Customer-Generated Data in SaaS M&A: Ownership, Consent and Separation Value

A Transaction Framework for Contractual Rights, Product Dependence and Carve-Out Readiness

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Customer-generated data can support workflow automation, benchmarking, product improvement and artificial-intelligence features in a software-as-a-service business. Its transaction value remains conditional. A buyer needs evidence that the target may collect, use, combine, retain and transfer the data for the activities reflected in the forecast. It also needs to know whether those rights survive a change of control, whether customers can require deletion or export, how the product depends on historical data, and what it would cost to separate the data from a seller's systems.

This paper develops a transaction framework for customer-generated data in SaaS mergers, acquisitions and carve-outs. It distinguishes legal ownership from contractual licence, operational control and permitted purpose. It connects customer contracts, privacy roles, data lineage, product dependence, portability and separation architecture to revenue, retention, cost and transaction terms. The approach combines a rights matrix, product-dependency map, replacement-cost analysis, separation-cost analysis and income scenarios.

The framework draws on the GDPR and UK GDPR, regulatory guidance from the European Data Protection Board and UK Information Commissioner's Office, the EU Data Act, Federal Trade Commission materials, California privacy rules, NIST privacy and cybersecurity frameworks, OECD work on data access and value, and IFRS requirements for intangible assets and business combinations [1-50]. These sources define relevant obligations and analytical boundaries. They do not determine title, compliance, fair value or transaction price for a particular dataset.

An illustrative acquisition demonstrates the method. Management assumes a SaaS target with USD 64 million of annual recurring revenue and USD 13 million of EBITDA. Seventy-eight per cent of annual recurring revenue depends materially on customer-generated operational data, while contracts covering 24 per cent of the relevant data corpus contain unclear language for derived-data use. Management assumes USD 8.4 million of separation and remediation expenditure, USD 11.6 million of replacement cost, a USD 31.2 million income indication and a USD 24 million to USD 40 million market corridor. An evidence-weighted indication of USD 28.5 million follows for the data-enabled economic contribution. Every amount, percentage and operational result is a management assumption used solely to demonstrate the framework.

The central conclusion is that customer-generated data creates transaction value when the acquirer can prove a permitted use, trace the data to a product and customer outcome, preserve service continuity, and execute separation or integration without breaching contractual and regulatory constraints. Uncertainty should be reflected in price, closing conditions, remediation plans, transition services, customer consents, warranties, indemnities and post-close governance.

JEL Classification: G24, G34, K11, K24, L86, M41, O34

Keywords: customer-generated data, SaaS M&A, data rights, consent, data portability, carve-out, separation value, privacy diligence

Introduction

SaaS businesses often describe customer data as a strategic asset. The phrase can conceal several different assets and obligations. A customer may upload records, create workflow events, generate usage telemetry, submit support material, configure business rules and produce outputs. The provider may create metadata, benchmarks, fraud signals, model features and aggregate statistics. Each layer can have a different contractual owner, privacy role, technical location, retention rule and economic function.

Transaction teams therefore need a narrower question than whether the target has valuable data. They need to establish which data the target controls, what it is permitted to do with that data, which contractual commitments limit transfer or reuse, which product functions depend on it, what customers can export or delete, and what architecture must be rebuilt during separation. Regulatory guidance for mergers and acquisitions requires due diligence on the data transferred, its original purposes, the lawful basis, transparency and security [1-7]. The EU Data Act adds obligations relevant to switching, exportable data and interoperability for data-processing services [14-16].

The commercial problem is equally important. Historical customer data can improve onboarding, recommendations, anomaly detection or benchmarking. It can also create concentration, model drift, privacy exposure and switching complexity. A forecast that assumes continued data use without testing the underlying rights can overstate revenue and margins. A carve-out that ignores data lineage can delay closing, disrupt customers and require expensive duplication or clean-room rebuilding.

This paper is designed for boards, founders, corporate-development teams, private-equity investors, lenders, product leaders, data officers, privacy counsel, technology teams and valuation specialists. It provides a transaction decision system. It does not provide legal, tax, accounting, cybersecurity or valuation advice. Qualified specialists should assess the actual contracts, data flows, jurisdictions, systems and transaction structure.

1 Define the data perimeter before assigning value

The first diligence output should be a data-perimeter schedule rather than a general data-room folder. The schedule should identify each material dataset, source, customer, jurisdiction, system, field class, data subject, controller, processor, subprocessor, retention period, export path, deletion method and product dependency. It should distinguish production data from backups, logs, derived features, test environments, analytics stores and model artefacts.

The economic unit is not always a database. A feature may depend on events held in several services. A benchmark may require aggregation across customers. A machine-learning model may embed statistical information from training data without retaining identifiable source records. A customer configuration may be commercially essential even though its volume is small. The perimeter should follow the product outcome and processing purpose through the technical stack.

The schedule should also classify data by restriction. Personal data, confidential business information, regulated records, export-controlled information, payment data and data subject to sector-specific obligations require different controls. Location and transfer mechanisms matter when data moves across jurisdictions. Sensitive classes should be identified at field and workflow level rather than through a generic label applied to the entire platform.

Table 1 Customer-data asset and obligation map

Data layer	Evidence to inspect	Economic role	Transaction question
customer content	master terms, order forms, data schedules and product records	supports the customer's workflow	may the target host, process and transfer it after closing
usage telemetry	notices, product settings, event schemas and retention rules	product analytics and service improvement	is collection expected, disclosed and proportionate
derived data	definitions, transformation logic and contract rights	benchmarking, prediction and automation	does permitted use extend to the forecast activity
model features	lineage, feature store and training records	powers AI-enabled product functions	can features be separated, reproduced and explained
support material	tickets, recordings and attachments	service quality and product insight	are retention and secondary uses controlled
aggregate statistics	aggregation thresholds and re-identification testing	market intelligence and benchmarks	is the output genuinely non-identifying and transferable
configuration data	workflow rules, integrations and permissions	creates customer-specific switching cost	can it be exported and reconstructed without disruption

Proposed diligence record; legal and regulatory conclusions require qualified advisers.

The perimeter prevents three valuation errors: counting data the seller cannot transfer, counting duplicate or obsolete records, and ignoring the operational assets needed to use the data. It also identifies missing evidence early enough for remediation before signing.

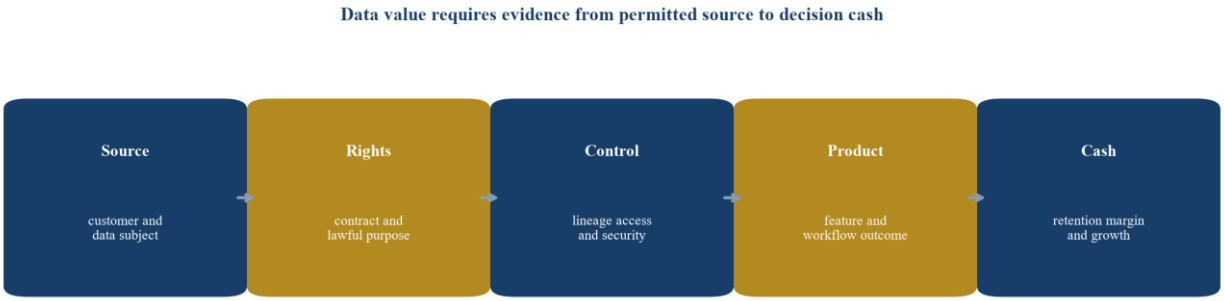
2 Distinguish ownership, control, licence and permitted purpose

Commercial contracts often state that the customer owns customer data while granting the provider a licence to process it. The word ownership rarely answers every transaction question. The licence may be limited to providing the service, may allow product improvement, may permit aggregation, or may terminate with the agreement. Confidentiality, intellectual-property, privacy and deletion provisions can impose further limits. A change-of-control clause, assignment restriction or customer termination right can affect continuity.

The rights review should separate four concepts. Ownership concerns title where the relevant law recognises it. Control concerns practical authority over systems and processing. Licence concerns the contractual permission granted by the customer or another party. Permitted purpose concerns the specific use allowed under the contract and applicable law. The acquirer should not treat operational possession as unrestricted economic control.

Definitions require close reading. Customer Data, Usage Data, Service Data, De-identified Data, Aggregated Data, Output and Feedback may overlap. A broad derived-data definition can be narrowed by confidentiality or privacy commitments elsewhere. Product terms, privacy notices, data-processing agreements, security exhibits and sales representations should be reconciled. Side letters and negotiated enterprise amendments can create customer-specific exceptions.

Figure 1 Rights-to-cash evidence chain



Proposed transaction framework; every connection requires deal-specific evidence.

Table 2 Contract-rights matrix

Right or restriction	Evidence	Economic consequence	Deal response
service-processing right	master terms and data-processing agreement	supports core delivery	confirm survival after closing
product-improvement right	express term and notice	supports analytics and feature development	align forecast with permitted scope
derived-data right	definitions and aggregation standard	supports benchmarks and AI	test confidentiality and privacy limits
assignment restriction	consent and change-of-control clauses	may threaten customer continuity	obtain consent or price attrition risk
deletion obligation	termination and retention terms	reduces historical corpus	model deletion and backup costs
portability obligation	export terms and applicable law	reduces lock-in and raises service cost	test export completeness and timing
audit and security duty	security exhibit and assurance reports	affects operating cost and liability	fund control remediation

Proposed review structure; wording and enforceability are contract- and jurisdiction-specific.

The output should identify rights that are uniform, rights that vary by contract and rights that remain uncertain. Revenue should be mapped to the applicable contract form. This reveals whether a small number of negotiated accounts control a large share of data-enabled value.

3 Reconcile privacy roles, lawful bases and transparency

Personal data creates obligations that operate alongside commercial contracts. The target can act as processor for customer-controlled workflows and controller for account administration, security, billing or its own analytics. The EDPB emphasises that controller and processor roles follow the factual allocation of purposes and means, not labels alone [4-7]. A SaaS provider that uses customer records for an independent purpose may move beyond the customer's instructions.

The diligence team should map each processing purpose to the role, lawful basis, notice, retention period, recipients, international transfers and rights-handling process. Consent should be tested where relied upon; it must meet the applicable standard and remain capable of withdrawal [8-10]. Legitimate-interest

assessments should identify the purpose, necessity and balancing analysis. Contract necessity should be tied to the service requested rather than general commercial convenience.

M&A due diligence itself requires controls. Early bidders rarely need unrestricted production data. The seller can use anonymised or aggregated information, clean teams, staged access, synthetic records and field-level redaction. The ICO advises organisations to establish what data is transferred, its original purpose, the lawful basis, governance, transparency and security during a merger or acquisition [1-3].

Post-close change matters. Combining datasets, training a new model or introducing cross-product personalisation can create a new purpose. The buyer should determine whether existing notices and lawful bases cover that use and whether customers or individuals must be informed. The transaction does not erase prior privacy promises. FTC materials likewise emphasise continued adherence to representations made when data was collected [19-22].

Table 3 Privacy-role and purpose matrix

Processing activity	Likely factual role to test	Core evidence	Value implication
hosting customer records	processor under customer instructions	DPA, instructions and subprocessor list	continuity depends on compliant processing chain
billing and account security	controller for provider purpose	privacy notice and retention schedule	required operating data with bounded use
product telemetry	controller, processor or mixed role	event schema, settings and notices	determines analytics permission and opt-out exposure
cross-customer benchmark	independent purpose to assess	aggregation logic and contract terms	value depends on permitted derivation and disclosure
model training	role depends on purpose and instructions	training lineage and governance record	affects ability to continue or expand AI features
M&A disclosure	separate transaction processing	clean-team protocol and diligence log	limits buyer access and future use

Proposed operating record; lawful basis and notice conclusions require jurisdiction-specific analysis.

The privacy map should feed the valuation model. A use case that requires new consent, customer amendment or deletion has a different probability, timing and cost from an established permitted use.

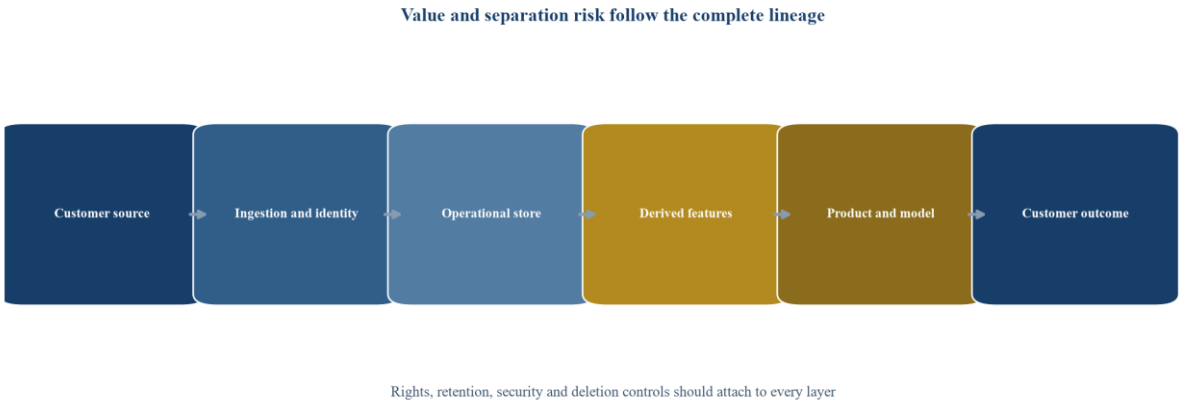
4 Trace data lineage through the product

Data lineage connects contractual rights to actual behaviour. It should show ingestion, validation, transformation, storage, feature generation, model training, inference, output, sharing, archival and deletion. Each step should identify the system, responsible team, legal entity, location, subprocessor and retention control. A policy statement without technical evidence provides weak transaction assurance.

Modern SaaS architecture complicates lineage. Data can pass through event buses, observability platforms, data warehouses, support tools, experimentation systems and third-party AI services. Copies may persist in logs and backups after deletion from the primary application. Model artefacts may retain patterns that require separate assessment. The acquirer should inspect schemas, infrastructure records, code, access controls and deletion tests.

Lineage should also identify commingling. Multi-tenant systems can deliver efficient service and make separation difficult. Shared feature stores or aggregate models can combine information from several customers. A seller carve-out may require logical partitioning, retraining, customer consent or an ongoing service from the parent. The deal perimeter should state whether each asset transfers, remains, is duplicated or must be rebuilt.

Figure 2 Customer-data and product-dependency layers



Proposed architecture model; actual systems and obligations require technical verification.

Lineage completeness can be tested through samples. Select high-value customers and trace representative records from source to output and deletion. Reconcile the observed path with architecture diagrams, processing records and contract terms. Exceptions should become quantified remediation items.

5 Measure product dependence and customer outcomes

The product-dependency map asks what fails when a dataset disappears. The answer can range from a minor analytics report to the core workflow. Teams should identify whether historical depth improves accuracy, shortens implementation, powers network benchmarks, reduces fraud, supports regulatory reporting or creates customer-specific automation. Each dependency should link to measurable product and financial outcomes.

Evidence can include feature adoption, workflow completion, time saved, error reduction, model performance, renewal, expansion, support volume and willingness to pay. Correlation should not be described as causation. Controlled tests, cohort analysis and customer interviews can strengthen the case. The team should record competing explanations such as account size, implementation quality or contract length.

Data dependence can also create fragility. A product may perform poorly for new customers because it relies on historical volume. A benchmark may be dominated by a few large accounts. A model may degrade when a customer deletes records or changes consent. A third-party platform may control the source data. These conditions affect scalability and concentration.

The transaction model should distinguish four mechanisms: current-service necessity, improvement of unit economics, support for retention or expansion, and creation of future options. Current-service necessity has strong evidence when removing the data prevents contracted delivery. Future-option value requires additional probability weighting because product, permission and demand remain uncertain.

Management should assign an evidence grade to every claimed benefit. Grade A can require audited or reproducible operating data. Grade B can reflect controlled internal analysis. Grade C can reflect observed association. Grade D can reflect a roadmap assertion. The valuation should place limited weight on unsupported option narratives.

6 Test data quality, provenance and isolation

Volume has limited meaning without quality. A high-value data corpus should be relevant, accurate enough for the use, timely, complete, representative and traceable to an authorised source. Duplicate, stale or malformed records can increase storage and compliance cost while reducing product performance. Diligence should therefore profile quality by use case rather than apply one platform-wide score.

Provenance establishes where data came from, under which agreement and through which transformation. It should connect a record or dataset to a customer, collection method, notice, purpose and permission. Purchased, scraped, partner-supplied or open data requires separate licence review. Provenance gaps can affect model training, product claims and transferability.

Isolation measures whether the target can identify, export and delete one customer's data without affecting others. It matters for termination, legal rights, incident response and carve-out execution. The team should test tenant identifiers, access boundaries, backup restoration, model-training exclusions and deletion verification. A documented procedure should be supported by operating evidence.

Table 4 Data-quality and isolation scorecard

Dimension	Evidence	Weak condition	Strong condition
provenance	source log and contract linkage	origin cannot be reconstructed	source and permission are traceable
accuracy	validation and exception data	errors materially affect workflow	measured error within approved tolerance
representativeness	cohort and bias testing	corpus dominated by narrow users	known coverage and monitored limitations
timeliness	latency and refresh records	stale data drives decisions	refresh meets product requirement
tenant isolation	access and deletion tests	commingled records lack control	tested logical separation and export
retention	system rules and deletion evidence	policy differs from operation	automated and verifiable lifecycle
security	access, encryption and incident records	broad access or unresolved findings	risk-based controls and monitored access

Proposed scorecard; thresholds should reflect the specific product and regulatory context.

Quality findings should be translated into cash and timing. Remediation may require engineering, customer outreach, retraining, licence fees, reduced claims, deletion or lost functionality. The model should identify which defects are curable and which permanently narrow value.

7 Evaluate switching, portability and interoperability

Customer exit rights influence retention and service cost. The EU Data Act establishes requirements relevant to switching between data-processing services, contractual terms, exportable data, technical support and interoperability [14-16]. The exact application depends on the service and facts. The diligence team should map applicable obligations and compare them with product capability and contract wording.

Portability has several dimensions: data format, schema documentation, configuration, metadata, identity, historical events, attachments, model outputs and integration dependencies. A CSV export may satisfy a narrow contract while failing to preserve functional continuity. The buyer should test actual exports with representative customers and measure completion time, manual intervention and missing fields.

Switching obligations can reduce artificial lock-in and increase engineering cost. They can also improve product trust and enterprise readiness. A platform with clean export interfaces, documented schemas and reliable deletion may face easier customer exit while winning regulated customers and reducing dispute risk. The commercial effect should be measured rather than assumed.

Interoperability affects separation value. Standard interfaces and modular architecture can reduce transition-services dependence. Proprietary connectors, undocumented transformations and parent-company identity systems can increase it. The separation plan should distinguish legal portability from technical reproducibility and operational continuity.

The valuation model should include exit-service cost, export infrastructure, support load and possible retention effects. It should also remove any forecast premium that depends on obstructive switching practices that cannot continue.

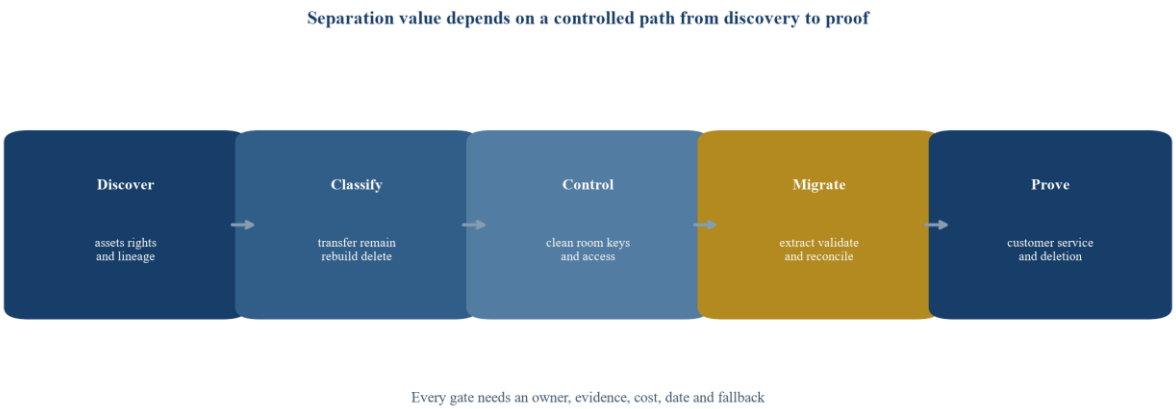
8 Build the carve-out separation architecture

A carve-out requires a target operating model for data on day one and at the end of transition. Each dataset and system needs a disposition: transfer, duplicate, remain, migrate, archive, delete or rebuild. The plan should identify legal authority, customer communications, technical method, responsible party, acceptance test and fallback.

Separation can be complicated by shared identity, billing, telemetry, data warehouses, security operations, support platforms and model pipelines. A parent may hold enterprise licences or encryption keys. Historical data may contain records from both the carved-out business and retained operations. Shared algorithms may constitute parent intellectual property while depending on transferred customer data.

Transition-services agreements should specify data access, purpose, security, service level, incident response, audit, subprocessor control, deletion, export and exit support. Duration should reflect the rebuild sequence. A low headline fee can conceal operational dependence if milestones and acceptance criteria remain vague.

Figure 3 Carve-out data-separation architecture



Proposed separation sequence; the actual plan should be tested against contracts, systems and regulation.

Table 5 Separation-cost model

Cost category	Primary driver	Evidence	Common omission
discovery and lineage	systems, fields and contracts	inventory and sample traces	shadow analytics tools
consent and customer remediation	affected revenue and contract variance	clause matrix and outreach plan	enterprise side letters
extraction and migration	volume, complexity and downtime	migration test and runbook	backups and historical logs
platform rebuild	shared services and licences	dependency map and target design	identity and observability
model retraining	data rights and performance	training lineage and benchmark	loss of shared parent corpus
security and assurance	control gaps and customer commitments	audit reports and remediation plan	inherited subprocessor risk
transition services	duration and service scope	TSA catalogue and exit milestones	stranded operating labour

Illustrative cost categories; amounts should be based on a tested system and contract inventory.

Cost estimates should include contingency tied to evidence quality. A system that has completed a test migration deserves a narrower range than one described only in an architecture slide.

9 Reconstruct revenue and retention dependence

The transaction team should map customer-data rights to annual recurring revenue, gross margin, renewal and expansion. Each customer or cohort should be linked to its contract form, data functions, product modules, export or deletion rights and known disputes. This produces a revenue-at-risk schedule.

Revenue dependence differs from data volume. A small regulated account can carry complex obligations. A large dataset can belong to a free tier. The model should weight cash flows by contractual permission and product necessity. It should also separate revenue already earned from forecast growth based on new analytics, benchmarks or AI features.

Retention analysis should test whether data history creates genuine workflow value. Cohorts can be compared by tenure, data depth, feature adoption and switching events. Customer interviews can test whether historical data is a reason to renew or simply accompanies a mature relationship. Exit records can reveal whether customers can migrate successfully and why they leave.

Gross-margin effects should include storage, compute, observability, security, privacy operations, export support and deletion. AI functions can increase revenue while raising variable compute and governance cost. The data contribution should be measured after these costs.

Forecast scenarios should include full continuity, restricted secondary use, deletion of uncertain records, customer-consent remediation, loss of a benchmark cohort and delayed product launch. The difference between scenarios provides a more useful decision range than a single data premium.

10 Estimate replacement cost and separation cost

Replacement cost asks what a market participant would spend to recreate an asset of equivalent utility, adjusted for obsolescence. It can be relevant when customer data, labelling, cleansing, lineage and integration would require substantial effort. It does not establish economic value when the resulting asset cannot generate cash or when the target lacks rights to use it.

The build-up can include customer acquisition needed to generate records, ingestion engineering, validation, transformation, annotation, governance, security, storage, integration and testing. Historical expenditure should be adjusted for failed work, inefficiency and technology change. The estimate should distinguish the cost of raw records from the cost of a functioning product-data system.

Separation cost is a different measure. It estimates the expenditure required to deliver the transferred business with compliant, controlled and operationally usable data. It can include discovery, customer remediation, migration, shared-service replacement, model retraining and TSA exit. The buyer should avoid adding replacement and separation cost when they cover the same work.

Management assumes a replacement-cost indication of USD 11.6 million in the illustrative case. The build-up includes USD 3.0 million for data generation and onboarding, USD 2.2 million for engineering and transformation, USD 1.8 million for quality and lineage, USD 1.5 million for governance and security, USD 2.1 million for product integration and USD 1.0 million for testing. Management assumes separation and remediation expenditure of USD 8.4 million. These figures are hypothetical and do not represent Matchpoint Partners or client results.

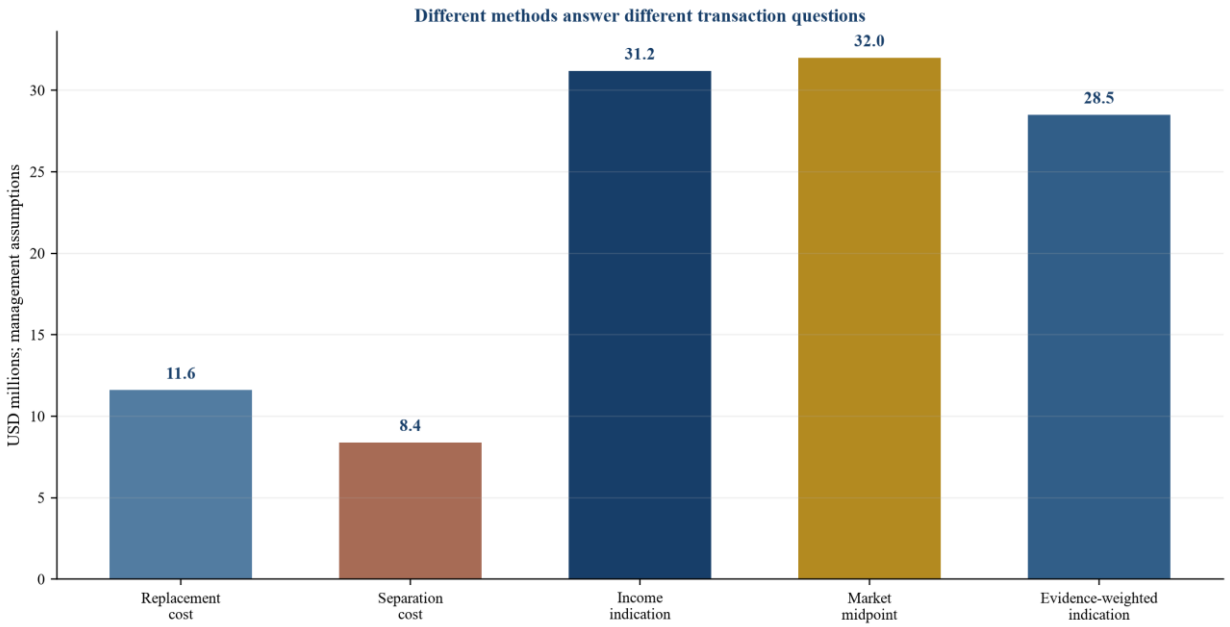
11 Develop income and with-and-without-data scenarios

The income approach should identify cash attributable to the data-enabled capability rather than the entire SaaS business. Relevant mechanisms can include incremental revenue, improved retention, lower service cost, reduced fraud, faster onboarding and avoided third-party data expense. Each mechanism requires a baseline and evidence.

A with-and-without analysis can compare the forecast with permitted, usable data against a scenario in which disputed rights are removed, product functions are rebuilt or customer permissions are delayed. The cash-flow difference should reflect revenue, margin, remediation, tax, capital expenditure and working capital. Probabilities and discount rates should reflect technical, legal and commercial risk without counting the same uncertainty twice.

Management assumes USD 64 million of annual recurring revenue, USD 13 million of EBITDA and 78 per cent of annual recurring revenue materially dependent on customer-generated operational data. Contracts associated with 24 per cent of the relevant corpus have unclear derived-data wording. Management assumes that remediation delays a new benchmark product, reduces near-term expansion and creates customer-outreach cost. The risk-adjusted income indication is USD 31.2 million. Every figure is a management assumption for illustration.

Figure 4 Illustrative data-value reconciliation



All amounts are management assumptions in USD millions and do not represent a transaction result.

The income result should be reconciled with replacement cost, separation cost and market evidence. A high income indication can be unsupported when rights are uncertain or product dependence is weak. A high replacement cost can exceed recoverable cash. The final conclusion should explain the weighting and unresolved evidence.

12 Use market evidence and accounting boundaries carefully

Market evidence for customer data is rarely directly comparable. Transaction prices usually include software, contracts, people, brand, intellectual property and growth options. Public descriptions seldom disclose data rights, quality or separation cost. A revenue multiple should not be converted into a data multiple without a defensible allocation.

Comparable evidence can still inform a corridor. The team can examine acquisitions where data-enabled products, network benchmarks or workflow histories were material to the rationale. It should adjust for recurring revenue, growth, margin, retention, customer concentration, rights, regulation, product maturity and transaction date. The result remains a reasonableness check.

Accounting and transaction valuation serve different purposes. IFRS 3 requires identifiable acquired assets to be recognised separately from goodwill when the relevant criteria are met. IAS 38 addresses identifiable intangible assets, IFRS 13 fair value, IAS 36 impairment and IFRS 15 revenue [39-45]. Customer-related data may interact with software, customer relationships, contracts and technology. The accounting unit of account and useful life require specialist judgement.

Table 6 Valuation-method reconciliation

Method	What it measures	Strength	Limitation
replacement cost	cost to recreate equivalent utility	useful for engineered and curated assets	does not prove demand or permission
separation cost	cost to deliver usable transferred capability	directly informs price and funding	can overlap with operating remediation
with-and-without income	incremental cash from data-enabled capability	connects rights and product to cash	sensitive to baseline and attribution

Method	What it measures	Strength	Limitation
relief from royalty	avoided licence payment	useful where licensable comparables exist	customer data is often not separately licensed
market corridor	observed transaction or licence evidence	provides external reasonableness check	bundled assets and sparse disclosure
option analysis	value of future permitted applications	captures staged decisions	highly sensitive to probabilities and milestones

Proposed reconciliation; method selection and weighting depend on evidence and purpose.

In the illustrative case, management assumes a market corridor of USD 24 million to USD 40 million and an evidence-weighted indication of USD 28.5 million. The weighting reflects uncertain derived-data language, separation cost and the stronger evidence for core-service use. The conclusion is hypothetical.

13 Convert uncertainty into transaction terms

Valuation findings should change the deal. A price adjustment can reflect quantified separation cost. A holdback or escrow can cover defined customer claims or remediation. Earn-outs can link payment to consent, product launch, retention or verified data migration. Closing conditions can require material consents, completed exports, security remediation or delivery of lineage records.

Representations should address contract rights, privacy compliance, notices, data sources, security, incidents, deletion, international transfers, subprocessors and model training. Knowledge qualifiers, materiality thresholds, survival and caps should match the risk. Specific indemnities can address identified matters. Insurance should be reviewed for coverage, exclusions and continuity.

The buyer should obtain operational covenants between signing and closing. These can restrict new secondary uses, changes to privacy terms, deletion of lineage records, material subprocessor changes and alterations to shared systems. A carve-out needs cooperation obligations, TSA detail, migration support and acceptance criteria.

Table 7 Data risk to transaction-term conversion

Finding	Economic exposure	Possible term	Verification
unclear derived-data right	lost product revenue or customer dispute	consent condition or earn-out gate	executed amendment and product test
incomplete lineage	remediation and regulatory uncertainty	holdback and funded work plan	approved lineage register
shared parent platform	delayed separation and service risk	TSA with milestones and service credits	migration rehearsal and acceptance test
deletion-control gap	customer claim and operating cost	specific indemnity and remediation covenant	deletion test across live and backup systems
material security finding	incident and churn exposure	closing condition or escrow	independent retest
model trained on disputed corpus	retraining cost and performance loss	price adjustment and performance milestone	clean-corpus benchmark

Illustrative deal tools; legal drafting should reflect the transaction and governing law.

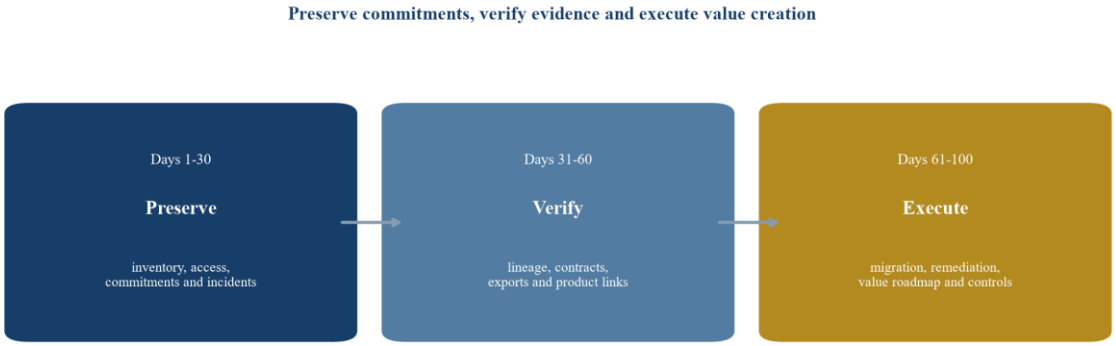
Terms should address evidence that can be produced. A vague warranty about owning all data provides limited protection when the commercial issue is a narrow permitted purpose. The schedule should identify the affected corpus, revenue, product and remedy.

14 Govern data value through integration and conclude

Post-close governance should begin at signing. A data-value committee can bring together product, legal, privacy, security, finance, engineering and commercial owners. Its first task is to preserve commitments while validating the combined operating model. New uses should pass rights, purpose, security, product and economics gates.

The first thirty days should secure the inventory, freeze unapproved changes, confirm subprocessors, preserve deletion and incident processes, and validate high-risk contracts. Days thirty-one to sixty should close lineage gaps, test exports, begin customer remediation and validate product dependencies. Days sixty-one to one hundred should complete priority migration rehearsals, approve the data-value roadmap and update the valuation with verified evidence.

Figure 5 One-hundred-day data-value governance roadmap



Proposed integration plan; timing should reflect transaction structure and risk.

Board reporting should track rights coverage, data lineage completeness, customer remediation, separation milestones, incidents, export performance, deletion evidence, product dependence, revenue at risk and realised value. Metrics should distinguish verified results from management assumptions. A quarterly revaluation can update scenario weights as rights, product evidence and customer behaviour change.

Practical execution gates

The governance system should operate through explicit gates. The first gate confirms the transaction perimeter. Finance, product, legal and engineering teams should agree which entities, customer contracts, applications, datasets, models, licences and people transfer. The gate should identify every dependency on the seller, affiliate or third party. An unresolved perimeter weakens every later cost and value conclusion.

The second gate confirms legal and contractual authority. Counsel should review the standard terms and the contracts representing the largest revenue, most sensitive data and most important product dependencies. The review should reconcile assignment, change of control, confidentiality, data-use, deletion, audit, security and subprocessor provisions. The decision record should quantify the annual recurring revenue and data corpus associated with each exception. A simple count of reviewed contracts can mislead when a few negotiated customers drive most exposure.

The third gate confirms technical control. Engineering should demonstrate the lineage of representative records, tenant isolation, access control, export, deletion and recovery. The demonstration should include live systems, downstream analytics and backups. Product owners should show which features fail, degrade

or lose commercial relevance when a dataset is removed. The gate should produce test evidence, named owners and remediation dates.

The fourth gate confirms economic attribution. Finance should reconcile product metrics to billing, retention, expansion and cost records. The team should explain why the data causes or enables an economic effect and identify other variables. Where causal evidence is unavailable, the model should use a conservative scenario range. Every valuation input should link to an evidence item, an owner and a date.

The fifth gate confirms separation or integration readiness. A migration rehearsal should test extraction, transformation, loading, reconciliation, customer service and rollback. The runbook should identify downtime, manual effort, data loss, control exceptions and unresolved dependencies. Transition-service milestones should derive from the tested sequence. Completion should require evidence that the buyer can operate the transferred business within the agreed control environment.

The sixth gate confirms transaction protection. The investment committee should see how each material uncertainty changes price, closing conditions, covenants, warranties, indemnities, insurance, escrow, earn-out or TSA provisions. Deal terms should identify an objective verification event. A generic protection offers weak control when the exposure concerns a specific corpus, customer group, product module or system dependency.

A controlled evidence register supports these gates. Each entry should state the question, evidence requested, source, date, reviewer, conclusion, financial exposure, remediation, transaction response and residual risk. Contradictory evidence should remain visible. Management assumptions should be time stamped and assigned for validation. Legal opinions, technical tests and valuation conclusions should be separated so that each specialist's responsibility remains clear.

Customer communication deserves a separate plan. Some transactions require consent or notice. Others preserve the contracting entity while changing systems, purposes or subprocessors. The team should classify customers by legal requirement, contractual commitment, commercial sensitivity and operational impact. Messaging should explain service continuity, data protection, support and any required action. High-value accounts should have named relationship owners and fallback plans.

Integration design should avoid expanding data use merely because two companies can combine systems. The combined business should define the intended purpose, customer benefit, lawful and contractual authority, minimum data, security control, retention and measurable economics before enabling a new use. A pilot can test product value and operating cost with a limited, approved corpus. Full deployment should follow evidence and governance approval.

The same discipline applies to artificial-intelligence features. Training data should be linked to source, permission, preprocessing, model version and evaluation. The buyer should know whether a model can be retrained without restricted records, how performance changes, whether outputs expose confidential information and what customer commitments apply. Model evaluation should include accuracy, robustness, bias, privacy, security and human oversight relevant to the use case. A roadmap claim without a permitted training corpus and a tested customer outcome should receive limited transaction value.

Operational resilience should be tested under adverse conditions. Scenarios can include a major customer deleting data, loss of a subprocessor, a cross-border transfer disruption, a security incident during migration, failure of a shared identity service and delayed customer consent. The board should see service, cash, cost and compliance consequences, along with recovery actions. This connects data governance to business continuity and financing capacity.

Financing stakeholders need a related view. Lenders should understand whether recurring revenue depends on data rights that can terminate, whether an incident or forced deletion can impair covenant capacity, and whether separation expenditure competes with debt service. Equity investors should see which data-enabled growth cases require customer amendments, regulatory clearance or additional

product investment. The diligence model should therefore bridge data findings to liquidity, covenant headroom and capital requirements under central and adverse cases.

The integration budget should separate mandatory control work from discretionary growth investment. Mandatory work can include contract remediation, migration, security, deletion, transfer mechanisms and TSA exit. Growth investment can include new benchmarks, cross-product analytics and AI features. Combining both categories obscures the cash required to operate safely at closing and can make a strategic option appear unavoidable. The board should approve each growth case after the permission, evidence and return gates are met.

Internal audit or an independent assurance function can review whether controls operate as designed. Sampling should cover high-value customers, sensitive data, major subprocessors and the most important data-enabled features. Exceptions should be graded by customer, regulatory, operational and financial consequence. The review should test the evidence chain rather than rely solely on policy documents.

Finally, the buyer should establish a stop rule. A data use should pause when the required right, purpose, lineage, security control or customer outcome cannot be evidenced within the approved risk threshold. The stop rule protects the transaction thesis from optimism after closing. It also creates a clear route to remediation, redesign or removal from the valuation case.

The decision record should remain available for future audits, refinancing, customer assurance and portfolio review.

The evidence register should remain active after closing. Verified findings can replace assumptions, release contingent consideration or trigger remediation. Product and finance teams can measure whether forecast benefits are realised. Privacy and security teams can confirm that processing remains within approved purposes. The board can stop or redesign a use case when the evidence no longer supports its value or control profile.

Customer-generated data creates defensible transaction value when four conditions align: the use is permitted, the data is controlled and traceable, the product benefit is evidenced, and the cash consequence is measurable. Separation readiness is part of that value because an asset that cannot move without disruption has limited transferable utility. The most reliable transaction process follows the evidence from contract and purpose through lineage and product to cash, then converts remaining uncertainty into price, terms and governance.

Frequently asked questions

Does a SaaS provider own customer-generated data?

The answer depends on the contract, the data type and applicable law. Many SaaS contracts state that the customer owns customer data and grants the provider limited processing rights. Operational possession does not establish unrestricted ownership or use. Transaction diligence should distinguish title, control, licence and permitted purpose.

Can customer data transfer automatically in an acquisition?

The transaction structure, contract assignment terms, privacy roles, notices and applicable law determine the answer. A share acquisition can preserve the legal entity while still changing processing purposes or systems. An asset transfer can require assignment or consent. The exact facts require legal review.

How should a buyer value derived data?

The buyer should first prove how derived data is defined, generated and permitted. It should then connect the derived output to a product and cash-flow mechanism. Replacement cost, with-and-without income,

separation cost and market evidence can be reconciled. Unsupported volume or uniqueness claims should carry limited weight.

Why does data lineage matter in M&A?

Lineage shows where data came from, what happened to it, where it resides and which outputs depend on it. It connects contract and privacy obligations to technical operation. It also supports migration, deletion, incident response, customer communication and valuation.

What is separation value in a SaaS carve-out?

Separation value is the economic utility that remains after the data and supporting systems can be transferred or rebuilt for the carved-out business. It reflects rights, portability, shared services, migration, model retraining, customer continuity and transition cost.

Can anonymised or aggregated data be used freely?

The answer depends on whether the data is genuinely anonymous under the applicable standard, the contractual promises, confidentiality duties and the proposed use. A label in a contract or system does not establish effective anonymisation. Re-identification risk and aggregation controls require evidence.

How do portability rules affect SaaS value?

Portability and switching obligations can increase export and support costs, reduce artificial lock-in and improve enterprise trust. The valuation should reflect actual customer behaviour, product quality, service cost and applicable legal obligations.

Which findings should change transaction terms?

Material uncertainty over rights, consent, lineage, security, separation or model training should be linked to a quantified exposure and evidence plan. Price adjustments, closing conditions, customer consents, escrows, indemnities, TSAs and milestones can allocate the identified risk.

References

[1] UK Information Commissioner's Office, Due diligence when sharing data following mergers and acquisitions, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/due-diligence/

[2] UK Information Commissioner's Office, Data Sharing Code of Practice, https://ico.org.uk/media/for-organisations/documents/4012020/data-sharing-code-of-practice.pdf

[3] UK Information Commissioner's Office, Data sharing advice, https://ico.org.uk/for-organisations/advice-for-small-organisations/information-security/data-sharing-advice/

[4] European Data Protection Board, Guidelines 07/2020 on controller and processor concepts, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[5] European Data Protection Board, Guidelines 2/2019 on Article 6(1)(b), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[6] European Data Protection Board, Guidelines 4/2019 on Article 25, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

[7] European Data Protection Board, Recommendations 01/2020 on supplementary transfer measures, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

[8] European Data Protection Board, Guidelines 05/2020 on consent, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[9] European Data Protection Board, Guidelines 8/2020 on targeting social media users, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

[10] European Data Protection Board, Opinion 28/2024 on AI models, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

[11] European Union, Regulation (EU) 2016/679 General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[12] UK Government, Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents

[13] UK Information Commissioner's Office, Guide to the UK GDPR, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

[14] European Union, Regulation (EU) 2023/2854 Data Act, https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[15] European Commission, Data Act explained, https://digital-strategy.ec.europa.eu/en/policies/data-act

[16] European Commission, Switching between cloud and edge services, https://digital-strategy.ec.europa.eu/en/policies/cloud-switching

[17] European Union, Regulation (EU) 2022/868 Data Governance Act, https://eur-lex.europa.eu/eli/reg/2022/868/oj

[18] European Union, Regulation (EU) 2022/1925 Digital Markets Act, https://eur-lex.europa.eu/eli/reg/2022/1925/oj

[19] US Federal Trade Commission, Facebook and WhatsApp privacy obligations, https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed-acquisition

[20] US Federal Trade Commission, Privacy promises prevail, https://www.ftc.gov/business-guidance/blog/2014/04/ftc-staff-facebook-whatsapp-privacy-promises-prevail

[21] US Federal Trade Commission, AI companies: uphold privacy and confidentiality commitments, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments

[22] US Federal Trade Commission, 23andMe bankruptcy impact letter, https://www.ftc.gov/system/files/ftc_gov/pdf/23andme-letter-ferguson.pdf

[23] California Legislature, California Consumer Privacy Act, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&chapter=1.&part=4.&lawCode=CIV&title=1.81.5

[24] California Privacy Protection Agency, CCPA regulations, https://cppa.ca.gov/regulations/

[25] US Department of Justice and Federal Trade Commission, 2023 Merger Guidelines, https://www.justice.gov/atr/2023-merger-guidelines

[26] European Commission, Guidelines on Article 102 TFEU enforcement priorities, https://competition-policy.ec.europa.eu/antitrust-and-cartels/legislation/application-article-102-tfeu_en

[27] NIST, Privacy Framework, https://www.nist.gov/privacy-framework

[28] NIST, Cybersecurity Framework 2.0, https://www.nist.gov/cyberframework

[29] NIST, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework

[30] NIST, Privacy Engineering Program, https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

[31] OECD, Enhancing Access to and Sharing of Data, https://www.oecd.org/en/publications/enhancing-access-to-and-sharing-of-data_276aaca8-en.html

[32] OECD, Data-driven innovation, https://www.oecd.org/en/publications/data-driven-innovation_9789264229358-en.html

[33] OECD, Recommendation on Enhancing Access to and Sharing of Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463

[34] OECD, Digital Security Risk Management for Economic and Social Prosperity, https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.html

[35] World Intellectual Property Organization, Intellectual property and data, https://www.wipo.int/about-ip/en/frontier_technologies/data/

[36] World Intellectual Property Organization, Valuing intellectual property assets, https://www.wipo.int/sme/en/value_ip_assets/

[37] International Organization for Standardization, ISO/IEC 27001 information security, https://www.iso.org/standard/27001

[38] International Organization for Standardization, ISO/IEC 27701 privacy information management, https://www.iso.org/standard/71670.html

[39] IFRS Foundation, IFRS 3 Business Combinations, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[40] IFRS Foundation, IAS 38 Intangible Assets, https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[41] IFRS Foundation, IFRS 13 Fair Value Measurement, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

[42] IFRS Foundation, IAS 36 Impairment of Assets, https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/

[43] IFRS Foundation, IFRS 15 Revenue from Contracts with Customers, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[44] International Valuation Standards Council, IVS 210 Intangible Assets, https://www.ivsc.org/standards/

[45] Financial Accounting Standards Board, Business Combinations topic 805, https://asc.fasb.org/topic&trid=2129119

[46] European Commission, Standard Contractual Clauses, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[47] European Commission, EU-US Data Privacy Framework, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[48] UK Information Commissioner's Office, Anonymisation, pseudonymisation and privacy enhancing technologies, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/

[49] UK Information Commissioner's Office, Contracts and liabilities between controllers and processors, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts/

[50] Cybersecurity and Infrastructure Security Agency, Secure by Design, https://www.cisa.gov/securebydesign

About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.