EMULEX®

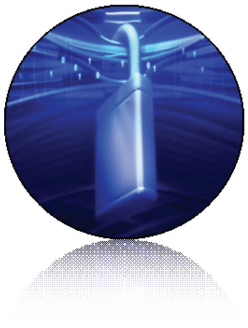
When Data Crosses International Borders, Look to Best-practice Security Solutions

At a Glance

As businesses become more global, as more security breaches occur and as thieves steal more money from companies and citizens of countries around the world, international data protection laws will become more important for two reasons:

1) Today almost every large company either does business globally or plans to do so in the future.
2) As new laws on data protection are developed in different countries, these new laws can be predictors of legal trends and laws internationally.

This paper is an overview of some pertinent global legal trends and laws as well as regional laws from the European Union (E.U.) and industry standards such as PCI that cover credit card transactions, no matter where they occur. Overall, when considering data security and encryption processes internationally, it is best to work with experts in compliance for each country with which you intend to do business.



EU Directive on Data Privacy

The European approach to privacy is more comprehensive than many other countries and unions. First, cybersecurity legislation is accomplished primarily through privacy laws in Europe. In Europe, privacy has always been considered to be a fundamental human right, and ECHR 1950 enforces this view across the European Community. The ECHR 1950 refers to The European Convention on Human Rights ROME 4 November 1950 that defined basic rights across Europe. While the EU Directive on Data Privacy directly impacts member states in the EU, several countries outside the EU follow the EU model, as it is seen as more comprehensive.

The EU Directive on Data Privacy is covered in two separate pieces of legislation:

1) 95/46/EC The Generic Data Protection Directive
2) 2002/58/EC The specific Data Protection Directive

The Generic Directive covers all sectors, while the Specific Directive covers only electronic communications. Overall, these directives cover the complete information lifecycle. The critical component that IT security professionals should be aware of is that after data is collected and processed, it must be secured. When securing personal information for the EU Directive, organizations must adhere to technical and organizational measures, and protect against data loss. For data center security, encrypting data for security and protection against data loss are essential pieces of the solution.

For each country in the EU, a separate national authority is created, and the U.K. Data Protection Act and the ICO are good examples of how this was accomplished in the U.K.

For EU data that leaves the EU, adequate data protection is required. To make this more complex, there are numerous agreements between the EU and other countries, such as the U.S., that affect how the EU Directive on Data Privacy impacts companies in different countries. The example of the Google executives being tried in an Italian court exemplifies how complex this really is. At the end of the day, following established best practices is an effective way to address the additional security requirements that companies face by doing business in the EU.

Data Protection Act (U.K.)

The 1998 Data Protection Act came into force early in 1999 and covers how information about living identifiable persons is used. It is much broader in scope than the earlier 1984 act, but does contain some provision for a transitional period for compliance with the new requirements. Although the Act itself does not mention privacy, it was enacted to bring U.K. law into line with the European Directive of 1995,

When Data Crosses International Borders, Look to Best-practice Security Solutions

which required member states to protect people's fundamental rights and freedoms, and in particular, their right to privacy with respect to the processing of personal data. Note that this act was passed nearly five years before the first U.S. data security breach disclosure law was passed in California, illustrating how many other countries may have more stringent requirements than what organizations face in the U.S.

The Data Protection Act gives individuals the right to know what information is held about them, and it provides a framework to ensure that personal information is handled properly. The important provision for IT security professionals is the section of the Act that states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

The critical aspect of this act is that personal information must be secure. Since there isn't a specific definition of "secure," and data cannot be transferred to other countries without adequate protection. IT security professionals will need to apply best practices for security, including the encryption of personal information that needs to be protected.

A new provision that allows for fines of up to £500,000 for any organization found to have committed a serious breach of the DPA should not be overlooked by companies. At worst, a breach will result in a fine of £500,000 ($800,000) by the ICO, though the first limitation to this provision is that only the worst data breaches will attract such a harsh penalty. Most fines will be much lower, so the headline figure is less imposing than at first glance.

Summary of U.K. Regulation of Investigatory Powers Act 2000, Part III

In 2000, the British government passed the Regulation of Investigatory Powers Act (RIPA), which covers the interception, surveillance, acquisition and disclosure of communications related to computer crime. Parts I and II are already in force, but Part III (hereafter referred to as RIPA 3), entitled the "Investigation of Electronic Data Protected by Encryption etc." requires the British Home Office to issue an order to begin enforcement.

The entire act has been mired in controversy since its introduction. Groups including Amnesty International, the British press and the Internet Service Providers Association have publicly challenged it. That controversy continues today with the debate on enforcing RIPA3.

Control of encrypted communications has been a goal of the British government for many years. The Electronic Communications Act of 2000 gave government the right to regulate companies selling encryption services. The powers in this act were subject to a five-year "sunset clause," which ran out in May 2005. The government is now looking to move RIPA 3 into force, which can be done by ministerial order, and without the involvement of Parliament.

RIPA 3 gives the police powers to order the disclosure of encryption keys or force suspects to decrypt encrypted data. Anyone who refuses to turn over keys to the police can be imprisoned for two to five years under RIPA and anti-terrorism legislation.

Opponents of the RIPA have argued that the police could struggle to enforce Part 3, as people can argue that they don't possess the key to unlock encrypted data in their possession. "It is, as ever, almost impossible to prove 'beyond a reasonable doubt' that some random-looking data is, in fact, cipher text and then prove that the accused actually has the key for it--and that he has refused a proper order to divulge it," encryption expert Peter Fairbrother pointed out on UKcrypto, a public e-mail discussion list. It is still not clear what the impact of Part III will be, but it should be taken into account when encryption is considered.

SECURITY IMPLICATIONS

RIPA 3 covers the recovery of encrypted information and may impact how companies store their keys and the encryption algorithms used to encrypt data, and may require storage of these two items for many years. More clarification is expected as RIPA's enforcement is clarified.

Helpful Resources:
The full text of the current regulation can be found at http://www.opsi.gov.uk/acts/acts2000/00023--e.htm.

Basel II

ISO 17799/ISO27001
ISO 17799 is actually a comprehensive set of controls comprising best practices in information security. It is, essentially, an internationally recognized generic information security standard. These are just a few of the pertinent controls that are specified:

- A policy on the use of cryptographic controls for the protection of information shall be developed. (Sec. A.10.3.1)

When Data Crosses International Borders, Look to Best-practice Security Solutions

- Encryption shall be applied to protect the confidentiality of sensitive or critical information. (Sec. A.10.3.2)
- Digital signatures shall be applied to protect the authenticity and integrity of electronic information. (Sec. A.10.3.3)
- A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques. (Sec. A.10.3.5)

Conclusion:

With literally thousands of privacy and security laws in place around the world, it can be complex to understand all of the requirements and implement a successful privacy and security strategy. However, there are a few things that can be done to make navigating this process a lot easier. First, remember to work with experts in compliance for each of countries with which you intend to do business. Pay particular attention to those countries that are at the forefront of privacy and security laws. Second, employ best-practices security solutions. By picking the best available technology, you are in a great position for compliance with the most stringent requirements across the world.

Emulex Host-based Encryption Solutions

Emulex has revolutionized the way data is secured with the release of host-based encryption solutions. Emulex OneSecure adapters protect data where it is created—in the server and in hardware—and protects it no matter where the data goes outside the server, improving the data center security stance against data theft and loss. Because encryption is done as close to the data source as possible, it meets the Storage Networking Industry Association (SNIA) best practices standard, and aligns with the National Institute of Standards and Technology (NIST) requirements for hardware protection of keys. For more information on Emulex security products go to http://www.emulex.com/solutions/it-initiatives/emulex-security-solutions.html

Useful Resources for International Data Protection/Privacy Laws

Argentina: Personal Data Protection Act of 2000 (aka Habeas Data)

Austria: Data Protection Act 2000, Austrian Federal Law Gazette part I No. 165/1999 (Datenschutzgesetz 2000 or DSG 2000).

Australia: Privacy Act of 1988

Belgium: Belgium Data Protection Law and Belgian Data Privacy Commission Privacy Blog

Brazil: Privacy currently governed by Article 5 of the 1988 Constitution.

Bulgaria: The Bulgarian Personal Data Protection Act, was adopted on December 21, 2001, and entered into force on January 1, 2002. More information at the Bulgarian Data Protection Authority.

Canada: The Privacy Act - July 1983, Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (Bill C-6)

Chile: Act on the Protection of Personal Data, August 1998

Colombia: Two laws affecting data privacy: Law 1266 of 2008 (in Spanish) and Law 1273 of 2009 (in Spanish) Also, the constitution provides any person the right to update their personal information.

Czech Republic: Act on Protection of Personal Data (April 2000) No. 101

Denmark: Act on Processing of Personal Data, Act No. 429, May 2000

Estonia: Personal Data Protection Act of 2003. June 1996, Consolidated July 2002.

European Union: European Union Data Protection Directive of 1998, EU Internet Privacy Law of 2002 (DIRECTIVE 2002/58/EC), with a discussion here.

Finland: Act on the Amendment of the Personal Data Act (986) 2000.

France: Data Protection Act of 1978 (revised in 2004)

Germany: Federal Data Protection Act of 2001

Greece: Law No.2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997

Guernsey: Data Protection (Bailiwick of Guernsey) Law of 2001

Hong Kong: Personal Data Ordinance (The "Ordinance")

Hungary: Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests (excerpts in English)

Iceland: Act of Protection of Individual; Processing Personal Data (January 2000)

When Data Crosses International Borders, Look to Best-practice Security Solutions

Ireland: Data Protection (Amendment) Act, Number 6 of 2003

India: Information Technology Act of 2000

Italy: Data Protection Code of 2003, Processing of Personal Data Act, January 1997

Japan: Personal Information Protection Law (Act) (Official English Translation) Law Summary from Jonesday Publishing; Law for the Protection of Computer Processed Data Held by Administrative Organs, December 1988.

Korea - Act on Personal Information Protection of Public Agencies Act on Information and Communication Network Usage

Latvia: Personal Data Protection Law, March 23, 2000

Lithuania: Law on Legal Protection of Personal Data (June 1996)

Luxembourg: Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data

Malaysia - Common Law Principle of confidentiality Draft Personal Data Protection Bill (not finalized) Banking and Financial Institutions Act of 1989 privacy provisions

Malta: Data Protection Act (Act XXVI of 2001), amended March 22, 2002, November 15, 2002, and July 15, 2003

Morocco: Data Protection Act

Netherlands: Personal Data Protection Act 2000

New Zealand: Privacy Act, May 1993; Privacy Amendment Act, 1993; Privacy Amendment Act, 1994

Norway: Personal Data Act (April 2000) - Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act)

Philippines: No general data protection law, but there is a recognized right of privacy in civil law.

Poland: Act of the Protection of Personal Data (August 1997)

Portugal: Act on the Protection of Personal Data (Law 67/98 of 26 October)

Romania: Law No. 677/2001 for the Protection of Persons Concerning the Processing of Personal Data and the Free Circulation of Such Data

Singapore - The E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce. Other related Singapore Laws and E-commerce Laws.

Slovak Republic: Act No. 428 of 3 July 2002 on Personal Data Protection

Slovenia: Personal Data Protection Act , RS No. 55/99

South Korea: The Act on Promotion of Information and Communications Network Utilization and Data Protection of 2000

Spain: ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data

Switzerland: The Federal Law on Data Protection of 1992

Sweden: Personal Data Protection Act (1998:204), October 24, 1998

Taiwan: Computer Processed Personal data Protection Law - applies only to public institutions.

Thailand: Official Information Act (1997) for state agencies (personal data protection bill under consideration)

United Kingdom: UK Data Protection Act 1998, Privacy and Electronic Communications (EC Directive) Regulations 2003 official text and a consumer-oriented site at the Information Commissioner's Office

Vietnam: The Law on Electronic Transactions 2008

World Headquarters 3333 Susan Street, Costa Mesa, CA 92626 +1 714 662 5600
Wokingham, UK +44 (0) 118 977 2929 | **Munich, Germany** +49 (0) 89 97007 177
Paris, France +33 (0) 158 580 022 | **Beijing, China** +86 10 68499547
Tokyo, Japan +81-3-5325-3261 | **Bangalore, India** +91 80 40156789

Connect with Emulex

twitter.com/emulex friendfeed.com/emulex bit.ly/emulexlinks bit.ly/emulexfb

EMULEX®

www.emulex.com

11-0380 · 10/10