Regulations and Standards: Where Encryption Applies

Dave Shackleford

SANS ANALYST PROGRAM

Sponsored by Utimaco

Regulations and Standards: Where Encryption Applies

A SANS Whitepaper – November 2007

Written by Dave Shackleford

Overview

There are a significant number of regulations in effect worldwide that relate to protection of private and sensitive data. Some are focused on protection of specific industry information, where others are more concerned with proper disclosure of data loss incidents and general privacy attributes.

Most of today's standards and compliance regulations are concerned largely with the protection of private data at rest, during transactions, and while it traverses network connections. Some of these regulations make specific recommendations or require particular technologies for compliance. For all of them, however, encryption can be employed to satisfy the protection requirements. By determining what data you are required to protect, locating the data at rest and in transit, and implementing the appropriate encryption technologies, you can significantly improve your overall security posture while complying with any number of data privacy regulations.

The following pages describe the types of data under regulation and describe basic best practices for implementing appropriate encryption technologies. After that are tables of U.S. and international data privacy regulator overviews, how encryption applies to them, and basic best practices for those applications. They are color-coded as follows: green for financial data regulations, red for medical data regulations, and blue for private individual data regulations.

Data Definitions

Although there are many distinct types of data of importance to regulators, most of them fall into several broad categories:

- **Financial data:** The types of financial data are numerous, but commonly include credit card account numbers and tracking data, bank account numbers and associated financial information, and a variety of credit-related data on individuals and businesses. Several regulatory standards, particularly Sarbanes-Oxley in the Unites States, are concerned with reporting financial data for public companies.
- **Personal health data:** Sensitive patient health data can include insurance-related data, actual medical information, and personal data about patients, such as social security numbers, addresses, and other sensitive information, which should not be publicly available.
- **Private individual data:** Such data includes social security numbers, addresses and phone numbers, and other personally-identifiable data that could potentially be used for identity theft and other illicit activity.
- **Military and government data:** Data specific to government programs, particularly those related to military departments and operations is carefully regulated.
- **Confidential/sensitive business data:** Data that has to be kept secret including trade secrets, research and business intelligence data, management reports, customer information, sales data, etc. falls into this category.

Data at rest is data that is commonly located on desktops and laptops, in databases and on file servers. In addition, subsets of data can often be found in log files, application files, configuration files, and many other places.

Data in transit is commonly delineated into two primary categories – data that is moving across public or "untrusted" networks such as the Internet, and data that is moving within the confines of private networks such as corporate Local Area Networks (LANs). A related concept is data in use, which refers to data that is being processed. One example would be a bank balance transaction update, which needs to occur in a secure tamper-proof environment.

Best Practices for Data Privacy Compliance

Implementing a sound protection strategy can be a daunting task – where do you start? What follows is a simple, step-by-step approach to protect the sensitive data in your environment.

1. Assess your organizational structure to understand where your business is being conducted.
2. Know what rules apply to your organization, particularly when you have international locations.
3. Know what you need to encrypt. Any sensitive data types that need to be protected for regulatory compliance or to comply with internal policies and standards can be strong candidates for encryption. If you have a data classification policy, encrypt the most sensitive or critical category or two.
4. Understand data format: **[3 digits][dash][2 digits][dash][4 digits]**. A number of techniques and technologies exist for searching for strings and data patterns, including the use of regular expressions. An excellent site that describes the use of regular expressions in detail can be found at http://www.regular-expressions.info/tutorial.html.
5. Locate data at rest that is housed in systems across the enterprise, including:

   - ☐ **Databases:** Data at rest is most commonly found in the form of relational databases, where data is stored in logical tables that can be linked to other related tables of information. Each row of a database comprises a single record made up of multiple distinct pieces of information, and each column of the database table represents an attribute of that record. For example, each row may represent a patient health record, and columns may include name, address, last doctor visit, Social Security number, etc.

     Determine which databases and database tables contain the private information, and then narrow this to the specific columns that contain the data that needs to be protected. In some cases, the entire tables or databases may be sensitive, but it is more likely that certain columns are considered more sensitive than others. You may be able to identify the sensitive information through specific SQL queries or by using built-in database management tools.

   - ☐ **File shares and large-scale storage (such as a Storage Area Network, or SAN):** The data residing on these systems can take any number of forms, including documents and word processor files, application-specific configuration or output files, and spreadsheets.

- ☐ **E-mail systems:** E-mail content may be stored in either databases or file shares. The use of e-mail for sending and receiving sensitive data is common. Content is also often stored on centralized mail servers, as well as cached locally on desktop systems and in e-mail backup archives.
- ☐ **Individual desktop and laptop systems, PDAs, smartphones, and removable media:** Such devices store data locally, either in an office environment or on systems that are often in the field. PDAs and other small personal computing devices may have Flash-based removable storage that contains data.
- ☐ **Backup media:** Often overlooked when locating sensitive data, backup tapes and other media can contain significant amounts of sensitive data and may be stored in remote locations for disaster recovery and business continuity purposes.
- ☐ **End-of-life status of devices/storage media and resale of such IT equipment.**

6. Locate data in motion, traversing network channels both within and outside organizations by:

- ☐ **Assessing the data trajectory:** This is the path the sensitive data traverses through your network.
- ☐ **Gaining visibility into the network traffic itself:** The goal is understanding the protocols and applications involved in actually encapsulating the content. This may be accomplished with sniffers or other network traffic capture and monitoring software. It is important to note that application-layer inspection is paramount to determine whether sensitive data is being transmitted and whether it is encrypted properly.
- ☐ **Determining whether certain network devices are storing sensitive data or related information:** Each network device that the data traverses may have varying levels of data storage in structures such as log files. These should not be overlooked when assessing the trajectory of sensitive data throughout a network.
- ☐ **Inspecting specific gateway devices such as mail servers and proxies:** Such devices may have different storage and communications methods than traditional network devices such as routers and firewalls.

7. Once sensitive data has been identified in a specific location, there are three primary options for protection:

- ☐ **Eradication:** This is not likely to be a practical option. Total removal of data is difficult to achieve, particularly in real-time. Additionally, there are often valid business reasons and even requirements for storing some sensitive data.

- ☐ **Obfuscation:** This involves modifying the stored format of data so that it is not easily readable or accessible. This option is often employed for transaction-related information such as credit card numbers. (For example, full payment card tracking data may be sent to a processor at the time of use, but the merchant may only store the last four digits of the card number and obfuscate the rest.)

- ☐ **Encryption:** Widely considered the most effective means of protection, by using proper key management and application, encryption can be used to protect database columns or tables, files on servers, entire communication channels, hard drives, and e-mail messages.

8. Align yourself with a reputable partner. Encryption is not a technology that lends itself to in-house development. Work with reputable vendors whose products meet your particular requirements to design your encryption system.

9. Create a sound and manageable set of encryption policies that your organization can adhere to and that meet organizational requirements. Policy points should include:

   - ☐ A test plan for implementing encryption solutions. Choose a sample group for implementation and ensure that the technology works properly.

   - ☐ Use of strong encryption with a well-known and community-tested encryption algorithm. Typically, 128-bit keys and larger are considered strong.

   - ☐ Auditing a sampling of systems after rollout begins to ensure data is properly encrypted and that there are no issues with the deployment.

   - ☐ Strong key management processes.

   - ☐ Role-based access controls in conjunction with encryption and key management implementation. You can use encryption to, in essence, guarantee confidentiality of data for distinct groups in your organization (e.g. the Sales group cannot read the HR data).

   - ☐ Routine audits of operational systems to ensure that policies are being followed and the system is working properly.

A good resource for determining questions to ask about encryption, ranging from implementation to encryption types and strength, is the SANS Encryption Request for Proposal sample, located at: http://www.sans.org/reading_room/analysts_program/Encryption_June07.pdf?portal=6fab43c64571fa89bc9818e3a4a69c3a.

Regulations & Standards: Where Encryption Applies

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (DSS)

FOCUS

Protection of payment card data and related consumer/business details during processing, transmission, and storage

SCOPE

Global → Specified by MasterCard and Visa as well as other payment card brands

PENALTIES

Significant fines for non-compliance, potential loss of payment card capabilities

Requirements	Crypto Discussion	SANS Best Practices
PCI DSS requirements are **only** applicable if a Primary Account Number (PAN) or specific track data is stored, processed, or transmitted.		
Req. 3: Protect stored cardholder data Full magnetic stripe data, PIN blocks, CVV2 and CVC2 card verification data cannot to be stored at any time. Stored data can include Primary Account Numbers (PANs), cardholder names, expiration dates, and service codes.	PAN data can be rendered unreadable by hashing or truncating the numbers, as well as by employing strong cryptography with proper key management.	Any solution must be both robust and manageable to meet DSS requirements, which include: • Strong key generation • Secure key storage and distribution • Periodic changing of keys • Proper destruction of keys • Protection of key integrity
Req. 4: Encrypt transmission of cardholder data across open, public networks Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.	E-mail encryption of payment card data is explicit. Any PAN data sent via e-mail should be encrypted prior to transmission.	SSL/TLS and IPSec (WPA/WPA2 for wireless) should be used to transmit sensitive data across public networks (such as the Internet).

GRAMM-LEACH-BLILEY ACT (GLBA)

FOCUS
Protection of private data in the financial services industry

SCOPE
USA → Banking and financial services industry

PENALTIES
Significant fines and potential criminal charges

Requirements	Crypto Discussion	SANS Best Practices
Sections 505 in Subtitle A and 521 under Subtitle B describe specific agencies and types of organizations mandated with protecting the security and confidentiality of consumer nonpublic personal information (NPI). Organizations include US national and Federal branches of foreign banks, member banks of the Federal Reserve System, credit unions, and any association insured by the Federal Deposit Insurance Corporation (FDIC).	While not specifically mandated, database, folder, full-disk and transport VPN/transport encryption all apply.	Choose encryption type (whole disk or file/folder) based on usage: • Whole disk on mobile devices • Folder encryption is best used on servers where only certain directories contain sensitive information • Encrypt all sensitive information in databases • Encrypted virtual private network (VPN) tunnels using SSL or IPSec Implement additional measures such as: • Key management and other administrative processes • Physical safeguards for cryptographic key storage
§ 6801(a): It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information.	Nonpublic personal information (NPPI) can be protected at rest or in transit with any number of different encryption solutions: • Whole disk or file/folder encryption • Database encryption • Encryption over Virtual Private Networks	
§ 6801(b): …each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.	Consider encryption your last line of protection against "anticipated threats." Traditional defense and protection measures will still apply for proper defense-in-depth, but encryption will always serve as the last, and possibly most effective, measure of protection.	

SARBANES-OXLEY ACT (SOX)

FOCUS

Protection of sensitive data related to financial reporting in public companies Provide guidance for public companies in designing and reporting on the controls in place for protecting financial information

SCOPE

Global → All industries

PENALTIES

Civil and criminal for exposure of data or fraudulent behavior

Requirements	Crypto Discussion	SANS Best Practices
DS5.7 Protection of Security Technology: Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	Accepted frameworks for use with SOX are COSO and CobiT.	**General:** • Employ remote management using secure encrypted channels (SSH, SSL, IPSec) • Encrypt security device log data at rest and in transit **Technologies:** • Dedicated key storage devices and applications • Key management applications that allow provisioning of keys and separation of duties with proper access controls **Procedures:** • Use of encryption technologies • Allocation of access rights to keys based on roles • Key recovery procedures • Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards and should directly relate to data classification schemas.
DS5.8 Cryptographic Key Management: Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	Proper key management is essential as key compromise undermines overall system security.	
DS5.11 Exchange of Sensitive Data: Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt, and non-repudiation of origin.	Implement encryption technologies for network connections that carry financial reporting data and related sensitive information. This could be VPN technology or dedicated encryption gateways that encrypt on-the-fly.	
DS11.6 Security Requirements for Data Management: Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, organizational security policy, and regulatory requirements.	Mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle.	

INTERNATIONAL **BASEL II ACCORD**

FOCUS
International standard for operational and financial risk management for banking institutions

SCOPE
Global → Banking

PENALTIES
Requirements to reserve greater levels of operating capital, less favorable pricing in financial markets

Requirements	Crypto Discussion	SANS Best Practices
There are three pillars of risk management under Basel II. The first pillar is concerned with financial and liquidity risk, describing how banks and financial institutions can prepare for credit, operational, and market-driven risks. The second and third pillars discuss regulator interaction with financial institutions, numerous other types of risk, and responsible disclosure.	Accepted frameworks for use with SOX are COSO and CobiT. Proper key management is essential as key compromise undermines overall system security. Implement encryption technologies for network connections that carry financial reporting data and related sensitive information. This could be VPN technology or dedicated encryption gateways that encrypt on-the-fly. Mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle.	The incorporation of a holistic information security strategy focused on risk management is the appropriate best practice to follow for Basel II compliance. This will include areas such as: • Security policy and procedures • Perimeter protection mechanisms • Data protection such as encryption • Data integrity measures like hashing and digital signatures • Appropriate access control and authorization controls

EURO-SOX

FOCUS
Protection of sensitive data related to financial reporting in public

SCOPE
EU → Banking and financial services industry

PENALTIES
Criminal (including incarceration) and civil, significant potential fines

Requirements	Crypto Discussion	SANS Best Practices
The European Union determined that better governance and financial controls legislation was needed to improve investor confidence in European businesses. The EU adopted a series of directives between 2003 and 2006, which are set to become law in 2007 and 2008. Key directives that directly relate to internal financial and IT controls for financial data include: • The European Union Financial Services Action Plan (FSAP) • The 4th Directive on annual accounts of specific type of companies • The 7th Directive on consolidated accounts • The 8th Company Law Directive on Statutory Audit • The 8th Company Law Directive and Corporate Governance • The 8th Company Law Directive Committees and Interpretations Several of these are directly focused on professional ethics, independence and objectivity in reporting and auditing, auditing standards, audit reporting, and auditors' liability. Additionally, assessment of internal controls and review of these controls is also discussed to some extent.	The program is somewhat similar in nature to the US Sarbanes-Oxley Act. Mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing must become part of the data's lifecycle. Implement encryption technologies for network connections that carry financial reporting data and related sensitive information. This could be VPN technology or dedicated encryption gateways that encrypt on-the-fly.	**General:** • Employ remote management using secure encrypted channels (SSH, SSL, IPSec) • Encrypt security device log data at rest and in transit **Technologies:** • Dedicated key storage devices and applications • Key management applications that allow provisioning of keys and separation of duties with proper access controls **Procedures:** • Use of encryption technologies • Allocation of access rights to keys based on roles • Key recovery procedures • Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards and should directly relate to data classification schemas.

Financial Instruments and Exchange Law of 2006

FOCUS

Protection of sensitive data related to financial reporting in public
Enhancement of internal controls over financial reporting data

SCOPE

Japan → Banking and financial services industry

PENALTIES

Yes

Requirements	Crypto Discussion	SANS Best Practices
Although the law does not take effect until 2008, companies are preparing by documenting internal controls, both IT-focused and financial, and ensuring security safeguards are in place for all financial reporting data. Definition of the maximum criminal penalties against various market frauds and expanding the scope of penalties against criminal and fraudulent behavior is also included in the law.	Encryption falls under the security safeguards category, which applies to data at rest and in transit.	**General:** • Employ remote management using secure encrypted channels (SSH, SSL, IPSec) • Encrypt security device log data at rest and in transit **Technologies:** • Dedicated key storage devices and applications • Key management applications that allow provisioning of keys and separation of duties with proper access controls **Procedures:** • Use of encryption technologies • Allocation of access rights to keys based on roles • Key recovery procedures • Specific guidance on handling of keys in various environments Policy should be fluid enough to respond to evolving encryption standards and should directly relate to data classification schemas.

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

FOCUS
Protection of electronic patient healthcare data and information

SCOPE
Global → All industries

PENALTIES
Civil and criminal for exposure of data or fraudulent behavior

Requirements	Crypto Discussion	SANS Best Practices
HIPPA addresses the implementation of administrative, physical, and technical safeguards for electronic protected heath information (ePHI). **Section 164.306 Security Standards:** Covered entities must: • Ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain, or transmit. • Protect against any reasonably anticipated threats to the security or integrity of such information. • Protect against any reasonably anticipated uses or disclosures of such information that are not permitted. **Section 164.312 Technical Safeguards 164.312(a)(2)(iv):** Implement a mechanism to encrypt and decrypt electronic protected health information. **164.312(e)(2)(ii):** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate ***(for transmission security)***	HIPAA provides specific recommendations for access control, risk analysis, data disposal and re-use, and data encryption. Policy and documentation requirements are also detailed. Encryption technologies can assist with ensuring the confidentiality of patient health information and also serve as a strong measure of protection against today's commonly anticipated threats, such as unauthorized access, modification, and disclosure. Encryption, though not specifically mandated, is listed as an addressable technical measure that can be implemented for data at rest and in transit.	**For data at rest:** • Employ strong whole-disk or folder-level encryption for all ePHI. • For ePHI in databases, implement full database or column-level encryption. • Implement sound key management procedures and processes that accommodate proper separation of duties and least-privilege for users and applications. • Employ data integrity measures that hash or digitally sign all electronically stored ePHI data. **For data in transit:** • Implement a Virtual Private Network (VPN) using either IPSec or SSL for all remote systems that may need to transmit ePHI. • Implement encryption for all systems and users that may need to send ePHI via e-mail.

FDA TITLE 21 CFR PART 11 (1997)

FOCUS

Defines the criteria whereby electronic records and signatures would be considered trustworthy and reliable

SCOPE

Global → Any drug makers and other FDA-regulated industries doing business in the US

PENALTIES

Financial and criminal

Requirements	Crypto Discussion	SANS Best Practices
The mandate includes information about controls, audits, documentation, and other validation needed to be considered compliant. Section 11.10 specifically mandate controls that should be in place to protect the integrity and security of electronic records and signatures on closed systems with limited access. These include validation, archival protection, access controls to limit exposure of data to authorized individuals, and written policies. Section 11.30 specifies controls for more open systems, including document encryption and digital signature standards.	Encryption technologies can assist with ensuring the confidentiality of data covered by the mandate. This may include any type of stored information relevant to drug manufacturing and distribution, as well as other FDA-regulated businesses. In addition, other related technologies can be used to provide non-repudiation and integrity measures as well.	**Authenticity:** Employ digital signatures for all communications and messages covered under the mandate. This may include email, documents, electronic voice messages, etc. **Integrity:** Use a recognized hashing algorithm such as MD5 or SHA-1 to create hash fingerprints of all stored data. This hash data should be considered sensitive, as well, and stored appropriately to avoid tampering or unauthorized access. **Confidentiality:** Use strong encryption for data at rest and in transit to prevent unauthorized access and exposure. This may include VPN technology, database or file encryption, whole-disk encryption, etc.

95/46/EC EUROPEAN UNION (EU) DIRECTIVE

FOCUS
General protection of individual's private information

SCOPE
EU → All industries and governments

PENALTIES
None specifically stated

Requirements	Crypto Discussion	SANS Best Practices
Personal data can only be processed when three basic conditions are met: • The person is informed of the processing (transparency) • The processing is for a legitimate purpose • The data processed is in proportion to the actual purpose. Brief mention is made directing responsible parties (processors) to take care in securing the data and ensuring confidentiality. **Article 17: Security of Processing** Member states shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.	This directive, one of the older, more well-established regulations related to protection of personal/ private data, defines personal data extremely broadly, basically anything that could be linked back to identify an individual. Although the language used is not technology-specific, both data at rest and in transit is referenced. The directive states that any responsible entity must take appropriate measures to protect individuals' personal data. Encryption certainly falls under this category.	Encryption solutions of all types, including whole-disk and file/folder encryption for data at rest and SSL/ IPSec VPNs for data in transit, could be implemented to prevent unauthorized access to or disclosure of sensitive data.

BUNDES-DATENSCHUTZ-GESETZ (BDSG)

FOCUS
General protection of an individual's private information

SCOPE
Germany → All industries and governments

PENALTIES
Various penalties for misuse

Requirements	Crypto Discussion	SANS Best Practices
Germany's Federal Data Protection Act has been revised several times over the last four decades and exists to protect the collection and dissemination of personal data by public and private organizations. The regulation deals with a broad range of use cases and penalties for misuse.	No specific technologies are mentioned in the regulation; however, it does require appointment of a data protection officer in certain organizations that process data. In addition, the document's Annex specifies the need for access controls, protection of data at rest, authorization, and other security-specific measures.	**General best practices for encryption apply:** • Strong access controls, including VPN technology for remote access and data in transit • Use of whole-database or column-level encryption for any private data stored in databases • Use of whole-disk or folder-level encryption stored on disk • Key management tools and procedures should be implemented for access controls to encrypted resources • Appropriate encryption policies should be in place

CALIFORNIA SENATE BILL 1386 (SB 1386)

FOCUS
General protection of individual's private information

SCOPE
USA → All organizations with customers and/or employees in the US State of California

PENALTIES
Yes

Requirements	Crypto Discussion	SANS Best Practices
This bill is foundation legislation that has prompted similar legislation in other states (38 as of August, 2007). The US Senate is currently considering a bill sponsored by Senators Leahy and Sanders called the Personal Data Security and Privacy Act of 2007, which would create a federal standard similar in nature to SB 1386.	For organizations with customers and/or employees in the state of California, the bill requires disclosure of a security breach where there is a reasonable belief that unauthorized access to unencrypted personal information has occurred. The bill specifically applies to data stored on computers. Any sensitive data not encrypted is subject to the disclosure provisions. A breach is defined as unauthorized access to or acquisition of computerized data that potentially compromises the security, confidentiality, or integrity of personal information.	**Encrypt the following data, at a minimum:** • Social Security number • Driver's license number or California identification card number • Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account Any of the aforementioned data, when connected with an individual's first name or initial and last name, is considered to be sensitive personal data. **General best practices for encryption apply:** • Use of VPN technology for sending private data in transit • Use of whole-database or column-level encryption for any private data stored in databases • Use of whole-disk or folder-level encryption stored on disk • Key management tools and procedures should be implemented for access controls to encrypted resources • Appropriate encryption policies should be in place

PERSONAL INFORMATION PROTECTION & ELECTRONIC DOCUMENTS ACT (PIPEDA)

FOCUS
Protection of personal and private data under certain circumstances

SCOPE
Canada → Electronic Commerce

PENALTIES
Federal mediation and negative press releases

Requirements	Crypto Discussion	SANS Best Practices
Support more secure electronic commerce by requiring protection of personal and private data that is collected, used, or disclosed in certain circumstances. Protection will include physical measures like locks, organizational measures like security clearances, and technical measures like passwords and encryption.	No specific technology is mandatory, but it applies in all areas where protected data travels and resides.	**General best practices for encryption apply:** • Use of VPN technology for sending private data in transit • Use of whole-database or column-level encryption for any private data stored in databases • Use of whole-disk or folder-level encryption stored on disk • Key management tools and procedures should be implemented for access controls to encrypted resources • Appropriate encryption policies should be in place

DATA PROTECTION ACT (DPA) OF 1984 (AMENDED 1998)

FOCUS
Handling of personal information

SCOPE
UK → All industries and business

PENALTIES
Criminal and civil fines, data forfeiture

Requirements	Crypto Discussion	SANS Best Practices
UK Parliament mandate dealing with information about proper disclosure, rights of access to information, transmission and processing, and proper protective measures.	No specific technical measures are mentioned in the DPA. Organizations are simply urged to take appropriate technical measures to prevent unauthorized access to or use of private data. Encryption should be one of those measures.	**General best practices for encryption apply:** • Use of VPN technology for sending private data in transit • Use of whole-database or column-level encryption for any private data stored in databases • Use of whole-disk or folder-level encryption stored on disk • Key management tools and procedures should be implemented for access controls to encrypted resources • Appropriate encryption policies should be in place

PERSONAL INFORMATION PROTECTION LAW (PIPL) OF 2003

FOCUS

Protection of the privacy of personal consumer data

Maintenance of adequate technical and administrative controls to protect stored data

SCOPE

Japan → All industries and business

PENALTIES

Fines, possible imprisonment up to 6 months

Requirements	Crypto Discussion	SANS Best Practices
Article 20 of the Act states that any entity handling personal information must take necessary measures to prevent leakage, loss, or damage to that information	No specific technical guidance is provided. Other administrative guidance is also mentioned. Encryption applies to protective measures necessary to prevent leakage.	**General best practices for encryption apply:** • Use of VPN technology for sending private data in transit • Use of whole-database or column-level encryption for any private data stored in databases • Use of whole-disk or folder-level encryption stored on disk • Key management tools and procedures should be implemented for access controls to encrypted resources • Appropriate encryption policies should be in place

About the Authors

Dave Shackleford, who serves as SANS GIAC Technical Director, has been involved in information technology, particularly the areas of networking and security, for over 10 years. Dave is currently Vice President at the Center for Internet Security and was previously the CTO of a security consulting firm in Atlanta, GA. Dave has also worked as a security architect, analyst, and manager for several Fortune 500 companies. In addition to these roles, Dave has consulted with hundreds of organizations on regulatory compliance, as well as security and network architecture and engineering. His areas of specialization include incident handling and response, intrusion detection and traffic analysis, and vulnerability assessment. He is also a courseware and exam author for the SANS Institute, where he also serves as a GIAC Technical Director. He is the co-author of Hands-On Information Security from Course Technology, as well as the "Managing Incident Response" chapter in the Course Technology book Readings and Cases in the Management of Information Security.

SANS would like to thank the sponsor

utimaco®
The Data Security Company.

Last Updated: November 30th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Essentials Australia 2021	**Melbourne, AU**	**Feb 15, 2021 - Feb 20, 2021**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**