

# EMAIL LEGISLATION

## A summary of UK, European & US legislation

This document provides a top line overview of key UK, European and US legislation that is currently enacted or under review, which will drive current and future adoption of email management and archiving solutions.

The content of this document does not constitute legal advice and should not be relied upon as such. If you need legal advice on a specific matter, please contact a lawyer.

Click on the hyperlink below to take you to information about the legislation that you are most interested in:

[Basel II Accord \(effective 2006\)](#)

[Canadian Privacy Act](#)

[Data Protection Act 1988](#)

[EU Data Protection Directive 95/46/FC](#)

[Federal Information Security Management Act \(FISMA\)](#)

[Federal Rules of Civil Procedure \(FRCP\)](#)

[Financial Services Act 198, regulated by FSA](#)

[Freedom of Information Act \(FOIA\)](#)

[Freedom of Information Act \(in force January 2005\)](#)

[The Gramm-Leach-Bliley Act \(GLB\)](#)

[Health Insurance Portability & Accountability Act \(HIPAA\)](#)

[IRS Circular 230](#)

[MiFID \(Markets in Financial Instruments Directives\)](#)

[PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#)

[The Public Information Act, Texas State](#)

[Sarbanes-Oxley 2002](#)

[SEC Rule 17a-4/ NASD 3010 \(Securities Exchange Act 1934\)](#)

[UK Companies Act 1985](#)

[UK Companies Act 2006 \(amended 2007\)](#)

## **Basel II Accord (effective 2006)**

### **Affects**

International Banking

### **Countries**

International

### **Summary**

Basel II is an international banking accord that replaces the original Basel agreement of 1988. The accord brings in a major shift in the way that financial institutions assess and manage risk in relation to investments

### **The need for an Archiver**

Given that the emphasis is in the main risk assessment, the impact on emails is likely to be the requirement to retain all emails relating to a trade for a period of not less than 5 years, starting from January 2003. Financial institutions must ensure that data and communication is secure, accessible and accurate.

### **Further information**

<http://www.bis.org/publ/bcbsca.htm>

<http://www.federalreserve.gov/generalinfo/Basel2>

<http://www.out-law.com/page-7096>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Canadian Privacy Act**

### **Affects**

This policy is applicable to anyone who is storing any personal data.

### **Country**

Canada

### **Summary**

The Privacy Act was established to protect the personal information of individuals collected by the government. It also gives these individuals the right to access this information. It is a law governing how private sector organizations collect, use and disclose personal information in the course of commercial business.

### **The need for an Archiver**

In order to comply with the Canadian Privacy Act, a law which guarantees individuals access to public records kept by government agencies, an efficient archiving system for compliance is a must. Email is a public record, just like any other document, it is vital that a system is in place to control the increasing amount of email data - in addition to the ability to quickly respond to compliance requests.

### **More information**

<http://laws.justice.gc.ca/en/P-21/index.html>

<http://www.statcan.ca/english/about/privact.htm>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Data Protection Act 1988**

### **Affects**

This policy is applicable to anyone who is storing any personal data.

### **Countries**

EU

### **Summary**

The purpose of the act is to protect the individual rights and freedoms of persons; especially their right to privacy with respect to the processing of personal data.

### **The need for an Archiver**

Given that email is a major medium for exchange and storage of personal information, principles 5 & 7 effectively rule out all current mail server platforms as effective means for storing personal data. Only a purpose built archiving system can meet these requirements. Furthermore, given the individuals right to issue "Subject Access Request", SAR's, detailed search capabilities are required within an archive repository to support these requirements in a cost effective manner. A standard mail server platform does not meet these requirements.

### **Further information:**

<http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>

[http://www.ico.gov.uk/Home/what\\_we\\_cover/data\\_protection.aspx](http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx)

<http://www.exclaimer.com/mailarchiver.aspx>

## **EU Data Protection Directive 95/46/EC**

### **Affects**

All organizations, members of EU member states

### **Countries**

EU

### **Summary**

The European Union adopted a Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("data protection directive"). A key objective of the data protection Directive was to allow the free flow of personal data between Member States by harmonizing the level of adequate protection granted to individuals. Similar to the UK Data Protection Act the principles of security and retention of data for only as long as is required are common.

### **The need for an Archiver**

The need for a comprehensive email archiving solution is clear. The Data Controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access – such elements cannot be provided by generic mail servers as already indicated by compliance with the UK Data Protection Act.

### **Further information**

[http://ec.europa.eu/justice\\_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/)

[http://en.wikipedia.org/wiki/Directive\\_95/46/EC\\_on\\_the\\_protection\\_of\\_personal\\_data](http://en.wikipedia.org/wiki/Directive_95/46/EC_on_the_protection_of_personal_data)

<http://www.exclaimer.com/mailarchiver.aspx>

## **Federal Information Security Management Act (FISMA)**

### **Affects**

United States Federal, State & Local Government

### **Country**

United States

### **Summary**

Federal Information Security Management Act (FISMA) places the onus squarely on agencies and their partners to develop information security risk assessments and mitigation strategies. It defines three security objectives for information and information systems (Confidentiality, Integrity and Availability) and requires every government agency to secure the information and information systems that support its operations and assets, including those provided or managed by another agency, contractor, or other source. As part of FISMA compliance, agencies and departments should implement ways to track the contents of all outgoing emails.

### **The need for an Archiver**

Email is a prime medium for exchange and storage of company records. Storage in the mail-server does not protect against falsification, nor does it protect against accidental loss or malicious removal. A purpose built email archive system will ensure that relevant data can be maintained for the desired retention period and maintain integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor.

### **Further information**

[http://www.whitehouse.gov/omb/inforeg/2004\\_fisma\\_report.pdf](http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf)

<http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03844>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Federal Rules of Civil Procedure (FRCP)**

### **Affects**

Any organization in any industry that has the potential of being involved in litigation in the U.S. Federal Court system.

### **Country**

United States

### **Summary**

The amendments, which went into effect on December 1, 2006, mandate that companies be prepared for electronic discovery. The organization must know where their data is, how to retrieve it, how to meet data requests and they must determine what data will not be subject to search.

### **The need for an Archiver**

Organizations that do not have an automated system in place to help them effectively store, search and retrieve email data in real-time face paying high costs for "rush job" discovery requests. In some instances, failure to produce the requested data in a timely fashion may even lead to the loss of a lawsuit.

### **Further information**

<http://www.law.cornell.edu/rules/frcp/>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Financial Services Act 198, regulated by FSA**

### **Affects**

Financial Services Industry Sector

### **Country**

UK

### **Summary**

The Financial Services Act was passed to consolidate the regulatory authority of numerous agencies in the United Kingdom. The FSA (Financial Services Authority) was created, which is an agency with broad regulatory powers to govern the financial industry. Whilst the act itself is not specific with regard to email retention, the FSA has imposed some guidance in relation to records retention. For example, in relation to guidance on Money Laundering, records relating to transactions, reports and "information not acted on" must be retained for a period of 5 years.

### **The need for an Archiver**

Financial organizations need to review their compliance with FSA guidance in relation to the email. Given the need to retain records for varying numbers of years, a dedicated email archive store is required to ensure that that these requirements are met.

### **Further information**

<http://fsahandbook.info/FSA/handbook.jsp>

<http://www.fsa.gov.uk/pubs/rules/R198.pdf>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Freedom of Information Act (FOIA)**

### **Affects**

United States Federal, State & Local Government

### **Country**

United States

### **Summary**

Freedom of Information Act requires that federal agencies disclose their records to anyone making a written request. The speed and economy of email often makes it the preferred means of delivery, carrying risks that the wrong information might be sent or the wrong recipient addressed. Because email has become so prevalent for interdepartmental communications, security of communications has become a serious concern.

### **The need for an Archiver**

In order to comply with the FOI, a law guaranteeing individuals access to public records kept by government agencies, an efficient archiving system for compliance is a must. Email is a public record, just like any other document, it is vital that a system is in place to control the increasing amount of email data. In addition to the ability to quickly respond to compliance requests

### **Further information**

<http://www.state.gov/m/a/ips/>

<http://www.exclaimer.com/mailarchiver.aspx>

## **Freedom of Information Act (in force January 2005)**

### **Affects**

All UK Government Organizations

### **Country**

UK

### **Summary**

The Freedom of information Act gives anyone the right to request information from a government organization (including central and local government, the health sector, police and armed forces, the education sector and other public bodies), about any subject that they are interested in.

### **The need for an Archiver**

It is clear that organizations reliant upon existing email technology will not be able to adequately meet the SAR (Subject Access Requests) in a timely and cost-effective manner. A centralized email archive store will address all these issues, ensuring that those covered by the FOI can meet their obligations.

### **Further information**

<http://www.opsi.gov.uk/Acts/acts2000/20000036.htm>

<http://www.dca.gov.uk/foi/foiact2000.htm>

<http://www.exclaimer.com/mailarchiver.aspx>

## **The Gramm-Leach-Bliley Act (GLB)**

### **Affects**

US Financial Institutions

### **Country**

United States

### **Summary**

The GLB Act applies to "financial institutions" – businesses that offer financial products or services to individuals to be used primarily for their personal, family, or household purposes. Financial institutions include, for example, banks, securities firms and insurance companies; such entities are covered by the SEC (Securities and Exchange Commission). Businesses that provide many other types of financial products and services to consumers fall under jurisdiction of the FTC (Federal Trade Commission) for the purposes of enforcing GLB.

Violation of GLBA may result in a civil action brought by the U.S. Attorney General. The penalties include those for the financial institution of up to \$100,000 for each violation. In addition, "the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation". Criminal penalties may include up to 5 years in prison.

### **The need for an Archiver**

Today, the vast majority of organizations use email to communicate internally and as a vehicle for the exchange of documents and correspondence between businesses and consumers. Since personal financial information can be transmitted by and retained in electronic formats, it is critical to ensure that the management of such records complies with GLB.

### **Further information**

[http://www.datagovernance.com/adl\\_gramm-leach-bliley\\_glb-USA.html](http://www.datagovernance.com/adl_gramm-leach-bliley_glb-USA.html)

[http://en.wikipedia.org/wiki/Gramm-Leach-Bliley\\_Act](http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act)

<http://www.exclaimer.com/mailarchiver.aspx>

## **Health Insurance Portability & Accountability Act (HIPAA)**

### **Affects**

Virtually all organizations that deal with electronic patient healthcare information are affected.

### **Country**

United States

### **Summary**

All patient information, authorizations, policies, procedures and contracts with business associates must be retained for at least 6 years. Information must be stored in robust data centers that provide minimum guarantees uptime and very high security. Anyone who obtains and discloses information with the intent to sell, transfer or use it for commercial gain or malicious harm can face penalties of up to \$250K in fines and 10 years in jail.

### **The need for an Archiver**

All patient information, authorizations, policies, procedures and contracts with business associates must be retained for at least 6 years.

### **Further information**

<http://www.cms.hhs.gov/HIPAAGenInfo/>

<http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR03103>

<http://www.exclaimer.com/mailarchiver.aspx>

## **IRS Circular 230**

### **Affects**

All Financial Services Organizations/Departments

### **Country**

United States

### **Summary**

The new Circular 230 regulations issued by the Treasury Department were effective on June 20, 2005 in response to some situations in which tax professionals issued tax advice or opinions to clients so that the clients would have penalty protection, even though the advice or opinions were based upon facts, assumptions, or representations that were not reasonable. These new regulations established very high standards that a tax advisor must meet if he or she wishes to provide a client with written tax advice that may be relied upon for tax penalty protection. Circular 230 prescribes standards of practice for lawyers and accountants before the Internal Revenue Service, including ethical and professional responsibilities.

### **The need for disclaimers**

As a result of the Circular 230 regulations, any written tax advice (including tax advice included in an email or other form of electronic written communication) must include a prominent disclaimer. The disclaimer must be near the top of an opinion in a typeface the same size or larger than the typeface of the tax advice. [Exclaimer Mail Utilities](#) helps ensure regulation compliance. For example, Circular 230 requires that the disclaimer must be inserted prior to the body of the email, and at a larger font size. Exclaimer Mail Utilities handles this requirement with ease.

### **Further information**

<http://www.irs.gov/pub/irs-pdf/pcir230.pdf>

<http://www.amerilawyer.com/circular230policy.htm>

<http://www.exclaimer.com/mailutilities.aspx>

## **MiFID (Markets in Financial Instruments Directives)**

### **Affects**

EU financial markets - Investment banks, Portfolio Managers, Stockbrokers, Broker Dealers, Corporate Finance Firms

### **Countries**

EU

### **Summary**

MiFID – the Markets in Financial Instruments Directive – comes into effect on 1 November 2007, when it will replace the existing Investment Services Directive (ISD). MiFID extends the coverage of the current ISD and introduces new and more extensive requirements that firms will have to adapt to, in particular for their conduct of business and internal organization.

### **The Need for an Archiver**

Email is a prime medium for exchange and storage of company records. Storage in the mail-server does not protect against falsification, nor does it protect against accidental loss or malicious removal. A purpose built email archive system will ensure that relevant data can be maintained for the desired retention period and maintain integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor.

### **Further information:**

<http://www.fsa.gov.uk/Pages/About/What/International/EU/fsap/mifid/index.shtml>

<http://www.exclaimer.com/mailarchiver.aspx>

## **PIPEDA (Personal Information Protection and Electronic Documents Act)**

### **Affects**

This policy is applicable to anyone who is storing any personal data.

### **Country**

Canada

### **Summary**

The Personal Information Protection and Electronic Documents Act is a Canadian law designed to ensure that personal information collected by businesses will be kept secure and will only be collected, used and given out under a strict set of circumstances. The Act, based on ten privacy principles was developed by the Canadian Standards Association.

### **The need for an Archiver**

In order to comply with the PIPEDA an effective archiving system for compliance is a must. Email is a public record, just like any other document, it is vital that a system is in place to control the increasing amount of email data. In addition to the ability to quickly respond to compliance requests

### **More information**

<http://laws.justice.gc.ca/en/showtdm/cs/P-8.6>

[http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h\\_gv00045e.html](http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00045e.html)

<http://www.exclaimer.com/mailarchiver.aspx>

## **The Public Information Act, Texas State**

### **Affects**

Anyone who is storing public records kept by government agencies.

### **Country**

United States, Texas State

### **Summary**

Texas Government Code, Chapter 552, gives anyone the right to access government records; and an officer for public information and the officer's agent may not ask why you want them. All government information is presumed to be available to the public. Certain exceptions may apply to the disclosure of the information. Governmental bodies shall promptly release requested information that is not confidential by law, either constitutional, statutory, or by judicial decision, or information for which an exception to disclosure has not been sought.

### **The need for an Archiver**

In order to comply with the Public Information Act, a law guaranteeing individuals access to public records kept by government agencies, an efficient archiving system for compliance is a must. Email is a public record, just like any other document, it is vital that a system is in place to control the increasing amount of email data. In addition to the ability to quickly respond to compliance requests

### **Further information**

[http://www.oag.state.tx.us/opinopen/og\\_training.shtml](http://www.oag.state.tx.us/opinopen/og_training.shtml)

<http://www.exclaimer.com/mailarchiver.aspx>

## **Sarbanes-Oxley 2002**

### **Affects**

All US public companies and many private organizations, and any UK companies trading on US stock exchange.

### **Country**

United States

### **Summary**

Sarbanes Oxley is all about corporate governance. It came as a result of the large corporate financial scandals involving Enron, WorldCom, Global Crossing and Arthur Andersen. Effective in 2004, all publicly-traded companies are required to submit an annual report of the effectiveness of their internal accounting controls to the US Securities and Exchange Commission (SEC). Essentially, SOX legislates what used to be IT security best practices. The major provisions of the Sarbanes Oxley Act (SOX) include criminal and civil penalties. Anyone who knowingly alters, falsifies, destroys, or otherwise tampers with a document or record can be fined and/or imprisoned for up to 20 years.

### **The need for an Archiver**

Specifically all relevant audit-related documentation must be retained for a period of at least seven years. This includes contracts, policies, authorizations, verifications, recommendations, performance reviews and financial data. SOX also addresses the need for companies to effectively manage risk in all its forms—including ensuring that data residing on corporate computers is adequately archived and protected from damage or tampering. To comply with these needs, an effective archiving system is

required that is can scale to the needs of archiving large amounts of data in a secure manner for long periods of time.

**Further information**

<http://www.soxlaw.com/>

<http://www.sec.gov/about/laws/soa2002.pdf>

<http://www.exclaimer.com/mailarchiver.aspx>

**SEC Rule 17a-4/ NASD 3010 (Securities Exchange Act 1934)**

**Affects**

All US Financial institutions and UK organizations trading on the NYSE

**Countries**

US, UK trading on US Stock Exchange

**Summary**

Among the most visible record keeping regulations are those imposed by SEC and related exchanges on communication between securities traders/brokers and the public.

SEC rules 17a-3 and 17a-4 require broker-dealers to create, and preserve in an accessible manner, a comprehensive record of each securities transaction they effect and of their securities business in general.

**The need for an Archiver**

The US Financial Services market is perhaps one of the most heavily regulated markets in the world when it comes to document and email archiving. All US financial organizations and any UK organizations that trade on the NYSE are required to meet these regulations.

The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

a) At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.

b) The audit results must be preserved for the time required for the audited records.

The need to guarantee capture, store and maintain messages in a non-erasable manner is a key requirement that mail servers or indeed home grown archive systems cannot deliver. Speed of retrieval is also a key factor when dealing with Legal Discovery orders. Noncompliance is not an option with huge fines in the region of several million dollars being leveled at organizations.

**Further information**

<http://www.sec.gov/rules/final/34-46473.htm#VK>

<http://www.law.uc.edu/CCL/34ActRls/rule17a-4.html>

<http://www.exclaimer.com/mailarchiver.aspx>

## **UK Companies Act 1985**

### **Affects**

All private and public companies

### **Country**

UK

### **Summary**

Every company must keep accounting records which sufficiently show and explain the company's transactions that (a) disclose with reasonable accuracy, at any time, the financial position of the company at that time, and (b) enable the directors to ensure that any balance sheet and profit and loss account prepared under this Part complies with the requirements of this Act. A company's accounting records shall be kept at its registered office or such other place as the directors think fit, and shall at all times be open to inspection by the company's officers. From the date on which the record is made, private companies must retain this information for 3 years and public companies must retain it for 6 years.

### **The need for an Archiver**

Email is a prime medium for exchange and storage of company records. Storage in the mail-server does not protect against falsification, nor does it protect against accidental loss or malicious removal. A purpose built email archive system will ensure that relevant data can be maintained for the desired retention period and maintain integrity of the records through tamper-proof mechanisms. Furthermore, the system will provide easy search access to recover data if required by an external auditor.

### **Further information**

[http://www.opsi.gov.uk/acts/acts1989/Ukpga\\_19890040\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm)

<http://www.exclaimer.com/mailarchiver.aspx>

## **UK Companies Act 2006 (amended 2007)**

### **Affects**

All private and public companies

### **Country**

UK

### **Summary**

In addition to the requirements of the UK Companies Act 1985, every company should list its company registration number, place of registration and registered office address on its website as a result of an update to the legislation of 1985. The information, which must be in legible characters, should also appear on order forms and in emails. Such information is already required on 'business letters' but the duty is being extended to websites, order forms and electronic documents.

### **The need for a Disclaimer**

If your business is a private or public limited company or a Limited Liability Partnership, the Companies Act 1985 requires all of your business emails (and your letterhead and order forms) to include the following details in legible characters:

- Your company registration number;
- Your place of registration (e.g. Scotland or England & Wales)
- Your registered office address

This information should also appear on your company's website. Failure to comply with these requirements puts a company at risk of a fine of up to £1000.

**Example footer**

Green Organisation is a limited company registered in England and Wales.

Registered number: 5464771.

Registered office: Green House, 21 Bloom Street, London, WC1 1AA.

**Further information**

<http://www.out-law.com/page-5536>

[http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga\\_20060046\\_en.pdf](http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060046_en.pdf)

<http://www.exclaimer.com/mailutilities.aspx>

## Disclaimer

The content of this document does not constitute legal advice and should not be relied upon as such. If you need legal advice on a specific matter, please contact a lawyer.

This document contains links to third party web sites and resources. Because this website has no control over these sites and resources, you acknowledge and agree that Exclaimer Ltd (www.exclaimer.com) is not responsible for the availability of such external sites or resources, and does not endorse and is not responsible or liable for any content, advertising, products, or other materials on or available from such sites or resources. You further acknowledge and agree that Exclaimer Ltd (www.exclaimer.com) shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods or services available on or through any such site or resource. Consequential, or indirect damages (including, but not limited to, damages for loss of profits, business interruption, loss of programs or information, and the like) arising out of the use of or inability to use the service, or any information, or transactions provided on the service, or downloaded from the service, or any delay of such information or service.