PGP® Compliance Brief

June 2008

E.U. Data Protection Directive 95/46/EC

Overview

The European Union Data Protection Directive 95/46/EC of 1995 requires that, “Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”[1]

The directive requires that E.U. member states (countries) protect the privacy of personal information that is processed using equipment in the member state, whether the processing is done by government agencies, businesses, or other organizations. “Personal data” includes, but is not limited to, name, address, phone numbers, email addresses, ethnicity, religion, gender, sexual orientation, birthdates, employment, and financial account numbers. The responsibility for compliance with the directive rests with the "controller," which is the person, group of people, public authority, agency, or other body that determines the purposes and means of processing personal data.

E.U. member states have implemented this directive to varying degrees. It is beyond the scope of this paper to outline the differences and status of their implementations; the information is available from each country. Organizations and businesses using equipment in member states to process personal data are concerned about compliance with the directive and its derivative laws. Most are equally concerned about data protection for the purposes of maintaining business integrity and brand value.

Only encryption can protect data itself. Encryption protects personal or other data by rendering it unreadable to unauthorized users who do not have the key. The Ponemon Institute found that enterprises that implement a strategic approach to encryption experience fewer data breaches, and that most of them seek a single solution for encryption to implement their data protection strategy.[2] As the leader in encryption solutions for enterprise data protection, PGP Corporation offers a platform-based solution that addresses the needs for compliance and brand protection.

Highlights

Directive 95/46/EC requires organizations to protect the integrity of personal data and take steps to prevent unauthorized access to it. Following are some of the requirements:

- “Member States …must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. …Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.”[3]
- Sending personal information from a member state to a non-member country is legal only with the consent of those persons whose data is sent. Furthermore, the data may only be sent to countries with similar laws protecting personal information.
- Individuals have the right to give their consent for the use and storage of personal information, and to revoke consent at any time.
- Penalties for violating member states’ directive implementations include fines and criminal liability for business owners or executives, data controllers, and employees who report to them.

Why Enterprise Data Protection?

Certain highly publicized data breaches have prompted some member states to strengthen their implementations of the directive. A consequence of the inconsistent regulatory environment across member states is that businesses and organizations have a heightened concern with compliance and avoiding embarrassing data breaches that result in brand damage, customer churn, litigation, and lower revenues. These consequences can be quite costly. Research by The Ponemon Institute concluded that the average cost of a 2007 data breach in the United Kingdom reached an average £47 per record compromised, costing an average of £1.4 million per incident.[4]

Multinational businesses can best avoid such consequences by implementing and enforcing a strategic enterprise data protection strategy that establishes policies that comply with the strictest implementations of the directive.

Encryption, combined with digital signature technology to ensure data integrity, is most effective as the foundation of an enterprise data protection strategy, which includes the processes and technologies that work in tandem to ensure data security. An effective strategy must include all four of these components:

- **Protection** of the data itself through encryption
- **Controlled Access** to data with strong authentication and authorization systems
- **Detection** of data at risk to prevent data leakage
- Comprehensive **Management** of data throughout its lifecycle from its creation through archive

Best Practices

To protect the privacy and integrity of personal information, member states such as the United Kingdom recommend following the ISO/IEC 17799:2005(E) standard,[5] which has been incorporated into the ISO/IEC 27002 standard. It lists a comprehensive set of best practices for securing the entire IT infrastructure, systems, and data. The best practices that pertain to data encryption include the following:[6]

Cryptographic Security Policies

- Assess applications and data sources and identify personal data.
- Conduct a risk assessment and identify the required level of protection, taking into account the type, strength, and quality of the encryption algorithm.
- Establish role-based change management processes on a “least-privilege” access basis. Individuals should be restricted to actions that allow them to do their jobs, but nothing further.
- Use encryption to protect sensitive information transported by mobile or removable media or devices, or across communication lines.

- Establish key management policies, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised, or damaged keys. This policy should also address long-term protection and recovery of archived data.

Message Integrity

- Identify requirements for ensuring authenticity and protecting message integrity in applications; then identify and implement appropriate controls.
- Encrypt messages containing confidential information to prevent unauthorized access and modification by a third party.

Key Management

- Protect all cryptographic keys against modification, loss, and destruction.
- Protect secret and private keys against unauthorized disclosure. Physically protect equipment used to generate, store, and archive keys.
- Define activation and deactivation dates for keys, so that the keys can only be used for a limited period of time.
- In addition to securely managing secret and private keys, consider how to verify the authenticity of public keys.

Why PGP Encryption?

PGP Corporation is the leading vendor of data and email encryption solutions worldwide. Its award-winning solutions free organizations from the embarrassment of data breaches and the penalties associated with violating implementations of Directive 95/46/EC.

PGP® encryption applications are managed through the central PGP® Encryption Platform. This flexible platform enables phased deployment of encryption applications. For example, an organization may begin with encrypting its email in transit, and later use the same platform to extend encryption to laptop computers and USB drives. Major features of the PGP Encryption Platform include:

- Centralized policy and key management
- Centralized logging and auditing of encrypted devices
- Standards-based encryption of data in transit and at rest, even beyond the enterprise network
- Patented PGP Additional Decryption Key (ADK) technology that ensures access to data protected by lost or forgotten keys
- Integrated digital signatures to verify data integrity

PGP encryption applications that can help protect organizations violations of Directive 95/46/EC include the following:

- PGP® Whole Disk Encryption: Enables encryption of files on desktop and laptop computers and removable media
- PGP® Endpoint: Prevents data loss resulting from the use of unauthorized devices and connections
- PGP® Mobile: Provides proven, easy-to-use data encryption for smartphones
- PGP Universal™ Gateway Email: Automatically encrypts email messages, without requiring client software
- PGP® Desktop Email: Provides automatic end-to-end encryption of email messages
- PGP® Support Package for BlackBerry®: Extends PGP Desktop Email functionality to BlackBerry devices
- PGP® Command Line: Encrypts and signs information for data storage, FTP transfer, and backup
- PGP® NetShare: Encrypts network-based files and folders for collaborating teams

PGP invites peer review of its source code, which is available online for download at http://www.pgp.com/downloads/sourcecode/index.html.

Learn more about enterprise data protection and PGP data encryption solutions at www.pgp.com, or contact your PGP account representative.

References

[1] http://www.cdt.org/privacy/eudirective/EU_Directive_.html, Chapter 1.

[2] The Ponemon Institute, *2008 Annual Study: U.K. Enterprise Encryption Trends,* April 2008, and *2008 Annual Study: German Enterprise Encryption Trends,* May 2008. Download at: http://www.pgp.com/downloads/research_reports/ponemon_reg_direct.html.

[3] http://www.cdt.org/privacy/eudirective/EU_Directive_.html, Chapter 17.1

[4] The Ponemon Institute, *2007 Annual Study: U.K. Cost of a Data Breach*, February 2008. Download at: http://www.pgp.com/downloads/research_reports/ponemon_reg_direct.html.

[5] http://www.out-law.com/page-409

[6] *Information technology — Security techniques — Code of practice for information security management*, ISO/IEC 27002, First Edition International Standard, June 15, 2005.