Cryptome

19 March 2010

Source:

http://abraxasapps.com/safeharbor.pdf

Scope

This Policy outlines our general policy and practices regarding personal information entered into our United States based systems by European Economic Area ("EEA") subscribing customers, and personal information entered into our EEA based systems which may be accessed from the United States.

Definitions

For purposes of this Policy, the following definitions apply:

"AA" means Abraxas Applications, Inc., a Reston, VA based company in the United States.

"Personal Information" means any information or set of information (such as name, address, date of birth, social security number, etc.) that may be used to identify an individual. Personal information does not include information that is encoded or anonymized, or publically available information that has not been combined with non-public information.

"Sensitive Personal Information" means personal information that confirms race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, or that concerns health or sex life.

Notice

AA is a risk mitigation technology and services company that designs, builds and markets software products intended to prevent terrorist and other criminal attacks directed against critical infrastructure, key assets and personnel. Our flagship product, TrapWire, has been designed to provide a simple yet powerful means of collecting and recording suspicious activity reports. Once a suspicious activity in entered into the system it is analyzed and compared with data entered from other areas within a network for the purpose of identifying patterns of behavior that are indicative of pre-attack planning. Generally, no Personal Information or Sensitive Personal Information is recorded by the TrapWire system, and no such information is used by the system to perform its various functions. In the event a system user were to enter either Personal Information or Sensitive Personal Information in a comments field, AA will not share or expose that information to any other subscriber on the system, unless required by law, and, in any case, will otherwise adhere to Safe Harbor Privacy Principles with respect to that information.

Choice

Since AA systems, in general, do not capture or store Personal or Sensitive Personal Information, there will be very few (if any) opportunities to offer opt-in or opt-out choices to individuals. On the rare occasion where such information is entered into the system, it is likely to be recorded as law enforcement sensitive and will not be shared outside the law enforcement community. To the extent Personal or Sensitive Personal Information is entered into the TrapWire system, and is not designated as law enforcement sensitive, AA will not share that information with any third party.

Transfer To Third Parties

TrapWire is designed to share only suspicious activity data which does not include any Personal or Sensitive Personal Information. In the event Personal or Sensitive Personal Information is recorded by a system user, that information will not be shared or transferred to other than law enforcement or other authorized agencies as required by law.

Security

The data center housing the TrapWire infrastructure was constructed to the highest level of physical security standards. Access to the facility is controlled and logged through a system of biometric hand geometry readers, and the facility is carefully monitored by security officials on guard 24 hours per day, 7 days per week, 365 a year.

System Security is also of critical importance and is designed into all levels of the TrapWire application and infrastructure. All connections to the TrapWire application are made through a 128-bit encrypted SSL connection which terminates in a network DMZ. User authentication is performed from the DMZ and must be successful before a connection to TrapWire is permitted.

Implemented security processes are intended to protect any information in the TrapWire system from loss, misuse, unauthorized access, disclosure, alteration or destruction.

Data Integrity

AA, by design and intent, attempts to avoid the collection of Personal or Sensitive Personal Information by the products it produces. However, when such information is entered into a TrapWire system, reasonable steps are taken to assure that information is relevant for the purposes for which it is to be used. We do, however, depend on our users to update and correct any information they enter.

Enforcement

AA has established procedures for periodically verifying the implementation of and compliance with the Safe Harbor principles. We conduct an annual self-assessment of our practices with respect to Personal and Sensitive Personal Information to verify that representations we make about our privacy practices are true and that related privacy policies have been implemented as represented.

Individuals may file a complaint with our Privacy Office at the address below. AA will investigate and attempt to resolve complaints and disputes in accordance with the principles contained in this Policy. If a dispute cannot be resolved by this process we will participate in the dispute resolution procedures of the panel established by the European Data Protection Authorities.

Limitations

Adherence by AA to these Safe Harbor Principles may be limited (a) to the extent required to respond to a legal or ethical obligation; and (b) to the extent expressly permitted by an applicable law, rule or regulation.

Contact Information

Please direct any questions or comments regarding this Policy to our corporate office:

Abraxas Applications, Inc.

1875 Campus Commons Drive – Suite 301

Reston, VA 20191

Attn: Legal Department/Safe Harbor

Amendments

This policy may be amended from time to time to remain consistent with the requirements of the Safe Harbor Principles. A notice will be posted on our website (www.abraxasapps.com) for 60 days whenever this Safe Harbor Policy is changed in any material way.

Effective Date

1 April 2008