fieldfisher

Vormetric Data Security™

The legal obligations for encryption of personal data

in the United States, Europe, Asia and Australia

June 2014

Contents

For further information, please do not hesitate to contact:

Phil Lee
Head of US Office
D: + 1 (650) 513 2769
E: phil.lee@fieldfisher.com
Follow: @euprivacylawyer.com
Blog: privacylawblog.fieldfisher.com

Executive summary

Introduction

Concerns about data security – or, more accurately, the lack of it – have entered the public consciousness over the past twelve months in a way never before seen. Over this period, we have witnessed countless stories making the headlines about cyber threats, covert surveillance, security breaches, and data loss. The response to this has been a global awakening in the minds of the public about the urgent need to address data security concerns. This, in turn, has prompted law makers and regulators the world over to become increasingly engaged in implementing new legal frameworks and defining new obligations for data security.

Prominent within recent developments has been a legislative and regulatory convergence on encryption as a key tool for protecting security, not only of portable equipment and storage media, but also of databases, unstructured data, the Cloud and application data. In some territories, a requirement to deploy encryption is '*hard coded*' into legal or regulatory standards; in others, encryption is implicitly endorsed as a readily available, market-standard solution that protects businesses from the most adverse legal consequences of a data breach.

As the world progresses from a mere "*information age*" into an age of "*big data*", it is a simple truism that the volume, granularity and sensitivity of data collected from and about us all with grow exponentially. And, as that happens, the risks and consequences of losing that data will become ever more severe. Keeping this in mind, and reflecting on the trends that developments in data security law have shown to date, we will undoubtedly see the law becoming even more prescriptive over time about the nature of the encryption technologies that must be adopted and rolled-out across organisations.

This White Paper

This White Paper examines the legal and regulatory obligations to encrypt personal data in three of the major economic regions of the world, namely:

- the European Union - exploring, in particular, the regimes that exist at present in the United Kingdom, France, Germany and Spain;
- the USA; and
- the Asia-Pacific region - exploring, in particular, the regimes that exist in Singapore, South Korea, Japan, Taiwan and Australia

In each case, this paper presents the argument that, whether expressly or by implication, the laws in those jurisdictions give rise to a clear need to deploy encryption technologies to protect personal data.

In addition to this, this White Paper also explores how financial services laws and regulations require encryption in some jurisdictions, examining particular obligations placed on the payments services industry, and the obligation to implement access controls and threat pattern recognition capabilities.

While it is a critical weapon in any data security armory, encryption is, of course, not the beginning and the end to data security compliance. Throughout this paper it is important for organizations to keep in mind the wider context of legal obligations to which they are subject. Specifically, organisations must ensure that they implement a robust policy framework, underpinned by compliance, managerial and technical processes that address the threats and risks to data, networks and communications systems in a truly holistic fashion.

To this end, organisations must address issues as various as:

- access rights and privileges (eg., are data accessed by the right people in the organisation or by too many people?);
- data segregation (eg., in a "*shared service*" environment of data centre consolidation, are data physically or logically separated so that specific country-level legal requirements can be met?);
- incident detection and threat pattern recognition (eg., if a failure event is suffered, such as a cyber incident, security breach or data loss, is that event detected early enough and acted upon?);
- auditing (eg., can the organisation prove that technologies are operating as required from time-to-time?); and
- training (eg., do staff understand their obligations with respect to the secure handling of data, so that the organisation has done all it can to minimize the risk of "*human error*"?).

A good illustration of the wider context of legal obligations for security has been provided recently by the expert body within the European Union that is responsible for the development of EU data protection. In its July 2012 Opinion on Cloud Computing, the Article 29 Working Party identified the core legal requirements for data protection in the Cloud to include requirements for logging and auditing of all processing operations; identification of all locations where data are processed; identification of all members involved in the provision of services in the supply chain; achievement of incident detection and breach reporting; detection of alterations to personal data, through the use of cryptographic authentication; encryption of data at rest and in transit; secure remote administration; isolation of data to achieve compliance with the purpose-limitation principle at the heart of EU data protection law (data should only be processed for the purpose for which they were obtained), through the management of access rights, roles and privileges; and the proper management of shared resources, so that one customer's personal data are separated from another's.

The UK Information Commissioner, who regulates the Data Protection Act 1998, published his own Cloud Computing guidance, in October 2012, which supports all of the key messages of the Article 29 Working Party. This guidance recommends the deployment of encryption for data at rest (subject to the need to provide unencrypted data that is required for processing) and data in transit, which should be supported by robust key management. The guidance also makes the point that cloud service providers need to be alert to the need for data segregation, so that customers' data do not become mixed.

The trend towards encryption is also repeated in the US. For instance, many US breach disclosure laws provide a "*safe harbour*" against the compulsory disclosure of security breaches where data are protected by encryption and, clearly, this will extend beyond encryption of mobile and portable devices to databases and applications. Legislations like HIPPA (Health Insurance Portability and Accountability Act) and Gramm-Leach-Bliley also contain express or implied requirements for the encryption of data.

What this all amounts to is that we are witnessing a global harmonisation of the legal and regulatory need for encryption.

Vormetric

This White Paper has been commissioned by Vormetric Inc., a leading IT security company focusing particularly on enterprise encryption and compliance solutions, whose Data Security solution provides a single, manageable and scalable solution to encrypt any file, any database, any application, anywhere it resides— without sacrificing application performance or creating key management complexity. Visit *http://www.vormetric.com/* for more information.

The legal framework for encryption in the EU

The EU data protection regime is built around the Data Protection Directive 1995 (the **1995 Directive**) and the Privacy and Electronic Communications Directive 2002 (**ePrivacy Directive**). However, in considering the legal framework for encryption it is important also to consider the new EU Payment Services Directive (**PSD 2**).

Data Protection Directive 1995

The 1995 Directive sets the overarching framework for data protection in the EU, and applies to data controllers (i.e. the organisations that determine how and why personal data is processed) that process "*personal data*" about living individuals. The 1995 Directive sets out certain core principles concerning the processing of personal data, and there is a specific requirement under Article 17 for Member States to implement "*appropriate technical and organisational measures*" to protect personal data against accidental loss or unauthorised disclosure, and to ensure those measures maintain "a *level of security appropriate to the risks represented by the processing and the nature of the data to be protected*".

By implication, therefore, we can see that a clear obligation exists to deploy encryption technologies in certain situations and this is supported by a wealth of regulatory expectations and guidance from many of the EU data protection authorities.

ePrivacy Directive

The ePrivacy Directive applies specifically to the electronic communications sector (i.e. to service providers, such as telecommunications companies and ISPs) and to the processing of personal data in electronic communications systems.

The ePrivacy Directive also places a number of significant obligations on organisations for the purposes of improving data security. Service providers must "*ensure that personal data can be accessed only by authorised personnel for legally authorised purposes*" and must "*protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure*".

In addition (and in contrast to the general requirements under the 1995 Directive), service providers must notify affected individuals of personal data breaches, without undue delay. This is a requirement of EU Regulation (No 611/2013) on the measures applicable to the notification of personal data breaches under the ePrivacy Directive, which came into force on 25 August 2013. However, there is no requirement for service providers to notify individuals of a breach where they can prove that they implemented appropriate technological measures which would "*render the data unintelligible*" to any third party. In other words, there is no obligation for telecommunications companies and ISPs to notify affected individuals where the data have been effectively encrypted.

EU Regulation (No 611/2013) provides an explicit exemption from the breach notification requirements where the data are rendered unintelligible to any person not authorised to see it. Specifically, data will be considered "*unintelligible*" if they have been effectively encrypted (provided, of course, that the encryption key has not been compromised and that it cannot otherwise be ascertained by available technological means).

In conjunction with EU Regulation (No 611/2013), the Commission plans to publish an indicative list of appropriate cryptographic measures, and in so doing will consult with the Article 29 Working Party and the EU Agency for Network and Information Security (**ENISA**). ENISA has, in fact, gone on to publish a guidance note and accompanying recommendations on cryptographic measures. This guidance was published in September 2013, and ENISA intends to update the specific technical recommendations on a yearly basis, having regard to the state of technological developments.

Payment Services Directive

The current EU directive on payment services provides the legal foundation for the creation of an EU-wide single market for payments, and applies to firms providing payment accounts, executing payment transactions, issuing payment instructions and providing money remittance services. In July 2013, the EU Commission published an update in the form of PSD 2, which is still in draft form but is expected to be agreed and fully implemented by 2016.

Once implemented by each EU Member State, PSD 2 will bring a range of new players inside the regulatory

regime, with the aim of encouraging new low-cost internet payment solutions such as mobile payment applications under defined and controlled conditions. Most importantly here, PSD 2 includes increased security requirements for payments instruments, with new operational, security and authentication obligations.

Payment services providers will also be required to comply

with the new EU Cyber Security Directive (also currently in draft form) which, like the 1995 Directive, mandates the use of "*appropriate technical and organisational measures*" to manage the risks posed by the security of applicable networks and information systems. In addition however, payment services providers will be required to use "*strong customer authentication*" when electronic payment transactions are initiated, and will be required to notify users, without undue delay, of security incidents which have the potential to impact their financial interests, as well as informing them of possible measures that they can take to mitigate against the adverse effects of the incident. If we follow the same line taken with the ePrivacy Directive, the use of effective encryption measures will be enough to circumvent these breach notification obligations.

These regulatory implications are likely to be far reaching. Once PSD 2 and the new Cyber Security Directive are embedded into the European legal system, we can expect other international legal regimes to follow suit. Even if other legal regimes do not follow suit immediately, we can at the very least expect regulators and citizens the world over to have sky-high expectations when it comes to the security of payments transactions. Put another way, strong user authentication will become the expected norm.

Encryption in the EU

This encryption safe harbor within EU law also extends to database and application. Critically, it should be understood that EU law is written so as to be "*technologically neutral*", so as to avoid redundancy in the law as technologies become obsolete. Therefore, organisations operating in the EU should be prepared for perceived ambiguities in the law. However, the law on encryption is not ambiguous and these are the key principles to note:

1. Some national legislations of EU Member States have specifically referred to encryption, but most have not.
2. The "*detail*" of the law is actually set by regulators and the courts, who develop the law as they address certain aspects of it.
3. The EU data protection regulators universally expect organisations to use encryption technologies to protect personal data, particularly where those data are highly sensitive or confidential, so that harm could not be suffered if there was a security breach.
4. The EU regulators have not yet got round to analysing all forms of encryption available in the market place, or all of the situations where encryption could be used, because regulation develops in a piecemeal way. However, ENISA's recommended cryptographic measures are highly conclusive, and it is clear from the way that the law has been developed and applied that organisations that process personal data must consider what is available on the market and the situations where encryption can be deployed, as they develop their IT strategies.

Taking EU data protection law as a whole, a very compelling conclusion is reached: there is a legal requirement for application encryption, database encryption, cloud encryption, server/PC/laptop/mobile encryption in the EU (which covers data at rest and data in transit), and a clear signal that there will be a legal obligation for adopting strong user authentication solutions.

It is worth noting that, in addition to PSD 2 and the Draft Cyber Security Directive, the EU general data protection legal framework is currently undergoing a process of revision. While this will not add greater specificity to the wording of the law, there is a clear expectation that non-compliance will be treated much more harshly in the future and where there is a lack of encryption there could be very large financial penalties, perhaps as much as €100,000,000 or 5% of annual worldwide turnover.

Access rights & pattern recognition intelligence

As the cyber and data security threat landscape persists, the reality is that we will continue to be faced with a growing number of targeted attacks, APTs, malicious hacks, and the unrelenting threat of personal information and financial data theft, and this threat landscape has not gone unnoticed by leaders the world over.

In the US and the EU the development of national cyber security strategies has highlighted the need to implement real-time access control measures to ensure data can be accessed only by those authorised to see it, and to have in place pattern recognition technologies to capture intelligence post-event to identify anomalous processes and user access patterns. Solutions like Security Information and Event Management (**SIEM**) and data security and IP logs can be deployed to achieve this, and we can expect that an organisation's failure to implement such measures will be met with tough regulatory scrutiny and heavy sanctions.

The certainty surrounding the obligation to implement access controls and pattern recognition capabilities goes beyond mere professional opinion. Global security standards such as ISO27001 have standards specifically mandating the business requirement for access controls, and in the EU there is established jurisprudence that implementing access controls are an essential component of citizens' fundamental right to privacy (see, for instance, the European Court of Human Rights case *I v Finland* [2008]).

The legal framework for encryption in the USA

In contrast with the EU, the US data protection regime is based on a '*sectoral model*' meaning that personal information is protected by various laws applicable to particular industry sectors. What's more, federal laws as well as laws of individual states will apply, so organisations are often faced with having to comply with a complex web of laws. That said, the picture is clear; there is a growing trend towards encryption in many sectors and in many US states.

For instance, breach disclosure laws in 47 States currently provide a "*safe harbour*" against the compulsory disclosure of security breaches where data are protected by encryption. Similarly, the proposed Consumer Bill of Rights (which reflects the US government's view on privacy) sets out a number of principles which should apply to personal information in online settings. This includes the principle of '*security*' which states that '*all consumers have a right to secure and responsible handling of personal data*'.

By implication, therefore, we can see that a clear level of expectation exists to deploy encryption technologies in certain situations and this is supported by a wealth of sector-specific and state laws.

State Level Breach Reporting and Data Security Law

Data protection law in the USA is not only sector-specific but also state-specific and the majority of states now have data breach notification laws in place.

The state of California, for instance, is regarded as one of the leading regulators in this area, whose laws are regulated and enforced by the Department of Justice's Privacy Enforcement and Protection Unit. California's new privacy law - Senate Bill 1386 - will come into effect on 1 July 2014 and introduces a requirement for any company conducting business in California which owns computerised personal data to notify Californian residents of any actual or suspected security breach that compromises the "*security, confidentiality or integrity*" of the information, unless the data have been encrypted.

Other states such as Massachusetts have passed laws which expressly require the encryption of electronically communicated personal data. Section 17.04 of Law 201 CMR 17.00 requires the implementation of adequate computer system security measures to protect personal data which includes '*encryption of all transmitted records and files containing personal information that will travel across public networks or wirelessly*' and '*encryption for all personal information stored on laptops or portable devices*'.

Federal Trade Commission (FTC)

The Federal Trade Commission, established in 1914 by the FTC Act and appointed by the US President, aims to protect consumers against anticompetitive, deceptive or unfair business practices and to increase consumer awareness of competitive practices.

There is no question that the FTC expects organisations to implement suitable encryption methods to protect consumer data. Firstly, it has interpreted the FTC Act as requiring encryption of data, with a recent case being brought against a hotel chain whose unencrypted financial data were stolen by hackers. In recent months we have also seen regulatory scrutiny surrounding the payments services industry in light of the massive data breaches at Target, Neiman Marcus, and Michaels Stores in which millions of citizens' personal information was compromised.

In another recent case in January 2014, the FTC found that it had the authority to penalise a company which had failed to implement acceptable security safeguards when electronically transmitting results to patients and providers. Ultimately it was found that the FTC is able to hold businesses accountable for inadequate security practices that may cause or are likely to cause substantial injury to consumers. In light of this, it is possible that the FTC may claim that because encryption is readily available, the failure to implement it constitutes an inadequate safeguard, which would then subject the organisation in question to enforcement action and intense regulatory scrutiny.

Health Insurance Portability and Accountability Act 1996 (HIPAA)

The US government, in recognition that the movement to electronic data exchange within the healthcare sector created new risks to privacy and security, enacted HIPAA which creates national standards for electronic protected health information (**EPHI**). The Office for Civil Rights enforces the numerous rules established under HIPAA which include the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule and the Patient Safety Rule.

The HIPAA Security Rule requires covered organisations to implement technical safeguards to protect all EPHI, making specific reference to encryption. For instance, section 164.312(a)(2)(iv) provides that entities must "implement a mechanism to encrypt and decrypt electronic protected health information", and according to section 164.312(e)(2)(ii) entities must also "*implement a mechanism to encrypt electronic protected health information whenever deemed appropriate*". The Security Rule then goes on to set out numerous examples of encryption methods which can be employed and the factors to consider when implementing and ensuring the success of an encryption strategy.

We can see then that there is no ambiguity in the law on encryption in the US health sector; organisations are expected to implement suitable encryption methods to protect EPHI.

Gramm-Leach-Bliley Act 1999 (GLB)

In 1999 the Financial Services Modernisation Act (known as the Gramm-Leach-Bliley Act, or GLB) was introduced as part of the reorganisation of financial services regulation in the USA. The GLB applies to financial institutions and governs the handling of non-public personal information. The GLB sets out basic requirements which financial institutions are expected to follow including securely storing personal financial information; giving notice of policies regarding the sharing of personal financial information; and giving consumers the ability to opt out of the sharing of some of their personal financial information.

Section 501(b) of the GLB requires financial institutions to follow agency standards to protect the security, confidentiality and integrity of non-public customer information through "*administrative, technical and physical safeguards*". It also requires each financial institution to implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size, complexity and scope of activities of the institution. Collectively, therefore, an obligation exists for organisations operating in the financial services sector to maintain data security and deploy encryption technologies for electronically submitted and stored customer information where appropriate.

Fair Credit Reporting Act 1970 (FCRA)

The FCRA was introduced to regulate the collection and use of consumer information, in particular consumer credit information, and its provisions are enforced by the FTC. It is aimed at ensuring the fairness, accuracy and privacy of personal information contained in the files of credit reporting agencies.

Under FCRA, consumers have numerous rights including the right to be told if information in his file has been used against him; to know what information is held in his file; to ask for a credit score; and the right to dispute incomplete or inaccurate information. Encryption is not specifically cited in the FCRA, however credit reporting agencies are expected to secure data and prevent wrongful leakage, loss or damage of consumer credit information, and therefore the inference is clear that encryption technologies should be deployed.

Federal Information Security Management Act 2002 (FISMA), and Federal Information Security Amendments Act 2013

FISMA – signed into law as part of the Electronic Government Act 2002 – was introduced to require federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity and availability of IT systems and related information. It defines a comprehensive framework designed to protect government information, operations and assets against natural or man-made threats.

Recently, the Federal Information Security Amendments Act 2013 was introduced, extending the security requirements of federal agencies to include responsibilities for complying with computer standards developed by the National Institute of Standards and Technology (**NIST**); ensuring complementary and uniform standards for information and national security systems; securing facilities for classified information and ensuring that information security performance indicators are included in the annual performance evaluations of all senior managers.

NIST, a unit of the US Department of Commerce (formerly known as the National Bureau of Standards) is responsible for promoting and maintaining standards. NIST has published various standards and guidance such as the '*Guide to Storage Encryption Technologies for End User Devices*' in which it states "*the primary security controls for restricting access to sensitive information stored on end user devices are encryption and authentication*", with further details of recommended solutions. NIST has also published '*Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems*' which was developed to support FISMA. It is the primary source of recommended security controls for use by Federal agencies, and it is therefore abundantly clear that, federal government agencies are required to protect and maintain the security of government data by deploying encryption technologies.

Cybersecurity Executive Order and NIST Developments

In February 2013 the White House, in collaboration with NIST, issued Executive Order 13636 entitled '*Improving Critical Infrastructure Cybersecurity*' (the **Order**) designed to improve the cybersecurity of critical infrastructures in the USA. The Order builds on NIST's development of cybersecurity technical standards and requires, among other things, for NIST to be responsible for leading the development of the Cybersecurity Framework in the US (the **Framework**), intended as a best practice guide for banking, defence, utilities and other industries to help protect against cyber-attacks.

NIST has, for instance, developed standards such as the '*NIST Framework and Roadmap for Smart Grid Interoperability Standards*' which recommends the IEC 62351 standards for secure communications, and sets out guidelines on the use of the Transport Layer Security protocol for data encryption. Most recently, NIST has reopened the public vetting process for introducing an encryption standard, and is currently working with the word's cryptography experts to support robust encryption and introduce an effective standard.

In February 2014, the US government officially introduced its final version of the Framework after publication of the draft Framework in October 2013 and a 45 day feedback period. NIST drew up the Framework with input from 3,000 industry and academic experts in response to the Order and is a step in the right direction towards implementing cyber security legislation in the USA. Adoption of the Framework is voluntary but the US Department of Homeland Security has established the Critical Infrastructure Cyber Community (C3) Voluntary Program to increase awareness. Although the Framework does not mandate that organisations implement encryption, the Framework is likely to affect companies across the USA as they will need to assess their use of personal information in cybersecurity activities to ensure it is properly secured. In any event, the encryption standards being developed by the NIST will have further impact on organisations as they will need to implement strategies and processes on mandatory access controls and intelligence pattern capabilities to demonstrate compliance with legal obligations, industry standards and regulatory expectations.

PCI DSS

The Payment Card Industry Security Standards (**PCI DSS**), produced by the PCI DSS Council, provide a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to any entity involved in payment card processing including merchants, processors, acquirers, issuers, and services providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data. The standards are revised every three years, and the latest version (**PCI DSS v3.0**) has been effective from 1 January 2014.

The significance of PCI DSS is that it specifically mandates encryption. For example, Requirement 2.3 of PCI DSS v3.0 requires entities implementing PCI DSS to '*encrypt all non- console administrative access using strong cryptography*'. Requirement 3 also provides details of the protective mechanisms that entities should put in place to protect cardholder data and the recommended protection methods specifically include encryption, truncation, masking and hashing.

While compliance with PCI DSS is enforced by the major payment card providers, it is also worth noting that cardholder data is treated as "*personal data*" for the purposes of EU data protection law. Either way, therefore, the position is clear: cardholder data must be encrypted. It is also likely that we will see much more regulatory focus in this area given the many recent data security incidents regarding the compromise of cardholder. Recent high profile examples include Target, Neiman Marcus and Michaels Stores, but it is likely we will see similar incidents, ramping up both regulatory and business attention on the need to adequately secure personal data.

The United Kingdom (UK)

Data protection

The Data Protection Act 1998 (**DPA**) requires data controllers to take "*appropriate technical and organisational measures*" to keep personal data safe and secure:

"*Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—*

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected."

These rules "*set up*" the obligation for encryption: quite simply, encryption technologies fall within "*the state of technological development*" and consequently should be deployed in appropriate situations.

The DPA is regulated and enforced by the Information Commissioner's Office (**ICO**) which has published regulatory guidance to promote good practice and explain enforcement policies and strategies. What is clear from the guidance is that the ICO mandates the use of encryption. The ICO published specific guidance on encryption in November 2007, and in the Practical Guide to IT Security (April 2012), encryption is highlighted as "*a means of ensuring that data can only be accessed by authorised users*". Most recently the ICO has published guidance on Bring Your Own Device (**BYOD**) policies which again reinforces the need for encryption, and has stated publicly that encryption is an important "*first step*" that businesses must consider when assessing their data processing operations. Further, in a security report concerning the protection of personal data in online services published in May 2014, the ICO highlighted failure to encrypt online communications as being among the top computer security vulnerabilities.

The ICO's regulatory guidance has legal effect and has formed the basis of regulatory enforcement action against many data controllers. Much of this enforcement action has been unchallenged, which points to a clear acceptance by data controllers of the need to encrypt personal data. Recent regulatory action has focused on unencrypted laptops, optical drives and memory sticks. Later cases reveal that the trajectory of the law is toward encryption of emails and other electronic communications. Other cases have pointed to a need for server encryption and database encryption online. In other words, the DPA has created a legal environment for encryption of personal data in the UK.

Financial services

Data controllers operating in the financial services sector in the UK are also regulated by the Financial Conduct Authority (**FCA**) (formerly the Financial Services Authority, or **FSA**), which derives its powers from the Financial Services and Markets Act 2000 (**FSMA**). The legal framework within FSMA obliges financial services companies to have regard for operational risk and to mitigate the risk of financial crime. Collectively, these obligations set up the obligation to encrypt data. Unlike the DPA, the FSMA's reach is not limited to personal data.

In February 2007, the encryption issue in the financial services sector came to a head when the then FSA fined a Building Society £980,000 following the loss of an unencrypted laptop computer containing customer data. In April 2008, the then FSA published a comprehensive report on financial crime and data security which repeated its expectation that financial services companies must encrypt portable devices and media. In 2010 an insurance company was fined £2,275,000 following the loss of unencrypted backup tapes in transit. These fines demonstrate that the financial services sector in the UK has also enhanced the importance of encryption of personal data.

France

Data Protection

Act No. 78-17 on Data Processing, Data Files and Individual Liberties 1978 (**French DPA**) requires data controllers to take "*all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties*" (Article 34).

The French DPA is regulated and enforced by the Commission Nationale de l'Informatique et des Libertés (**CNIL**) who, in its regulatory guidance, highlights the existence of numerous threats to IT systems and networks including computer fraud, fraudulent data collection, data loss and dissemination of confidential information, and urges data controllers to take these threats seriously. Much consideration has been given to cloud technologies, and the corresponding need for new security standards to bolster the security of personal data. The CNIL has stressed the importance of using encrypted links like "*https*" for electronic exchanges of data and the CNIL also requires the encryption of data at rest in the Cloud.

Regarding breach disclosure the provider of electronic communications services must promptly notify the CNIL and also the affected party, except where the CNIL finds that "*appropriate protection measures*" were applied to the data. The CNIL clearly defines encryption as an "*appropriate protection measure*" and advises that risks to an individual would be limited where, for example, that individual's customer file was subject to computer hacking but where there was "*no possibility of its being opened without prior decryption with a confidential password that had not been hacked*".

Financial services

Organisations in the financial sector in France are bound by professional secrecy obligations (for example in the Monetary and Financial Code which incorporates the main provisions of the Banking Act 1984, Financial Activity Modernisation Act 1996 and the Financial Act 2010) and so must ensure that they have appropriate measures in place to ensure compliance.

Autorité de contrôle prudentiel (**ACP**) and Autorité des marchés financiers (**AMF**) are each responsible for regulating financial institutions who must have regard for the operational risks in this sector, and implement measures necessary to mitigate against financial crime. Collectively, therefore, an obligation exists for data controllers operating in the financial services sector to maintain data security and deploy encryption technologies where appropriate.

Germany

Data Protection

The Federal Data Protection Act (Bundesdatenschutzgesetz) (**BDSG**) places an obligation on bodies processing personal data to take "*appropriate technical and organisational measures*" to preserve data security, and explicitly refers to encryption technologies for that purpose. In particular, the Annex to Section 9 of the BDSG states "*A measure in accordance with sentence 2 nos. 2 to 4 [i.e. a measure of access and transport control] in particular is the use of an up-to-date encryption method*".

Specifically, the BDSG places an obligation on organisations to process data in such a way as to prevent unauthorised access or disclosure, ensure such unauthorised access is capable of being ascertained and ensure that personal data are protected against accidental loss or destruction. In addition, organisations must ensure that data collected for different purposes can be segregated. The requirement to segregate data is laid out in the Annex to Section 9 which provides that measures shall be taken to "*ensure that data collected for different purposes can be processed separately*".

As with French law, the data controller must take all "*useful precautions*" having regard to the nature of the data and the risks of processing for the purposes of data security, though "*appropriate measures*" shall be required only if the effort involved is reasonable in relation to the desired level of protection.

It is clear then that there is a risk-based approach to the obligation to protect personal data; the implication being that encryption technologies must be deployed in appropriate situations. Notwithstanding this, the Federal Commissioner for Data Protection in Germany (the **BFDI**) has, like the CNIL in France, published guidance on its website about cloud technologies which advocates cryptography as a means of ensuring the confidentiality of personal data.

It is also worth noting that there are, in addition, several other laws in which the use of encryption is expressly prescribed, including Section. 6 of the Ordinance on the Database-Supported Information System on Medical Devices, Section. 7 of the Cancer Register Act, and Section 3 No. 33 of the German Telecommunications Act.

Financial services

The Federal Financial Supervisory Authority (BaFin) and Deutsche Bundesbank operate together to regulate the financial sector. The Securities Trading Reporting and Insider List Regulation (Wertpapierhandelsanzeige und Insiderverzeichnisverordnung (**WpAIV**), which operates pursuant to the Securities Trading Act, requires the deployment of measures to guarantee the confidentiality and integrity of data, and there is a specific requirement that "*there is sufficient protection in place against unauthorized access or amendments to the data, and that confidentiality and safety of the transmission are also guaranteed by the nature of the means of transmission used or by state-of-the- art encryption of the data.*" In addition, Section 87a (1) of the German Tax Code also mandates the use of encryption.

Spain

Data Protection

The Spanish Data Protection Law (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (**LOPD**) establishes a general obligation for data controllers, and, where required, data processors (who process on behalf of the data controller) to adopt technical and organisational measures to guarantee the security of the personal data they process. Royal Decree 1720/2007 developed this requirement further by establishing a layered approach whereby data controllers would implement different levels of security (i.e. basic, medium and high) accumulatively depending on the types of personal data they process. The application of high level security measures is only required when certain types of personal data (e.g. sensitive personal data) are processed. In this context, when the application of high level security is required, encryption mechanisms (or other mechanisms that guarantee that information is not intelligible or manipulated by third parties) must be deployed to public or wireless networks.

Australia

Data Protection

The Privacy Act 1988 is the core legislation in Australia and, in December 2012, the Australian Parliament passed the Privacy Amendment (**Enhancing Privacy Protection**) Act 2012 (**the Privacy Act**) which came into effect on 12 March 2014. The original Privacy Act contained the National Privacy Principles (**NPPs**) which will be replaced by the Australian Privacy Principles (**APPs**). Principle 4 of the NPPs governs data security and provides that 'an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'. By implication, encryption is likely to be considered a reasonable measure to implement in order to protect personal information.

The requirement to encrypt personal data is also set out in regulatory guidance published by the Office of the Australian Information Commissioner (**OAIC**) in April 2012. The 'Data breach notification – A guide to handling personal information security breaches' is designed to assist organisations in responding effectively to data breaches. Crucially, it outlines some key considerations which organisations should follow in order to comply with Principle 4 of the NPPs which include *'implementing privacy enhancing technologies to secure personal information held by the agency or organisation, including through such measures as access control, copy protection, intrusion detection, and robust encryption'*.

Financial services

Australia's financial services industry is organised by function as opposed to institution. Therefore, financial services providers may find themselves regulated by more than one regulator. However, credit reporting in Australia is regulated by a new Part IIIA of the Privacy Act – the Credit Reporting Privacy Code – which comes into effect on 12 March 2014. The Privacy Act already strictly controls organisations and government agencies who handle credit information, but this new Code is set to introduce an even more comprehensive credit reporting regime accompanied by enhanced privacy protections to ensure data quality and appropriate access to data. The Code specifically includes an obligation for credit reporting bodies to *'surround the information with appropriate technical and organisational security'* to put the information 'beyond use'. While encryption is not listed as a specific method of ensuring information is 'beyond use', the inference is clear.

Japan

Data protection

The Japanese Act on the Protection of Personal Information (**APPI**) applies to organisations (or information handlers) who utilise for their business databases containing personal information relating to 5000 or more individuals. Article 20 of the APPI includes an express obligation to take "*necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data*".

In order to understand what those necessary measures may be, we must look to guidance imposed on businesses by certain regulatory authorities which ensure the security of the personal information they handle. While these guidelines are not legally binding, they are well respected and very persuasive in Japan.

It is also important to note that enforcement of the APPI is handled by the appropriate minister with jurisdiction over an organisation's business operations.

The Ministry of Economy, Trade and Industry (**METI**), for instance, has produced guidelines regarding the APPI and specifically mentions encryption as being a measure necessary for the security of personal data. In particular, Clause 2-2-3-2 the METI guidelines refers to certain "*technical security control measures*" and specifically advise on the use of encryption for any personal information that is transmitted electronically or stored on portable media.

Financial services

The Japan Financial Services Agency (**JFSA**) has responsibility for regulating the financial sector, and has issued guidelines regarding the APPI for organisations handling personal information in the financial field. Similar to METI's guidance, the JFSA advises, at Article 10 of the guidance, that necessary and appropriate measures for securing personal data must include "*technological security control measures*" such as access controls and setting up preventative measures against leakage and damage to personal data. While encryption is not specifically cited, the inference is clear; financial sector organisations must encrypt data to prevent wrongful leakage, loss or damage of personal information.

South Korea

Data Protection

The Personal Information Protection Act (**PIPA**), which came into force on 30 September 2011, is one of the strictest data protection regimes in the world. It is also supported by sector specific legislation such as the Act on Promotion of Information and Communication Network Utilization and Information Protection (the **IT Network Act**) and the Use and Protection of Credit Information Act (**UPCIA**).

PIPA places many new obligations on organisations in both the public and private sectors including mandatory data breach notification to data subjects and other authorities including the Korean Communications Commission (**KCC**). PIPA imposes a duty on information managers (i.e. data controllers) to take the "*technical, administrative and physical measures necessary for security safety [...] in order to prevent personal information from loss, theft leakage, alteration or damage*" Organisations are required to establish an official statement of those security measures, and an internal privacy officer must be appointed (regardless of the size or nature of the organisation) to oversee data processing activities. The internal privacy officer will be held accountable, and be subject to any criminal investigations following a breach.

Article 24(3) of PIPA places express restrictions on the management of unique indentifying information, and requires information managers to take "*necessary measures*", "*including encryption*" in order to prevent loss, theft, leakage, alteration or damage. Similarly, Articles 25(6) and 29 require "*necessary measures*" to be implemented to ensure that personal information may not be lost, stolen, altered or damaged.

It is also notable that South Korea has a track record of enforcement of data protection laws and Chapter 9 of PIPA contains severe sanctions for data security breaches including substantial fines and imprisonment. For instance, Article 75 provides that "*a person who has failed to store and manage personal information separately is in violation of Article 21(3)*" (which deals with preservation of personal information) shall be subject to a fine for negligence of up to 10 million won. Any person "*who has failed to take necessary measures to ensure the safety in violation of Articles 24(3), 25(6) and 29*" (as referred to above) may also be subject to a fine of up to 30 million won.

Financial services

The South Korean Financial Services Commission (**FSC**) is the supervisory body responsible for financial policy making, and is making steps towards enforcing new regulations regarding data security by imposing stricter rules and harsher penalties for companies that suffer data security breaches. The FSC can issue five levels of sanctions to organisations' executives, ranging from cautions to dismissal, and the respective companies will also be subject to regulatory enforcement action including prohibitions on pursuing new investments.

South Korea has recently suffered a number of data security breaches, the most recent of which involved in the region of 100 million credit card account details being leaked from the databases of three South Korean banks by a contractor working for the personal credit rating company, Korea Credit Bureau. The databases contained personal data relating to 20 million citizens (approximately 40% of the country's population) and the FSC has highlighted that the data was easy to steal because it was unencrypted; a clear message to all concerned that highly sensitive data of this nature must be protected using adequate controls. Clearly this also raises the issue of access controls and pattern recognition intelligence, and supports the points made above that the both the legal obligations and regulatory and consumer expectations in this area will be far reaching.

This particular incident was so serious for the South Korean economy that the FSC and relevant ministries held an emergency meeting in January this year to identify measures necessary to protect personal data from being illegally- circulated and used for fraudulent transactions, including that the FSC will conduct inspections on all financial firms to check how they manage customers' personal data. The FSC has also said that the chief executives of the three banks involved should take responsibility, and indeed they have since resigned as have many other executives there.

Singapore

Data Protection

The Singapore Personal Data Protection Act (**PDPA**) was passed into law on 15 October 2012. The provisions related to the creation of the Personal Data Protection Commission (the Commission) came into force on 2 January 2013 with the remainder of the main data protection provisions (including those related to the National Do-Not-Call Registry (**DNC Registry**) due to come into force on 2 July 2014, and enforcement activity commencing soon afterwards. The Commission also issued Advisory Guidelines on Key Concepts in the PDPA and for Selected Topics on 24 September 2013 and a further set of Advisory Guidelines on the DNC Registry were published on 26 December 2013. Chapter 15 of the Advisory Guidelines on Key Concepts provides that Section 24 of the PDPA requires organisations to protect personal data in its control by making "*reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks*". There is no guidance about what constitutes "*reasonable security arrangements*" but following the basis of the discussions above, it would be reasonable to conclude that encryption would be deemed not only reasonable, but also a necessary means of protecting personal data.

Financial services

The Monetary Authority of Singapore (**MAS**) supervises financial instructions in Singapore. A Consultation Paper entitled '*Technology Risk Management Guidelines*' was issued in June 2012 and as a result of feedback the MAS published the Technology Risk Management Notice and Guidelines on 21 June 2013. The guidelines provide detailed advice on '*the establishment of sound technology risk management and security practices to address existing and emerging technology risks*'. The guidelines also outline the requirements for ensuring high levels of reliability, availability and recoverability of IT systems through the implementation of effective access controls. It specifically states that "*sensitive information stored on IT systems, servers and databases should be encrypted*". Further detailed advice on the principles of encryption and cryptography is also set out in the guidelines.

Taiwan

Data Protection

On 26 May 2010, the Computer Processed Personal Data Protection Law (**CPPL**) was renamed and amended to create the Personal Data Protection Act (**PDPA**) and came into force on 1 October 2012. The PDPA places increased obligations on companies, individuals and public organisations, including in relation to security. Article 27 of the PDPA requires private entities to adopt 'proper security measures' to prevent personal data from being stolen, amended, damaged, destroyed or disclosed. In addition, Article 12 of the Enforcement Rules of Personal Data Protection Act provided for by the PDPA set out specific security measures which private entities can use to protect personal data. The Rules do not specifically include encryption but include ensuring there is '*an internal procedure for the collection, processing and use of personal data*' which by implication could include implementing encryption technologies.

Financial Services

The Financial Supervisory Commission (**FSC**) supervises the banking, insurance and securities industries in Taiwan. The FSC was established in July 2004 and took over the role from the Ministry of Finance. There are four bureaus which sit under the FSC including the Securities and Futures Bureau (**SFB**), the Banking Bureau, the Insurance Bureau and the Financial Examination Bureau. Currently, the FSC has not published any specific guidance concerning the use of encryption. However, in a regulated industry by implication there is an obligation for data controllers operating in the financial services sector to maintain data security and deploy encryption technologies where appropriate.

Regulatory heat map

This table summarises the key legal requirements for encryption in the jurisdictions under analysis, giving an impression of how seriously the law treats security breaches.

COUNTRY	LEGAL FRAMEWORK FOR ENCRYPTION	SERIOUSNESS (likelihood of fines being imposed and civil litigation)
USA	Multi-faceted, consisting of Federal and State legislations and guidance published by various regulators. Breach disclosure law contains exemption for encrypted data.	Security breaches are met with serious punishment in the forms of high regulatory fines. High possibility of harmful civil litigation.
UK	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus. Breach disclosure law contains exemption for encrypted data.	Security breaches are met with serious punishment in the forms of high regulatory fines.
AUSTRALIA	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus.	Very high probability that legal regime in Australia will mirror that in UK and Germany soon
FRANCE	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus. Breach disclosure law contains exemption for encrypted data.	Very high probability that legal regime in France will mirror that in UK and Germany soon.
GERMANY	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus. Breach disclosure law contains exemption for encrypted data.	Security breaches are met with serious punishment in the forms of high regulatory fines. High possibility of harmful civil litigation.
SPAIN	Principally based on EU Data Protection and e-Privacy law. Breach disclosure law contains exemption for encrypted data.	Very high probability that legal regime in Spain will mirror that in UK and Germany soon.
JAPAN	Contained in legislation that mirrors the EU Data Protection legal framework.	Very high likelihood that legal regime in Japan will mirror that in UK and Germany in the medium term.
S.KOREA	Contained in legislation that mirrors the EU Data Protection legal framework with sectoral financial services focus.	Security breaches are met with serious punishment in the forms of high regulatory fines.
SINGAPORE	Contained in legislation that mirrors the EU Data Protection legal framework with sectoral financial services focus.	Very high likelihood that legal regime in Singapore will mirror that in UK and Germany in soon.
TAIWAN	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus.	Very high likelihood that legal regime in Taiwan will mirror that in UK and Germany in the medium term.

Non-compliance with encryption laws have very serious consequences in the form of high regulatory fines and/or a high possibility of harmful civil litigation

In the near future non-compliance with encryption laws will lead to very serious consequences

In the medium term noncompliance with encryptions laws will lead to very serious consequences

Conclusion

The detailed work on encryption is being done. Regulators and courts are in much closer contact with developments, because they have to move with the times, and they will understand the need for organisations to look closely at the technologies in the market place when they make procurement decisions.

So, organisations need to understand this simple truth; as far as data security law is concerned, the legal obligation to be secure is a legal obligation to act reasonably and when the law is viewed in this way, it becomes easy to understand that a key part of acting reasonably is surveying the technological landscape, an exercise that delivers an obvious conclusion – organisations must reflect on the technologies in the market place and make a conscious decision on the question "what technologies can I reasonably apply to keep my data computers databases and applications secure?". Clearly the use of encryption technologies and access control, authentication and pattern recognition solutions form part of the answer, because they are readily available in the market and relatively cheap and easy to deploy.

We will undoubtedly continue to see more moves towards increased transparency following security breaches and data loss, tougher penalties and sanctions for those that fail to keep data secure, and an increase in prescriptive regulatory guidance to provide organisations details about the nature of their legal obligations. Encryption technologies and access control, authentication and pattern recognition solutions must be deployed to avoid regulatory and other sanctions being imposed.

About Fieldfisher

Fieldfisher is a European law firm with market leading practices in many of the world's most dynamic sectors including Real Estate, Energy, Financial Services, Government & Public Services, Hotels & Leisure, Life Sciences, Media, Telecoms and Technology.

Clients choose to work with us because we deliver commercial, pragmatic and innovative solutions through our exceptional legal expertise and experience, on time and on budget.

We have more than 400 lawyers working with large businesses like Pearson, Vodafone, BP, Citigroup and Accenture but also with private wealth and social enterprises as trusted advisers, providing highly commercial advice based on an in-depth understanding of their needs. We operate across our international offices in Brussels, Dusseldorf, Hamburg, Paris, London, Munich, Manchester, Palo Alto and Shanghai.

Fieldfisher is the trading name of Field Fisher Waterhouse LLP.

www.fieldfisher.com

Please follow our blogs for regular and up to date commentary on developments within the technology and privacy and information legal arenas:

http://technologyandoutsourcingblog.fieldfisher.com/

http://privacylawblog.fieldfisher.com/

fieldfisher

fieldfisher.com