COMPLIANCE CONSIDERATIONS
DATA PRIVACY

Digital Communications Governance and Archiving considerations for aligning with localized data privacy and protection requirements

THETALAKE

CONFIDENTIAL

SUBJECT

This brief sets out the compliance considerations that financial services firms should consider when enabling digital communications governance and archiving (DCGA) controls for globally deployed unified communications and collaboration tools (UCC), specifically in relation to meeting localized data protection and privacy requirements.

This brief outlines approaches to deploying UCC platforms and supporting compliance systems globally, describes popular scenarios for system deployments, and describes the applicability of relevant legal and regulatory requirements. Finally we analyze a few DCGA use cases and how localized data privacy mandates apply to those scenarios.

GLOBALLY DEPLOYING UCC AND DCGA PLATFORMS WHILE COMPLYING WITH LOCAL DATA PRIVACY RULES

Cloud based UCC tools can be deployed within multiple geographical locations to support dispersed user populations. The platforms handle vast volumes of communications generated by both employees and customers—whether within the same region or across international boundaries. These communications can occur through multiple channels such as chat, audio, video, screen sharing, and file sharing, using platforms like Zoom, Microsoft Teams, RingCentral, Cisco Webex, Asana, Monday.com, and Miro. They also take place across various devices, including mobile phones, desktop computers, and tablets.

These interactions include communications that need to be retained to meet the record keeping obligations of a firm's financial services regulators. In addition, organizations need to comply with localized data privacy and security regulations according to where employees and customers are geographically located.

The privacy and data protection obligations include mandates for storing, securing, accessing and transferring communications data as well as ensuring that individuals can access, correct, or delete their data.

DCGA platforms provide compliance and security controls that enable global firms to retain communications records in accordance with localized data privacy requirements. These include technical controls supporting data storage, access and deletion as well as audit certifications and agreements to document compliance.

To illustrate, below are three real-world use cases of geographically dispersed, global communications deployments in financial services organizations that are subject to archiving, data privacy and data protection rules. We will revisit these use cases in Section 5 and provide guidance about how to apply relevant regulatory requirements to interactions on these platforms.

EXAMPLE A

USA-based investment bank with multiple registered broker-dealers

A New York-headquartered investment bank has locally registered broker-dealer entities in the USA, UK, and EU. The bank uses Microsoft O365 email and Teams across all of its global businesses. The bank maintains a cloud-based, DCGA platform hosted in the USA, with additional local storage in the EU to manage its global communications infrastructure.

EXAMPLE B:

Indian-regulated securities entity with investors located in the USA

A global bank has an Indian-regulated securities entity which services investors located in the USA. Client communications relating to tax documentation and information about portfolio holdings are shared with US customers and through Zoom.

EXAMPLE C:

Global firm with customers in China

A global investment firm with headquarters in the USA uses Webex as its primary platform for staff to communicate with customers. The firm has a China-registered securities entity that interacts with local institutional and individual investors via Webex.

KEY CAPABILITIESOF DCGA TOOLS THAT ENABLE COMPLIANCE WITH LOCALIZED PRIVACY RULES

Given the regulatory obligations governing the management and processing of electronic communications data, it is imperative that DCGA platforms are able to meet these requirements. Understanding the capabilities of DCGA platforms is critical for adherence to both recordkeeping and data privacy requirements. The capabilities span flexible deployment options, technical built-in technical controls as well as legal and assurance mechanisms.

The ability for DCGA tools to support regional storage enables organizations to meet regulatory requirements to store data in a specific region or country. Firms must consider platforms that can support multi-location storage management in any location supported by cloud providers like AWS or Azure.

DCGA platform controls enable organizations to meet customer requests to access, correct, amend, restrict, or dispose of personal data. These include search capabilities to identify records from all UCC tools as well as the ability to redact or remediate and remove personal and sensitive data from communications records. Other features include the ability to delete data on request, set retention periods to ensure data is kept no longer than for its required purpose, and export data.

Technical, physical and organizational measures ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. These include controls for the encryption of data during transmission and storage and physical security of locations at which personal data are processed. Safeguards include user identification and authorization and ensuring consistency of baseline system configuration and changes. Business continuity and disaster recovery measures ensure that data is accessible in a timely manner in the event of a physical or technical incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures ensure the security of the DCGA platform processing of data is critical. These processes include annual SOC 2, Type II, PCI DSS, and TruSight audits as well as other frameworks such as ISO 27001, HIPAA, and CSA STAR. Audit-ready documentation and reports from independent assessments such as SOC 2 Type II, PCI DSS, and TruSight can be used to demonstrate compliance with applicable obligations.

DCGA vendors that have both the knowledge of the privacy requirements and an understanding of how to deploy UCC tools across regions are able to support organizations in meeting both archiving and privacy obligations. Legal agreements include data processing addenda relevant to different jurisdictions, such as the EU Commission's standard contractual clauses for transfers outside of the EU.

KEY REGULATIONS THAT APPLY

Financial services recordkeeping

The requirements for capturing electronic communications are set out by global regulators. These include rules from the Security & Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) in the US; the Financial Conduct Authority (FCA) in the UK and the Canadian Investment Regulatory Organization (CIRO). As a baseline, any written communications related to a firm's business must be captured, retained, and supervised. US rules set out detailed expectations for retaining written electronic communications relating to a firm's "business as such." These include the SEC's Exchange Act Rule 17a-4, and FINRA Rule 4511. The applicable FCA rules include SYSC 10A.1.6, in conjunction with the requirements for MiFID II business.

Legal and technical requirements for protecting and transferring data

Organizations must ensure that data transferred across jurisdictions is safeguarded by adequate levels of protection. The General Data Protection Regulation (GDPR) sets guidelines for the collection and processing of personal data from individuals within the EU. The EU GDPR applies to the EU and EEA member states and is enforced by the European Data Protection Board (EDPB) and the individual member state supervisory authorities. The UK GDPR is enforced by the Information Commissioner's Office (ICO).

Most relevant in the DCGA context are the EU's Standard Contractual Clauses, which enable transfer of data outside the area. The Standard Contractual Clauses contain minimum security and legal protections to ensure a high level of data protection is maintained when data is transferred outside the EU/EEA. For the United Kingdom, transfer outside of the country is enabled through the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK IDTA").

The GDPR requires firms capturing personal data to follow data protection principles to ensure the information is used fairly, lawfully and transparently, used for specified, explicit purposes and in a way that is adequate, relevant and limited to only what is necessary. The data needs to be accurate and handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage. GDPR provides a legal mechanism that allows individuals to request access to their personal data held by an organization through a Subject Access Request (SAR). The GDPR allows for the transfer of personal data outside the EU/EEA if certain contractual and technical mandates are met.

The legal and technical requirements of the EU and UK GDPR essentially act as a global baseline for data protection and security requirements. Many jurisdictions borrow concepts from the GDPR as the basis for new and emerging data protection regulation.

Local mandates for securing, storing, and accessing data

In some regions, specific security requirements for cloud computing platforms used to store financial data may exist. These regulations may require that all data reside in the country.

One example is the Securities and Exchange Board of India's (SEBI) Framework for the Adoption of Cloud Services, which mandates that cloud-based data storage and processing should reside within the legal boundaries of India and must use specific technical security controls. This ensures SEBI's access to data and its regulatory powers remain unaffected, regardless of the storage location. Based on the requirements outlined in Principle 3 of the Framework regarding Data Ownership and Data Localization, cloud storage requirements vary depending on the jurisdiction where the SEBI-registered entity is incorporated. For entities incorporated in India, the data should be processed within the boundaries of India. However, "for the investors whose country of incorporation is outside India" those entities may "keep the original data/transactions/logs, available and easily accessible in legible and usable form, within the legal boundaries of India."

Other jurisdictions may have similar rules describing mandatory controls for use of the cloud to store financial services data.

In China, data is highly controlled with rules requiring personal data to be stored within its jurisdiction by China-registered corporate entities. The Personal Information Protection Law (PIPL) of the People's Republic of China specifically mandates that personal information shall be stored within the mainland territory of the People's Republic of China. This requires a DCGA provider to either work with a local China-incorporated service provider to provide its services, or to register a local China entity.

INTERPRETATIONS OF THE RULES AND APPLICATION TO THE USE CASES

To illustrate how archiving controls can be applied in practice to meet data privacy obligations we can consider the use cases outlined in section 2.

EXAMPLE A

USA-based investment bank with multiple registered broker-dealers

In the first example, the New York-headquartered investment bank which has locally registered broker-dealer entities in the UK and EU uses Microsoft O365 email and Teams across all of its global businesses. The cloud-based DCGA platform it has deployed is hosted in the USA, with additional local storage in the EU to manage its global communications infrastructure.

The firm's DCGA vendor enables the firm to meet its privacy obligations under GDPR including Chapter 5 Article 6 by having the appropriate safeguards in place to enable data to be transferred to the US from the EU or UK.

The firm's legal agreements and Data Processing Addendum with its DCGA vendor contain the EU's Standard Contractual Clauses and the UK's IDTA which set out the security and legal protections to ensure a high level of data protection is maintained when data is transferred outside the EU/EEA and UK. The legal agreements set out the security controls that the DCGA vendor has in place including role-based access controls and the controls described in its SOC 2, Type II and PCI DSS reports, which enable the firm to limit access based on user role or location, for example enabling it to ensure that data residing in EU data storage can only be accessed by EU based staff.

EXAMPLE B:

Indian-regulated securities entity with investors located in the USA

In scenario B, the Indian entity within the bank's structure is 100% Indian owned and the data therefore needs to reside in India in accordance with SEBI's Framework for the Adoption of Cloud Services.

The firm's DCGA vendor enables the firm to meet its privacy obligations by setting up a multi-region storage account in a Hyderabad-based cloud data center. The DCGA platform is deployed with robust security controls like encryption of data in transit and at rest as well as BCP/DR protocols, vulnerability management processes, and incident response plans. The security protocols are tested annually as part of the DCGA's platforms SOC 2, Type II, PCI DSS, and TruSight audits. This allows the firm to meet its obligation to securely store data locally and to demonstrate to SEBI that records are accessible to the regulator, and can be searched and produced in the region.

As there are no specific restrictions in the Framework regarding users outside of India having access to SEBI-regulated data stored in India, tailored access controls are implemented. These permit US based staff to view communications relating to tax and portfolio holdings in a single archiving platform and interface.

EXAMPLE C:

Global firm with customers in China

In example C, the US headquartered investment firm uses Webex as its primary platform to communicate with its customers in China. In this scenario the communications data needs to be stored within the mainland territory of the People's Republic of China in accordance with the Personal Information Protection Law (PIPL).

Because of the mandatory data residency and corporate mandates, the DCGA vendor should engage a local, China-owned service provider to procure cloud services from the local AWS or Azure China entity. The local service provider will assist the DCGA vendor with obtaining the relevant certifications and licenses to operate in the region. The DCGA vendor can then deploy its platform in China using the cloud services procured by the local service provider.