GDPR COMPLIANCE POLICY AND DATA INITIATIVES

PRIVACY POLICY UPDATES, INVENTORY DISCOVERY AND PERSONAL DATA

The European Union ("EU") sponsored General Data Protection Regulation ("GDPR") lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It also protects the fundamental rights and freedoms of natural persons, and in particular, their right to the protection of personal data.

The GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These rules are more detailed and specific than the verbiage found in typical data processing agreements ("DPA"), and they place an emphasis on making privacy notices easily understandable and accessible.

As of May 25, 2018, IT Knowledge Hub LLC, a Pennsylvania corporation doing business as "Knowledge Hub Media" (the "company"), on behalf of itself, its parents, subsidiaries, and other corporate affiliates, has taken all appropriate measures by updating its Terms of Use agreement and Privacy Policy to become fully GDRP compliant.

The GDPR carries provisions that require all businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. Furthermore, GDPR also regulates the exportation of all personal data outside of the EU.

Though not all "cookies" are used in a way that can personally identify user data, some potentially are. As such, these types of cookies are also subject to the GDPR compliance. This includes cookies for analytics, advertising, and functional services, such as survey and chat tools. We have taken appropriate measures by updating our Cookie Policy to become fully compliant with the new guidelines.

TERRITORIAL SCOPE

GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behavior as far as their behavior takes place within the Union.

Finally, GDPR applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

INITIATIVES FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) AND SENSITIVE PERSONAL DATA

In light of this legislation, the company has taken full inventory of its lead generation tactics, across all channels and sources, to ensure that its submission forms, opt-in practices, and data transfer processes are fully compliant with GDPR policy.

As a B2B publisher and content provider, the company does not process, transfer, or store any data defined as "sensitive personal information" (i.e., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, etc.).

However, the company does process some of the records and data fields that are identifiable under the GDPR's definition of Personally Identifiable Information ("PII"), such as the data subject's:

- First Name
- Last Name
- Email Address
- Telephone Number
- IP Address

The company does not, however, process or retain any other personally identifiable information – sensitive or otherwise – as defined by GDPR legislation. This includes, but is not limited to: credit card records, social security numbers, tax ID numbers, social media interactions and/or digital images as they relate to any single data subject.

FULLY COMPLIANT OPT-IN LANGUAGE AND SUBMISSION PROCESSES

The GDPR defines prospect consent strictly, and any company processing personal data must ensure that each lead data source uses language and processes that adhere to this definition:

> "The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it."

All indications of "consent" provided by the company involve a clear, affirmative action on behalf of the data subject.

Consent is unbundled and separate from the company's standard Terms of Use agreement. All opt-in boxes are distinct from "Terms of Use" popups, side boxes, and copy. Furthermore, opting in for any

type of communication is not a precondition for registering to download and/or receive onsite content, white papers, webinars, eBooks or any other gated research materials.

Furthermore, the GDPR specifically bans pre-ticked opt-in boxes. As such, the company has made all communication opt-in boxes unchecked by default for EU citizens.

Permissions language and processes provide granular options for data subjects to consent separately – for each different type of data processing, and from each party, publisher and/or advertiser.

The company clearly – and deliberately – names our organization, and any/all third parties who will be relying on the consent of the data subject.

Under GDPR legislation, prospects have the right to withdraw their consent. To ensure compliance, the company informs prospects about their right to withdraw, and provides them with easy ways to withdraw consent, at any time.

SECURE AND COMPLIANT DATA TRANSFER AND STORAGE PRACTICES

All PII is transferred and stored in a manner that keeps private data secure. Lead reports, and all other internal emails with PII are fully secured with Transport Layer Security (TLS) encryption. TLS is a symmetric cryptography transmission protocol which provides private data encryption - as well as preserved data integrity - between two communicating applications.

All third-parties are also required to comply with cross-border data transfer regulations, as prescribed by GDPR.

All direct data injections – and API calls – into any internal or external database, are also fully GDPR compliant. Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser, as such, all onsite and external forms are fully secured at the server level, via strict SSL encryption, from server to client.

DOCUMENTED GDPR COMPLIANCE MEASURES

Timestamps are recorded and maintained for all landing pages containing forms.

Furthermore, these records clearly show the language used, and processes required, for all prospects to opt in.

DATA PORTABILITY AND REQUESTED UPDATES TO PII RECORDS AND COMMUNICATION PREFERENCES

According to Article 20 of the GDPR, data subjects of the European Union have the right to receive the personal data concerning him or her, which he or she has provided to a controller. Knowledge Hub

Media upholds the right to data portability by providing all requested personal data in a structured, commonly used, and machine-readable format via an encrypted and fully secured request form.

Furthermore, the company also provides EU data subjects with a simple means to transmit their PII data to another controller, without hindrance from the controller from which the personal data has been provided.

Finally, EU data subjects have the right to update, delete and/or change their contact information and communication preferences at any time, and on a granular level. The company readily provides this opportunity to all EU data subjects via an encrypted and fully secured communication preferences request form.