HITACHI
Inspire the Next

WHITE PAPER

Hitachi Content Platform and Compliance Obligations in the European Union

Intelligent Archiving To Support Law, Regulation and International Standards

By BEP Systems Limited

February 2019

Contents

Executive Summary

As organizations in the age of both big and dark data seek to leverage content to unlock value and identify risk, it is increasingly important for "archive" data to be readily accessible and properly governed. Hitachi Content Platform (HCP) is the ideal active archiving solution for these requirements.

Organizations face increasing data growth, data complexity, cost pressures and compliance risks and obligations. A growing body of law and regulation in areas such as corporate governance, tax, privacy, health and safety, financial crime, as well as industry-specific obligations, have implications for the security, integrity, retention and disposal of data.

Hitachi Content Platform is a proven solution in terms of scalability and performance. HCP can handle high ingestion volumes while also providing effective response times for document search and retrieval, either to meet business needs or in response to litigation, investigation or regulatory enquiry. Architected for big data and built to accommodate billions of objects, HCP facilitates continuous searchability and accessibility of data over time.

HCP allows organizations to store, protect, preserve and retrieve unstructured content within a single, unified online storage platform. Leveraging this open, standards-based archiving management allows organizations to overcome the need to maintain siloed archival solutions to support a variety of applications, protocols and content types.

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 stored data is guaranteed. The digital fingerprint of each stored content object 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.

Introduction

About Hitachi Content Platform

Hitachi Content Platform (HCP) is an active-archiving solution capable of managing high volumes of data that remains readily available online, and it is especially effective 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. A 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 Vantara 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. For example, the Moravian Land Archive in Brno, Czech Republic, uses HCP.
- **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.”
- **Cloud hosting:** Specialist outsourced hosting providers leverage HCP to deliver timely, flexible and secure cloud storage. For example, it is used by Telefonica Acens, a leading hosting provider.

About This Paper

This paper has been produced by BEP Systems Limited. BEP is specialist information and records management consultancy and a partner of Hitachi Vantara within the Enterprise Information Governance (EIG) Service.

The EIG Service helps organizations implement the roles, responsibilities, policies, procedures and appropriate technology to ensure that information is leveraged and managed as a vital business asset.

The focus of paper is on compliance with legal and regulatory obligations within the EU, as well as adherence to international standards, for revision-safe archiving, rather than storage economics. There are, of course, many cost benefits in implementing HCP.

There will be compliance considerations in each of the use cases identified above.

The paper explores:

- Key areas of applicable law and regulation, as well as international standards.
- The key qualities of an archiving solution in ensuring compliance:
  - Capture and management.
  - Access and availability.
  - Privacy and security.
  - Integrity and authenticity.
  - Retention and preservation.
  - Disposal and defensibility.
- How HCP provides features and functionality to meet these requirements.

Disclaimer

The authors make no warranties on the accuracy of any information and accept no responsibility for any actions taken based upon the contents of this paper.

Compliance Obligations

Introduction

Any private, public or third-sector organization within the EU will have to ensure that its record-keeping practices comply with European, national-level law and regulation, as well as international law and standards where applicable. There will also be drivers relating to the management of legal risk, administrative and operational use and internal policy and regulation.

There will therefore be obligations for how long different record types are retained as well as security and storage methods.

Commercial and Tax Law

Organizations must follow the rules of corporate governance regulation and company, fiscal and tax law relating to board meetings, corporate establishment and shareholder and investor administration, as well as retention of accounting documents and other books and records. Commercial and tax law, as well as the regulations of revenue authorities, will often dictate record retention periods and the need to keep information in a manner that it is secured and protected.

Health, Safety and Environment

This is a highly regulated aspect of business. Organizations must hold records relating to injuries, diseases, dangerous occurrences, occupational health and the control of substances hazardous to health and environmental protection for lengthy periods of time.

Employees and Benefits

There are statutory record-keeping obligations for employee and benefits management, including social security and pension legislation.

E-Discovery and Disclosure

To facilitate disclosure in tribunals, litigation, regulatory investigations and internal reviews, there is the need to capture, collect, preserve, search, review and produce information. This includes the far-reaching investigation powers of the European Commission in competition cases (including “dawn raids”) and the inspection powers of tax authorities and many industry-specific regulators.

Data Protection

Data protection and privacy legislation (with national laws in place to implement EU Data Protection Directive 95/46/EC) will give various rights to individuals in respect of the personal data held about them, including the right of subject access and the right to rectify, block, erase or destroy inaccurate data. This legislation also requires that measures must be in place to prevent unauthorized or unlawful access or processing of data and, among other things, prevent alteration, corruption, loss or access by unauthorized third parties. Records retention and disposal is a fundamental aspect under the principle that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Upcoming EU data protection reform under the draft General Data Protection Regulation (GDPR) means there will be modernized and unified rules. The GDPR applies to processing carried out by organizations operating within the EU.

The GDPR significantly raises the stakes in terms of compliance penalties. Regulators will have the authority to issue fines equal to the greater of €10 million or 2% of the entity's global gross turnover for violations of record-keeping, security, breach notification and privacy impact assessment obligations. However, violations of obligations related to legal justification for processing (including consent), data subject rights and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross turnover.

It also applies to organizations outside the EU that offer goods or services to individuals in the EU. It includes the fact that individuals can make subject access requests, and right to erasure ("to be forgotten"), which removes data that is no longer required for the reasons for which it was collected, and to data portability. This regulation means that archiving solutions must enable the identification and retrieval of personal data, and comprehensive deletion of information about a person or business if they request the action. It must allow the person or business to move their data and receive it in a reusable format. Breaches must be reported to the relevant regulator without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. This regulation means that tracked and auditable security is essential.

One of the changes due to be implemented under the new General Data Protection Regulation is the explicit recognition of the concepts of "privacy by design" and "privacy by default." For the former, organizations will need to design compliant policies, procedures and systems at the outset of the development of any product or process. For the later, data controllers implement appropriate technical and organizational measures to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

Freedom of Information (FOI)

FOI legislation gives the right to access recorded information held by public-sector organizations. Related to this is other legislation on public access to environmental information to implement Council Directive 2003/4/EC.

Evidence and Limitation of Legal Action

Records are retained by organizations to support and evidence title, intellectual property, contract-related or other legally enforceable rights and obligations. This data must be retained for appropriate minimum periods of time, often aligned to statutory limitation periods for legal action or enforcement.

Product Safety and Consumer Protection

For manufacturers, there is the need to comply with product and consumer safety law and regulations relating to the protection of consumers from defective and unsafe product hazards. These mandates include keeping technical, design, instructional and other information for potentially lengthy periods of time in line with statutory obligations and limitation or liability periods.

Evidential Weight and Legal Admissibility

There is the need to ensure that electronic information can be used in court and investigations or for submissions to relevant authorities. A primary, internationally recognized benchmark for this is BS 10008 Evidential Weight and Legal Admissibility of Electronic Information, the British Standard for ensuring the authenticity and integrity of electronic information. BS 10008 is aligned to the ISO 15801 standard for information stored electronically, and recommendations for trustworthiness and reliability. This has recommendations for the manner in which content is captured, stored and processed.

Corporate Reporting and Accountability

There is the need to keep accurate, dependable records with full audit trails under the Statutory Audit and the Company Reporting Directives (EuroSox), for example. If an EU company itself or the parent company is listed in the United States, the retention, security and other provisions of the Sarbanes-Oxley Act must be observed. With the life sciences sector, the implementation of system security is required by The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC and 91/412/EEC.

Money Laundering and Financial Crime

Typically, a financial services organization must keep records of a customer's identity, as well as supporting records of the business relationship or transaction. These records must be kept for five years after the date the business relationship ends or, in the case of an occasional transaction, five years after the transaction is completed. This applies to credit institutions, financial institutions, auditors, insolvency practitioners, external accountants and tax

advisers, independent legal professionals, trust or company service providers, estate agents, high-value dealers and casinos.

Securities and Exchange Commission

For firms registered with and under the oversight of the U.S. Securities and Exchange Commission (SEC), SEC Rules 17a-3 and 17a-4 specify the rules surrounding supervision, records retention, non-rewriteable storage, and ease of retrieval and viewing. Paragraph (f)(2)(ii)(A) of SEC Rule 17a-4, requires broker-dealers maintaining records electronically to use a digital storage medium or system that "preserves the records exclusively in a non-rewriteable, nonerasable format."

Dodd-Frank

Under the Dodd-Frank Act, end users must keep records throughout the term of each swap and for a period of five years after termination and information must be preserved on WORM (write once, read many) disks for five years beyond the life of the deal.

Market Abuse Directive

Under the Market Abuse Directive, institutions must maintain lists of staff that might be exposed to inside information. The lists will have to be kept for at least five years and the advisers will have to note when staff come off the list because they are no longer dealing with sensitive information.

Undertakings for Collective Investment in Transferable Securities

Under the Undertakings for Collective Investment in Transferable Securities (UCITS) directives, there is the requirement for keeping records for a minimum of five years, making records available to a successor management company.

Markets in Financial Instruments Directive

There are requirements for records retention and protecting the integrity of transaction data within the Markets in Financial Instruments Directive (MiFID). Under MiFID, EU Member States shall require investment firms to retain all the records required under Directive 2004/39/EC and its implementing measures for a period of at least five years. Additionally, records that set out the respective rights and obligations of the investment firm and the client under an agreement to provide services, or the terms on which the firm provides services to the client, shall be retained for at least the duration of the relationship with the client.

European Market Infrastructure Regulation

Under European Market Infrastructure Regulation (EMIR), all counterparties to a derivative contract must keep a record of that contract, and of any modifications to that contract, for a period of at least five years following the termination of the contract.

Basel III

For banking organizations, there are security implications related to operational risk within Basel III, a global, voluntary regulatory standard on bank capital adequacy, stress testing and market liquidity risk.

International Standards

Compliance with international standards on information security, records management and archiving, setting out requirements for sustainability, integrity and security of electronic documents, will improve performance, minimize risk and enhance reputation.

This includes specific requirements within, for example, ISO 27001 Specification for Information Security Management Systems, the Payment Card Industry Data Security Standard (PCI DSS) or ISO 27018 code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

For records management and archiving, there are: the ISO 15489 Records Management standard; the MoReq2010 Model Requirements for the Management of Electronic Records; the International Council on Archives (ICA) Principles and Functional Requirements for Records in Electronic Office Environments; ISO 16175, which covers principles and functional requirements for records in electronic office environments; ISO 14721, which defines the reference model for an open archival information system (OAIS); and ISO 16363, which defines a recommended practice for assessing the trustworthiness of digital repositories.

Within the UK, there are the Records Management code of practice under Section 46 of the Freedom of Information Act 2000 and Requirements for Electronic Records Management Systems published by The National Archives.

In France, the NF Z 42-013 standard (specifications for the design and operation of computer systems to ensure the conservation and integrity of documents stored in these systems) sets out guidelines on the maintenance of an archiving system, including protection and retention. This standard implements the French law of March 13, 2000: Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature electronique.

There is also the NF Z 42-020 standard, functional specifications of a safe digital component for preserving digital information in conditions that ensure their integrity over time, for compliance with NF Z 42-013.

There are also recommendations of the French administrative regulatory body, the Commission nationale de l'informatique et des libertés (CNIL), on the security of personal data.

In Germany, there is the code of practice Grundsätze der elektronischen Archivierung (Principles of Electronic Archiving) of the VOI (Federation of Organisation and Information Systems e.V. 1996), as well as the DOMEA Standard for Document Management and Electronic Archiving in Germany's Federal, Municipal and State Administrations and the BSI Grundschutzhandbuch (Basic Protection Manual).

Research Data

Research councils require that data produced by the activities that they fund is made publicly available for the long term and will often set minimum retention periods.

Heritage

There is the need for organizations to keep records where there are enduring cultural and/or historical considerations. At a national level, for governmental organizations, there would be the need also to adhere to public records or similar legislation, which establish requirements for selecting and preserving records within national archives as well as setting standards for public record-keeping.

Data Capture and Management

Overview

There are many compliance obligations (including commercial and tax law) to keep accurate and complete records of the governance, fiscal and operational activities of organizations over potentially lengthy periods of time. Given the many methods available now for recording and communicating information, this necessitates the handling, with common management and search capabilities, of multiple content types, including: email, files, instant messages, voice, video, social media and web pages, collaboration applications such as Microsoft SharePoint, and structured data.

Within, for example, the financial services sector, there are obligations for the capture and supervision review of trades and communications. Organizations involved in the swaps market for instance, must adhere to the Dodd-Frank Act, which requires institutions to keep full, complete and systematic records together with all pertinent data and memoranda, including electronic mail, instant messages and recordings of telephone calls. These must be retained until the swap has been fully terminated for five years. Since financial instruments can last for many years, as in the case of long-term bonds, the aggregate retention period could conceivably extend up to 30 years and in some extreme cases even longer. Additionally, MiFID allows EU Member States to require (if they wish) firms to

record telephone conversations or electronic communications regarding client orders. MiFID II proposes to introduce organizational requirements for firms, which mandate that they record telephone conversations or electronic communications relating to certain investment services, with a minimum retention period of five years.

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 80PB 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.

Data Access and Availability

Overview

When HCP is deployed, there will of course be the need for suitably authorized internal and external consumers to access the content stored on an informational, reference or research basis. There are also compliance obligations to have information quickly and readily available (often within a specified time period); it may be required as part of a legal process, to meet statutory information access requests, as part of an audit, or in response to an internal or external investigation.

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 re-use.
- 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, HS3), 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.

Data Privacy and Security

Overview

There is always the need to protect confidential personal and commercially sensitive information from unauthorized access, use, theft, damage or destruction. There are a number of compliance obligations relating to information security, particularly for personally identifiable information, especially with the forthcoming GDPR.

Under legislation relating to data protection, computer crime and other information law, as well commercial and tax law, and the regulations of revenue authorities and industry regulators, measures must be in place to prevent unauthorized or unlawful access or processing of data. And, among other things, measures must prevent alteration, corruption, loss or access by unauthorized third parties.

Compliance with international standards on record-keeping and archiving also specify requirements for ensuring sustainability, integrity and security.

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 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.

Data Integrity and Authenticity

Overview

A key consideration for the admissibility and evidential weight of electronic data for litigation and investigation, as well as general confidence in information being reliable, is trust in its authenticity. The authenticity of stored data is in large part derived from protecting its integrity. There are also certain compliance obligations relating to the manner in which data is stored, including commercial and tax law, as well as the regulations of revenue authorities and industry regulators.

A primary, internationally recognized benchmark for this is BS 10008 Evidential Weight and Legal Admissibility of Electronic Information, the British Standard for ensuring the authenticity and integrity of electronic information.

Compliance with the code does not guarantee legal admissibility. It defines best practices, by which a company may demonstrate at any time, in a manner acceptable to a court of law, that the contents of a specific data file created or existing within a computer system have not changed since the time of storage (that is, when the file is “frozen”). The best practices also apply to a company demonstrating that where a data file contains a digitized image of the physical source document, the image is a true facsimile of that source document. The issue being addressed is essentially one of authenticity.

Compliance with other international standards on record-keeping and archiving also specify requirements for ensuring sustainability, integrity and security.

Hitachi Content Platform Capabilities

- Within HCP, 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 analyzed 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

Overview

There are many statutory and other compliance obligations, including limitation periods for legal or investigatory action, to keep certain record types for varying minimum periods of time. Equally, under data protection legislation (and the forthcoming GDPR), personal data shall not be kept for longer than is necessary.

Records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for lengthy periods of time.

Where information is retained for lengthy periods of time (even permanently where they have cultural or historic value) it must be digitally preserved in a manner such that it remains accessible and readable, with its longevity as an asset to the organization or the public guaranteed. Each record must be periodically refreshed, and when the hardware that created or stored a record becomes obsolete, the record must be automatically moved to a new device. As data formats become outdated, records themselves must be evolved to support the new standards.

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 and WebDAV). There are no proprietary lock-ins.

Data Disposal and Defensibility

Overview

When data is deleted and destroyed, these actions must be completed in a systematic manner with an audit trail that is defensible in court or to a regulator. There are some specific compliance requirements driving both disposal and the need for safeguards to be in place.

At the end of a retention period, destruction must of course be held over if there is any pending or threatened litigation, suit, action, subpoena, proceeding, dispute, audit or investigation, whether civil, criminal, governmental, administrative or otherwise.

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.

Hitachi Content Platform and Archives Compliance in France

In France, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in France, under Article L123-22 of the French Commercial Code, there is the need to keep accounts, records and other data that provide information on the rights and obligations of a company for a period of 10 years. The standard contract limitation period (under rules of extinctive prescription and the French Civil and Commercial Codes) is five years; however, there are a number of exceptions to this and practice may be to retain them for 10 years in support of tax records.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes. Equally, under the French Data Protection Act and recommendations of the CNIL, there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislations and regulations, including Decree No. 2009-874 of July 16, 2009, (pris pour application de l'article L. 561-15-II du code monétaire et financier), and Decree No. 2009-1087 of September 2, 2009, (relatif aux obligations de vigilance et de déclaration pour la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et de financement du terrorisme). Financial entities are required to retain all documents relating to the identity of their regular and occasional customers and documents pertaining to transactions for five years following the closing of the account or the termination of the business relationship, or the date of completion of the transaction.

Access rights to public sector information is guaranteed, for example, under:

- Act No. 78-753 of July 17, 1978, on various measures for improved relations between the Civil Service and the public and on various arrangements of administrative, social and fiscal nature.
- Decree No. 2005-1755 on Freedom of Access to Administrative Documents and the Reuse of Public Information.
- National Heritage Code Ordinance 2004-178.

Controls relating to the management of electronic records are established, for example, in:

- Articles 1315, 1316 and 1348 of the French Civil Code.
- The French General Tax Code (Code Général des Impôts).
- The Tax Procedure Handbook (LPF).
- Law no.2004-575 of June 21, 2004, Articles 323 Digital Economy Law.
- The WORM requirement of French NF Z 42-013 standard (from of the French Association for Standardization AFNOR) for guidelines on the maintenance of an archiving system. This standard implements the French law of March 13, 2000 (Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature electronique). This is the French adaptation of the ISO 15489 international standard for records management.
- There is also the NF Z 42-020 standard, functional specifications of a safe digital component for preserving digital information in conditions that ensure their integrity over time, for compliance with NF Z 42-013.
- The Commission nationale de l'informatique et des libertés (CNIL) recommendations on the security of personal data.

Hitachi Content Platform and Archives Compliance in Germany

In Germany, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in Germany, under Sec. 257 of the German Commercial Code (Handelsgesetzbuch, HGB) and Sec. 147 of the Fiscal Code (Abgabenordhung, AO), there is the need to keep financial statements, audit reports, records, profit and loss accounts, tax assessment documents and commercial books for a period of 10 years. There are also similar considerations in the Value Added Tax Act (Umsatzsteuergesetz, UStg).

The standard contract limitation period (under the German Civil Code - Bürgerliches Gesetzbuch, BGB) is three years; however, there are exceptions to this and the practice may be to retain them for 10 years in support of tax records.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes.

Equally, under the German Data Protection Act (Bundesdatenschutzgesetz), there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislation and regulations, including the 2008 Act amending the Money Laundering Suppression Act and various sections of the German Criminal Code. Covered institutions are obligated to record all details obtained for the purposes of identification. The information obtained is to be recorded in the data files of the institution or a copy of the identity documents may be made and retained. In addition to the recording and retaining of customer identification data, along with the accompanying contractual and/or account opening documents and relevant correspondence, institutions must also keep a complete record of the information pertaining to all transactions effected by the customer within the scope of a business relationship.

Access rights to public sector information is guaranteed, for example, under:

- Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act) on September 5, 2005.
- A number of the Bundesländer have approved individual "Informationsfreiheitsgesetze" (Freedom of Information laws).
- Federal Archives Act.

Controls relating to the management of electronic records are established, for example, in:

- Sec. 371a Code of Civil Procedure (Zivilprozessordnung, ZPO).
- Sec. 239 and 257 of the German Commercial Code (Handelsgesetzbuch, HGB).
- The Generally Accepted Accounting Principles (Sec. 238-9 HGB).
- German Principles of Data Access and the Auditability of Digital Records (GDPdU).
- GoBS (Principles of Regular Data Processing-supported Accounting Systems).
- Sec. 147 of the Fiscal Code (Abgabenordhung, AO).
- DIN ISO 15489.
- BSI Grundschutzhandbuch, Basic Protection Manual (Chapter 9.5).

Hitachi Content Platform and Archives Compliance in Italy

In Italy, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in Italy, under Sec. Article 2214 of the Italian Commercial Code, there is the need to keep accounting books and records (including the Libro giornale and Libro inventari) for a period of 10 years. There are also similar considerations for the VAT book under Presidential Decree no. 600 of 1973.

The standard contract limitation period is also 10 years (under the general provision of Articles 2220, 2934-2963 of the Italian Civil Code); however, there are a number of exceptions to this.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes.

Equally, under the Italian Data Protection Code, there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislation and regulations, including Article 119 of the Banking Law, Article 2 of the AML Law (such as modified by Article 2 of Legislative Decree 56/2004), and standardized procedures set by the Bank of Italy (art. 36 and 37 Legislative Decree 231/2007). Records must be retained for a period of ten years after the continuous relationship or professional service has ended.

Access rights to public sector information is guaranteed, for example, under:

- Chapter V of Law No. 241 of 7 August 1990, as amended in 2005.

Controls relating to the management of electronic records are established, for example, in:

- Section 2220 of the Italian Civil Code.
- Legislative Decree, 7 March, 2005, No. 82: Digital Administration Code (as amended by Legislative Decree No. 159/2006), including Article 44.
- Decree of the President of the Council of Ministers dated 30 March, 2009, which includes technical rules relating to the generation, attachment and verification of digital signatures and time validity of electronic documents.
- Technical parameters set by Centro Nazionale per Informatica nella Pubblica Amministrazione CNIPA (contained in Resolution 11/2004 for document retention).
- For tax purposes, the Decree of the Ministry of Economy and Finance dated 23 January 2004.
- UNI ISO 15489-1 2006.
- UNI ISO 15489-2 2007.

Hitachi Content Platform and Archives Compliance in Spain

In Spain, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in Spain, under Article 30 of the Spanish Commercial Code, there is the need to keep all books, correspondence, documentation and receipts for a period of 10 years.

The standard contract limitation period (under article 1964 of the Spanish Civil Code) is 15 years; however, there are a number of exceptions to this. Practice may be to retain accounting records for this 15 year period as evidence.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes.

Equally, under the Spanish Data Protection Act, there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislation and regulations, including “Ley 10/1010 de prevención del blanqueo de capitales y de la financiación del terrorismo” and Royal Decree 304/2014, approving the Regulation Developing Act 10/2010 on certain measures for prevention of money laundering and financing of terrorism. The original documents, records or copies evidencing the transactions, the transacting parties, and the business relationships shall be kept for at least 10 years.

Access rights to public sector information is guaranteed, for example, under:

- Law on Transparency, Access to Information and Good Governance 2013.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Controls relating to the management of electronic records are established, for example, in:

- Order of the Department of Economy and Finance 962/2007.
- State Tax Administration Agency Resolution of 24 October 2007.
- Spanish Tax Agency (electronic invoice department) Certified Digitization.

Hitachi Content Platform and Archives Compliance in Sweden

In Sweden, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in Sweden, under the Swedish Accounting Act (Bokforingslagen), there is the need to keep all accounting books and records for a period of seven years.

The standard contract limitation period (under the Swedish Limitations Act, Preskriptionslag) is 10 years; however, there are a number of exceptions to this. The practice may be to retain accounting records for this 10 years period as evidence.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes.

Equally, under the Swedish Data Protection Act, there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislation and regulations, Money Laundering and Terrorist Financing Act (2009:62) and Act on Criminal Responsibility for Financing Particularly Serious Crime (2002:444). The AML/CFT Regulations and Guidelines contain guidance on record-keeping measures, which require legal persons as well as natural persons conducting business operations to maintain comprehensive accounts and accounting records for 10 years. The New AML Act 2009 introduces record-keeping requirements in line with provisions in the third European Union (EU) AML Directive.

Access rights to public sector information is guaranteed, for example, under:

- Freedom of the Press Act of 1766.
- Principle of Public Access (offentlighetsprincipen).
- Arkivlagen 1990.
- Legal Deposit Acts.

Controls relating to the management of electronic records are established, for example, in:

- Requirements of the Swedish Tax Agency (Skatteverket).
- Requirements of the Swedish Financial Supervisory Authority (Finansinpektionen).
- SS-ISO 15489.

Hitachi Content Platform and Archives Compliance in the United Kingdom

In the United Kingdom, there are laws and regulations that dictate the accessibility, retention and disposal of data as well as the manner in which it is kept to ensure authenticity and integrity.

Regarding records retention in the UK, under the Companies Act 2006, Value Added Tax Act 1994 and Finance Act 1998, there is the need to keep all accounting books and records for a period of at least six years from the close of the tax year.

The standard contract limitation period (under the Limitation Act 1980) is six years; however, there are a number of exceptions to this.

Note that records relating to corporate governance and establishment, health, safety and environment, buildings and property occupation, pensions and insurance, intellectual property and so forth, may need to be kept for much longer periods of time for legal and evidential purposes.

Equally, under the UK Data Protection Act 1998, there will be considerations for not keeping personal data for longer than is necessary.

Financial crime is covered by various legislation and regulations, including the Money Laundering Regulations 2007. Relevant persons and institutions must keep records of a customer's identity, as well as supporting records of the business relationship or transaction, for five years after the date the business relationship ends or, in the case of an occasional transaction, five years after the transaction is completed.

Access rights to public sector information is guaranteed, for example, under:

- Freedom of Information Act 2000.
- Freedom of Information (Scotland) Act 2002.
- The Environmental Information Regulations 2004.
- The Environmental Information (Scotland) Regulations 2004.
- The Re-use of Public Sector Information Regulations 2005.
- Public Records Acts 1958 and 1967.
- Public Records Act (Northern Ireland) 1923.
- Public Records (Scotland) Act 2011.
- Government of Wales Act 2006.

Controls relating to the management of electronic records are established, for example, in:

- BS 10008 Evidential Weight and Legal Admissibility of Electronic Information, the British Standard for ensuring the authenticity and integrity of electronic information.
- Records Management Code of Practice under Section 46 of the Freedom of Information Act 2000.
- BS ISO 15489.

WP-498-D T. Desai February 2019