

Privacy Policy

Last Updated: December 20, 2018

I. What's covered by this policy

This Privacy Policy explains how information is collected, used and disclosed by Mark Business Intelligence Systems, LLC ("MarkBIS"). Capitalized words in this policy are defined terms with meanings described in the [Definitions](#) section below. This Privacy Policy applies to information we collect when you:

A. use or access our Public Website;

This Privacy Policy applies when you use or access our online website available to the general public at <http://www.myCM.com>, which you can also navigate to from our other owned URLs such as www.mycompliancemanager.com, www.markbis.com, and www.mycm.solutions ("Public Websites").

B. contact us or participate in our Promotions; or

This Privacy Policy applies when you access, respond, subscribe or unsubscribe to newsletters, surveys, informational e-mails, and other marketing materials or activities promoting our services ("Promotions"); or you otherwise contact us.

C. use or access our myComplianceManager Services.

This Privacy Policy applies when you use or access our products and services, including our myComplianceManager Applications that are available via the Internet only to the Customers that license them, and their authorized users (collectively, the "myComplianceManager Services").

Our myComplianceManager Applications are identified by URLs that contain the [mycompliancemanager.com](http://www.mycompliancemanager.com) or [myCM.com](http://www.myCM.com) domain with a customer-name prefix, for example, [https://\[customer-name\].mycompliancemanager.com](https://[customer-name].mycompliancemanager.com). It is important to note that each of our Customers is the exclusive licensee and primary Controller of its specific myComplianceManager Application, and as such has independent access and control over all Content, including data, files, tasks, reports or other information that you upload, download, collaborate on or share within the myComplianceManager Application. For any Content or Personal Data Processed via a myComplianceManager Application, the Customer is the Controller and we are the Processor, which is why our Customer contracts for myComplianceManager Applications inform our Customers that they may be responsible to provide privacy notices and access to individuals whose Personal Data is transferred to the U.S. Additionally, our Customer contracts typically require our Customers to comply with all applicable laws, however, we cannot control, and are not responsible for, how our Customers collect, use or disclose your information and Content; therefore, before connecting to or using a myComplianceManager Application and before providing any Personal Data or Content, we encourage you to review the privacy policies of the Customer organization who is the Controller of that myComplianceManager Application. Lastly, please note that the

terms of our Customers' contracts for myComplianceManager Applications may restrict our collection or use of your information more than what is described in this Privacy Policy.

D. Prohibited information

MarkBIS does not knowingly collect the following information, and if we become aware of it, we will take steps to delete such information. You are prohibited from providing, uploading, or using the following information, and MarkBIS disclaims all liability for all such information:

- Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 as amended ("HIPAA"), unless you have purchased a myComplianceManager Application license and you have entered into a separate, mutually executed amendment to your MarkBIS Master Services Agreement that explicitly defines the information and the security measures in place to protect it;
- 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 or criminal convictions or related security measures;
- Personal Data from children under 13; and
- Unsolicited job applications or résumés, unless such information is provided in response to a currently posted job opening.

II. Where to find this policy

A current version of this Privacy Notice is always available by clicking the "Privacy" link on any page of our Public Website, or our myComplianceManager Applications, or you can request a copy by contacting us at:

info@mycm.com, or

Mark Business Intelligence Systems
14747 N Northsight Blvd, Ste 111-134
Scottsdale, Arizona 85260
Attn: Data Protection Officer
+1 (888) 219-8024

III. Changes to this policy

We may change this Privacy Policy from time to time. If we make any changes, we will notify you by revising the "Last Updated" date at the top of this Privacy Policy and, in some cases, we may provide you with additional notice (such as adding a statement to our homepage or sending you an e-mail notification). We encourage you to review our Privacy Policy whenever you access our Public Website or our myComplianceManager Services to stay informed about our information practices and the ways you

can help protect your privacy. Your use of our Public Website or any of the myComplianceManager Services after the posting of such changes shall constitute your consent to such changes.

IV. Notice

This Privacy Policy serves as our legal notice to you of important information about our privacy program and what you can do to protect your Personal Data.

Prior to collecting or requesting Personal Data from you, we or our Customers may supplement this Privacy Policy with an additional clear, conspicuous and contextual privacy notice regarding the specific Personal Data being collected or requested at that time (collectively, "Privacy Notice"). Please read all such Privacy Notices prior to providing Personal Data or Content.

In all cases, our Privacy Notice is provided when individuals are first asked to provide Personal Data or as soon thereafter as is practicable. For example, before deciding whether to submit any Personal Data, individuals can review this privacy notice by clicking the "Privacy Policy" link, which is displayed on our Public Website, myComplianceManager Application, and in Promotion emails or other materials they receive.

In this Privacy Policy, we specifically are providing you notice of the following items. Please read this entire Privacy Policy carefully. Thank you.

- [International Consumers: Our Participation in EU-US and US-Swiss Privacy Shield;](#)
 - [Submitting complaints under Privacy Shield;](#)
 - [Independent resolution of complaints under Privacy Shield;](#)
 - [Binding arbitration under Privacy Shield;](#)
- [How to submit inquiries or complaints;](#)
- [What types of data we collect;](#)
- [Our purpose and use of collected data;](#)
- [When and to whom we share or disclose data;](#)
- [Our accountability for onward transfer;](#)
- [Your choices to limit use and disclosure;](#)
- [Your right to access your Personal Data;](#)
- [Security;](#) and
- [Enforcement.](#)

V. International Consumers

MarkBIS is located in the United States. If you are providing Personal Data and are not a resident of the United States, your country's privacy laws may differ from those in the United States. By accessing or using the myComplianceManager Services or otherwise providing information to us, you consent to the terms of

this Privacy Policy and the Processing and transfer of information in and to the U.S. and other countries and territories, which may have different privacy laws from your country of residence.

A. Our Participation in EU-US and Swiss-US Privacy Shield

MarkBIS complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (“Privacy Shield”) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and the United Kingdom and/or Switzerland to the United States in reliance on Privacy Shield. MarkBIS has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

1. Submitting complaints under the Privacy Shield

In compliance with the Privacy Shield Principles, MarkBIS commits to resolve complaints about the privacy, collection or use of our Consumers’ Personal Data. European Union, United Kingdom or Swiss Consumers with inquiries or complaints regarding this Privacy Policy should first contact MarkBIS at:

info@mycm.com, or

Mark Business Intelligence Systems
14747 N Northsight Blvd, Ste 111-134
Scottsdale, Arizona 85260
Attn: Data Protection Officer
+1 (888) 219-8024

We will respond to your inquiry or complaint within 30 days and inform you of the actions implemented to resolve it. If you have any questions regarding the resolution of your inquiry or complaint, please contact us.

2. Independent resolution of complaints under the Privacy Shield

MarkBIS has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. After first submitting your inquiry or complaint to MarkBIS, if you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint.

3. Binding Arbitration

Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

VI. Types of data we collect

The following types of information may be collected:

A. Information you voluntarily provide

1. Via our Public Website and Promotions

When interacting with our Public Website, responding to Promotions, or otherwise interacting with us, you may choose to provide Personal Data, such as your name, employer's name, employer's address, job title, work e-mail address, work telephone number, or other contact information for the purpose of requesting a demonstration of our services, customer support or other information, or for the purpose of subscribing or unsubscribing to our Promotions, myComplianceManager Services alerts, blogs, or other service-related information.

2. Via our myComplianceManager Services

When using our myComplianceManager Services, you may choose to provide Personal Data when you are a Customer, or a Customer's authorized user, and:

- You register for an account, and create or modify your profile and online account;
- You access, use or request information in connection with the myComplianceManager Services;
- You participate in any interactive features of the myComplianceManager Services, request customer support, or otherwise communicate with us;
- You upload, download, collaborate on or share data, files, tasks, reports or other information within the myComplianceManager Applications; or
- You participate or complete an online form in connection with a task that was assigned to you, such as an invitation to collaborate on Content, projects, surveys, questionnaires, training, tests, self-assessments, audits, declarations, certifications, documents, corrective action, or other tasks and online activities.

B. Information We Collect Automatically

1. Via our Public Website and Promotions

Log Information: When interacting with our Public Website or responding to Promotions, we may automatically collect public information about you, including a) browser type, name, version, platform and capabilities, and your b) Internet Protocol ("IP") address. Our Public Website may also utilize analytics or other technologies to collect information, which may include saving cookies to your computer or mobile device. Cookies are small data files stored on your hard drive or in device memory that help us to: i) count visitors to our Public Website, ii) improve the Public Website and your experience, and iii) understand which areas and features of the Public Website are most popular. We may also collect information using Web beacons in connection with Promotions. A Web beacon is a graphic image, such as a pixel tag or clear GIF, which is placed on a Web page or in an e-mail message to monitor user activity, such as whether the Web page or e-mail message is accessed or clicked. Some of our Web pages and HTML-formatted e-

mail newsletters may use Web beacons in conjunction with cookies. For more information about cookies and how to disable them, please see "Your Choices" below.

2. Via our myComplianceManager Services

Log and Usage Information: When you use our myComplianceManager Services, our system automatically collects Log Information (described above) and Usage Information of Customers and their authorized users. Collecting Usage Information means that our system monitors user activity in connection with our myComplianceManager Services and automatically collects information about the applications and features you use, the sizes, names and types of data, files or folders you upload, download, share or access while using the myComplianceManager Services, the Content you access and any actions you take in connection with your access and use of Content in the myComplianceManager Services. We do not utilize any cookies in connection with our myComplianceManager Services, except only when you authorize it for the sole purpose of accessing the myComplianceManager Services without re-entering your User ID and/or password.

C. Information we collect from other sources

We may also obtain information from third parties and combine that with information we collect through our Public Website and the myComplianceManager Services. For example, we may have access to certain information from a Customer with whom you are associated (like your employer, university, business partner, customer, supplier, or contractor). Any access that we may have to such information from a Customer is in accordance with our Customer's contract and the authorization procedures determined by that entity or organization.

VII. Purposes and uses for collected data

We may use the information we collect about you for a variety of purposes, including to:

- Provide, operate, maintain and improve our Public Website or the myComplianceManager Services;
- Enable you to access and use the myComplianceManager Services, including uploading, downloading, collaborating on and sharing Content and sending e-mails on your behalf;
- Send you technical notices, updates, security alerts and support and administrative messages;
- Provide and deliver the services and features you request, process and complete transactions, and send you related information, including e-mail confirmations and invoices;
- Respond to your comments, questions, and requests and provide customer service and support;
- Communicate with you about services, features, surveys, newsletters, offers, promotions, and events, and provide other news or information about MarkBIS and our myComplianceManager Services;
- Monitor and analyze trends, usage, and activities in connection with our Public Websites or the myComplianceManager Services and for marketing or advertising purposes;
- Investigate and prevent fraudulent transactions, unauthorized access to the myComplianceManager Services, and other illegal activities;

- Personalize and improve the myComplianceManager Services, and provide content, features, and/or marketing information that match your interests and preferences or otherwise customize your experience on the myComplianceManager Services;
- Link or combine with other information we receive from third parties to help understand your needs and provide you with better service;
- Enable you to communicate, collaborate, and share Content with users you designate; and
- For other purposes about which we notify you.

VIII. Data Integrity and Purpose Limitation

Consistent with the Privacy Shield Principles, MarkBIS limits its collection of Personal Data to only the information that is relevant for the purpose of Processing, and will take reasonable steps to ensure that Personal Data is reliable for its intended use, accurate, complete, and current. For Customer-Controlled myComplianceManager Applications, our Customers are responsible for ensuring that Personal Data is reliable for its intended user, accurate, complete and current. We and our Customers typically achieve data integrity and purpose limitation by 1) narrowly limiting the scope of Personal Data initially requested, and 2) redacting or deleting Personal Data that is out of scope or irrelevant for the purpose of processing.

IX. Sharing and disclosure of data

We will NOT share Personal Data about you or any Content with any third parties except as described in this Privacy Policy or any Privacy Notice. For example, we may share Personal Data about you as follows:

A. Sharing of collected data regardless of its source

1. Compliance with Laws

We may disclose your information to a third party if (a) we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process or governmental request, (b) to enforce our agreements, policies and terms of service, (c) to protect the security or integrity of the myComplianceManager Services, (d) to protect MarkBIS, our customers or the public from harm or illegal activities, or (e) to respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person. Please note that we may be required to release personal information in response to a lawful request by public authorities including to meet national security or law enforcement requirements.

2. Business Transfers

We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company. Should such a sale or transfer occur, MarkBIS will use reasonable efforts to direct the transferee to use your information and Content in a manner that is consistent with this Privacy Policy.

3. Aggregated or Anonymized Data

We may also share aggregated or anonymized information with third parties that does not directly identify you.

B. Sharing of Public Website and Promotion collected data

We may share data collected from our Public Website and Promotions as follows:

1. Vendors, Consultants and Other Service Providers

We may share your information with certain third party vendors, consultants and other service providers who have first signed a contractual obligation of confidentiality and non-disclosure, and who are working on our behalf and require access to your information to carry out that work, such as to manage and improve our Public Website and Promotions.

C. Sharing of myComplianceManager Services collected data

Data collected from our myComplianceManager Services may be shared as follows:

1. Vendors, Consultants and Other Service Providers

We may share your information with certain third party vendors, consultants and other service providers who have first signed a contractual obligation of confidentiality and non-disclosure, and who are working on our behalf and require access to your information to carry out that work, such as to process billing, provide customer support, etc.

2. Organizations Related to You

If you use or access the myComplianceManager Services as part of, or at the invitation of, one of our Customers (for example, our Customer may be your employer, business partner, customer, supplier, or contractor), then that Customer organization is the Controller, and has independent access and control over the Personal Data and Content you upload or provide into the myComplianceManager Services. In these situations, except for our responsibility as a Processor of such information, MarkBIS disclaims all liability. Our Customer contracts typically require our Customers to comply with all applicable laws, including those restricting disclosure, sharing and onward transfer of Personal Data; however, we cannot control, and are not responsible for, how our Customers collect, use or disclose your Personal Data and Content; therefore, we encourage you to review the privacy policies of that Customer-Controller organization to learn more about their information and privacy practices, before connecting to or using our myComplianceManager Services and before providing any Personal Data.

3. For Collaboration

With regards to myComplianceManager Applications, your information may be shared when you choose to use collaboration features in the myComplianceManager Services that by their nature support sharing with third parties who you choose. Your name, e-mail address, information from your profile and online account, and any Content you choose to share will be shared with such third parties, and such third parties may communicate with you (such as by responding to surveys, posting comments, entering Content or e-mailing you) in connection with your use of the collaboration features of the myComplianceManager Services. For example, third parties who you invite to collaborate with you as system users may, by using

the collaboration features of the myComplianceManager Services, modify Content that you have shared, upload/download data and documents or other Content you have shared, share such Content outside of the myComplianceManager Services, and provide other third parties with rights to view the Content you have shared.

4. Third Party Applications

The myComplianceManager Services may provide you with opportunities to connect with third-party web sites, applications or services, such as through URLs displayed on system pages. If you choose to use any such third-party web site, applications or services, we may share information about you including your username and any Content you choose to use in connection with those web sites, applications and services, and such third parties may contact you directly as necessary. This Privacy Policy does not apply to your use of such third-party web sites, applications and services, and we are not responsible for how those third parties collect, use and disclose your information and Content. We encourage you to review the privacy policies of those third parties before connecting to or using their web sites, applications or services to learn more about their information and privacy practices.

D. Accountability for Onward Transfer

Please note that MarkBIS is potentially liable in cases of onward transfer to third parties of Personal Data owned by our Consumers, received pursuant to the EU-US and Swiss-US Privacy Shield.

X. Your choices to limit use and disclosure of Personal Data

The following describe the choices and means we offer individuals to limit the use and disclosure of their Personal Data.

A. Information you voluntarily provide

1. You can choose not to provide information

Your first choice is simply to not provide us with your Personal Data. Except for a User ID and password needed to login to any myComplianceManager Service, we do NOT require you to provide Personal Data to use or access our Public Website or our myComplianceManager Services. Please note that we will never ask you in an e-mail, postal letter or telephone call for sensitive Personal Data such as your User ID, password, social security number, or any of the "Prohibited information" described above. In addition, MarkBIS will never intentionally use your Personal Data for any purpose that is materially different from the purpose(s) for which it was collected or authorized, without first obtaining your affirmative express consent or providing you notice and opportunity to opt-out via a clear and conspicuous on-screen mechanism, e-mail or other direct notification.

2. Opt-out via myComplianceManager Services

If you use or access one of our Customer-Controlled myComplianceManager Applications as part of, or at the invitation of, one of our Customers (for example, our Customer may be your employer, business partner, customer, supplier, or contractor), then that Customer organization may permit you to opt-out of

uploading, downloading or collaborating on Personal Data or Content by following the opt-out instructions provided either in the task assignment e-mail or the on-screen privacy notice. For example, in most cases the Customer will identify Personal Data fields as optional, or request your affirmative express consent (opt-in) when those fields are required.

3. Right to access your Personal Data

You have the right to access your Personal Data, and to correct, amend, or delete that information where it is inaccurate, or, in the case of European Union and Swiss Consumers, has been Processed in violation of the Privacy Shield Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. You can request access to your Personal Data by sending us a request with 1) your contact information, 2) e-mail or postal address, and 3) sufficient information to identify and locate your Personal Data (e.g. please identify whether you used or accessed our Public Website, myComplianceManager Services, or responded to a Promotion), and send to either:

info@mycm.com, or

Mark Business Intelligence Systems
14747 N Northsight Blvd, Ste 111-134
Scottsdale, Arizona 85260
Attn: Data Protection Officer
+1 (888) 219-8024

We will respond to your access request within 30 days and inform you of the actions implemented to resolve it. If you have any questions regarding the resolution of your inquiry or complaint, please contact us.

Please note that we cannot respond to requests-for-access related to Content or Personal Data that you provided directly to one of our Customers, or that you Processed via one of our Customer-Controlled myComplianceManager Applications, because it would violate the rights of our Customer and may violate the rights of other individuals. In those situations, please first submit your request directly to the Customer to whom you provided the Personal Data or Content. If your request is not processed by the Customer within 30 days, then please contact us at the above address so that we can assist you.

B. Account Information & Retention

You may update, correct or delete information about you at any time by logging into your myComplianceManager Services' online account and modifying your user information or preferences. You can also e-mail us at info@mycm.com. Your personal information will be retained for the period necessary to fulfill the purposes outlined in this Privacy Policy. If you wish to deactivate your account, please e-mail us at info@mycm.com, but note that certain information may be retained as required by law or for legitimate business purposes. We may also retain cached or archived copies of information about you for a certain period of time. We will respond to your access request within 30 days. To request removal of your personal information from our blog or testimonials, contact us at the e-mail address listed above. In some

cases, we may not be able to remove your personal information, in which case we will let you know if we are unable to do so and why.

We will retain your information for as long as your account is active or as needed to provide you services. We will retain and use your information to comply with our legal obligations, resolve disputes and enforce our agreements.

C. Promotional Communications

You may opt out of receiving Promotion e-mails from MarkBIS by following the opt-out instructions provided in those e-mails. You may also opt-out of receiving Promotion e-mails and other Promotional communications from us at any time by e-mailing info@mycm.com with your specific request. If you opt out, we may still send you non-promotional communications, such as security alerts and notices related to your access to or use of the myComplianceManager Services or those about your online account or our ongoing business relations.

D. Cookies

Most web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove or reject browser cookies or to prompt you before accepting such a cookie. Please note that, if you choose to remove or reject browser cookies, this could affect the availability or functionality of the myComplianceManager Services.

XI. Security

While no service is completely secure, MarkBIS employs reasonable and appropriate measures to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the Processing and the nature of the Personal Data. For example, we accomplish this by:

- Establishing policies and procedures for securely managing information;
- Limiting employee access to sensitive information;
- Encrypting your information and Content in transit over the Internet to the myComplianceManager Services;
- Protecting against unauthorized access to Personal Data by using data encryption, authentication, virus detection technology, threat management and intrusion detection systems (IDS), as required;
- Requiring service providers with whom we do business to comply with relevant data privacy legal and regulatory requirements;
- Conducting background checks on employees and providing data privacy training to our team members; and
- Continually assessing our data privacy, information management and data security practices.

Additionally, the servers on which personal information is stored are kept in a controlled environment with limited access. While we take reasonable efforts to guard Personal Data, no security system is impenetrable. In addition, we cannot guarantee that any passively collected personal information you choose to include in documents you store on our systems are maintained at levels of protection to meet specific needs or obligations you may have relating to that information.

We further protect information by requiring all users to access account information and our myComplianceManager Services only through the use of an individual user ID and password. To protect the confidentiality of personal information, you must keep your password confidential and not disclose it to any other person. Please advise us immediately if you believe your password has been misused. In addition, always logout and close your browser when you finish your session. Please note that we may be required to release personal information in response to a lawful request by public authorities including to meet national security or law enforcement requirements.

XII. Enforcement

MarkBIS is subject to the investigatory and enforcement powers of the Federal Trade Commission (“FTC”). In addition, our privacy protection program includes procedures to periodically investigate and assess the effectiveness of our privacy practices. These procedures require both internal self-assessments, as well as independent, third party audits and assessments of our data center’s physical security, operational security and system security. For example, independent third-party auditors annually verify the data protection controls at our data centers pursuant to internationally accepted standards such as ISO 27001, and AICPA SSAE-16 (SOC 1, SOC 2 or SOC 3).

XIII. Blogs

Our Public Website may offer publicly accessible blogs or community forums. You should be aware that any information you provide in these areas may be read, collected, and used by others who access them.

XIV. Testimonials

We display personal testimonials of satisfied customers on our Public Website in addition to other endorsements. We may post your testimonial along with your name or company name.

XV. Links to Third Party Websites

We may place links on our Public Website or the myComplianceManager Services. When you click on a link to a third party website, your activity and use on the linked website is governed by that website’s policies, not by those of MarkBIS. We encourage you to visit their websites and review their privacy and user policies.

XVI. Our Policy Toward Children

myComplianceManager Services are not directed to individuals under 13. We do not knowingly collect personal information from children under 13. If you become aware that a child has provided us with personal information, please contact us at info@mycompliancemanager.com. If we become aware that a child under 13 has provided us with personal information, we will take steps to delete such information.

XVII. Definitions

For purposes of this Privacy Policy:

- “myComplianceManager Application” means proprietary software owned by MarkBIS that is licensed to a Customer and is accessible via the Internet by the Customer and its authorized users at a website address typically in the format of [https://\[customer-name\].mycm.com](https://[customer-name].mycm.com) or [https://\[customer-name\].mycompliancemanager.com](https://[customer-name].mycompliancemanager.com).
- “myComplianceManager Services” has the meaning set forth in Section I.C.
- “Consumer” means any natural person who is located in the European Economic Area (EEA), the United Kingdom or Switzerland, whose Personal Data has been Processed by MarkBIS.
- “Content” means all data, files, tasks, reports or other information that an individual uploads, downloads, collaborates on, shares or otherwise processes in, from or through the myComplianceManager Application.
- “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- “Customer” means any individual or entity that legally purchases, installs or activates myComplianceManager Services, including employers, businesses and other organizations that purchase licenses to use or access myComplianceManager Applications.
- “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.
- “Genetic Data” means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development.
- “MarkBIS” means Mark Business Intelligence Systems LLC, a Nevada limited liability corporation.
- “Personal Data” means any information that (i) is Processed in any form, (ii) relates to an identified or identifiable person, and (iv) can be linked to that person.
- “Process” means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, retrieval, use, erasure or destruction.

- “Processor” means a natural or legal person or entity which Processes Personal Data on behalf of the Controller.
- “Public Website” means the online website available to the general public at <http://www.mycm.com>, which you can also navigate to from our other owned URLs such as www.mycompliancemanager.com, www.markbis.com, www.cm.solutions, www.mycm.solutions, www.compliancemgr.com and www.compliancemanagersolutions.com.

XVIII. Contact us

MarkBIS is committed to resolving inquiries and complaints about your privacy and our collection or use of your Personal Data. If you have any inquiries or complaints regarding this Privacy Policy, please submit your inquiry or complaint to:

info@mycm.com, or

Mark Business Intelligence Systems
14747 N Northsight Blvd, Ste 111-134
Scottsdale, Arizona 85260
Attn: Data Protection Officer
+1 (888) 219-8024

We will respond to your inquiry or complaint within 30 days and inform you of the actions implemented to resolve it. If you have any questions regarding the resolution of your inquiry or complaint, please contact us.