HITACHI
Inspire the Next

fieldfisher

Compliance Obligations in APAC

July 2017

Contents

Executive Summary

During the last 10 years, businesses have seen an exponential growth in the volume of data created, stored and accessed. As a result there has been a shift in focus from both the regulators and the regulated. There are now a myriad of regulations that businesses are required to comply with when creating, storing and using data both as a result of local law as well as extraterritorial legislation.

To navigate this new regulatory landscape, businesses need robust, reliable and flexible storage solutions that are "compliance ready." Yet, it is not easy to assess exactly what compliance ready means. Organizations need to carry our regulatory assessments to understand how to translate top-level regulation into real-life solutions. This self-assessment can be complex and requires an appreciation of both the regulation and the potential technology solutions.

This paper helps those choosing technology solutions to understand how to translate regulation into reality. It provides an overview of applicable data retention legislation for global businesses in the Asia-Pacific region and explains how the Hitachi Content Platform ("**HCP**") solution can help a business achieve and maintain compliance.

Hitachi Content Platform is an object-storage solution that enables organizations to store, share, sync, protect, preserve, analyze and retrieve data from a single system. It is more efficient, is easier to use, and can handle much more data than traditional unstructured storage solutions. HCP automates day-to-day IT operations like data protection and readily evolves to changes in scale, scope, applications, storage, server and cloud technologies over the life of data. In IT environments where data grows quickly or must live for years, decades or even indefinitely, these capabilities are invaluable.

HCP provides the security requirements to meet compliance obligations, protecting documents that are private, confidential, secret, critical or otherwise privileged. This includes the use of advanced encryption techniques.

Data can be retained in-line with retention and disposal policies in a revision-safe, unalterable manner. This approach allows HCP to meet compliance obligations for both records retention and guaranteeing the authenticity and integrity of information stored. When disposal is required, the HCP shredding function ensures no trace of a record is recoverable from disk after deletion.

For content that must be preserved for lengthy periods of time, even permanently, HCP mitigates digital obsolescence to ensure data remains accessible and readable in the future.

The integrity and authenticity of data stored is guaranteed. The digital fingerprint of each content object stored is a badge of uniqueness. It plays a critical role in the prevention of alterations to records and in the prevention of deliberate or inadvertent “overwriting” of a record by a new version, thereby aiding records retention and preservation. Due to this fingerprinting technology, records stored in systems like HCP do not change and so can be proved to be authentic in a court of law. Every action within the system is fully auditable.

HCP, therefore, delivers to organizations:

- The ability to find and use content for insight, research, business intelligence and investigation.
- Mitigation of information and compliance risks around disclosure, security, retention and disposal across all data formats on a holistic basis.
- Mitigation of cyber risk in the event of attack.
- Avoidance of fines and reputational damage.

About This Paper

This paper has been prepared for Hitachi Data Systems ("**HDS**") in conjunction with Fieldfisher LLP ("**Fieldfisher**"). Fieldfisher is a leading technology law firm, with offices in Belgium, China, France, Germany, Italy, the Netherlands, UK and the US.

Overview of Data Retention Obligations

Historically, data storage and management obligations were borne out of a need for record-keeping. Various company records, tax and audit requirements necessitated the storage of accurate records for specified time periods. Market failures during the early 2000s (such as the Enron scandal and the credit crunch) exposed many institutions (particularly financial institutions) as having records-management systems that were not fit for purpose. This recognition led to significant legislative reforms, particularly in relation to the integrity of records and reporting obligations. Game-changing regulations, such as the Sarbanes-Oxley Act mandated strict fraud prevention reforms, to improve financial disclosure by corporations and prevent accounting fraud for companies listed on US exchanges. Some requirements apply to affiliates within international groups; therefore, even those businesses that are not domiciled in a particular jurisdiction may find themselves caught by extraterritorial legislation. For the first time, the detailed implementation of this reforming wave of regulation *required* technological solutions.

Regulators have become wise to the fact that technology is an intrinsic part of effective risk management and reporting by organizations. Today, regulators have an even more sophisticated understanding of the power of technology in advancing the compliance agenda. Requirements can include real-time reporting, record integrity enhanced by digital signatures and fingerprinting, data analytics, pharmacovigilance, monitoring traders, and encryption and information security capabilities. New global legislation, such as the Markets in Financial Instruments Directive II ("**MiFID2**"), Dodd-Frank and, looking ahead to 2018, the General Data Protection Regulation ("**GDPR**") further extends the influence and power of regulators to require corporations to comply. Therefore, the demand for effective solutions to help businesses achieve compliance is growing significantly. Around the world, regulators in every region are learning how big data, analytics and even robotics and artificial intelligence ("**AI**") can enhance regulatory compliance.

Businesses have to adapt to comply with the various legislative requirements. To assist them to do so several voluntary records management reporting standards help ascertain compliance with data retention obligations, including SSAE 16/ISAE 3402 (including SOC reporting), ISO 27000, ISO 15489-1, which will be discussed in more detail below. Some of these standards are recognized by regulators as providing assurance regarding compliance, and so are particularly valuable.

The principles on which the regulations and standards are based give rise to common requirements for data capture, storage and management, which are capable of being met through technology solutions. In particular, regulation is supported by the following key qualities around which the HCP data archiving solution has been developed:

1. Capture and management.
2. Access and availability.
3. Privacy and security.
4. Integrity and authenticity.
5. Retention and preservation.
6. Disposal and defensibility.

This paper focusses on how HCP helps businesses to achieve compliance with local and international data compliance obligations. To cut through the complexity, this paper explains what the requirements of the regulations are, whom the regulations apply to, the risks of noncompliance and how HCP works to support its customers achieve and retain compliant status.

Compliance Explored

The Compliance Conundrum

While it may be relatively straightforward to identify which regulations are applicable and to whom, how to achieve compliance may be less clear-cut.

This is because regulation often provides frameworks and guidance, which must be applied in order to ascertain an appropriate technical or organizational structure. This is very different from say, product compliance. For example, an electrical component adhering to electrical safety standards must tick the boxes by reference to a predefined set of requirements. This is quite distinct from most of the regulation referred to this paper, which requires a business to interpret broad principles and use its judgment as to whether the solutions it implements are sufficient in their operational environment to meet the regulatory standards required of them. Choosing the right solutions to manage data means choosing systems with the right capabilities, to be managed and configured to meet a business' compliance needs.

Falling short of regulatory and compliance standards can be costly: Regulators may take enforcement action, including fines calculated as a percentage of turnover and revocation of operating licenses. An organization may also suffer reputational damage inflicted as a result of being exposed as noncompliant.

With these factors in mind, below are some of the specific benefits HCP can provide to support a client's compliance program.

Capture and Management

Businesses need to create and store data every day and in an ever more regulated environment. Data capture and management must enable a company to comply with all its reporting and retention requirements, as well as a way of self-certifying to certain national and international standards.

Regulations

As well as local law requirements to keep records for accounting and auditing purposes, Dodd-Frank requires financial institutions to keep full, complete and systematic records in relation to all financial dealings. Its reach goes beyond the borders of the USA to extend to overseas affiliates and providers of outsourced business functions. The need to capture and retain data is typical of modern requirements laid down by other financial regulations, such as MiFID II. While MiFID II is primarily a piece of EU legislation, Asian banks with a presence in Europe will need to be compliant, and European fund managers looking to invest in Asia may ask for various report required under the legislation.

Regulators will expect firms to carry out internal audit and report transaction anomalies; this is typical for affiliates of US listed companies under the Sarbanes-Oxley Act as well as for most banking regulators. Appropriate creation and management of records is essential to this process and where regulators have uncovered issues with timely or accurate reporting they have imposed fines on regulated financial firms. Anomalies in records may more broadly lead to a failure of the board's audit committee or its auditors to

sign off on accounts and ultimately to exposure of those failures through financial failings, leading to shareholder concerns and potentially enforcement action by the SEC or other relevant exchange.

Privacy laws around the world also place importance on the ability to capture both data and metadata in order to demonstrate issues like data accuracy, user consent or the length of time the data can be retained.

International Standards

Compliance with international standards gives the necessary assurance to customers and regulators alike that an organization has effective data management systems in place. Business customers are increasingly requiring service providers to meet various international standards supporting compliance. For example, Statement on Standards for Attestation Engagements ("**SSAE**") 16 (and outside of the Americas ISAE 3402) is an auditing standard demonstrating a service organization has in place effective internal controls. The standard provides for independent SOC 1 and SOC 2 reports, which can be used to demonstrate that a service organization's security, availability, processing integrity, confidentiality, or privacy controls are Sarbanes-Oxley compliant.

As a separate example, privacy regulators in Europe in relation to local and global compliance have pointed to ISO 27000 as a suitable standard for information security.

Hitachi Content Platform Capabilities

- HCP facilitates wide and complete capture of records. HCP can capture data types from any data creation application, retaining the original file name, properties and format, and enable the classification of records and creation of metadata.
- HCP is able to handle multiple content sources with differing needs, offering automated archival and intelligent object classification, based on granular policies.
- HCP has scalability to 500PB and billions of objects; it can be virtualized into multiple tenants and namespaces. Servers and storage are independently scalable.
- HCP provides compression, deduplication and support for various storage types, tiers and media, even removable media and spin-down disk for low-cost, long-term storage.
- Based upon performance benchmarking, over 90,000 items can be archived per hour from single source.

Access and Availability (Access and Disclosure, Data Management)

Having systems in place that allow data to be stored, classified, searched and retrieved is key to answering regulation that requires verification and protection of information, audit, fraud detection and record management.

Auditing

Generally, companies are under local companies' law obligations to regularly disclose financial information and audit; these obligations are magnified for any company listed on a stock exchange in Asia or throughout the world. Companies may also be regulated in relation to subject-specific audits in relation to sectors, such as financial services or regulation, such as privacy. Audit will be concerned not just with ensuring documents are available but also with ensuring that access to records and alteration of data is controlled. Proper document keeping, protecting the accuracy and ensuring documents are readily available for disclosure, as well as adhering to confidentiality obligations and preventing the unintended disclosure of price sensitive information are essential.

The main areas are to consider in relation to document access are:

- Access and authentication – considering who has access to the documents and ensuring proper approvals and authorizations for contracts, agreements, payment reports and other similar documents are present.

- Document management – availability and access to complete and accurate records. It is vital that documents are retained in a consistent manner and documents are fully searchable and retrievable.

- Security and integrity of documents – protecting documents from intentional or accidental modification or deletion, while knowing that you can access them when you need to.

- Retention and destruction – ensuring compliance with regulations and having effective policies to ensure documents are available when necessary, stored for periods as prescribed and destroyed in a timely manner.

Some examples of legislation requiring accessibility of data and controlled document management include the Australian Corporations Act 2001, which lays down extensive obligations in respect of the preparation of financial reports for financial institutions regulated by the Australian Securities and Investments Commission and the Hong Kong Monetary Authority's regulatory framework is based on Basel II regulations and requires Basel II compliance reports and GDPR sets out requirements for specific data protection audits. These kinds of regulation are pervasive for organizations in the APAC region and around most of the world.

Data Protection

Regulators have responded to the exponential growth in data creation, and specifically personal data creation, by adopting a "data protection approach" to regulation. The rights of the data subject, that is, the individual to which the data relates, to have access to and assurances concerning use of their data are key. Businesses are required to ensure that personal data is protected, managed and disclosed only in accordance with defined data protection principles. Examples of this include subject access requests (where individuals can request all of the data a company holds about them), the "right to be forgotten" and the option to opt-out of marketing. Proactive compliance is encouraged and the financial penalties for noncompliance can be significant and are growing.

EU data privacy laws have long driven regulation. And any business that is established in the EU, provides goods and services within the EU or monitors behaviour of EU residents will find itself in scope of the new General Data Protection Regulation ("**GDPR**") due to be implemented in 2018. As individuals gain more rights in relation to the data about them, so the systems implemented by companies need to be flexible enough to respond. Under GDPR, individuals are entitled to receive and port their data over to a new controller on request, which means that the storage system used needs to be flexible enough to respond to such requests. Corporate customers are going to require certainty that their service providers can comply with security obligations under the GDPR, for the first time service providers may be liable to the regulators for a security breach in relation to data they process for corporate customers.

Data protection legislation across the APAC region is not yet following a consistent approach, although countries such as Hong Kong and Australia have similar requirements. However the aim of Asia Pacific Economic Cooperation ("**APEC**") Privacy Framework is to introduce consistency and there is no doubt that APEC will take its lead from Europe.

Hitachi Content Platform Capabilities

- Both standard and custom metadata and file content are indexed and searchable. HCP uses a metadata query mechanism, as well as an option for content search and indexing for 370 file formats and 77 languages, to promptly meet search challenges. These advanced capabilities enable the rapid location of documents related to keywords, file properties and custom metadata.
- As HCP can store multiple application content types, overall retrieval times are lowered when compared with searches across separate storage silos. The ability to search content by keyword or metadata can also lower retrieval times.
- Metadata mining and full content search help gather metrics, look for trends and find relationships among data.
- HCP provides support from simple to more complex search string capabilities for discovery purposes and results can be saved for reuse.
- The end user takes advantage of an easy-to-use browser interface.
- HCP allows access to stored data by means of several industry-standard protocols. The HTTPS (REST, S3, OpenStack Swift), WebDAV, CIFS and NFS protocols enable access to the data with a web browser, the HCP client tools, third-party applications, Microsoft® Windows® Explorer, or native Windows or UNIX tools.
- Integration is available with third-party discovery platforms.
- HCP architecture enables search performance to be maintained as the archive scales.
- HCP architecture is resilient to drive and/or node failures with no impact to data integrity. If an HCP node fails, alternate copies of an object or index are always available.
- Progressive replication technology within HCP means a replica would be available for maintaining data availability and serving as a source of disaster recovery. Applications and content on the primary system automatically failover to the replica(s), which provide transparent object-level restore, automatic read recovery and automatic object repair.

Privacy and Security (Information Security)

Information Security

Implementing technical and organizational measures to prevent unauthorized access to data (whether in digital or hard format) has been a longstanding requirement in the European Union and several Asia-Pacific countries, including Hong Kong (Government IT Security Policy and Guidelines) and Australia (Government Information Security Manual). More recently, China, India and Singapore are developing a more rigorous approach to information security with technology in mind. These countries are publishing guidelines and standards which they expect organizations doing business in the region to adhere to or certify compliance with. The Monetary Authority of Singapore's MAS Internet Banking and Technology Risk Management Guidelines set out to highlight the fact that technological innovation has led to increased risk of cyber-attacks and an increased need to maintain systems integrity. It also reaffirms the point that technology is both part of the problem and the solution. In China, the China Certification of Information Security mark is required for all information security products used by Chinese State agencies, but increasingly private businesses are requiring this certification, too. The China Compulsory Certification is required for many international products looking to enter the Chinese market. And the requirements are focused on authentication and access controls, encryption, data security and audit.

Regulations

Guidance from regulators often points to the use of encryption and other access controls to prevent unauthorized access, and penalties for noncompliance can be large. Under the GDPR, an organization can be fined up to 4% of global turnover for failure to implement appropriate technical and organizational measures that work to protect the personal data of data subjects. And it is clear from a variety of sources, including increasing insurance claims and growth in legal support requirements that the number of breaches and costs of remediation are increasing.

Standards

The International Organization for Standardization published ISO/IEC 27001:2013 is an information security standard that provides a specification for information security management systems. ISO 27001 compliant status can be certified by an independent, accredited certification body following audit: the standard lays down a number of required controls in relation to access, management and handling of incidents. ISO is recognized by a number of regulators as a framework for assuring compliance with security obligations.

Integrity

Security is vital to guarantee the integrity of records in order to be certain that they have not been tampered with, to protect price-sensitive data and confidential information. As well as being necessitated by regulations, these are often business-critical issues for financial institutions and quoted companies, as well as many other types of organizations. To meet these needs, a business must implement solutions that enable access control, multilayer encryption capability and firewalls suitable for the criticality of data they handle.

Regulated entities that engage Asia-Pacific-based service centres or outsourced service providers will require such service providers to demonstrate how they conform to local requirements, as well as how they can help the customer support its own regulatory requirements.

Hitachi Content Platform Capabilities

- Granular, multilayer access rights and permissions can be set within HCP or within the controlling file and content management applications.
- Records stored within HCP can be encrypted, providing protection against unauthorized access.
- HCP supports encryption at rest for seamless encryption and decryption of data on the repository's physical volumes. At HCP installation time, you can choose to encrypt all data and metadata stored in the repository, thereby ensuring data privacy in a compliance context. Since the encryption key is generated at system installation time and stored internally, the need for external key management schemes is eliminated. Encryption prevents unauthorized users and applications from directly viewing repository content. HCP handles data encryption and decryption automatically, so no access or process changes are required.
- The internal encryption key is broken into a number of pieces and distributed among HCP nodes. If a disk or node were stolen, the data would be entirely unreadable. HCP protects content from being recovered from stolen media using patented "secret sharing" technology. All Content Platform encryption methods adhere to the U.S. National Security Agency ("**NSA**")-approved Advanced Encryption Standard ("**AES**") algorithm before being written to disk.
- HCP leverages both IP filtering technology and Secure Sockets Layer ("**SSL**") for HTTP (REST, S3, OpenStack Swift and WebDAV) access. HCP grants IT the control to set or restrict administrative access to individual IP addresses or a range of allowable addresses. Each access gateway on HCP

has its own security mechanisms. HCP also uses an embedded firewall to protect all of the ports not needed for the interfaces.

Integrity and Authenticity (Integrity of Records)

Authenticity

Companies are under general obligations both from local and international laws to keep accurate records that can be relied upon to accurately portray the financial standing of a company and audit trail. An authentic record has integrity and is reliable; an authentic record's content and character are fixed, unchangeable. The way a record is stored must work to ensure that such authenticity and integrity is preserved.

Data protection principles impact the integrity and authenticity of records, and being able to tag and trace records for the duration of retention is a key part of demonstrating compliance with these principles. The ability to quickly flag duplicate records further adds to integrity, to ensure that the original and authentic record is the one that is stored.

Under Sarbanes Oxley, companies are required to assure the public that accounts are accurate and have not been tampered with, and failure to do so may attract personal liability for senior executives. More generally, reporting and disclosures at an organizational level to regulators requires signoff by the board. Thus, the onus is on the business to ensure that the solutions it implements work, to assure these individuals that they can confidently certify the accuracy of the data being presented.

When presenting digital evidence in litigation, authenticity of records can be called into question and counter-evidence that records have been tampered with or deleted can be extremely detrimental.

Hitachi Content Platform Capabilities

- Within HCP, "write once, read many" ("**WORM**") functionality together with the object's unique identifier (or digital fingerprint), guarantee immutability and the protection of records from inadvertent and deliberate overwriting. Once it is in the repository, this fixed-content data cannot be modified.
- Deletions or unintended changes before the retention period expires are prevented by object-versioning protection. To modify an object, HCP allows a new, different object to be created from the original.
- Since HCP can store multiple versions of an object, it provides a history of how the data has changed over time. Each version is an object in its own right, with system metadata and, optionally, custom metadata.
- Each record sent to storage by the controlling application is analysed for uniqueness by the storage system's software, a hashing algorithm. This process generates a unique hash, or digital fingerprint, that is permanently associated with the record during its life cycle. One of the following hashing algorithms creates the unique identifier: MD5, SHA-1, SHA-256, SHA-384 or SHA-512. The digital signature for each object is periodically computed and compared by HCP against the original value that was stored when the file was first archived.
- Content is continually checked throughout its retention period for integrity, with proactive data repair; hash algorithms use the ID or digital fingerprint of each data object to compare it to other copies of the data. During the life cycle of the record the hash is regularly recalculated and is then compared with the original. If there is any difference in the hash on recalculation, this means (1) that the record has changed and (2) the change has been detected. If there is any discrepancy or integrity breach, HCP automates object repair to fully restore the original data object.

- If a record is retrieved from the storage system by its controlling application, its hash will be recalculated when it is resent for storage by the controlling application. If the record was altered while out of storage, the storage system's software will detect the changes during recalculation and will store the record as a new record with a new, unique digital fingerprint, rather than overwriting the original record. The original record will remain stored in the storage system along with the new version, until the expiry of any retention periods.
- Similarly, if a copy of a record already in storage is sent for storage by the controlling application, the system will identify that it is a copy, because its fingerprint will be the same as the original, and will "block" the copy's entry into storage. This means that the storage system cannot accidentally store duplicates of records.
- However, HCP also supports "appendable" objects. An appendable object is one to which data can be added after it has been successfully stored. Appending data to an object neither modifies the original fixed-content data, nor creates a new version of the object. Once the new data is added to the object, that data also cannot be modified.
- Similarly, if a record is corrupted while in storage, the change will be detected during recalculation of the hash.
- Dynamic data protection levels ("**DPL**") is provided, with up to four replicas per HCP cluster of the original data object for redundancy to avoid simultaneous points of failure.
- Metadata protection level ("**MDPL**") is configurable redundancy to protect valuable metadata.
- There is automated technology refresh for migrations.

Data Retention and Preservation (Record-Keeping)

An effective data retention and preservation system is general good practice for governance, audit and legal reasons in any business, and particularly for financial institutions given the highly regulated environment in which they operate and the sensitive nature of the data stored. In any regulatory or legal proceedings, rapid access to complete documentation and a chain of authenticity add significant credibility to an organization's case and can help provide vital support in pursuing claims or defending an organization.

Companies operating in Asia-Pacific jurisdictions, including branches of foreign companies operating in different jurisdictions to a parent company, must register with local government registries in order to submit certain information and documents on a regular basis. There are minimum retention periods of accounting records so that a company can demonstrate its financial position at any point in time, although the period of retention varies widely across the region from 3 to 12 years. For example: the Singapore Companies Act requires records to be kept for 5 years; the Australia Corporations Act 2001 and the New Zealand Companies Act 1993 require 7 years; in Hong Kong and India various ordinances and laws specify that records be retained for a minimum of 10 years; and in China records can be required to be retained permanently, depending on the nature of the record.

Dodd Frank requires all financial institutions dealing in swaps and security-based swaps to keep full, accurate and systematic records for a period of 5 years from the transaction. Swap dealers are obliged to ensure records of the swap are readily accessible for the first 2 years of the 5 year period and swap data repositories are required to keep records for the duration of the swap plus 15 years. For the 5 years following final termination of the swap the repository must ensure the records are readily available via real-time access, and then in archival storage for the remaining 10 years, retrievable within 3 business days.

SEC data retention rules are vital for investor protection as preserved records are the main method for monitoring compliance with applicable securities laws. Measures are needed to be in place to protect record integrity following recent events involving the deletion of emails by broker-dealers, which came to light as a result of scandals such as the one perpetrated by Bernie Madoff. Under SEC rules, many records (including communications that relate to a broker-dealer's business) must be retained for 3 years.

Hitachi Content Platform Capabilities

- HCP provides the ability to set retention periods to guard records from inadvertent and deliberate premature deletion.
- Retention periods can be set explicitly or inherited from the controlling application.
- Retention can be set on an individual object-by-object basis if required or by selecting related retention policies.
- HCP delivers data retention enforcement. HCP provides retention with WORM functionality.
- A retention class is a named duration that can be used as the retention setting for an object. When an object is assigned to a retention class, the object cannot be deleted until the specified length of time past its creation date.
- In compliance mode, objects that are under retention cannot be deleted through any mechanism. Additionally, retention classes (see above) cannot be deleted, and retention class durations cannot be shortened.
- In enterprise mode, users and applications can delete objects under retention if they have explicit permission to do so. This is called privileged delete (see below). Also, in enterprise mode, authorized administrative users can delete retention classes and shorten retention class durations.
- HCP utilizes content protection mechanisms that protect against the degradation of records.
- Open architecture facilitates technology refresh at all levels. HCP can store standard file formats, such as XML, HTML and PDF/A. It operates using standard protocols, such as NFS, CIFS, SMTP and HTTP (REST, S3, OpenStack Swift and WebDAV). There are no proprietary lock-ins.

Disposal and Defensibility

A data storage system must have inherent features preventing accidental or deliberate deletion other than those in accordance with predetermined rules. It must also enable the complete and irreversible destruction of records, which can then be appropriately evidenced. This is particularly important to mitigate the risk of future litigation: A robust storage solution will provide for the systematic review, retention and recall of documents created in the course of business as well as permanent deletion, when required.

As already demonstrated, periods of retention required by law vary across the Asia-Pacific region and, therefore, it is important that the system implement has the ability to meet these differing obligations.

The Asia-Pacific countries have generally all passed legislation recognizing that electronic records have legal status, which for the most part is based on the United National Commission on International Trade law ("**UNCITRAL**"). Electronic records can generally satisfy evidential requirements, provided that the record accurately preserves all content, that the record remains readable throughout the retention period and that printed copies can be made upon request. Supporting hardware and software to enable the reading and retrieval of records must remain available throughout the retention period.

When a business does find itself in a dispute, being able to rely on the data it has stored and being able to retrieve the right data (which will be evidence) quickly is essential. A global movement towards the legal recognition of electronic communications has resulted from the UNCITRAL Model Law on E-commerce: It

gives legal effect to their use in e-commerce activities, so that they can be admitted in evidence in court and so that countries can shift their economies from paper-based ones to more efficient electronic ones. The Electronic Transactions legislation in Australia, New Zealand, Singapore and India typifies this movement and provides very helpful guidance for those responsible for implementing records management systems; these systems must have as their goal the integrity of the record, as does the HCP solution.

Hitachi Content Platform Capabilities

- The HCP shredding function ensures no trace of a record is recoverable from disk after deletion. To ensure files are truly unrecoverable, HCP uses a digital shredding feature that overwrites deleted files with a random pattern, a technique that complies with the internationally recognized United States Department of Defense ("**DOD**") specification 5520.22-M.
- Data shredding actions can be performed on individual objects or configured to adhere to deletion governance policies in place.
- Some localities require that certain data be destroyed in response to changing circumstances. For example, companies may be required to destroy particular information about employees who leave. Privileged delete is an HCP feature that enables authorized users to delete objects, even if they are under retention. With each privileged delete operation, the user is required to specify a reason. HCP logs all these operations, including the specified reasons, thereby creating an audit trail.
- HCP facilitates complete and comprehensive monitoring and auditing of all events during the information life cycle. Object tracking and event logging are available for audit support. All delete actions are logged within HCP. Logs can be extracted using the system's auditing mechanisms.
- To support legal discovery, users and applications can place a hold on selected objects. While an object is on hold, it cannot be deleted through any mechanism, regardless of its retention setting.

Country Summaries

While we have drawn attention to some of the major global compliance drivers in this paper, there are many local requirements for data management, such as those confirmed below. The specific legal requirements from country to country can be complex, and many organizations undertake significant records management projects in order to analyse and implement solutions appropriate to their own environments.

Applicable Global Legislation

Table 1 sets out additional key extra-territorial legislation, its applicability and scope. As well as compliance with national law, certain foreign businesses carrying out activities related to or in other jurisdictions will also be required to adhere to additional the laws of other countries if they wish to conduct business there.

Table 1

Legislation	Applicability	Scope of Obligations	Penalties for Noncompliance
Sarbanes-Oxley Act 2002 ("**SOX**")	International companies that have registered equity or debt securities with the U.S. Securities and Exchange Commission.	Corporate governance, financial disclosure and accounting requirements.	Formal penalties for noncompliance with SOX can include fines, removal from listings on public stock exchanges and invalidation of D&O insurance policies. Under the Act, CEOs and CFOs who wilfully submit an incorrect certification to a SOX compliance audit can face fines of $5 million and up to 20 years in jail.
Dodd-Frank Wall Street Reform and Consumer Protection Act 2010 ("**Dodd-Frank**")	Non-US financial institutions with US branches, agencies, or certain commercial lending subsidiaries.	Swap data record-keeping and reporting programs to regulators.	Tiered penalties of up to $150,000 for individuals and $725,000 for companies per offense for each act of non-compliance, commensurate with the nature of the offense.

Legislation	Applicability	Scope of Obligations	Penalties for Noncompliance
EU General Data Protection Regulation ("**GDPR**")	All companies processing the personal data of data subjects residing in the European Union, regardless of the company's location.	Keep and maintain records regarding data-processing activities; hold and process only data absolutely necessary for the service being performed; limit access to personal data to those actually processing the data.	Any organization found to be in breach of GDPR can be fined up to 4% of global turnover or €20 million.

Australia

Company record-keeping obligations are enshrined in the Corporations Act 2001.

There is a strict liability requirement that written financial records must be kept as correct and would "enable true and fair financial statements to be prepared and audited." Records must be retained for 7 years after the transactions are completed.

Financial records may be kept electronically; however, Section 288 of the Corporations Act requires that if financial records are kept in electronic form, they must be convertible into hard copy within a reasonable period of time.

A number of acts cover data protection and privacy in Australia. Originally, The Commonwealth of Australia enacted the Privacy Act 1988 ("**PA**"), this has since been updated by various amendments[1]. A range of Australian states and territories have also enacted specific local privacy law of their own, including New South Wales, the Australian Capital Territory, the Northern Territory, Queensland, Tasmania and Victoria.

Any handling of personal data (for example, use, holding or processing) is potentially subject to the PA through the Australian Privacy Principles (the "**APPs**"), which are contained in schedule 1 of the PA and govern the handling of personal data. These principles cover the open and transparent management of personal information including having a privacy policy:

- An individual having the option of transacting anonymously or using a pseudonym where practicable.
- The collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection.
- How personal information can be used and disclosed (including overseas).
- Maintaining the quality of personal information.
- Keeping personal information secure.
- Designed to allow individuals to access and correct their personal information.

In particular, in order to achieve principles (iv), (v), (vi) and (vii) organizations need effective data retention and management systems in place.

Longer term, the PA contains obligations on the organization to destroy records containing personal data or permanently "de-identify" the personal data when it is no longer needed for the purpose for which the information was used or disclosed.

[1] The Privacy Amendment (Private Sector) Act 2000 (Cth) and The Privacy Amendment (Enhancing Privacy Protection) Act 2012.

New Zealand

Company record-keeping obligations are enshrined in the Companies Act 1993 (as amended). There is a prescribed 7-year retention period for records, with criminal penalties imposed for noncompliance. The act requires that records be kept in written form or be easily convertible into written form and that the board must implement adequate measures to prevent the falsification of records and to enable the detection of any falsification.

In terms of New Zealand data protection laws, the Privacy Act 1993 (the **"Privacy Act**") and the Information Privacy Principles ("**IPP**") within the Privacy Act mainly govern this area. These can be superseded by certain sector specific codes[2]. In general, however, the collection, use and disclosure of personal information by organizations must comply with the 12 IPPs, which include:

- Collection. Data must not be collected unless it is lawful or necessary.
- Source. Personal information must be collected directly from the individual concerned.
- Agency collection. Agency must take steps to ensure the individual is aware of the purpose for collection, recipients and consequences.
- Manner. Personal information must be collected for lawful means.
- Storage and security of personal information.
- Access to personal information. Information must be easily retrievable by the individual.
- Correction. There must be an entitlement to correct personal information.
- Accuracy. Personal information must be accurate.
- Retained. Data must not be retained longer than necessary.
- Purpose of use. Personal information must not be used for another purpose.
- Disclosure. There must be limits on disclosure.
- Unique identifiers. These are not used unless necessary.

Again, with principle (v), data must be stored effectively to safeguard against loss, misuse or disclosure. Although the Privacy Commissioner has very limited powers with no ability to make rulings or issue fines, a dissatisfied individual is able to file proceedings with the Human Rights Review Tribunal, which has the power to award a maximum fine of NZ$200,000 (approximately £110,000)

[2] The Civil Defence National Emergencies (Information Sharing) Code, the Credit Reporting Privacy Code, the Health Information Privacy Code, the Justice Sector Unique Identifier Code, the Superannuation Schemes Unique Identifier Code and the Telecommunications Information Privacy Code.

Hong Kong

Hong Kong has passed numerous ordinances requiring companies to comply with record-keeping requirements. Typically, records are required to be stored and accessible for a minimum of 10 years.

Consider the Inland Revenue Ordinance requirements, in Section 51C, which states that every company carrying out business in Hong Kong must keep sufficient records in the English or Chinese language of its income and expenditure to enable the assessable profits to be readily ascertained.

In relation to data protection, Hong Kong's Legislative Council amended its main data protection regulation, the Personal Data (Privacy) Ordinance (Cap. 486), in June 2012.

The ordinance sets forth principles related to the:

- Purpose and manner of collection of personal data.
- Accuracy and retention of personal data.
- Use of personal data.
- Security of personal data.
- Information that should be made generally available.
- Access to personal data.

Hong Kong’s privacy commissioner is actively enforcing the legislation, naming and shaming companies found to be in breach and issuing guidelines on various matters.

China

Under China's revised *Measures on the Administration of Accounting Records,* retention periods range from a minimum of 10 years up to permanently, depending on the nature of the record.

China imposes various record-keeping obligations, specifically in relation to the financial sector, but there is limited detail as to what form the records should take and how long they should be retained. Generally, financial institutions should establish internal controls to ensure authenticity, integrity and timeliness of business records, accounting records, financial records and other management information.

There is currently no single law that deals with the regulation of personal data protection across China. The *Resolution of the Standing Committee of the National People's Congress relating to Strengthening the Protection of Information* (the "**Digital Data Protection Rule**") contains high-level national rules relating to the protection of personal data in the digital form.

Principles and rules that relate to data protection are found in various laws, regulations and local provisions, including:

- General principles relating to privacy in the Chinese Constitution, the General Rules of Civil Law and the Tort Liability Law.
- Sector-specific provisions, laws and regulations relating to the credit reference, Internet, financial, telecommunications, and consumer protection sectors.
- Legislation with personal data protection at local level, such as the Shanghai Consumer Protection Rules and the Jiangsu Information Ordinance.
- Chinese Criminal Law.

The Personal Data Protection Guidelines issued in 2013 by the General Administration of Quality Supervision, Inspection and Quarantine do not contain compulsory obligations. Instead they offer nonbinding technical guidelines that relate to the collection, use and disclosure of personal data by organizations (excluding governmental authorities) through information systems.

When dealing with issues like access under the Personal Data Protection Guidelines, data subjects should be able to access their personal data. Generally, the administrator of personal data must inform the *data subject* regarding whether it owns his or her personal data, the contents of the personal data and the status of its processing.

Once again, effective document retention and management systems are paramount to allowing a data subject access to their personal data.

Singapore

The Singapore *Companies Act* states that a company must keep accounting and other records for 5 years that will:

- Sufficiently explain the transactions and financial position of the company.
- Enable true and fair profit and loss accounts and balance-sheets and any documents required to be attached thereto to be prepared from time to time.
- Be kept in such manner as to enable them to be conveniently and properly audited.

The Personal Data Protection Act 2012 ("**PDPA**") governs data protection in Singapore. The PDPA regulates the collection, use and disclosure of personal data by organizations. Generally, collection, use and disclosure of personal data is permitted where the individual as to who the personal data relates to consents, the organization is exempt from obtaining consent, or, the activity is required by law.

The PDPA includes obligations on the organization to ensure that:

- Personal data held is accurate.
- Personal data is not held for longer than necessary.
- Data protection policies are drafted and adopted.
- Security arrangements are in force to prevent unauthorized access collection, use, disclosure, copying, modification or disposal or similar risks.
- Any contractual data intermediary that processes data under written contract on behalf of the organization is subject to security and retention obligations.

If an individual suffers loss as result of a breach of these rules, they have a right of action in civil proceedings.

India

India's Companies Act has been updated with the passing of the Companies Act 2013.

The act contains wide-ranging document retention requirements, stating at section 128(1) that every company shall prepare and keep, for every financial year, books of account and other relevant books and papers and financial statements. These should give a true and fair view of the state of affairs of the company.

A push for electronic records and filing systems can be evidenced by a requirement by the Companies (Accounts) Rules 2014 for the books of account to be kept in electronic mode by companies. It is prescribed that any relevant books or records maintained as electronic documents shall remain accessible in India, shall remain in complete and original format and shall not be altered.

There is currently no single law that addresses data protection across India. However, the Information Technology Act (2000) (the "**IT Act**") has been amended to include the obligations on organizations collecting or disclosing sensitive data and the right of an individual to compensation for improper disclosure of personal information[3]. Equally over time, data protection has also been enshrined into common law principles.

Although there are no rules that specifically govern the processing of personal data, there are rules included in the IT Act that require reasonable security practices and procedures to be maintained by the organization. These procedures must also be certified and audited by an independent auditor (approved by central government) on an annual basis.

[3] Section 43A (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011) and Section 72A of Information Technology Act (2000)

About Hitachi Content Platform

Hitachi Content Platform is an intelligent object storage solution capable of managing high volumes of data that remains readily available online, especially for the longer-term storage of fixed content. It is a distributed, object-based storage system designed to support large, growing repositories of both structured and unstructured data. An HCP system consists of both hardware (physical or virtual) and software.

HCP stores objects that include both data and metadata that describes the data. It distributes these objects across the storage space, which is partitioned into tenants and namespaces.

A tenant is an administrative entity created for the purpose of owning and managing namespaces.

Namespaces are owned and managed by tenants. Each namespace consists of a distinct logical grouping of objects with its own directory structure. Namespaces are configured independently of each other and, therefore, can have different properties and policies.

There are a variety of potential use cases.

- **Active archive for enterprise content management ("ECM") applications:** Supporting existing ECM or file-sync-and-share deployments, HCP can deliver dynamic data storage, with HCP supporting multiple versions of the same content; HCP provides added-value storage management capabilities and the federated implementation of information-governance policies across content repositories. Content life-cycle management is completed using standard ECM functions. For example, approximately 7,000 Hitachi Data Systems employees, who work, travel and live worldwide, use HCP in conjunction with Hitachi Content Platform Anywhere (HCP Anywhere).
- **Active archive for real-time content:** HCP provides a robust, cost-effective and secure system that adds intelligent structure to high-volume unstructured content and computer-report output, often in mission-critical environments.
- **Archive for inactive or retired content:** HCP provides a scalable platform for consolidating inactive or retired content from multiple systems and geographical locations. It offers secure, revision-safe archiving, with the implementation of information governance policies.
- **Compliance and discovery platform:** HCP enables organizations to meet requirements to collect, preserve, find, review and produce information for legal proceedings, regulatory and other investigations.
- **Public portal for historic records:** HCP provides an accessible knowledge platform that preserves historical content over time, as used, for example, by the National Archives of Korea and the Stadsarchief Amsterdam (Amsterdam City Archive). It is also used by the U.S. National Archives and Records Administration ("**NARA**"), which relies on Hitachi Content Platform to enable its “archive of the future.”

Hitachi Data Systems Corporation

Corporate Headquarters

2845 Lafayette Street, Santa Clara, California 95050-2639 USA www.HDS.com community.hds.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hds.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hds.com

Asia Pacific: +852 3189 7900 or hds.marketing.apac@hds.com

Australia and New Zealand: +61 2 8379 5000 or anz.marketing@hds.com

WP-421-A DG July 2017