

**HEXAWARE**

# Secure Digital Transformation with Region-Specific Data Sovereignty & Compliance.

How Hexaware enabled country-specific isolation  
with localized cloud hosting to meet data  
compliance and regulatory requirements

---

**Case study**

---



# Client

| Client

- Challenge
- Solution
- Benefits
- Summary

## An International Law Firm

The client needed to separate country-specific systems from its globally integrated IT footprint to strengthen data sovereignty, improve control of sensitive information, and comply with regional data laws.



# Challenge

- Client
- Challenge**
- Solution
- Benefits
- Summary

## Integrated Footprint vs. Regional Compliance Needs

This initiative was driven primarily by the need to comply with a specific country's Personal Information Protection Law (PIPL) and Data Security Law (DSL), enabling the firm to operate independently and securely in the event of regulatory-driven geographic separation. The client relied on shared platforms across regions. This created operational and compliance risks in the specific country, particularly in jurisdictions with stringent data laws, which included:

- Limited jurisdictional control of sensitive data shared across global infrastructure.
- Inconsistent access management & complicated regulatory compliance.
- No proper optimization of cloud services for localized hosting and scalability.
- Increased urgency due to emerging data compliance and regulatory requirements.



# Solution

- Client
- Challenge
- Solution**
- Benefits
- Summary

## Two-Phase Separation with Localized Cloud Hosting

Hexaware executed a structured program to achieve data sovereignty while maintaining global efficiency.

### Key solution highlights:

- Performed an extensive data compliance and regulatory assessment to validate controls across cloud environments, applications, and data flows.
- Analyzed all applications and data repositories to identify Personally Identifiable Information (PII) and determine whether data was stored in compliance with jurisdictional requirements.
- Classified applications into firm-owned data systems versus client-specific data systems, collaborating closely with the General Counsel (OGC) to establish clear data handling and residency rules in alignment with regional laws and firm policies.
- Built a dual-pronged strategy to support security modernization and data center exit planning.
- Executed a 2-phased roadmap
  - **Phase 1:** Logical separation of user access controls with strong SSO and RBAC.
  - **Phase 2:** Physical segregation of country offices and assets.

- Delivered region-specific data separation by implementing localized cloud hosting for country-specific applications, infrastructure, and datasets.
- Migrated high-priority workloads from US (Global instance) to the target country -based cloud environments.
- Enabled seamless integration with US platforms to maintain workflow continuity.
- Established a dedicated domain environment in target country, segregating all relevant users and resources from the US environment.
- Migrated targeted user groups and applications to a separate Exchange server instance in the target country, ensuring email and collaboration tools were compliant and regionally isolated.
- Defined the target-state architecture to support scalable, regulator-approved cloud transformation.

### Technology Stack utilized in the engagement:

- |           |                     |
|-----------|---------------------|
| • iManage | • Tableau           |
| • DMS     | • Azure Cloud       |
| • SSRS    | • COTS applications |
| • Qlik    |                     |



# Benefits

- Client
- Challenge
- Solution
- Benefits**
- Summary

## Strengthening Compliance and Future Readiness

The country separation initiative delivered measurable improvements in compliance, scalability, and operational continuity.

### Data Sovereignty

Country-specific applications and data hosted independently from global systems.

### Compliance

Architecture aligned with regional compliance frameworks and local data laws.

### Business continuity

Governed integration ensured seamless access with SSO and RBAC.

### Scalability

Target-state blueprint supported local country growth and regulatory adaptability.

### Future readiness

Separation model can be extended to new countries where there are such data sovereignty and compliance needs.



# Summary

- Client
- Challenge
- Solution
- Benefits

| **Summary**

Hexaware enabled the client to achieve data sovereignty by disentangling applications, data, and infrastructure from global systems. Through localized cloud hosting and a phased separation approach, the solution ensured compliance with regional data protection regulations, prioritized immediate needs in that country, and instituted a scalable architecture to streamline regulatory adherence as the client expands into additional markets.



Secure. Comply. Scale.

Hexaware helps enterprises achieve data sovereignty with localized cloud hosting, regulator-ready controls, and secure separation for target country operations. Contact us at [marketing@hexaware.com](mailto:marketing@hexaware.com) to learn more.

## About Hexaware

Hexaware is a global technology and business process services company. Every day, Hexawarians wake up with a singular purpose: to create smiles through great people and technology. With this purpose gaining momentum, we are well on our way to realizing our vision of being the most loved digital transformation partner in the world. We also seek to protect the planet and build a better tomorrow for our customers, employees, partners, investors, and the communities in which we operate. With offices across the world, we empower enterprises to realize digital transformation at scale and speed by partnering with them to build, transform, run, and optimize their technology and business processes.

Learn more about Hexaware at <https://www.hexaware.com>.

Get in touch