then our obligations to protect your and your Users' data are set forth in our Terms of Service and other documents in our Agreement, but this DPA does not apply. You agree that MarkBIS is not responsible for personal data that you have elected to process through Third Party Services or outside of the Services, including the systems of any other third-party cloud services, offline or on-premises storage.

## 3. Prohibited Data and Files

---

You and your Users are prohibited from processing the following personal data ("Prohibited Data") through the Services:

- (a) Personal Data from children aged 13 or under;
- (b) Personal Data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of Genetic Data or Data Concerning Health or sex life; and
- (c) Personal Data revealing Criminal Convictions, Protected Health Information ("PHI") as defined under the US Health Insurance Portability and Accountability Act of 1996 as amended ("HIPAA"), or personal data embedded in Files, unless, prior to processing such Content through the Services: (a) you have purchased a license and have agreed to a separate, duly executed amendment to your Terms of Service that explicitly defines the personal data, processing instructions, and the Security Measures in place to protect it, and (b) to the extent required by applicable law, you obtain timely consent from the data subjects during the course of your use of the Application.

Notwithstanding anything to the contrary in the Agreement (including this DPA), with regards to Prohibited Data, we disclaim all responsibility and liability for such Personal Data and you agree to release, indemnify and hold us harmless from all claims, costs, losses and liabilities related to such Prohibited Data.

## 4. Details of Data Processing.

---

- (a) Subject Matter. The subject matter of the data processing under this DPA is Your Controlled Data.

- (b) Duration. As between you and us, the duration of the data processing under this DPA is determined by you.
- (c) Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by you from time to time.
- (d) Nature of the Processing. The nature of the processing consists of the Services, as described in a Statement of Work between you and us, and initiated by you from time to time.
- (e) Type of Personal Data. The types of personal data processed consist of Your Controlled Data relating to you, your Users or other individuals, whose personal data is included in Content which is processed as part of the Services in accordance with instructions given by you or your authorized Users.
- (f) Categories of Data Subjects. Data subjects consist of you (our Client), your Users and any other individuals whose personal data is included in Content.

## 5. Processing Roles and Activities.

---

- (a) MarkBIS as Processor and You as Controller. You are the controller and MarkBIS is the processor of Your Controlled Data.
- (b) MarkBIS as Controller. MarkBIS may also be an independent controller for some personal data relating to you or your Users. Please see our [Privacy Policy](#) and Terms of Service for details about this personal data which we control. We decide how to use and process that personal data independently and use it for our own purposes. When we process personal data as a controller, you acknowledge and confirm that the Agreement does not create a joint-controller relationship between you and us. If we provide you with personal data controlled by us, such as in any access to data regarding your Users' interactions with the Services, you receive that as an independent data controller and are responsible for compliance with EU Data Protection Law in that regard.
- (c) Description of Processing Activities. We will process Your Controlled Data for the purpose of providing you with the Services, as may be used, configured or modified from within your Application (the "Purpose"). For example, depending on how you use the Services, we may process Your Controlled Data to: (a) enable you to assign tasks to Users; (b) invite Users to collaborate on Content in the Application; or (c) email your Users on your behalf.
- (d) Compliance with Laws. You will ensure that your instructions comply with all laws, regulations and rules applicable in relation to Your Controlled Data and that Your Controlled Data is collected lawfully by you or on your behalf and provided to us by you in accordance with such laws, rules and regulations. You will also ensure that the processing of Your Controlled Data in accordance with your instructions will not cause or result in us or you breaching any laws, rules or regulations (including EU Data Protection Law). You are responsible for reviewing the information available from us relating to data security pursuant to the Agreement and making an independent determination as to whether the Services meet your requirements and legal obligations as well as your obligations under this DPA.

MarkBIS will not access or use Your Controlled Data except as provided in the Agreement, as necessary to maintain or provide the Services or as necessary to comply with the law or binding order of a governmental, law enforcement or regulatory body.

## 6. Our Processing Responsibilities.

---

- (a) How We Process. We will process Your Controlled Data for the Purpose and in accordance with your instructions. You agree that the Agreement including this DPA, along with your use and configuration of the Services, are your complete and final documented instructions to us in relation to Your Controlled Data. Additional instructions outside the scope of this DPA require prior written agreement between you and us, including agreement on any additional fees payable by you to us for carrying out such instructions. We will promptly inform you if, in our opinion, your instructions infringe applicable EU Data Protection Law, or if we are unable to comply with your instructions. We will notify you when applicable laws prevent us from complying with your instructions, except if such disclosure is prohibited by applicable law on important grounds of public interest, such as a prohibition under law to preserve the confidentiality of a law enforcement investigation or request.
- (b) Notification of Breach. We will provide you notice without undue delay after becoming aware of and confirming the occurrence of a Breach for which notification to you is required under applicable EU Data Protection Laws. We will, to assist you in complying with your notification obligations under Articles 33 and 34 of the GDPR, provide you with such information about the Breach as we are reasonably able to disclose to you, taking into account the nature of the Services, the information available to us and any restrictions on disclosing the information such as for confidentiality. Our obligation to report or respond to a Breach under this Section (b) is not and will not be construed as an acknowledgement by MarkBIS of any fault or liability of MarkBIS with respect to the Breach. Despite the foregoing, MarkBIS's obligations under this Section (b) do not apply to incidents that are caused by you, your Users, any activity in your Application by you or your Users, and/or Third-Party Services.
- (c) Notification of Inquiry or Complaint. We will provide you notice, if permitted by applicable law, upon receiving an inquiry or complaint from a User, or other individual whose personal data is included in your Content, or a binding demand (such as a court order or subpoena) from a government, law enforcement, regulatory or other body in respect of Your Controlled Data that we process on your behalf and instructions.
- (d) Reasonable Assistance with Compliance. We will, to the extent that you cannot reasonably do so through the Services, your Application or otherwise, provide reasonable assistance to you in respect of your fulfillment of your obligation as controller to respond to requests by data subjects under Chapter 3 of the GDPR, taking into account the nature of the Services and information available to us. You will be responsible for our reasonable costs arising from our provision of such assistance.
- (e) Security Measures. We will maintain the Security Measures. We may change these Security Measures but will not do so in a way that adversely affects the security of Your Controlled Data. We will take

steps to ensure that any natural person acting under our authority who has access to Your Controlled Data does not process it except on our instructions, unless such person is required to do so under applicable law, and that personnel authorized by us to process Your Controlled Data have committed themselves to relevant confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

- (f) Sub-Processors. You agree that we can share Your Controlled Data with our Data Center and any other Sub-Processors, if any, in order to provide you the Services. We will impose contractual obligations on our Sub-Processors, and contractually obligate our Sub-Processors to impose contractual obligations on any further sub-contractors which they engage to process Your Controlled Data, which provide the same level of data protection for Your Controlled Data in all material respects as the contractual obligations imposed in this DPA, to the extent applicable to the nature of the Services provided by such Sub-Processor. A list of our current Sub-Processors is available upon request by sending an email to [info@mycm.com](mailto:info@mycm.com). If we change a Sub-Processor, then we will notify you at least 30 days prior to the change. If you object to the new Sub-Processor and your objection is reasonable and related to data protection concerns, we will use commercially reasonable efforts to make available to you a means of avoiding the processing of Your Controlled Data by the objected-to Sub-Processor. If we are unable to make available such suggested change within a reasonable period of time, we will notify you and if you still object to our use of such Sub-Processor, you may cancel or terminate your Services or, if possible, the portions of the Services that involve use of such Sub-Processor. Except as set forth in this Section (f), if you object to any Sub-Processors, you may not use or access the Services. You consent to our use of Sub-Processors as described in this Section (f). Except as set forth in this Section (f) or as you may otherwise authorize, we will not permit any Sub-Processor to access Your Controlled Data. MarkBIS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of any Sub-Processor or their further sub-contractors that process Your Controlled Data and cause MarkBIS to breach any of MarkBIS' obligations under this DPA, solely to the extent that MarkBIS would be liable under the Agreement if the act or omission was MarkBIS' own.
- (g) MarkBIS Audits. As described in our Agreement, MarkBIS and its Sub-Processors may use external or internal auditors to annually verify the adequacy of our Security Measures at our Data Center.
- (h) Customer Audits and Information Requests. You agree to exercise any right you may have to conduct an audit or inspection by instructing MarkBIS to carry out the audit described in Section (g). You agree that you may be required to agree to a non-disclosure agreement with MarkBIS before we share any such report or outcome from such audit with you and that we may redact any such reports as we consider appropriate. If MarkBIS does not follow such instruction or if it is legally mandatory for you to demonstrate compliance with EU Data Protection Law by means other than reviewing a report from such an audit, you may only request a change in the following way:
- i. Information Request. First, submit a request for additional information in writing to MarkBIS, specifying all details required to enable MarkBIS to review this request effectively, including without limitation the information being requested, what form you need to obtain

it in and the underlying legal requirement for the request (the "Request"). You agree that the Request will be limited to information regarding our Security Measures.

- ii. Response to Request. Within a reasonable time after we have received and reviewed the Request, you and we will discuss and work in good faith towards agreeing on a plan to determine the details of how the Request can be addressed. You and we agree to use the least intrusive means for MarkBIS to verify MarkBIS' compliance with the Security Measures in order to address the Request, taking into account applicable legal requirements, information available to or that may be provided to you, the urgency of the matter and the need for MarkBIS to maintain uninterrupted business operations and the security of its facilities and protect itself and its customers from risk and to prevent disclosure of information that could jeopardize the confidentiality of MarkBIS, our customers' or our users' information.
  - iii. Response Costs. You will pay our reasonable costs in considering and addressing any Request. Any information and documentation provided by MarkBIS or its auditors pursuant to this Section h) will be provided at your cost, except for any annual SOC1, SOC2 or SOC3 audit report that MarkBIS has agreed to provide at no additional cost pursuant to the Agreement.
- (i) Questions. Upon your reasonable requests to us for information regarding our compliance with the obligations set forth in this DPA, we shall, where such information is not otherwise available to you, provide you with written responses, provided that you agree not to exercise this right more than one (1) time per calendar year (unless it is necessary for you to do so to comply with EU Data Protection Law). The information to be made available by MarkBIS under this Section (i) is limited to solely that information necessary, taking into account the nature of the Services and the information available to MarkBIS, to assist you in complying with your obligations under the GDPR in respect of data protection impact assessments and prior consultation. You agree that you may be required to agree to a non-disclosure agreement with MarkBIS before we share any such information with you.
- (j) Data Disposition Requests. Through the Services, you can access a copy of all of Your Controlled Data, and delete most of Your Controlled Data (including all Files, which are your responsibility), with the exception of archived copies on back-up systems. For any of Your Controlled Data which may not be deleted or accessed through the Services, upon your written request, we will, with respect to any of Your Controlled Data in our or our Sub-Processor's possession that we can associate with a data subject, subject to the limitations described in the Agreement (including this DPA) and unless prohibited by applicable law or the order of a governmental, law enforcement or regulatory body, delete, and request that our Sub-Processors delete, such data (excluding such data which is archived on back-up systems, which we shall protect from any further processing and which we shall ensure is deleted from the back-up systems at the end of the back-up cycle rotation as set forth in your Agreement, except to the extent required by applicable law). Otherwise, we will delete Your Controlled Data in accordance with the Agreement. This Section (j) does not apply to personal data held by Third Party Services.

## 7. Data Transfers.

---

You authorize us to transfer Your Controlled Data away from the country in which such data was originally collected. In particular, you authorize us to transfer Your Controlled Data to the US. We will only transfer Your Controlled Data to outside the EEA using the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks or another lawful data transfer mechanism that is recognized under EU Data Protection Law as providing an adequate level of protection for such data transfers.

## 8. Liability.

---

The liability of each party under this DPA is subject to the exclusions and limitations of liability set out in the Agreement. You agree that any regulatory penalties or claims by data subjects or others incurred by MarkBIS in relation to Your Controlled Data that arise as a result of, or in connection with, your or your Users' failure to comply with your obligations under this DPA or EU Data Protection Law shall reduce MarkBIS's maximum aggregate liability to you under the Agreement in the same amount as the fine and/or liability incurred by us as a result.

## 9. Conflict.

---

In the event of a conflict between this DPA and the Agreement, this DPA will control.

## 10. Miscellaneous.

---

You are responsible for any costs and expenses arising from MarkBIS's compliance with your instructions or requests pursuant to the Agreement (including this DPA) which fall outside the standard functionality made available by MarkBIS generally through the Services.