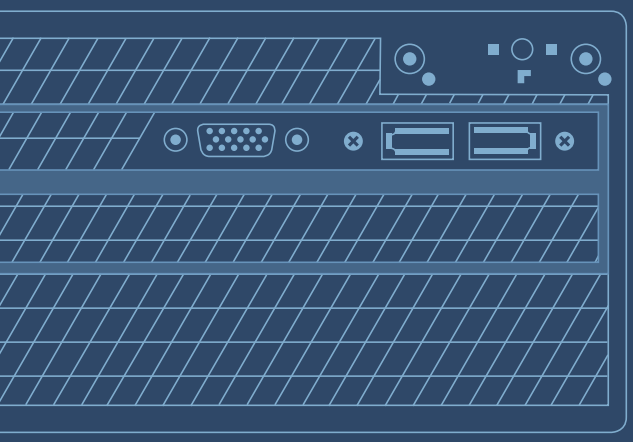
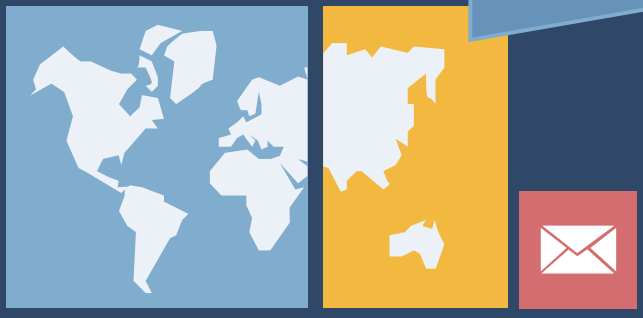
Email Legislation





www.exclaimer.com

Email Legislation

A summary of international legislation

This document provides a top line overview of key email legislation that is currently enacted in various geographic locations for 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 III Accord

Affects

International Banking.

Countries

International.

Basel III is an international banking accord that replaces the second Basel agreement of 2006. The Accord seeks to improve the banking sector's ability to deal with financial and economic stress, improve risk management and strengthen banks' transparency. A focus of Basel III is to foster greater resilience at the individual bank level in order to reduce the risk of system wide shocks.

The need for an Archiver

Given that the emphasis of Basel III is on risk management and in light of the fact that the global economy has recently been through the worst recession since the 1930s, it is a fundamental requirement of financial institutions to retain all emails that relate to trade for no less than five years. With stricter regulations in place, it is imperative that data and electronic communications are secure, accessible and accurate via an easy-to-use email archiving solution.

Learn more >>

Further information

- International regulatory framework for banks (Basel III)
- Implementing Basel III Europe - European Banking Authority
- Basel III for Dummies!
- Basel III - The Guardian

Canadian Anti-Spam Law

Affects

All Canadian business and international organizations sending email to Canada.

Countries

Canada.

Canada's Anti-Spam Law (CASL) requires businesses to obtain either express "opt-in" or implied consent to send commercial electronic messages (CEMs) to any recipient. This can be anything from email, to SMS and social media messages, meaning that this legislation is far broad than others such as **CAN-SPAM** which are just targeted at emails. In addition, all electronic marketing messages need to clearly identify the sender, include the sender's contact information and provide an unsubscribe mechanism, unless fully exempted from the Act. It came into effect on 1 July 2014.

Three Canadian government agencies are responsible for this law and if you are found not to comply with it 'to the letter', you could receive a fine of up to **$10 million and face criminal charges**. These fines are imposed per violation daily.

The need for email disclaimers

The larger your organization is, the harder it is to enforce a CASL email policy for all email messages. You need to ensure that all email signatures contain information required by CASL and include appropriate opt-out hyperlinks for unsubscribing. It is the responsibility of all organizations to ensure that each employee has a compliant email disclaimer added to their email signature and the best way to do this is to centrally manage this process.

Learn more >>

Further information

- Canadian Anti-Spam Legislation (full text)
- About Canada's Anti-Spam Legislation
- Managing the message: Canada's new anti-spam law sets a high bar

Canadian Privacy Act

Affects

Anyone who is storing any personal data.

Countries

Canada.

Applicable to anyone who is storing personal data, the Canadian Privacy Act was established to protect personal information collected by the Canadian government. It gives individuals the right to access this information and governs how private sector organizations collect, use and disclose personal details 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 required. Email is a public record, just like any other document, so it is vital that a system is in place to control the increasing amount of email data with the ability to quickly respond to compliance requests.

Learn more >>

Further information

- Privacy Legislation in Canada
- Privacy Act - Government of Canada

EU Directive 2003/58/EC

Affects

All organizations, members of EU member states.

Countries

European Union (EU).

Introduced in 2007, the **EU Directive 2003/58/EC** concerns emails sent by companies as part of their business operations. Previous regulations applying to written correspondence by letter or fax were extended to emails and other forms of electronic communication.

- All business emails must include the company's registration number, the place of registration and the registered office address.
- Each member of the EU had to enforce this law before 31 December 2006.

To this end, several key members adopted the directive in a number of ways.

United Kingdom

The Companies Act 1985 was already in place, applying to private and public limited companies or a Limited Liability Partnership. All business emails, letterheads, order forms and corporate websites must include

- The company's registered name (e.g. ABC Ltd).
- Registration number (listed on Companies House).
- Place of registration (e.g. England).

N.B. You cannot just provide a link to information on your email disclaimer.

This is enforced by Trading Standards with fines for non-compliance starting at £1,000 with an additional fine of £300 per day if the breach continues. If the disclosure of the content of an email leads to a dispute, it can be argued in court that the recipient should have known to not disclose the information.

Ireland

The EU Directive was implemented by the Minister for Enterprise, Trade & Employment on 1st April 2007. Company's email communications have to include:

- The name of the company.
- Place of registration.
- Registered number.
- Registered office.
- Whether the company is a limited company.
- If it is exempt from the obligation to include Limited in its name.
- If it is being wound up, in liquidation etc.
- Any reference to share capital must be paid-up share capital.

Failure to display this information constitutes a criminal offense that is subject to a maximum fine of €2,000.

Germany

Implemented on 1st January 2007, all corporate electronic communication must include:

- The company's registered name.
- The office location.
- Court register.
- Registration number.
- The name of the managing director and the board of directors.

Failure to comply with this comes with a maximum fine of €5,000. On another note, privacy statements intended to act unilaterally, confidentiality disclaimers, and liability disclaimers have no legal standing under German law.

France

Enacted on 9th May 2007, all companies in France must include the following in all electronic communications:

- Company name.
- Registration number.
- Registry location.
- Registered office.
- If they are in the process of insolvency proceedings.

If the body corporate is a commercial company having its registered office overseas, then these have to be included:

- Its name.
- Legal form.
- Address of its registered office.
- Registration number of relevant country.
- If it is subject to insolvency proceedings if it is appropriate.
- If it is run by a lease manager or an authorized management agent.

Any infringement of any of these points is subject to a fine of €750 per infringement.

Italy

All Italian companies electronic communications must include:

- Company registered name.
- Registration number.
- Place of registration.
- Registered office address.

If applicable, whether the company is going into liquidation or being wound up.

The Netherlands

There is a Dutch law that requires every company to display their CoC number on all outgoing written communications including email. Failure to follow this law can result in a fine of up to €16,750 or up to six months imprisonment as it constitutes an economic crime.

Denmark

From 4th May 2006, all Danish companies were required to include their name, location and Central Business Register (CVR) number.

The need for email disclaimers

With all the regulations that are out there and the stiff penalties that can be applied to a company, it is better to prepare for all eventualities than to do nothing. The **EU Directive 2003/58/EC** forces companies to be more transparent so it is best practice to create a disclaimer that is specific to your organization and the country you are based in, which is then strictly enforced as company policy. This means that you are less likely to run into any legal complications in the future.

Learn more >>

Further information

- Directive 2003/58/EC of the European Parliament

EU Data Protection Directive 95/46/EC

Affects

All organizations, members of EU member states.

Countries

European Union (EU).

The European Union adopted **Directive 95/46/EC** to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially relating to processing, using, or exchanging such data.

A key objective of the data protection Directive is to allow the free flow of personal data between Member States by harmonizing the level of adequate protection granted to individuals. It encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence.

Learn more >>

The need for an Archiver

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

Further information

- Directive 95/46/EC of the European Parliament

Federal Information Security Management Act (FISMA)

Affects

United States Federal, State & Local Government.

Countries

United States.

The **Federal Information Security Management Act (FISMA)** places the onus squarely on agencies to ensure the security of data within the different branches of the US government (federal, state and local).

The Act defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. Every government agency is required to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner. As part of FISMA compliance, agencies and departments must 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.

Learn more >>

Further information

- Federal Information Security Management Act of 2002
- FISMA Resources
- NIST FISMA Implementation Project

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.

Countries

United States.

The **Federal Rules of Civil Procedure (FRCP)** are regulations that specify procedures for civil legal suits within United States Federal Court system. A revision to the Rules which went into effect on December 1, 2006 was established to for companies to make provisions for the handling of electronic records and to accommodate electronic discovery (using electronic data for civil legal actions). An 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.

Learn more >>

Further information

- Legal Information Institute - Federal Rules of Civil Procedure

Financial Services Act 2012

Affects

Financial Services.

Countries

United Kingdom.

The Financial Services Act was passed to consolidate the regulatory authority of numerous agencies in the United Kingdom. The FSA (Financial Services Authority), which had previously been given broad powers to regulate the financial industry, was replaced with two new regulators, namely the Financial Conduct Authority and the Prudential Regulation Authority, which created the Financial Policy Committee of the Bank of England. This framework went into effect on April 1 2013.

The purpose of the amended Act is to restructure and broaden the law relating to market manipulation, misleading statements and impressions as well as modernize the financial regulation that failed to protect the UK economy from the fallout of the 2008 recession. Whilst the Act itself is not specific with regard to email retention, there is 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 in relation to 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.

Learn more >>

Further information

- Financial Services Act 2012

Freedom of Information Act (FOIA)

Affects

United States Federal, State & Local Government.

Countries

United States.

The **Freedom of Information Act** is a federal freedom of information law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government.

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. As 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 FOIA, a law guaranteeing individuals access to public records kept by government agencies, means that an efficient archiving system is a must. Email is a public record, just like any other document, so it is vital that a system is in place to control large amounts of email data.

Learn more >>

Further information

- U.S. Department of State Freedom of Information Act (FOIA)

Freedom of Information Act 2000

Affects

All UK Government Organizations.

Countries

United Kingdom.

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. However, the Act does not necessarily cover every organisation that receives public money. The Act also does not give people access to their own personal data (information about themselves) such as their health records or credit reference file.

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.

Learn more >>

Further information

- Freedom of Information Act 2000
- Guide to Freedom of Information

Gramm-Leach-Bliley Act (GLB)

Affects

US Financial Institutions.

Countries

United States.

The GLB Act applies to "financial institutions" – businesses that offer financial products or services to individuals to be used primarily for personal, family, or household purposes. Financial institutions like banks, securities firms and insurance companies 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 the Act may result in a civil action brought by the U.S. Attorney General. The penalties include 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 Act has been cited by many as the cause of the 2007 subprime mortgage financial crisis, which triggered the recession of 2008.

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.

Learn more >>

Further information

- Gramm-Leach-Bliley Act (full copy)
- Gramm-Leach-Bliley Act - Bureau of Consumer Protection Business Center

Health Insurance Portability & Accountability Act (HIPAA)

Affects

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

Countries

United States.

The **Health Insurance Portability and Accountability Act (HIPAA)** offers protection for millions of American workers by improving portability and continuity of health insurance coverage. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems.

Information must be stored in robust data centers that provide minimum guaranteed 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. Information must be stored in robust data centers that provide minimum guaranteed uptime and very high security.

Learn more >>

Further information

- Health Insurance Portability and Accountability Act
- Health Information Privacy

Markets in Financial Instruments Directive (MiFID) 2004/39/EC

Affects

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

Countries

European Union (EU).

The **Markets in Financial Instruments Directive 2004/39/EC** came into effect on 1 November 2007, when it replaced the **Investment Services Directive (ISD)**, which directly affects EU financial markets.

MiFID extended the coverage of **ISD** and introduced new and more extensive requirements that firms have to adapt to, in particular for their conduct of business and internal organization.

The European Commission (EC) revised the Directive, known as MiFID II, which was adopted by the European Parliament on 15 April 2014. EU Member States are required to implement the MiFID II Directive by June 2016 and the package of measures by January 2017. This is designed to make financial markets more efficient and improve investor protection, which is of particular relevance in the aftermath of the 2008 recession.

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.

Learn more >>

Further information:

- The Markets in Financial Instruments Directive II (MiFID II)
- Legislation in force: MiFID 1

PIPEDA
(Personal Information Protection and Electronic Documents Act)

Affects

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

Countries

Canada.

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. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA incorporates and makes mandatory provisions of the **Canadian Standards Association's** Model Code for the Protection of Personal Information, developed in 1995.

The need for an Archiver

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

Learn more >>

Further information

- Personal Information Protection and Electronic Documents Act - Government of Canada
- Privacy in the Digital Economy

The Public Information Act, Texas State

Affects

Anyone who is storing public records kept by government agencies.

Countries

United States, Texas State

The **Texas Public Information Act** is a series of laws incorporated into the **Texas Governmental Code** that guarantee an individual's unrestricted access to public records kept by government agencies. 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, an efficient archiving system for compliance is a must. Email is a public record, just like any other document, so it is vital that a system is in place to control the increasing amount of email data. In addition, it is vital that there is an ability in place to quickly respond to compliance requests.

Learn more >>

Further information

- The Public Information Act, Texas Government Code Chapter 552

Sarbanes-Oxley 2002

Affects

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

Countries

United States.

The Sarbanes-Oxley Act of 2002 (often shortened to SOX) is legislation passed by the U.S. Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures. It came as a result of the large corporate financial scandals in the early 2000s involving Enron, WorldCom, Global Crossing and Arthur Andersen. It also affects any UK companies trading on the US Stock Exchange.

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

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.

Learn more >>

Further information

- A Guide to the Sarbanes-Oxley Act
- The Sarbanes-Oxley Act of 2002 (full copy)

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.

Among the most visible record keeping regulations are those imposed by **SEC** and related exchanges on communication between securities traders/brokers and the public. All US financial organizations and any UK organizations that trade on the NYSE are required to meet these regulations.

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. An audit system is vital for accountability.

At all times, a member, broker, or dealer must be able to have the results of an 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.

Any 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 comes with huge fines in the region of several million dollars being levelled at organizations.

Learn more >>

Further information

- Support for SEC-17a-4, NASD 3010 and 3110

UK Companies Act 1985

Affects

All private and public companies.

Countries

United Kingdom.

The **Companies Act of 1985** is an important part of UK company law that governs various aspects of the registration and management of companies.

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.

Learn more >>

Further information

- UK Companies Act

UK Companies Act 2006 (amended 2007)

Affects

All private and public companies.

Countries

United Kingdom.

In addition to the requirements of the **UK Companies Act 1985**, every company has to list its company registration number, place of registration and registered office address on its website and any electronic communication. This is due to an update to the 1985 legislation and came into effect on 1 January, 2007.

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 also has to appear on a 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.

Learn more >>

Further information

- Companies Act 2006
- Email notices and email footers based on UK law

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.