EPI-USE LABS
value through innovation

Data masking in non-production SAP environments: The impact of unsecured data

A White paper written by Louis Emmanuel Ojuwu and Sotiris Panagopoulos

Introduction

Security attacks and breaches of personal and business data comprise one of the most formidable threats to organisations. Security attacks are on the rise and the impact upon society and commerce is significant. Hackers are gaining access to customer and employee personal data as well as confidential documents, pricing conditions and financial information.

The outlook for 2015 seems to be no different. For example, in the first week of 2015, CNBC announced the Morgan Stanley data security beach, where an employee (now fired) stole hundreds of thousands of the company's wealth management clients. With the exponential growth of data volumes exacerbated by cloud, electronic payment, mobile and social media, data breaches will continue to pose an immense threat to both large and small enterprises.

Companies are trying hard to keep their sensitive data protected, generally unsuccessfully. Attackers are always honing their skills to find new ways of exploiting gaps in security. Company reputations are at risk and reputation and goodwill hold considerable value. (According to International Financial Reporting Standards (IFRS), management must value goodwill each year and determine if an impairment has occurred.) On top of this, when sensitive data is compromised, huge government fines and penalties can be levied and large legal costs incurred. The cost of reputational damage to an organisation varies - what is it worth to you?

According to Heimerl, research shows that internal breaches and the lack of technical skills are big threats to data security. It remains the responsibility of organisations and their employees to follow adequate data handling policies and procedures, yet the human factor is undoubtedly the weakest link in the data security chain. Figure 1 below shows current statistics of reported data security breaches of 2012 [1]. These stats have risen considerably on a yearly basis [2].

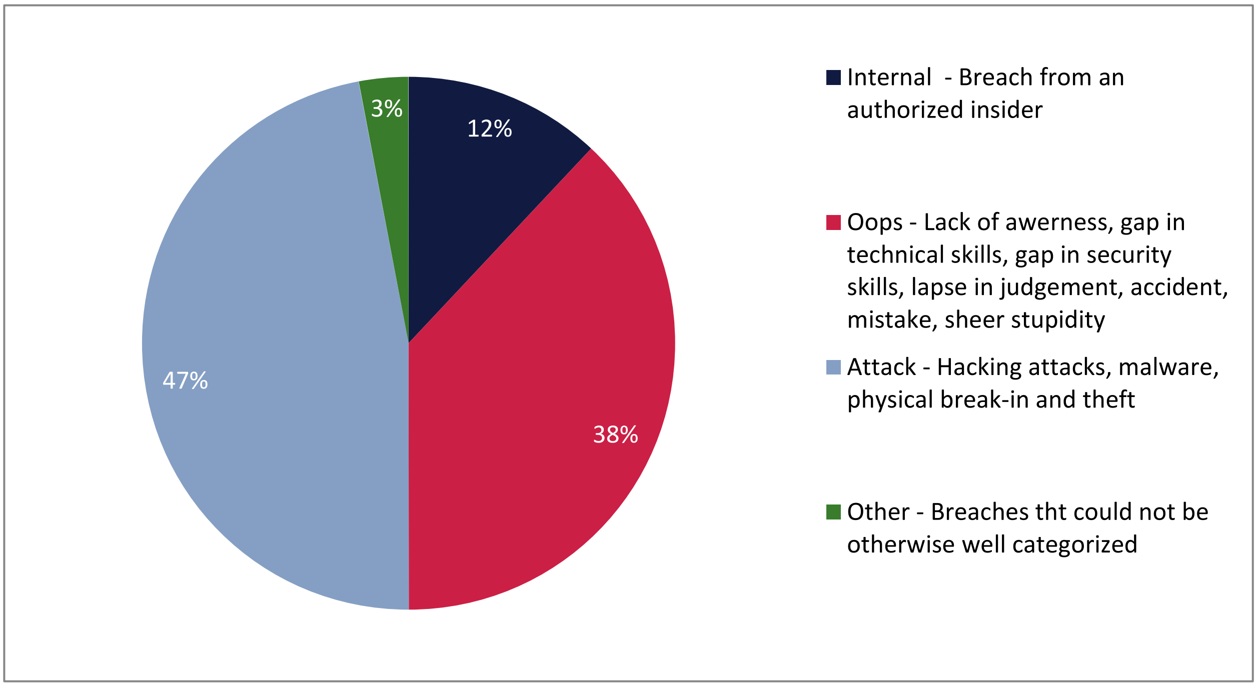

Figure 1: Categories of data breach statistics [1]

The challenge is to allow your business teams to access Test, Training, Sandbox, Project and Development systems effectively but, at the same time, keep your most sensitive business data anonymous.

Throughout this paper, the terms scrambling, masking and anonymization will be used interchangeably for the concept of data de-identification.

Cost of data breaches

Many companies are unaware that the costs of implementing a solution to secure sensitive data pale in comparison to the huge costs associated with a breach in security.

They believe that the likelihood of their company being fined is minimal because a breach is very difficult to predict. However, the prevalence and recurring nature of these attacks over the years are a significant concern for consumers, government and any organisation handling data. Regrettably, data breaches are becoming the new norm and cannot simply be ignored by organisations that intend to remain in business. According to the Identity Theft Resource Center (ITRC), over 760 data-security breaches compromised 83 million records of data in 2014 [2]. With so many data breaches, who pays for the cost of identity theft, credit card theft and issuance of new cards? The obvious burden falls on the individuals whose identity is at risk, the issuing banks, credit unions and ultimately the consumers in the form of higher rates.

Companies who are responsible for the secure management of consumer data are themselves not left alone. Research done in 2014 by the Ponemon Institute rated the average cost of cybercrime per company in the US at $12.7 million in 2014, with litigation, fines and levy costs in the tens of millions of dollars [7]. Of course, the costs to reputation and esteem are inestimable.

Regulations, compliance and legislation implications

The Data Protection Act (DPA) defines personal data as any data which can be used to identify a living person [8]. This applies to all information which is in the possession of, or is likely to come into the possession of, the data controller [8]. It is therefore the responsibility of the data controller, the data collector and third parties handling sensitive and personal data to maintain confidentiality by ensuring maximum protection. Protective measures can be achieved by adhering to the DPA, and country-specific industry policies and regulations. However, this is not the case with the majority of organisations in business today. Rather than integrating security and data-protection legislation from the onset (a privacy by design approach), companies apply a 'bolt-on' approach, often seeking security control measures after a data breach occurs.

Organisations that use live data in non-production environments will need to ensure that their data is masked and de-identified in accordance with the proposed new DPA law. If this draft law is passed, then data processed in a non-production environment, such as a test or development system, will no longer be able to be 'live' unless the company has notified the individual and received their consent [3,8].

Moreover, the proposed EU Data Protection Act (DPA) stipulates that organisations which unlawfully process personal data or fail to notify the regulators, will be subject to penalties, with regulators being given the power to fine an organisation up to 5% of their annual global turnover or €100 Million. This stipulation also opens the possibility for individuals and associations, acting in the public interest, to bring claims for non-compliance [3]. This is irrespective of whether your company is an EU-registered business or not. As long as you process and hold information concerning EU citizens you are bound by the same DPA regulations. For example, in the UK the Information Commissioner's Office (ICO) imposes penalties of up to £500,000 for breaches of the Data Protection Act [4]. To avoid reputation damage and costly fines, companies must adopt policies and prepare for these upcoming changes. There are other compliance requirements to be adhered to [5] that businesses need to be aware of and provide for.

The cost of non-compliance with regulation is high and detrimental to business:

- In October 2009, the data protection authority of Berlin imposed a fine of EUR 1,123,503.50 on Deutsche Bahn AG because of significant violations of the data protection law.
- The 2013 data breach attack on the US retailer Target led to millions of customers' data being compromised. This cost the company $162 Million [6] according to their 2014 financial annual report and the resignation of both their CEO and CIO.

Common security measures and their disadvantages

Currently, most organisations are making attempts to protect customer data by applying a variety of different security measures. These include:

- Isolation of production and test system on an isolated network environment.
- Firewall and hardware-based security on the network infrastructure.
- Database encryption, outsourcing of custom ABAP Z-programs or in-house development for scrambling data in a test environment.
- The use of Standalone database(s), scrambling tools and products that are not tailored specifically for the SAP environment.
- The use of 3rd party software for SAP, like Data Secure from EPI-USE Labs, to have a long term data scrambling solution.

The arduous task of implementing your own data scrambling is time-consuming and not necessarily consistent across your SAP landscape. It has the following disadvantages:

- If your firewall is breached or bypassed, any data that is not masked remains vulnerable. Writing your own custom Z-programs is time-consuming and invariably inconsistent across SAP systems.
- Every SAP component and enhancement pack upgrade adds complexity, because manpower resources are needed each time to rewrite and retest written scrambling programs.
- The financial, time and human capital cost is expensive and difficult to manage.
- It is less effective for supporting your present and future SAP environment(s).
- You or your company may not have the internal knowledge to capture all the links and dependencies between objects.

What is data masking?

Data masking refers to the process of obfuscating real and sensitive data within a database to ensure complete confidentiality and non-exposure of personal identifiable information. This helps organisations meet compliance requirements for PCI, HIPAA, GLBA and other data privacy regulations [1].

In the Magic Quadrant for Data Masking Technology report by Gartner, they define: “Data masking technologies should satisfy a simple, yet strict, rule: Masked data should be realistic and quasi-real — that is, it should satisfy the same business rules as real data. This is to ensure that the application running against masked data performs as if the masked data is real. Data masking must not limit a user's ability to adequately use applications.”[9]

Data masking makes it impossible to identify sensitive information in your SAP environment but keeps the overall system behaviour consistent. This enables you to create safe and effective test and QA environments.

Data masking is an effective security approach within a global data-security measure. Data masking policies can be applied along with other security controls such as encryption, access control, monitoring and auditing controls. Each of these measures play a key role in securing data in a production environment. However, data masking is the becoming the best practice for securing sensitive data in a non-production environment.

The objectives of masking data are to:

- Minimize risk of disclosure resulting from providing access to the data.
- Protect intellectual property and company trade secrets.
- Comply with regulatory requirements from Government and Auditors.

Introducing Data Secure

Data Sync Manager is a trusted data copy solution developed by EPI-USE Labs and has been in the market for more than 18 years. Data Secure is part of the Data Sync Manager (DSM) product suite, and protects confidential information by enabling organisations to mask data fields deemed sensitive in non-production SAP environments. DSM Data Secure mask data before it leaves the production system (source client) to SAP non-production environment (target client[s]). Figure 2 below shows data masked in production system enroute to test environment. Masked data is also consistent across SAP landscape environment.

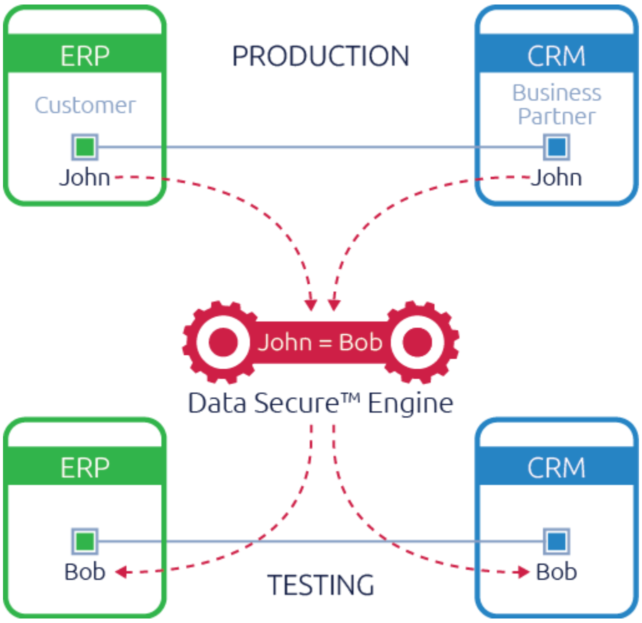

Figure 2: Data Secure Cross Landscape Masking Capabilities

Data Secure is delivered with pre-defined masking rules, and empowers organisations to customise rules to scramble any non-key field on any client-dependent SAP table in a number of different ways (e.g. replace with data from mapping-table, replace with constant value, clear a field). These rules can be extended to cover more specific security needs relevant to an organisation's business.

Data Secure enables companies to comply with all well-known data protection standards such as Sarbanes Oxley, the UK/EU Data Protection Act (DPA), the BDSG (Bundesdatenschutzgesetz), and even the Payment Card Industry Data Security Standard (PCI DSS).

It is important to use a product that is robust and can handle large volumes of data. For example, at British Petroleum (BP) Data Secure scrambled a 3.1 TB System with 23,829 Employees, 992,393 Customers, 94,846 Vendors, 272,849 Business Partners, and 1.6 million Addresses in only 25 minutes.

EPI-USE Labs' consultants are well-equipped to advise you on how to implement a data security policy across your non-production SAP landscape. This usually commences with a workshop for training on Data Secure. The business units and functional teams identify the tables and data that need to be scrambled, then define profiles and create rules. The Basis team then takes charge of the technical implementation – Data Secure was developed for Basis teams to do mass scrambling. It can be used on its own to scramble data in place, or with other products of the Data Sync Manager suite, such as Client Sync and/or Object Sync, to scramble data as you create a new client or copy selected data.

Summary

This paper highlights the concept of data masking, with reference to its relevance, impact and the consequences of using production data in SAP non-production and test environments. In light of the rise in data security violations, staying compliant with industry regulations and government policies/legislations whilst sharing production data in non-production environments is fundamental to all organisations.

Data Masking is essential to secure the data and Data Secure from EPI-USE Labs is one of the best options available. This product was listed on the independent study done by Gartner (Magic Quadrant for Data Masking Technology) [9].

Data Secure performs consistent data masking and de-identification with a user-friendly interface that puts the control into the hands of both basis and functional users.

The implementation of Data Secure as the instrument of data protection in non-production environments, has benefited numerous multi-national organisations across public, private and health sectors in Europe,

Africa, Asia-Pacific and the Americas. The product ensures compliance with regulatory requirements as well as numerous other laws and regulations that govern the use of actual customer data.
The protection of your enterprise landscape is of paramount importance. Contact the EPI-USE Labs team at info@labs.epiuse.com to arrange a demo or an assessment of your data security compliance.

About EPI-USE Labs

EPI-USE Labs provides software and services to help customers manage their SAP landscapes. Our customers work with us to reduce costs of landscape management, comply with various government legislations, data security policies and to implement significant changes to their landscape, like moving to the cloud, mergers, acquisitions and divestitures and heterogeneous migrations. For more information regarding our products and advisory conultancy services visit http://www.epiuselabs.com

References

[1] J.L; Heimerl, Security is Not Just External - Don't Forget the "Other" Security, http://www.securityweek.com/security-not-just-external-dont-forget-other-security , [Acessed on 08/03/2015].

[2] S. Schober, Real cost of data breaches still on the rise, http://www.cutimes.com/2015/03/01/real-costs-of-data-breaches-still-on-the-rise [Accessed on 03/03/2015].

[3] W. Long, EU Data Protection Regulation: fines up to €100m proposed, http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed , [Accessed on 03/03/2015].

[4] L. Whitfield, ICO spells out £500,000 penalty plans, http://www.ehi.co.uk/news/EHI/5542/ico-spells-out-%C2%A3500000-penalty-plans [Accessed on 03/03/2015].

[5] R. Mckeane, EU data protection reform: 12 things businesses need to know, http://www.theguardian.com/media-network/olswang-partner-zone/2014/dec/04/eu-data-protection-reform-business-fines , [Accessed on 02/02/2015].

[6] D. Worth, Target takes $162m hit from cyber attack data breach, http://www.privacyrisksadvisors.com/news/target-takes-162m-hit-from-cyber-attack-data-breach-by-dan-worth , [Accessed on 03/03/2015].

[7] Ponemon Institute, The State of Data-Centric Security, http://www.banktech.com/pdf_whitepapers/incoming/1411503329_ponemon_infa_security.pdf , [Accessed on 05/03/2015].

[8] M. Greenway, Data Obfuscation - managing data privacy in development and test environments, http://www.ncc.co.uk/article/?articleid=15506 , [Accessed on 26/02/2015].

[9] Gartner, Magic Quadrant for Data Masking Technology, https://www.gartner.com/doc/2636081/magic-quadrant-data-masking-technology, [Accessed on 18/03/2015]

Appendix

BELGIUM

Belgium implemented the EU Data Protection Directive 95/46/EC with the adopted law of 8 December 1992 on privacy protection in relation to the processing of personal data. These have been further modified to include the Royal Decree of 13 February 2001. In Belgium, the Privacy commission oversees the enforcement of all data protection laws (DPL).

Belgium data security requirements

- Data controller must put in place adequate technical procedures to protect personal data loss, theft and unauthorized alteration or access (Article 16 & 4, DPL).
- Organisation processing and collecting data must apply state-of-the-art technology in ensuring security and confidentiality of personal data.
- Article 114/1, section 2 of the Electronic Communications Law of 13 June 2005 amended in 2014, requires companies in the electronic communication sector to notify the Privacy Commission of personal data breaches within 24 hours.

Sanctions for non-compliance with Data Protection Law

The DPA provides criminal sanctions for most provisions, including the duty to inform the data subject and the duty to file a prior notification.

- Penalties range from EUR 600 to EUR 600,000.
- Potential imprisonment of up to 2 years depending on severity of breach.
- Loss of organisation's data security policies.
- Publication of penalty judgement and confiscation of data system(s).
- An order to erase the data or prohibition of using the personal data for up to 2 years.

DENMARK

In 2000 Denmark implemented the EU Data Protection Directive 95/46/EC. This was accompanied by the Processing of Personal Data Act. The Danish Data Protection Agency (DDPA) is the body responsible for enforcing data protection regulations.

Denmark data security requirements

The data controller must employ necessary precautions to maintain the security of the data, and prevent the modification, corruption or unauthorised access by third parties.

Sanctions for non-compliance with Data Protection Law

- The controller shall compensate any damage caused by the violation of the DPA.
- Data breach exposure shall be liable to a fine or imprisonment of up to 4 months.
- Criminal liability may be imposed on companies, or legal persons pursuant to the rules laid down in Chapter 5 of the Danish Penal Code.

FINLAND

In Finland, the privacy right of an individual is protected by Finnish Constitution 731/1999. This applies to a number of enacted laws, including the Personal Data Act (523/1999) (henkilötietolaki) (PDA). The DPA is overseen by The Data Protection Ombudsman (DPO) and the Data Protection Board (DPB). The following sectoral laws have priority over PDA.

- Protection of Privacy in Electronic Communications Act.
- Protection of Privacy in Working Life Act. This regulates the processing of employee data.
- Credit Data Act.
- Status and Rights of a Patient Act. This regulates the rights of a patient to access health data.

Data security requirements in Finland

The data processor/collector must carry out both technical and organisational security policies necessary for protecting personal data against:

- Unauthorised access.
- Unlawful destruction, manipulation, disclosure and transfer.

Sanctions for non-compliance with Data Protection Law

- Data secrecy violation offence is liable to a fine or one year imprisonment.
- The DPO can revoke an organisation’s permission to process personal data at the request of the board (DPB).
- The data processor/collector is mandated to compensate a data subject for any economic and other loss suffered by them due to processing in breach of the law.

FRANCE

France enforces the Data Process Act (DPA), which implemented Directive 95/46/EC on data protection (Data Protection Directive). The French data protection authority, Commission Nationale de L'Informatique et des Libertes (CNIL), enforces and gives sanctions governing DPA in france. There are other sectoral laws governing data security in France such as :

- The Public Health Code, Articles L. 1110-4, L. 1111-8, L. 1112-3, L. 1121-3, L. 1142-24-4, L. 1343-3, and L. 2132-1.
- The Monetary and Financial Code, Articles L. 440-4, L. 464-1, L. 464-2, and L. 612-17.
- The Postal and Electronics Communications Code, Article L. 34-5 for electronic marketing and Article L. 34-1 et seq for electronic communications operators.

Data security requirements in France

The data controller must employ necessary precautions to maintain the security of the data, prevent the modification, corruption or unauthorised access by third parties (Article 34, Data Process Act (DPA)). CNIL recommendations for ensuring security include but not limited to the following:

- Strong password management.
- Adopting an information systems security policy.
- Secure physical access.
- Secure local networks.
- Secure workstations.
- Training users on information technology risks
- A process for the creation and deletion of user accounts.
- Ensuring confidentiality.
- Identification of who accesses the data.

Sanctions for non-compliance with Data Protection Law

- E-communication services providers (including ISPs and mobile phone operators) must notify the CNIL within 24 hours of becoming aware of a data security breach.
- The CNIL also has the power to employ on-site inspections, document reviews, warnings and notices, hearings, injunctions and fines.
- There are fines of up to EUR 150,000 for a first violation and fines of up to EUR 300,000 for a second violation within 5 years. E-communication services providers (including ISPs and mobile phone operators) must notify the CNIL within 24 hours of becoming aware of a data security breach.
- A criminal fine of up to EUR 300,000 (or EUR1.5 million for a corporate entity) and/or 5 years' imprisonment.
- New DPA draft to increase fines of up to EUR 100 million or 5% of annual turnover for serious breaches of personal data.

GERMANY

The main law for protection of personal data in Germany is the Federal Data Protection Act (Bundesdatenschutzgesetz) 1990. This was amended in 2003 and 2009 to include major reforms such as federal Data Protection Act Amendment Law (Novelle des Bundesdatenschutzgesetzes). The Act generally applies to all businesses, irrespective of size and sector, that collect or process personal data. There are also sectoral laws of importance such as :

- Telemedia Act (Telemediengesetz), which applies to providers of telemedia services (such as websites).
- Telecommunication Act (Telekommunikationsgesetz), which applies to providers of telecommunication services.
- Criminal Act (Strafgesetzbuch).
- Social Security Code I, II; IV, V and X, regulates the processing of personal and health related data with the provision of medical and social security services.

Data security requirements in Germany

- Prevent unauthorised persons from gaining access to data processing systems for processing or using personal data.
- Prevent data processing systems from being used without authorisation.
- Personal data collected on behalf of others must be handle in strict compliance with the controller's instructions .
- Ensure that personal data is protected against accidental destruction or loss (availability control).
- Particularly sensitive data (such as bank credit card data, telecommunications and online collected data, and data related to criminal offences) are abused, stolen or lost, and a third party acquires knowledge of the contents.

Sanctions for non-compliance with Data Protection Law

- A maximum EUR 300,000 fine for administrative offences. However, In October 2009, the data protection authority of Berlin imposed a fine of EUR 1,123,503.50 on Deutsche Bahn AG because of significant violations of data protection law.
- Violation of data protection law may be a criminal offence punishable with imprisonment of up to two years or a fine, depending on the seriousness of the violation.
- Reputational damages consequences gives rise to bad publicity.
- The German government has proposed a new draft law introducing class actions for data protection violations.

NORWAY

The Personal Data Act (PDA) is the main legislation that regulates the collection and use of data in Norway. The Personal Data Regulation (PDR) sets out comprehensive regulations on specific topics covered by the PDA. In Norway, the EU DPA directive 95/46/EC has been implemented via the PDA and PDR. There are also provisions governing collection and use of personal data across the following laws:

- The Health Register Act.
- The Health Research Act.
- The Bio Bank Act.
- The Police Register Act.
- The Schengen Information Systems Act.
- The National Register Act.
- The Penal Register Act.

The sectoral Acts above are not covered within the scope of this appendix.

Data security requirements in Norway

Confidentiality, integrity and accessibility (section 13, paragraph 1, PDA) must be retained.

- The controller and processor must document the information system and the security measures adopted.
- Security audits on the information system used to house data must be conducted on a regular basis to assess whether it is appropriate for the enterprise, and whether the security strategy of the company provides adequate security (PDR section 2-3).
- The control must carry out ongoing risk assessment to assess the probability and consequences of security breaches (PDR section 2-4).
- Adequate configuration of the information system must be carried out to achieve sufficient security of data (PDR section 2-7).
- Adequate measures must be put in place to prevent unauthorized access to equipment used to process personal data (PDR section 2-10).
- Encryption and protection mechanisms must be applied to data in transit to ensure confidentiality of data (PDR section 2-11).

Sanctions for non-compliance with Data Protection Law.

- Fines of up to ten times the national insurance basic rate, therefore approximately EUR 110,000 (in 2015).
- Data controllers are liable to compensate data subjects for damages incurred due to data breach exposure.
- The penalty for gross negligence of breaches of several provisions of the PDA shall be a fine or one to three years' imprisonment, depending on severity of the the breach.

SPAIN

The Protection of personal data is regarded as a constitutional right in Spain. Directive 95/46/EC on data protection was formally implemented in November 1999 through the Data Protection Act 1999. The Spanish Data Protection Agency (Agencia Española de Protección de Datos) (AEPD) enforces data protection legislations.

There are numerous legislations affecting data protection, of which notable examples include:

- Law 34/2002 of 11 July on information society services and electronic commerce (LSSI). This law implemented Directive 2000/31/EC on certain legal aspects of information society services such as electronic commerce.
- Telecommunications Law 9/2014 (which replaces General Telecommunications Law 32/2003) governs the communications confidentiality and the protection of personal data within electronic communication networks and services.

Data security requirements in Spain

- Organisations handling personal information to which "medium" or "high" security requirements apply must appoint a data protection officer.
- A high level of security must be applied to databases with sensitive data.
- It is mandatory to apply stringent access control and data encryption when transferring the data.
- There must be control of employees’ access to data.
- The data controller and all parties involved in the processing of personal data must keep the data confidential, even after processing is complete.

Sanctions for non-compliance with Data Protection Law

Spain has one of the most stringent penalty systems in the entire EU in the event of breach of the DPA. Google was fined €900,000 in 2012 for changing its privacy policy approaches to data retention. Both data controllers and data processors (outsourcers) are liable for breaches of data protection law. The Data Protection Act (LOPD) identifies a large number of different offences, which are classified as follows:

- Minor breaches incur fines of EUR 900 to EUR 40,000, for example for neglecting to register a database with the Spanish Data Protection Agency.
- Medium breaches result in fines from EUR40,001 to EUR 300,000, for example for failure to obtain the consent of a data subject to process personal information when legally required.
- Serious data breaches incur fines from EUR 300,001 to EUR 600,000.

THE NETHERLANDS

The Wet bescherming persoonsgegevens (the Data Protection Act) is The general data protection law. Data protection enforcement is through the Dutch Data Protection Authority (Dutch DPA) ("College Bescherming Persoonsgegevens")).
Article 10 (right to privacy) of the Dutch constitution has an impact on protection of data. This is particularly true for determining legitimacy of data breaches in favour of right to privacy. Article 162 of book 6 of the Dutch Civil code may be invoked when a data subject who's right to privacy has been compromised.

Data security requirements in the Netherlands

- The Dutch DPA guidelines encourages a privacy by design approach.
- Access the risk of data being processed for the data subject(s).
- Make use of all generally accepted data security standards.
- Conduct periodic audits to evaluate general security standards implemented.
- There are sectoral (Financial, Healthcare and Telecommunication) requirement to report data breaches to data subjects and the Dutch DPA.

Sanctions for non-compliance with Data Protection Law

- Non-compliance with the data protection acts and reporting of breaches will incur a maximum administrative fine of EUR 450,000.
- Claim for damages under the Dutch civil code.
- As of March 2014, Intentional offence is liable to six months prison sentence or a fine amounting to EUR 20,250 if it is an individual and up to EUR 78,000 for a legal entity.

THE UNITED KINGDOM (UK)

The 1998 Data Protection Act is the national law in the United Kingdom. The information Commissioner's office (ICO) is the UK data protection authority (DPA). Publications pertaining to data protection (ICO guide) along with certain codes (ICO codes) are readily available reference guidelines. In the UK, the following sectoral laws are also in enforcement;

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (the implementing national legislation for Directive 2002/58/EC on the protection of privacy in the electronic communications sector (e-Privacy Directive)).
- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR Amendments) (Implementing national legislation for the amended e-Privacy Directive).

Data security requirements in United Kingdom.

An organisation's Information security may vary by circumstances. It is therefore the ICO'S recommendation for organisations to adopt a risk-based approach in deciding level of security need.There are applicable British Standard Institute (BSI) and ISO/IEC 27001,27002 information security management practices and data security guidelines that should be integrated as part of an organisation's data privacy policies. In addition, the following are required by the ICO;

- Design and organise your security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear of whose responsibility it is to enforce information security in your organisation.
- Ensure you have an assessed appropriate physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
- Be ready to act on any security breach swiftly and effectively.
- Privacy by design although not yet a mandatory requirement of the ICO, is encouraged to be a key consideration in the early and lifecycle stages of a project.

Sanctions for non-compliance with Data Protection Law

- An organisation who commits a serious violation of the DPA or PECR or violation likely to cause substantial damage is liable fines up to £500,000 (DPA, section 55A).
- Failure to comply with enforcement is an offence prosecutable in the crown court with unlimited fines.
- Violation of any data protection law is likely to receive negative press (publicity).

www.epiuselabs.com | info@labs.epiuse.com