

CREDANT Solutions for Safe Harbor Compliance

Data security is a global issue in today's economy.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that Safe Harbor encryption and security mandates are consistently and efficiently enforced – regardless of where the data resides.

Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

CMG's Intelligent Encryption provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CRE DANT, organizations can:

- › Ensure data security without the risk of users placing data in areas that are not encrypted.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

The European Commission's Directive on Data prohibits the transfer of personal data to non-European Union nations that do not meet the European adequacy standard for privacy protection. In response, the U.S. Department of Commerce consulted with the European Commission to develop a "safe harbor" framework as a way for U.S. companies to continue their business dealings with the EU. Certifying to the safe harbor assures EU organizations that U.S. companies provide "adequate" privacy protection, as defined by the EU's Directive.

The compliance challenge

Multinational organizations routinely share a vast array of personal information among their different offices and with customers, suppliers and business associates across the Internet. However, nations around the world are increasingly concerned about information privacy. Converging technologies and mobile communications have increased the risk and opportunity for the illegal access, corruption and theft of sensitive personal data ranging from credit card numbers to medical records.

To ensure consistency between how U.S. and European organizations safeguard their data, the EU Directive includes seven broad principles for data protection. These principles apply to all data processing (on-line and off-line, manual as well as automatic) and to all organizations holding personal data. Under the Directive, personal data includes information such as medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union memberships. The principle for security applies to how an organization stores, processes, maintains and protects customer information. The principle for data integrity requires that "an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current."

The stakes are high for Safe Harbor compliance. The European Union and the U.S. have the largest bilateral trade relationship in the world. Trade flowing across the Atlantic amounts to almost \$2 billion every day. [Source: http://ec.europa.eu/trade/issues/bilateral/countries/usa/index_en.htm]

CREDANT

More than 700 enterprises and government agencies – including 50 of the Global 500 – rely on CRE DANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.