Independent Insurance Agents & Brokers of America, Inc.

act. AGENTS COUNCIL FOR TECHNOLOGY

OFFICE OF THE GENERAL COUNSEL

MEMORANDUM REGARDING PRIVACY COMPLIANCE AND SAMPLE WEBSITE PRIVACY NOTICE

Prepared July 2018

This memorandum is not intended to provide specific advice about individual legal, business, or other questions. It was prepared solely as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional, such as an attorney, should be sought.

Background and Rationale

Privacy is a hot-button issue of late. Coming on the heels of several major data breaches and data use scandals, state, federal and international legislators and regulators are paying close attention to consumer privacy issues. Some notable laws emerging from this landscape include the following: the National Association of Insurance Commissioners' (NAIC) Insurance Data Security Model Law, the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, the California Consumer Privacy Act of 2018, and the European Union (EU) General Data Protection Regulation (GDPR), which is perhaps the most sweeping and onerous legislation to date.

The GDPR is intended to regulate companies that monitor, market to or otherwise offer any goods or services to EU citizens. EU regulators have the authority to impose stiff fines on violators who fail to comply with the GDPR's requirements, which include obtaining explicit consumer "opt-in" consent. Fortunately, the vast majority of independent agents in the US are not subject to the GDPR. For more on the potential impact of the GDPR, members may review an article on the topic from the Insurance Agents & Brokers, accessible **HERE**.

One key component of any effective compliance program is a privacy policy or notice, which serves as the external-facing statement of an agency's practices regarding the collection and use of consumer data. Although the GDPR has prompted a flurry of privacy policy updates, the US has not yet adopted any similar uniform data privacy laws. Instead, companies must comply with a patchwork of federal and state law concerning consumer privacy, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and an increasing number of state-specific requirements of which agents need to be aware. The failure to comply with a company's own stated privacy policy or privacy laws in general could result in government investigation or other potential liability. Of note, Title V of the GLBA establishes minimum notice and opt-out requirements for financial sector companies. For more information on the GLBA and its requirements, agents may review a memo on the topic from the IIABA's Office of General Counsel, accessible **HERE**.

A sample website privacy policy is attached as Exhibit A. This sample is focused on US requirements. While it includes some notes about the GDPR (*highlighted in blue*), merely adopting those changes and publishing a notice does not ensure compliance with the GDPR or other specific laws and regulations not expressly addressed therein. Any agencies subject to more specific privacy regulations should consult other resources and/or professionals and take all necessary action. Any questions regarding this sample should be directed to Ron Berg, Scott Kneeland or Eric Lipton. The Agents Council for Technology (ACT) also provides members with a wide variety of other resources regarding privacy and data security compliance via their "**Security and Privacy**" web pages.

EXHIBIT A

OFFICE OF THE GENERAL COUNSEL

SAMPLE WEBSITE PRIVACY POLICY/NOTICE

IMPORTANT DISCLAIMER. THIS DISCLAIMER MUST BE READ BEFORE YOU USE THE SAMPLE.

This sample privacy policy/notice ("Sample") has been prepared for IIABA member agencies for general information purposes only. This Sample may assist agencies that collect and use personal data from clients and potential clients, particularly through the use of a website, in establishing an external privacy policy/notice. The agency should ensure that any policy accurately reflects its own practices and procedures. The agency should also be sure to remove any IIABA guidance notes and post its privacy policy in a prominent location on its website with clear and conspicuous links. **The agency may need to take other action in connection with and in addition to adopting an appropriate privacy notice to comply with the requirements of specific state, federal or international privacy laws (such as the GDPR), to the extent applicable to the agency's business.**

By providing this Sample to member agencies, IIABA does not intend to provide, and is not providing, a legal opinion or legal advice, and it should not be acted upon or relied upon as such. The states where your agency conducts business and the carriers with which your agency transacts business may have legal, regulatory, contractual, or other requirements that provide for additional or different privacy policies and practices. Moreover, this Sample includes only general information and comments, and is not intended to provide specific advice about individual legal, business, or other questions. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional, such as an attorney, should be sought.

[Please see next page for sample resource.]

PRIVACY POLICY

[AGNECY NAME] ("Agency"), respects the privacy rights of individuals who visit, use, and interact with (collectively "Users") this website and/or portal ("Site"). Information may be collected from Users during their visits to this Site in order to allow the Agency to provide better service. The Agency is concerned about treating this information with care, so it has implemented this Privacy Policy ("Policy"). This Privacy Policy has been updated effective [DATE].

Types of Information Collected and How it is Used

[*NOTE: Unlike U.S. opt-out requirements, the GDPR requires explicit consent to collect and process the personal data of EU citizens, and such consent must be freely given, specific, informed and an unambiguous indication made by a statement or clear affirmative action, such as opt-in consent.*]

Aggregate Information: The Agency may collect information that is not personal information about Users to measure traffic on the Site. This information is collected automatically on an aggregate basis ("Aggregate Information") through the use of a "cookie" or small text file placed on the User's hard drive by the User's Internet browser. The cookie allows the Agency to track the number of hits or visits to various pages on the Site. The cookie is used only during a single connection to the Site, and is not used to track User activity after leaving the Site. The cookie is permanently disabled when the User exits the Site, and information about individual Users is not collected, saved or distributed to others by Agency except as provided for in this Policy. Aggregate Information helps Agency understand Users' needs, improve the Site, and demonstrate to others the volume and nature of Site traffic. Aggregate Information may be shared with third parties as described in the section called "Information Provided to Third Parties" below. [*NOTE: Agents should consult with their internal IT and/or external service provider to evaluate the Agency's data collection practices and ensure they comply with applicable regulations and are accurately reflected in the Agency's privacy policy.*]

User Information: User information from the Site may be obtained, retained, and/or used (collectively "Used") by the Agency to facilitate Users' access to, use of, and/or participation in any products/services/resources/surveys (collectively "Services") from the Site. Information about Users may be provided by the Agency to other entities, such as insurance carriers; vendors; agents/agencies brokers/brokerage firms and any others providing Services through the Site (collectively "Service Providers"), and such information may be Used by the Agency and Service Providers. [*NOTE: The GDPR requires a detailed description of what data is collected, the purposes and legal basis of any data collection, how the data is processed, including the existence of any automated decision-making, and the manner in which and how long the data is stored. The Agency may wish to inform consumers of what information is collected, such as: (i) Individual personal information, including but not limited to, names, addresses, telephone numbers, email addresses, and other identification details, such as date and place of birth, social security numbers, tax identification numbers, driver's license numbers and employment history; (ii) financial information, including but not limited to, credit card numbers, bank account numbers, income and credit score; (iii) insured risk and policy data, including but not limited to health data or other special demographic data.*]

Services Information: Information from Users on the Site may be Used by the Agency, such as, but not limited to, for processing requests for and/or participation in Services offered by or through the Agency, including, but not limited to, from Service Providers. Such information about Users also may be provided to and Used by Service Providers, as described in the section called "Information Provided to Third Parties" below.

E-mail Information: Information that the Agency receives from Users via e-mail may be Used by the Agency and may be provided to and Used by third parties as described in the section called "Information Provided to Third Parties" below.

Information about Children Under 13: Our Site is generally intended for adults interested in obtaining insurance and it is unlikely that children under the age of 17 will use the Site. It is the Agency's policy not to collect personal

information of children under age 13. If it is necessary to collect such personal information from a child identified as being under age 13, Agency will do so only after obtaining verifiable parental consent. If Agency becomes aware that it has inadvertently collected personal information from a child under age 13 without parental consent, such personal information will be deleted from Agency's system.

Information Provided to Third Parties: Information collected on this Site will only be provided to third parties in the manner specified in this Policy. Those who do not want their information shared in this manner should not provide the information. Information Used by Agency may be provided to third parties, such as, but not limited to, Service Providers. Information shared with such third parties may be Used to conduct business, including, without limitation: i) completing the transaction(s) requested by the User; and ii) serving Users and/or reporting on transactions, activities, and Services conducted with or facilitated by Agency. Agency also may disclose such information to comply with the law or legal process; to exercise Agency's legal rights or defend against legal claims; to enforce Agency's policies (including, without limitation, its Terms of Use); and/or to protect the rights, property or safety of others. [*NOTE: The GDPR requires more detailed disclosures about how personal data is shared, including safeguards taken and specific identification of third parties with whom data is shared.*]

Security

The Agency uses a combination of industry typical security measures to protect personal information it collects. Such measures will change from time to time. The Agency makes no representations or warranties of any kind, express or implied, that such measures will protect all personal information collected, however the Agency will make reasonable efforts to protect such information from unauthorized access.

Links to Other Sites

This Site contains links to Internet sites of Service Providers, other Agency partners/vendors, and other businesses and resources (collectively "Linked Resources"), and each Internet site of Linked Resources may have its own privacy and data collection policies and practices. The Agency is not responsible for the privacy and data collection policies and practices of any Linked Resources or for the content of their Internet sites. Users interested in the privacy and data collection policies and practices of Linked Resources should review the policies of the Internet sites they choose to access.

Agency makes no representations or warranties of any kind, express or implied, about the Internet sites of Linked Resources, and Agency disclaims all warranties and responsibilities of any kind, including, without limitation, warranties and responsibilities with respect to Linked Resources' Internet sites, content, privacy and data collection policies and practices, and actions. Links to other Internet sites, including, but not limited to, Linked Resources, do not imply Agency's endorsement or approval of such Internet sites or the resources and information contained within them, nor are such links or references indications that Agency has received specific authorization to provide these links or resources. Agency does not endorse, approve, certify or control such external Internet sites, and is not responsible for the accuracy, timeliness, completeness, efficacy, merchantability, usefulness, fitness for any particular purpose or correct sequencing of information located at such Internet sites. The links and references on this Site to other Internet sites, including, but not limited to, Linked Resources are provided solely as a convenience to Users of this Site.

Your Rights to Access and Amend Your Personal Information

You have the right to request access to the personal information that is maintained about you on this Site to ensure that it is accurate. Subject to certain exceptions required by law, and provided we can authenticate your identity, you also can request corrections, amendments or deletions of any personal information obtained through this Site or otherwise in our possession as appropriate. You may also request changes to your preferences regarding how we use or disclose your information or how we communicate with you.

To obtain access to, or seek to correct, amend, or delete any of your personal information, or for any other questions or concerns about the Agency's personal data policies and practices: Submit a request in writing to [CONTACT NAME/DATA PROTECTION OFFICER, AGENCY NAME AND EMAIL/ADDRESS]

[*NOTE: The GDPR requires the appointment of a Data Protection Officer (DPO) who is tasked with overseeing data security compliance within the company*]. The request must include your name; address; telephone number; the specific personal information at issue; the identity of the document or record that contains the disputed personal information; and the desired correction, amendment or deletion (along with any appropriate supporting documentation). We will notify you within 30 business days after receipt of your request with all required information to notify you whether we require additional information, have made the requested correction, amendment or deletion or that we cannot do so and the reasons for that decision.

Policy Changes

The Agency reserves the right to and may change this Policy at any time without notice to you, and changes will become effective when the revised Policy is posted on this Site. We may email periodic reminders or notices about changes, but you are encouraged to review this Policy frequently, so you are informed about the Agency's privacy practices and policies.