SPAMINA
Securing Digital Communications

Encryption Laws and Compliance for the European Union

There is no "OOPS" clause in privacy legislation

Spamina suite of products can help organizations reduce the challenges and complexity of regulatory compliance by allowing IT and Administrators total control of their email environment. It provides them with the tools needed to help them comply with industry regulations.

These tools can help organizations identify compliance issues and manage their infrastructure. Once applied, they can re-direct, prevent distribution or encrypt confidential information based on pre-defined policies.

3 steps to Compliance:

1. Develop privacy policies and

- **a.** Define policies
- **b.** Create clear rules for the distribution of confidential info
- **c.** Provide and support an easy to use technical solution to enforce policies and procedures

2. Eliminate human error

- **a.** People make mistakes
- **b.** Most data is compromised inadvertently
- **c.** Up to 80% of breaches are caused internally

3. Protect confidential information

- **a.** Apply encryption to all confidential info
- **b.** Enforce encryption automatically using policy-based encryption at the gateway

Cloud Email Encryption & DLP

Spamina policy engine automatically enforces compliance. All encrypted messages are digitally signed and can be validated to prove compliance as and when required.

Legislation

Email has become a dominant channel for personal and business communications. Everything from meeting requests to messages containing highly sensitive business or client information is sent by email. **Everyone should take positive steps to protect their confidential communications**. Lawyers, financial advisors, accountants, educators, healthcare providers and other professional advisors have ethical and fiduciary duties to keep personal information about their clients confidential. Businesses need to be able to trust their email communications and reduce the risk of damage to their brand resulting from information obtained through intercepted email as personal security, privacy, fraud and identity theft are a big concern for all.

Data Protection Act 1998

The Data Protection Act 1998 (DPA 1998) is an act of the United Kingdom (UK) Parliament defining the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them.

The UK Information Commissioner's Office (ICO) has been given new statutory powers effective from 6 April 2010 with the introduction of new penalties for breaches of the Data Protection Act (DPA) 1998. The ICO has also been granted new statutory powers to audit government departments.

Penalties available to the ICO

- Fines of up to £500,000 for serious contraventions of the DPA
- 25 Monetary Penalty Notices (MPNs) are expected to be issued each year by the ICO
- Prison Sentences for deliberate or negligent customer data leaks by individuals within an organization may also become available
- DPA compliance costs are set to rise accordingly, for UK organizations

The new statutory powers the ICO has just gained gives them the power to audit government departments without consent, thanks to the passing of the Coroners and Justice Act 2009.

EC Data Protection Directives and relevant national laws

The European Community in 1995 issued 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 (the 'Data Protection Directive'). National governments in all 25 member states to the European Union, as well as the member countries to the European Economic Area (EU member states plus Iceland, Norway and Liechtenstein) have transformed the Data Protection Directive into their national laws. Also, Switzerland which is neither a member of the EU or EEA has enacted legislation, which is modeled after the Data Protection Directive. Thus, **all European countries have also enacted strict legislative measures to protect the privacy of personal information that expressly apply to personal information communicated electronically**. These legislative measures apply regardless of industry or field of business though additional measures and rules may apply where specially regulated professions are concerned (see above). The enacted legislation protects the privacy of personal information. The Data Protection Directive, as well as all data protection legislation in all EU and EEA member states, imposes a general obligation on anyone who processes personal data (except where such data are merely processed for private purposes) to protect the privacy and security of personal information.

Security measures requires by law

The Data Protection Directive in Article 17 (1) provides that "Member states shall provide that the data controller must implement appropriate technical and organization measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission over a network, and against all other forms of unlawful processing." Article 17(1) has been implemented within all EU and EEA member states (and similar legislation applies in Switzerland) so that every handler of personal data there is required to take appropriate technical measures to protect against unauthorized disclosure of electronically stored or communicated personal information. **The test is whether 'appropriate measures' have been considered and implemented to protect the privacy of personal information. There is no longer an appropriate expectation that email cannot be intercepted and read without authorization**. Spamina Cloud Email Encryption & DLP, encrypting email provides the necessary protection of this information and is an 'appropriate measure' that should be used when communicating personal information via email.

Neither the Data Protection Directive nor the majority of national legislation in EU and EEA member states differentiate between industry specific measures to be adopted. Art. 17(1) of the Data Protection Directive provides that "…Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."
Therefore, higher security standards apply where either so-called 'sensitive data' (defined by Art. 8 Data Protection Directive as personal data revealing racial or ethnic origin political opinions, religious or philosophical beliefs, trade-union membership or data about health or sex life) or personal data that due to their nature imply specific higher risks (including but not limited to financial data or data that are subject to professional confidentiality obligations) are processed.

Secure Mail and Privacy Legislation

There are, however, specific countries such as Spain and Italy for example that mandate the use of encrypted transmission of specific data.

Encryption required by law for health data under the Italian Personal Date Protection Code

Section 24 of Annex B to the Italian Personal Data Protection Code (Technical Specifications on Minimum Data Security Measures) requires that "Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code …; the data shall have to be encrypted for the purpose of electronically transferring them." **Therefore any transfer of health data or data on a person's sex life between healthcare bodies and professionals in Italy must be performed only using encryption technology.**

- Non-compliance as a criminal offence
- Non-compliance with the minimum security measures set forth in the Italian Personal Data Protection Act is a criminal Offense and may be punished by up to two years in prison or by a fine between 10,000 and 50,000 Euros

Encryption requires by law for all sensitive data under Spanish law

Pursuant to the Spanish Royal Decree 994/1999 on security measures for automated databases, any sensitive data **may only be transmitted through telecommunications networks if it has been previously encrypted** or made illegible to any unauthorized third party. This obligation generally applies to sensitive data transmitted through a public network.
Thus, private networks used within a company or group (not accessible to the public) would be exempted from this obligation.

In addition, as set forth by the referred Royal Decree, the distribution of means containing sensitive data w**ill be conducted by encrypting such data or by setting up any other protection mechanism that warrants that such data** will not be legible nor handled during its transit.

According to Spanish law, the following data qualify as 'sensitive data': (i) ideology; (ii) beliefs; (iii) religion; (iv) trade union membership; (v) health; (vi) ethnic origin; (vii) sexual preferences and (viii) criminal offences and administrative sanctions data. However, pursuant a draft regulation currently under discussion, the following data may be considered as well in the near future as sensitive: data processed for police purposes without data subjects' consent, traffic and location data (applicable to telecom operators) and information necessary to issue a digital certificate for e-signature purposes (save for public data).

Other examples where encryption may be mandated or recommended by applicable laws

Strict security requirements apply not only where so-called sensitive data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data about health or sex life) but also where personal data that due to their nature imply specific higher risks are affected. This would for example typically be the case with regard to financial data or data that are subject to professional confidentiality obligations **(lawyers, accountants, etc.).**

To this end, the sector of financial institutions seems to be most important. Financial institutions are required to design, implement and maintain technical and organizational safeguards to protect customer personal data on the basis of general data protection legislation, the principle of banking secrecy (which has varying legal basis in different
EU/EEA member states) and special rules and regulations issued by the applicable regulatory bodies having jurisdiction over financial institutions in the individual member states. Such rules and regulations may not only apply to financial institutions that collect information from their own customers, but may also apply to institutions (e.g. credit reporting agencies) that receive customer information from financial institutions. Particularly, credit rating agencies have always been under special attention from data protection authorities in the EU/EEA.

Who is affected?
Any business or private individual who are engaged in the processing personal data which is not for private purposes.

Therefore, not only doctors, hospitals, health care providers, financial institutions, credit reporting agencies, lawyers, financial advisors, accountants, and educators, but anyone who processes personal data is required to take appropriate measures to control how such personal data are used, disclosed and protected. Where so-called sensitive data or data that due to its nature implies higher risks are concerned, appropriate measures in many cases may directly or indirectly include the duty to encrypt electronic messages.

Why encrypt email?
As outlined above, specific national data protection laws require the use of encrypted email technology for specific data i.e. 'sensitive personal data' in Spain or health data and data relating to sex life in Italy. Irrespective of such specific rules, all EU/EEA member states require more stringent security measures where the 'sensitive data' or personal data imply higher risks (including but not limited to financial data or data that are subject to professional confidentiality obligations) by mandating that protection measures must be adequate to the relevant risks and the specific data.

In order to avoid sanctions, such as damage claims by the individual data subjects, protective orders or high fines by data protection authorities or even criminal liability for non-compliance with security requirements, use of encryption technology for secure email communication seems to be a must.

Liability for breaches of data protection laws

Breaches of applicable data protection requirements in any member state to the EU or EEA may have far reaching consequences, such as for example:

- Damages claims by individuals
- All EU and EEA member states' national legislation provides for damage claims, which the relevant individuals whose personal data have been processed in violation of applicable data protection law are entitled to against the relevant data controller
- Orders of the data protection authorities

In addition to damage claims by individuals, the data protection authorities with EU and EEA member states have a wide range of powers. Data protection authorities have broad investigative powers and powers of intervention. Where personal data are processed allegedly in an illegal fashion, they may order, amongst others, the blocking, erasure or destruction of data, of imposing temporary or definitive ban on such processing.

Administrative fines
Furthermore, national laws of the EU and EEA member states also provide for administrative fines where data protection laws have been breached. Such fines vary for example from maximum amounts of 1.5 million Euros in France, of 600,000 Euros in Spain or of 250,000 Euros in Germany.

The Spanish data protection authority alone has fines businesses for non-compliance with data protection requirements in the amount of 16.4 million Euros.

Recent enforcement action and proactive enforcement strategies in Europe

The following provides a brief overview of recent enforcement action during 2004 partly also relating to breaches of applicable technical and organizational security requirements undertaken within a number of EU member states. It also makes clear that all member states' data protection authorities have adopted or are in the midst of adopting proactive enforcement strategies to also ensure compliance with required security measures that seem to focus on the health, banking, telecom sectors, direct marketing sectors as well as on the public sector.

Czech Republic
Undisclosed sanctions were imposed for f**ailure of an educational institution to meet measures against unauthorized and accidental access to personal data** of students. The pro-active enforcement strategy of this country will focus amongst other organizations, on banks, insurance companies and other financial institutions, direct marketing companies and advertising agencies, telecom operators, recruitment agencies.

Denmark
Undisclosed sanctions in a case where a **public psychiatric hospital sent an unencrypted email containing sensitive data regarding a data** subject's health and criminal record to an employed psychiatrist, which were forwarded to a large number of third parties through a computer virus.

France
France's data protection authority (CNIL) will adopt a new enforcement policy, which will amongst other issues have a special focus on whether appropriate security measures are put in place.

Germany
Fines were imposed in the health sector for **unauthorized disclosure of health data to the wrong insurance company** and in the financial sector against a credit rating agency for illegally disclosing consumer financial information. Also, German data protection authorities carry out more than 200 audits investigating compliance with applicable data protection laws.

Italy
Fines of up to 60,000 Euros were imposed for n**on-compliance with notification requirements for sensitive data**, and in such cases bans were imposed prohibiting any further use of personal data, which had not been notified correctly.

Lithuania
The small country of Lithuania alone carried out 365 inspections in 2004 to determine compliance with applicable data protection laws.

Spain
The Spanish data protection authority carried out investigations and imposed penalties mostly in the health sector and telecommunication sector. The most common problems identified and penalized in the health sector related to **non-compliance with applicable security measures.**

Click here for further information on how Spamina can help your organisation stay compliant in your Email communications.