

IDV SAFE HARBOR PRIVACY POLICY

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:

"**IDV**" means **International DataVault, Inc.**, a Nashville, TN 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 publicly 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

IDV is a Remote Data Backup and Recovery service that offers products intended to prevent business or personal data loss and aids in disaster recovery for its Clients. Our flagship product, **IDV Backup Pro**, has been designed to provide a simple yet powerful means of securing Client data against catastrophic loss. Before a Client's data is entered into the system it has been encrypted with a key that **ONLY** the Client can access. No Personal Information or Sensitive Personal Information is recorded on our systems unencrypted, 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, **IDV** will not share or expose that information to any other subscriber on the system or any 3rd party, unless required by law, and, in any case, will otherwise adhere to Safe Harbor Privacy Principles with respect to that information.

Choice

Since **IDV** 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 **IDV** system, and is not designated as law enforcement sensitive, **IDV** will not share that information with any third party.

Transfer To Third Parties

IDV is designed not to allow the sharing of any Client data, with the sole exception being Law Enforcement. And then, only when subpoenaed by such Enforcement Agencies. In the event Personal or Sensitive Personal Information is recorded by a system user, that information will not be shared or transferred other than to law enforcement or other authorized agencies as required by law.

Security

The data centers housing the **IDV** infrastructure are all constructed to the highest level of physical security standards. (All are Carrier Grade facilities.) Access to the facilities is controlled and logged through a system of biometric hand geometry readers, and they are 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 **IDV** application and infrastructure. All connections to the **IDV** application are either made directly on the Clients system or through an encrypted SSL connection which terminates in a network DMZ. User authentication is performed from the DMZ and must be successful before a connection to **IDV** Servers is permitted. Implemented security processes are intended to protect any information in the **IDV** system from loss, misuse, unauthorized access, disclosure, alteration or destruction.

Data Integrity

IDV, 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 **IDV** 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

IDV 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. **IDV** 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 **IDV** 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:

International DataVault, Inc.
Box 33
Nashville, TN 37202-00331
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.usdatavault.com) for 60 days whenever this Safe Harbor Policy is changed in any material manner.

Effective Date for this modified Document is: 15 December 2008

Copyright 2008-2009 International DataVault, Inc.