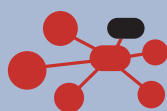


# SECURITY + DATA PRIVACY COMPLIANCE GUIDE

By Alex Teu, Director of Sales & General Counsel, LeapFILE, Inc.

In today's digital environment, it's easier and more convenient than ever to share, access, and store data. Many organizations depend on technologies that make the data easily accessible and communicated to colleagues, partners, and clients in order to go about their daily business. However, transferring private client information and confidential documents electronically does not come without pitfalls. Identity theft has been on the rise and the need for greater transparency and accountability in the handling of sensitive private data calls for stricter security controls. Legislative bodies at the state, federal, and even international level are now requiring businesses to take both proactive and reactive measures to address the concerns around data privacy.

Many organizations are either not aware of these regulations or don't know how to effectively address this issue. Yet this does not excuse them from complying with these requirements. Thus, this resource is a guide to the various regulations requiring data encryption and privacy breach notification laws, as well as providing some best practices for implementing a secure environment for private data.



**LeapFILE**™

*Service On Demand*

# SEVEN BEST PRACTICES FOR SECURING PRIVATE DATA

## 1 Use Encrypted Transfer Methods

Identify acceptable methods of transferring or communicating private data. Only transmit private data electronically via encrypted channels. Standard email and ftp systems do not have security measures or encryption, nor does instant message clients.

## 2 Track All Access to Private Data

Implement systems for auditing and tracking all access and communication of private data, including the ability to detect and report incidents of unauthorized access. You should be able to know exactly who accessed private data, what data was accessed, and when it was accessed.

## 3 Physically Protect Where Data is Located

Lock and password-protect unattended computers or other data storage media containing private data, even if the user is away for a few minutes. This is especially critical if the storage media is in a location that is accessible by the public.

## 4 Establish Protection Safeguards

Protect your organization against malware, viruses, network breaches, etc., by installing and updating anti-virus software on all computers, restricting the use of non-approved file sharing or P2P programs or even certain websites, setting up firewalls, closing commonly open ports to your IT infrastructure, etc.

## 5 Manage User Profiles

Centrally monitor user IDs, passwords, and access levels to private data. For example, terminated employees should have their IDs and access immediately blocked or disabled. Larger firms typically utilize an active directory server to easily manage user profiles.

## 6 Select Reliable Solution Vendors

If you are using a solution from a third party service provider to transfer or store private data, stick to those that have a track record for reliability and strong industry reputation for supporting data security. SAS70 certification, service level agreements (SLAs), and an established presence in your industry are good indicators of a trustworthy and reliable service provider.

## 7 Train Your Staff on Security Guidelines

Having a comprehensive security policies program is useless if your employees do not know about it or abide by it. Communicate and train your staff on proper security procedures, including educating users about phishing scams and not clicking or opening suspicious emails or links, keeping passwords in a safe location (a post-it note on your desk is NOT secure), making sure that laptops or laptop bags are not left in open view in cars or unattended locations, etc.

Stay up-to-date with security and data privacy laws as well as learn best practices from others. Learn more and join our discussion group at

<http://www.leapfile.com/Data-Security-Compliance>

# SECURITY + DATA PRIVACY

## ENCRYPTION REQUIRED FOR THE ELECTRONIC TRANSMISSION OF PERSONAL DATA

State laws requiring protection or encryption of personal data as a preventative measure

There is no national data protection law at the moment, but two states are adopting their own legislation. However, the scope of the both laws cover all persons (or companies) that own, license, store or maintain personal information about a resident of the state, which essentially means that any business outside of those states who has data on clients residing within that state needs to comply with the law. Please verify with your state legislature on the details of the governing act.

State	Regulation	Summary
Massachusetts	<a href="#">Mass. 201 CMR 17</a>	The Massachusetts Office of Consumer Affairs and Business regulation (OCABR) extended the deadline for compliance to Mass. 201 CMR 17 to January 1, 2010.  This state law requires the data of MA residents be protected (notably by encryption) by “persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts,” is said to be the strictest data security law in the country.  Section 17.04 – Part (3) of Computer System Security Requirements mandates encryption for all records and data containing personal information transmitted wirelessly as well as across all public networks. Part (4) requires a reasonable monitoring of systems, for unauthorized use of or access to personal information.
Nevada	<a href="#">NRS 597.970</a>	Restrictions on personal information transferred through electronic transmission - A business in this State shall not transfer any personal data through an electronic transmission outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.  Effective October 1, 2008

## DATA SECURITY BREACH NOTIFICATION

State laws and regulations mandating notification of security breaches of personal information

Most of these laws require persons who conduct business to notify consumers or customers of breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by the business. Typically, these laws not only apply to the company based in that state, but also apply if a business has customers or even one employee in that state. Most of these acts are a result of prior bills passed to prevent identity theft. Please verify with your state legislature on the details of the governing act.

State	Regulation	State	Regulation
Alaska	<a href="#">2008 H.B. 65, Alaska Stat. §45.48.010</a>	Nebraska	<a href="#">L.B. 876, Neb. Rev Stat. 87-801 et seq.</a>
Arizona	<a href="#">SB 1338, Ariz. Rev. Stat. § 44-7501</a>	Nevada	<a href="#">SB 347, Nev. Rev. Stat. 603A.010 et seq.</a>
Arkansas	<a href="#">SB 1167, Ark. Code Ann. § 4-110-101 et seq.</a>	New Hampshire	<a href="#">HB 1660 FN, NH RS 359-C:19 et seq.</a>
California	<a href="#">SB 1386, SB 20, Cal Civil Codes 1798.29, 1798.80-1798.84</a>	New Jersey	<a href="#">N.J. Stat. 56:8-163</a>
Colorado	<a href="#">Co. Rev. Stat. §6-1-716(1)(a)</a>	New York	<a href="#">A4254, A3492, NY Bus. Law Sec. 899-aa</a>
Connecticut	<a href="#">Con. Gen. Stat. §36a-701.</a>	North Carolina	<a href="#">SB 1048, N.C. Gen. Stat. 75-65</a>
Delaware	<a href="#">Del. Code Ann. Title 6 Section 12B-101 to 12-B-106.</a>	North Dakota	<a href="#">SB 2251, N.D. Cent. Code 51-30-01 et seq</a>
District of Columbia	<a href="#">DC Code Sec 28-3851 et seq.</a>	Ohio	<a href="#">HB 104, Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192</a>
Florida	<a href="#">Fla. Stat. Ann. 817.5681 et seq.</a>	Oklahoma	<a href="#">HB 2245, HB 2357, Okla. Stat. 74-3113.1</a>
Georgia	<a href="#">SB 230, Ga. Code Ann. 10-1-910 et seq.</a>	Oregon	<a href="#">SB 583</a>
Hawaii	<a href="#">Haw. Rev. Stat. Sec 487N et seq.</a>	Pennsylvania	<a href="#">SB 712, 73 Pa. Cons. Stat. 2303</a>
Idaho	<a href="#">Idaho Code Ann. §28-51-104 to 28-51-107</a>	Rhode Island	<a href="#">H. 6191, RI Gen. Law 11-49.2-1 et seq</a>
Illinois	<a href="#">ILCS Sec. 530/1 et seq.</a>	South Carolina	<a href="#">2008 S.B. 453, Act 190</a>
Indiana	<a href="#">Ind. Code Sec. 24-2-9 et seq., 4-1-11 et seq.</a>	Tennessee	<a href="#">SB 2220, Tenn. Code § 47-18-2107</a>
Iowa	<a href="#">Iowa Code § 715C.1 (2008 S.F. 2308)</a>	Texas	<a href="#">SB 122, Tex. Bus &amp; Com. Code Ann. 4-48-103, 48.001 et seq.</a>
Kansas	<a href="#">SB 196, Kansas Stat. 50-7a01, 50-7a02.</a>	Utah	<a href="#">SB 69, Utah Code 13-44-101 et seq</a>
Louisiana	<a href="#">La. Rev. State. Ann. Sec. 51:3071 et seq.</a>	Vermont	<a href="#">Vt. Stat. Tit 9 Sec. 2435</a>
Maine	<a href="#">Me. Rev. Stat. Ann. 10-21-B-1346 to 1349</a>	Virginia	<a href="#">Va. Code § 18.2-186.6</a>
Maryland	<a href="#">Md. Code, Com. Law § 14-3501 et seq</a>	Washington	<a href="#">SB 6043, Wash. Rev. Code § 19.255.010</a>
Massachusetts	<a href="#">HB 4144, Mass. Gen. Laws § 93H-1 et seq.</a>	West Virginia	<a href="#">W.V. Code §§ 46A-2A-101 et seq.</a>
Michigan	<a href="#">Mich. Comp. Laws § 445.72</a>	Wisconsin	<a href="#">SB 164, Wis. Stat. § 134.98 et seq.</a>
Minnesota	<a href="#">H.F. 2121, Minn. Stat. 325E.61 et seq.</a>	Wyoming	<a href="#">Wyo. Stat. § 40-12-501 to -501</a>
Montana	<a href="#">HB 732, Mont. Code § 30-14-1701 et seq.</a>		

\* States with no security breach law: Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota.

## FEDERAL REGULATIONS

Healthcare Insurance Portability and Accountability Act (HIPAA)	Limits the use and disclosure of individually identifiable information relating to the physical or mental health of individuals absent the consent or authorization from the patient.  Requires all records be managed as part of the organization’s official records management program.  Requires training to ensure employees are aware of the requirements.  Security Rules under the Act became effective in April 2006.  Applies to doctors, hospitals, pharmacies, medical billing services, health care plans, HMOs, and business associates of these entities such as their accountants and attorneys.  Imposes strict data disposal requirements, including overwriting or physically destroying all magnetic media that is no longer in use or that is given away or sold.
Gramm-Leach-Bliley Act (GLBA)	Requires financial institutions to ensure the security and confidentiality of customers’ non-public, personal information.  Organizations are required to automatically send privacy notices to customers.  Harm caused by “identity theft” has led the federal government to create mandates such as this to prevent the negligent disclosure of private information.
Sarbanes-Oxley Act (SOX)	Implements multiple sweeping reforms for public companies, auditors, board members and lawyers.  Applies to all U.S. and non-U.S. public companies that have issued securities in the U.S. public markets and are required to file periodic reports with the SEC.  Prescribes a system of federal oversight of public auditors.  Imposes new criminal penalties relating to fraud, conspiracy, destruction of evidence and interfering with investigations.  Requires management to establish and maintain internal control structure and procedures for financial reporting.  Requires establishment of a process for employees to submit, in confidence and with anonymity, concerns regarding questionable accounting matters.

## INTERNATIONAL BUSINESS REGULATIONS

These regulations apply to companies that conduct business or have clients located in these countries.

Safe Harbor Act	In October 1998, the European Union passed the EU Data Protection Directive. It places requirements on businesses that process personal data from an EU Member State.  The transfer of personal information from an EU Member State to a non-EU country is forbidden unless the receiving country provides an “adequate” level of privacy protection.  In order to avoid disruptions in trade between the U.S. and the EU, the U.S. Dept. of Commerce developed the Safe Harbor framework, which allows U.S. companies a means of assuring European consumers that they will provide an adequate level of privacy protection, thereby satisfying the requirement of the EU Data Protection Directive.
Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)	Governs the collection, use, and disclosure of personal information in commercial activities by organizations of all types, including the Canadian offices or subsidiaries of foreign companies.  Applies to both traditional paper-based business as well as online commercial activities.

## About the Author

Alex brings a unique background and perspective to the accounting and tax community. He practiced law for ten years in New York City and Silicon Valley, specializing in business litigation and insurance law. He is now a veteran of Silicon Valley high-tech, and has worked for several cloud-based computer services.

Currently, he is General Counsel and Director of Sales at LeapFILE, the leading enterprise provider of secure file transfer services. From working closely with accounting firms in resolving their file transfer concerns, Alex has developed a deep understanding of data security laws and how firms can meet regulatory compliance.

## About LeapFILE

LeapFILE is the industry-leading provider of on demand secure file transfer and collaboration solutions for businesses. Founded in 2003 with the mission to facilitate secure file transfer for businesses and to make the process as easy as possible, we have been constantly improving our products and services to bring you the best-in-class file exchange solution platform. Our goal is to make exchanging business-critical files easy for end-users and to make the management of the file exchange solution easy for IT administrators.

With LeapFILE, there are no email size limits, FTP hassles, or overnight delivery fees to deal with. LeapFILE is a web-hosted service so the solution can be implemented within minutes. Our core product is as easy to use as email for end users, and easy to deploy and manage by IT administrators. The success of LeapFILE lies in our product's enterprise-grade yet user-friendly features including bullet-proof security and tracking capabilities, our uncompromising reliability and client support, and our web-based on demand model. Over 2,000 businesses worldwide depend on LeapFILE to manage their secure file transfer and file sharing needs.

For more information about LeapFILE, please visit [www.leapfile.com](http://www.leapfile.com) or call us at (888) 716-9380.

## Additional Resources

The FAQs about SB-1386". SearchCIO.com.

[http://searchcio.techtarget.com/news/article/0,289142,sid182\\_gci941077,00.html](http://searchcio.techtarget.com/news/article/0,289142,sid182_gci941077,00.html)

Stricest data law in nation". SC Magazine

<http://www.scmagazineus.com/Stricest-data-law-in-nation/article/123432/>

State Security Breach Notification Laws". National Conference of State Legislatures

<http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

Notice of Security Breach State Laws". Consumers Union

[http://www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf)

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

National Institute of Standards and Technology (NIST)

<http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>



8000 Jarvis Ave, Suite 100, Newark, CA 94560 USA :: [www.leapfile.com](http://www.leapfile.com)  
+1-510-456-1860 :: sales: +1-888-716-9380 :: fax: +1-510-456-2800