Cross-Border Carve-Outs: How to Plan for Data Separation

Are you planning a cross-border carve-out or interfacing with highly regulated industries, such as healthcare? Then beware, because a recent survey by TMF Group found that 34 percent of senior executives with buy-side experience at private equity firms said their most recent cross-border carve-out failed to deliver on expectations, with 24 percent saying costly overruns impacted deal returns.[1] With sensitive data at risk and regulatory compliance requirements only increasing, companies must take proactive steps to ensure the success of these transactions. In this article, we unveil some key areas where careful planning is critical for success and discuss the complexities involved in these deals. Whether you're a private equity firm, healthcare organization or global enterprise, these insights will help you navigate the carve-out process and avoid costly mistakes.

Figure 1 – Four Focus Areas for IT Planning During Carve-Out

1. **Data Privacy Considerations**
2. **Commercial Strategy**
3. **Business Application Separation**
4. **Operational Transition**

What Makes Data Highly Regulated?

Financial technology (fintech), healthcare and telecom companies must comply with multiple levels of regulation to protect customer data. In the United States, fintech companies follow the Gramm-Leach-Bliley Act (GLBA) and California Privacy Rights Act (CPRA) to govern the collection, usage and disclosure of individual financial information.[2] Healthcare companies adhere to the Health Insurance Portability and Accountability Act (HIPAA), while GDPR, LGPD, PIPEDA and other regulations apply in other countries.[3] In many cases, individual consent is required to handle sensitive data.

Telecom companies face similar regulations to those of healthcare companies. All companies must comply with antitrust laws, which prohibit sharing of competitor pricing information to prevent anti-competitive behavior. Compliance is crucial to avoid legal violations and protect customer data from breaches and misuse. Understanding the complex regulatory landscape is essential to maintaining a company's reputation and ensuring customers' privacy is maintained.

Identify Data Impacts

It is essential to accurately ascertain the nature of assets being transferred in a carve-out and to implement appropriate measures to ensure compliance with relevant data privacy and sharing regulations.

Keeping all this in mind, we believe the following are four focus areas to consider as you dive deeper into your planning.

1. Data Privacy Considerations

Regulated Data

Certain categories of data are regulated, meaning there are policies and laws governing secure and appropriate processing, control and sharing, where the right data assets go to the right place at the right time.

Sizable fines have been assessed for data breaches — the top 12 penalty amounts levied since 2019 add up to $5B.[4]

Below are several examples of the types of regulated data that must be accounted for and that are subject to various audits:

Figure 2: Regulated Data Handling

TYPE OF DATA	DATA DESCRIPTION	SHARING RESTRICTIONS
PII (Personally Identifiable Information)[5]	GLB Act, GDPR (EU), CPRA, FCRA, Data Protection Act (UK), LGPD (Brazil), PIPEDA (Canada), APPI (Japan), APPs (Australia)[6]	SSN, driver's license, credit card numbers, passport
Medical or Health Records	HIPAA Act,[7] GDPR[8]	Patient records, healthcare history, mental health records, test results
Educational Records	FERPA Act[9]	Students' educational records
Intellectual Property	IPE (USA)[10]	Trade secrets, patents, trademarks, etc.
Personal Financial Information	PCIDSS (USA),[11] LGPD (Brazil),[12] GDPR[13]	Bank accounts, credit card info, passwords, PINs, transaction records
Financial Accounting	U.S. GAAP, SEC[14]	Access to financial records such as assets, liabilities, P&L, revenue, expenses
Competitive Pricing	Antitrust Laws (various countries)	Competitive pricing for products and services
HR Data	GDPR,[15] CCPA, FCRA,[16] PIPEDA (Canada)[17]	Employee data must be protected and must comply by various laws
Gov't Data	Mandated by various governments[18]	Federal data (PII), defense & national security
Intermingled Data	NDA required	If data separation is not possible, will need clean room to view sensitive data

Unregulated Data

Unregulated data is company confidential, customer confidential, competitively sensitive (requires special handling on case-by-case basis) and **could be audited** by the customer. If unregulated data without authorization, it can result in reputational harm.

Effective management of regulated and unregulated data requires comprehensive planning and coordination, as data separation policies have implications across multiple areas of the organization. **Business functions are frequently reliant on IT systems' handling of data separation, and inadequate handling of such policies will negatively impact operations and customer experience**. Therefore, it is crucial to transition the appropriate product and customer data in accordance with the target operating model.

Figure 3: Unregulated Data Handling

TYPE OF DATA	EXAMPLES OF DATA	INFO TO PROTECT
HR Data	Job performance, feedback, location	Consent required by law
Social Media	Data collected by various social media platforms	Consent required in some cases by law
Historical Financial Statements	Public companies already submit financial statements to regulators	Consent required
Operational Data	Data related to servicing existing customers	No confidential data can be shared
Commercial Agreements	Data related to doing business within commercial agreements	No pricing data can be shared by law
Transitional Service Agreement (TSA) Services	Data associated with applications under TSA	Will need additional NDA in most cases
Operational Reports	Operational reports not subject to data privacy regulations	Will require access separation in most cases

2. Commercial Strategy

In the context of commercial strategy, the data strategy plays a crucial role, particularly when dealing with unregulated data. Data strategy involves developing a comprehensive plan for **managing and utilizing data in the sale of products to customers**. This includes considerations such as data separation with regard to pricing, discounting, and inter-company agreements, as well as establishing a charging and charge-back mechanism. The data strategy also encompasses ensuring **data privacy and compliance with relevant regulations**.

Moreover, the data strategy is essential when expanding sales into specific countries. **It entails understanding the legal and regulatory requirements of operating in a new country**, creating the necessary legal entity if it does not already exist, and addressing the implications of the tax structure. **For example, in Germany, companies must adhere to Works Council Section 79a, which protects employee data**.[19]

Additionally, data strategy involves establishing the required bank accounts to support the operations, and **implementing data separation practices to maintain the integrity and confidentiality of customer and pricing information**.

By having a well-defined data strategy within the overall commercial strategy, organizations can effectively manage data assets, ensure compliance and support decision-making processes related to pricing, customer segmentation, and cross-selling of goods and services.

Let's consider a situation where a company **carves out its internet service business from a larger entity that provided bundled internet and cable TV services**. After the carve-out, the **newly established internet service business needs to bill customers separately for their internet usage** while ensuring a smooth and unified billing experience.

In this case, the data strategy becomes crucial to enable accurate and efficient billing processes. The strategy involves implementing systems and processes to **separate customer data, usage information and billing details specifically for the internet service business**.

The data strategy would address key considerations such as **creating distinct databases or data structures for internet-related customer information, designing new pricing models and rate structures specific to the internet service**, and developing a billing system capable of generating separate invoices for internet usage.

Furthermore, the data and commercial strategies need to **account for data migration from the existing system, ensuring data integrity during the transition, and establishing data privacy and security measures for the internet service customers**. It will also involve updating customer communication channels to inform them about the changes in billing procedures and payment methods.

By carefully implementing a data strategy that focuses on the carve-out of the internet service business, the company can effectively manage the separation of billing processes while maintaining a unified experience for customers. This approach ensures accurate billing, improves customer satisfaction and retention, and supports the smooth operation of the newly established internet service business.

3. Business Application Separation

How does data privacy affect business application separation?

Data privacy guidelines and commercial agreements play a crucial role in determining the necessity for data separation and the establishment of new systems within business applications. This requirement varies depending on the industry and the specific nature of the business carve-out process.

For instance:

a) Human Resources data must adhere to strict data privacy regulations dictated by local laws, necessitating its immediate separation on Day 1.

If for any reason HR data cannot be separated immediately, a third party must be put in place to handle this data post-Day 1.

b) Pricing and quoting systems should be segregated to prevent visibility of sensitive data by the other company, as mandated by antitrust laws. This ensures compliance and transparency in SalesOps.

c) Customer data within customer-facing portals must be separated from the outset to safeguard the privacy of customer information, in accordance with data protection laws.

d) Financial data, per SEC guidelines, must be isolated within the financial systems of each respective company after Day 1.

e) In situations where data is not regulated, separation of systems may not be feasible. This is primarily due to significant disparities between the technology, compatibility and functionality of the buyers' and sellers' system landscapes. This discrepancy poses challenges to the smooth operation of a carve-out. **To address this, transitional service agreements (TSAs) are often established to maintain access to IT systems until the target architecture is defined and data migration is completed**. Effective coordination between the buyer and seller is crucial to ensure operational continuity during this transitional period.

4. Operational Transition

After establishing a commercial strategy and evaluating its implications on IT systems, **the operations team must promptly initiate an assessment of how these changes will affect access to business applications and existing processes**. These effects can permeate throughout end-to-end business flows, encompassing the entire sales cycle and customer operations. In certain scenarios, it may be necessary to recreate automation or document manual workarounds as temporary measures.

Additionally, any changes to IT systems might impact operational or financial reports, underscoring the need to identify these effects and diligently recreate and test the reports prior to Day 1.

Equally vital is the assurance that these changes will not disrupt products or services already sold to customers, nor the operational flows associated with them. Any prospective modifications to these flows must undergo meticulous analysis, testing and documentation to preempt any adverse impact on business operations.

Sufficient time must be allocated for **comprehensive end-to-end testing to ensure thorough examination of any changes in operational processes resulting from data segregation**, with corresponding updates made to operational playbooks.

This critical phase is one where many companies often encounter challenges and potential delays. To avoid such pitfalls, proactive measures should be taken.

First, it is essential to foster effective communication and collaboration between the commercial strategy, IT and operations teams. Regular meetings and discussions should be held to ensure a clear understanding of the strategy and its impact on IT systems and operations. This alignment will enable teams to anticipate potential issues and address them in a timely manner.

Second, establish a comprehensive project plan with clear milestones and deadlines with dependencies between cross-functional workstreams. This plan should outline the tasks and responsibilities of each team involved in assessing the impact of the changes. By adhering to a defined timeline, the company can prevent delays and ensure that all necessary actions are completed before the target date.

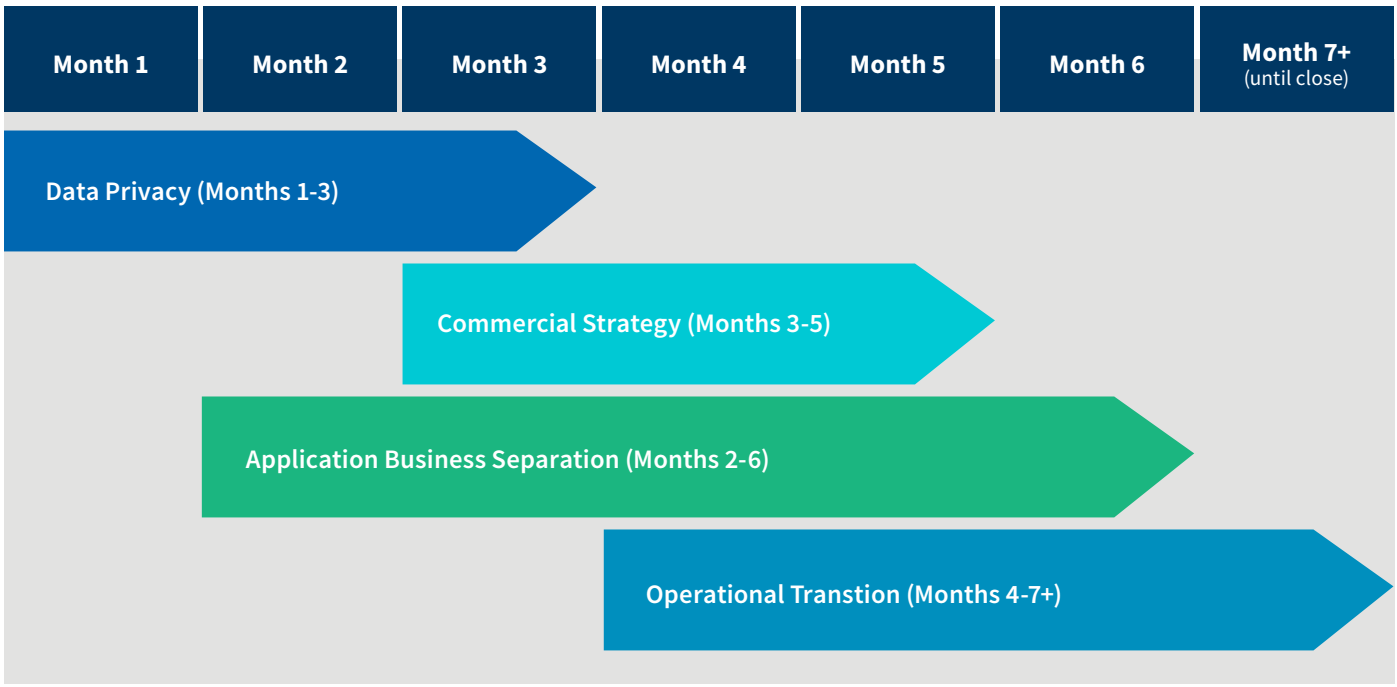
Third, invest in automated testing tools to significantly expedite the process. These tools can streamline the testing of access to business applications, operational flows, and the recreation and testing of reports. By automating these tasks, companies can save time and resources while increasing the accuracy and efficiency of the testing process.

Moreover, creating a dedicated cross-functional team specifically focused on managing the impacts and changes can be highly beneficial. This team should consist of representatives from IT, operations, and relevant business units. Their expertise and collaborative approach will help identify potential roadblocks, implement effective solutions and ensure a smooth transition without major disruptions.

Finally, engaging external consultants or experts with experience in similar projects will provide valuable insights and guidance. Their expertise will certainly help identify blind spots, offer best practices, and mitigate risks that will arise during this process.

By implementing these proactive measures, companies will be able to navigate this common challenge with greater ease, avoid unnecessary delays, and ensure a successful transition to the new commercial strategy while minimizing any adverse effects on business operations.

Figure 4: Suggested Timeline From Deals' Initial Signing Through Close (Can Vary by Industry)



Conclusion

Carving out a portion of a company is a complex process that requires careful planning and execution. It is crucial to have a clear understanding of the goals of the carve-out and the resources needed to achieve them. To successfully plan a carve-out, **companies must consider four focus areas: data privacy, commercial strategy, business application separation and operational transition**.

Within these areas, there will be a significant amount of detail and many potential pitfalls, particularly when it comes to ensuring compliance and delivering the separation in a timely manner. Therefore, it is important to give due consideration to these areas **to develop a clear strategy for the carve-out and ensure that the necessary resources and support are in place to execute it successfully**.

To assist with the process, companies can benefit from working with experienced advisors or consultants **who can provide valuable insights and expertise** such as domain knowledge in privacy laws, offer expert advice during commercial negotiation, define business separation rules and guide teams during E2E Business Process testing. This will be especially helpful in navigating the complexities of data privacy regulations and developing a commercial strategy that aligns with the goals of the carve-out.

Overall, proper planning and execution of a carve-out is crucial to achieving success. By taking a comprehensive approach that considers all relevant focus areas, companies will increase their chances of achieving their goals and avoiding potential pitfalls.

AUTHORS

ERIC NELSON
Managing Director
+1 202.848.1521
eric.nelson@fticonsulting.com

GARY JACOBS
Managing Director
+1 212.499.3640
gary.jacobs@fticonsulting.com

GOPINATH TADAPATRI
Senior Director
+1 678.468.7189
gopinath.tadapatri@fticonsulting.com

JAMAL AL SHEIKHLY
Director
+1 415.215.8712
jamal.al-sheikhly@fticonsulting.com

Endnotes

[1] "One-third of global carve-out deals fail to go to plan, says TMF Group study," Private Equity Wire (April 9, 2020).

[2] Robb Hiscock, "Navigating the CPRA as a GLBA-compliant business," OneTrust (November 29, 2022).

[3] "HIPAA for Professionals," U.S. Department of Health and Human Services (February 3, 2022).

[4] Osman Husain, "The 25 Significant Data Breach Fines & Violations (2012-2023)," Enzuzo (February 27, 2023).

[5] Peter Hu, "Understanding PII Laws and Regulations Worldwide," Strac (March 13, 2023).

[6] Ibid.

[7] "Summary of the HIPAA Privacy Rule," U.S. Department of Health and Human Services (Oct 19, 2022).

[8] "Data Protection in the EU," European Commission.

[9] "What is FERPA?," U.S. Department of Education: Protecting Student Privacy.

[10] "Intellectual Property Enforcement," U.S. Department of State.

[11] "PCI DSS Quick Reference Guide," PCI Security Standards Council, LLC (March 2022).

[12] "Brazilian General Data Protection Law," IAPP (May 2024).

[13] "Data Protection in the EU," European Commission.

[14] "US GAAP: Generally Accepted Accounting Principles," CFA Institute Research & Policy Center (October 2, 2023).

[15] "Data Protection in the EU," European Commission.

[16] "Fair Credit Reporting Act," Federal Trade Commission.

[17] "PIPEDA," Office of the Privacy Commissioner of Canada (April 25, 2024).

[18] "Rules and Policies – Protecting PII – Privacy Act," U.S. General Services Administration.

[19] "Co-determination at workplace level in Germany," DGB (December 2022).