Data and AI Rights in a Joint Venture: Ownership, Access, Training and Commercial Use

A Rights Architecture for Contributed Data, Generated Assets, Models and Outputs

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Joint ventures increasingly combine proprietary datasets, customer and operational information, software, models, domain expertise and computing resources. Value can grow through shared analytics and artificial intelligence, while legal and commercial rights fragment across contributors, individuals, vendors, jurisdictions and the venture itself. This paper develops a rights architecture for ownership, access, training and commercial use. It distinguishes data from database rights, personal data, confidential information, trade secrets, software, model weights, fine-tuning artefacts, prompts, retrieval stores and outputs; maps background and venture-created assets; defines permitted purposes, territories, users, models and channels; and translates those permissions into technical controls. The framework addresses privacy roles and lawful bases, provenance, third-party licences, copyright, trade secrets, competition-sensitive information, cross-border transfers, the EU Data Act, the EU AI Act, UK data reforms, security, model evaluation, incident response, valuation, revenue allocation, audit and exit. Five figures and five tables provide a rights taxonomy, provenance maturity curve, access-control architecture, commercial-rights bridge and exit certificate. Eight frequently asked questions and forty primary or authoritative references support application. Numerical values are illustrative analytical scenarios. Transaction-specific conclusions require verified legal, privacy, intellectual-property, competition, technical, tax, valuation, regulatory and jurisdiction-specific evidence and advice.

JEL Classification: G34, K11, K24, O34, L24

Keywords: joint venture, data rights, artificial intelligence, training data, model rights, access, commercialisation, governance

1. Define the venture use cases

The partners should state the decisions, products, users, markets and benefits that require data or AI. The required output is a purpose-and-value memorandum. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [1][2].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that rights can be granted more broadly than the venture thesis requires. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

2. Map every legal and operating role

The partners should identify contributors, controllers, processors, providers, deployers, vendors, licensors and users. The required output is a role-allocation map. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [3][4].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that one entity can assume duties that the contract assigns elsewhere. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

3. Build the asset taxonomy

The partners should separate raw data, databases, metadata, features, labels, code, models, weights, adapters, prompts, retrieval stores and outputs. The required output is an asset register. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [5][6].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the word data can conceal materially different assets and rights. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

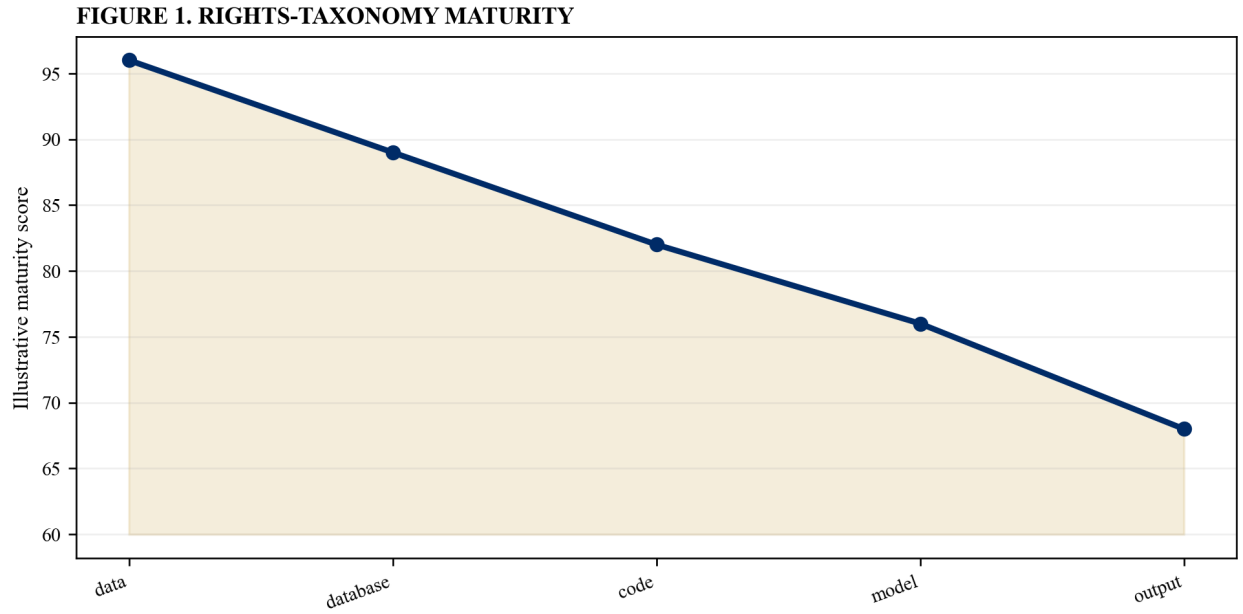
Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

Table 1. Data and AI asset taxonomy

Asset	Primary right question	Control
source data	lawful collection and use	provenance
model	copy and deploy	custody
workflow	modify and operate	knowledge transfer
output	use and commercialise	human review

Illustrative analytical structure; verified transaction evidence and specialist review govern.

Figure 1. Rights-taxonomy maturity



Illustrative analytical scenario; verified transaction evidence should replace index values.

4. Separate background and foreground assets

The partners should record what existed before the venture, what is created jointly and what is derived from each input. The required output is a background-foreground schedule. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [7][8].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that venture-created value can be claimed as pre-existing property. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

5. Verify provenance and lawful control

The partners should trace source, collector, licence, consent, notice, restriction, transformation and custodian. The required output is a provenance ledger. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [9][10].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that possession can be mistaken for lawful authority to use. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

6. Map personal-data lawful bases

The partners should document purpose, lawful basis, fairness, transparency, minimisation and retention for each processing activity. The required output is a processing record. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [11][12].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that commercial permission can be mistaken for a privacy-law basis. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

7. Allocate controller and processor duties

The partners should decide purposes and means, instructions, assistance, subprocessors, security, rights requests and breach handling. The required output is a privacy responsibility matrix. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [11][13].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that joint influence can create shared responsibility absent from the contract. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

8. Protect sensitive and regulated data

The partners should identify special-category, biometric, financial, health, children, employee and sector-regulated information. The required output is a sensitivity-control matrix. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [12][14].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that high-impact information can enter general training pipelines. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

9. Test third-party licences

The partners should review vendor, open-source, data-provider, cloud, platform and customer terms for access and model-training rights. The required output is a licence compatibility register. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [15][16].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a contributor can promise rights it received only for internal use. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

10. Identify database and compilation rights

The partners should separate rights in individual records from selection, arrangement and substantial database investment. The required output is a database-rights analysis. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [17][18].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that ownership of a database can be confused with rights in its contents. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

11. Protect trade secrets and confidentiality

The partners should define secrecy, reasonable measures, authorised recipients, permitted analysis and residual knowledge. The required output is a trade-secret control plan. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [19][20].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that sharing can destroy protection or expand permitted use. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

12. Allocate software and model IP

The partners should map source code, object code, architecture, documentation, models and modifications. The required output is a software-and-model rights schedule. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [7][21].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that model access can be granted without deployable code or dependencies. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

13. Define training permissions precisely

The partners should specify datasets, models, purposes, territories, compute, retention, re-training and prohibited uses. The required output is a training-rights licence. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [22][23].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that general access can be interpreted as permission to train any model. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

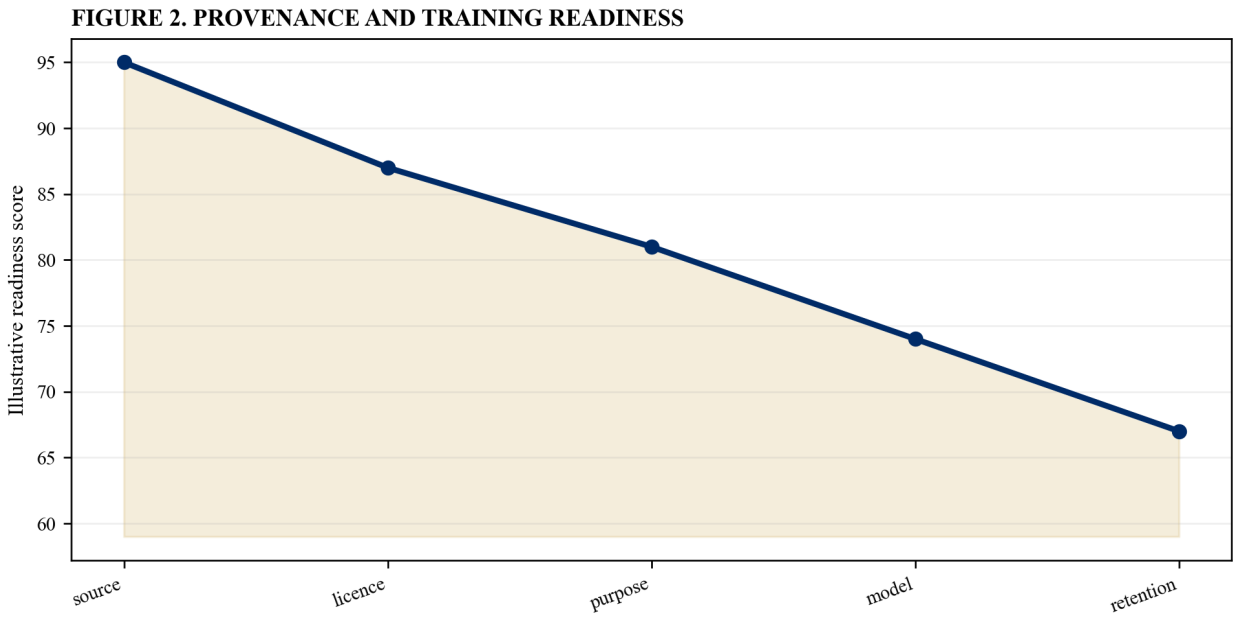
Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

Table 2. Training-rights specification

Dimension	Example boundary	Evidence
dataset	named sources	lineage
purpose	approved use case	decision memo
model	named family/version	registry
term	training and retention window	logs

Illustrative analytical structure; verified transaction evidence and specialist review govern.

Figure 2. Provenance and training readiness



Illustrative analytical scenario; verified transaction evidence should replace index values.

14. Control fine-tuning artefacts

The partners should allocate adapters, checkpoints, embeddings, synthetic data, evaluation sets and learned parameters. The required output is a derivative-artefact schedule. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [5][24].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that valuable adaptation can fall between data and model definitions. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

15. Treat model weights separately

The partners should define possession, hosting, copying, export, security, modification and post-termination use. The required output is a model-weight custody plan. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [3][25].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that API access can be confused with ownership of the underlying model. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

16. Define prompt and workflow rights

The partners should allocate system prompts, templates, tools, agents, orchestration, policies and process know-how. The required output is a workflow asset register. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [19][24].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that operating know-how can leave with one partner. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

17. Govern retrieval and vector stores

The partners should trace source chunks, embeddings, refresh, access, deletion and output attribution. The required output is a retrieval-governance map. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [11][26].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that deleted source material can persist in derived stores. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

18. Allocate output rights cautiously

The partners should define permitted use, review, attribution, confidentiality, infringement response and reuse. The required output is an output-use policy. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [27][28].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the agreement can promise exclusive copyright that law does not recognise. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

19. Require human contribution records

The partners should retain instructions, selection, arrangement, editing and accountable approval where copyright or authorship matters. The required output is a human-contribution record. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [27][29].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that machine generation can be presented as protected human authorship. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

20. Set access by purpose and role

The partners should grant least-privilege access by user, asset, task, duration, environment and export right. The required output is a purpose-bound entitlement model. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [30][31].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that broad technical access can defeat narrow contractual permissions. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

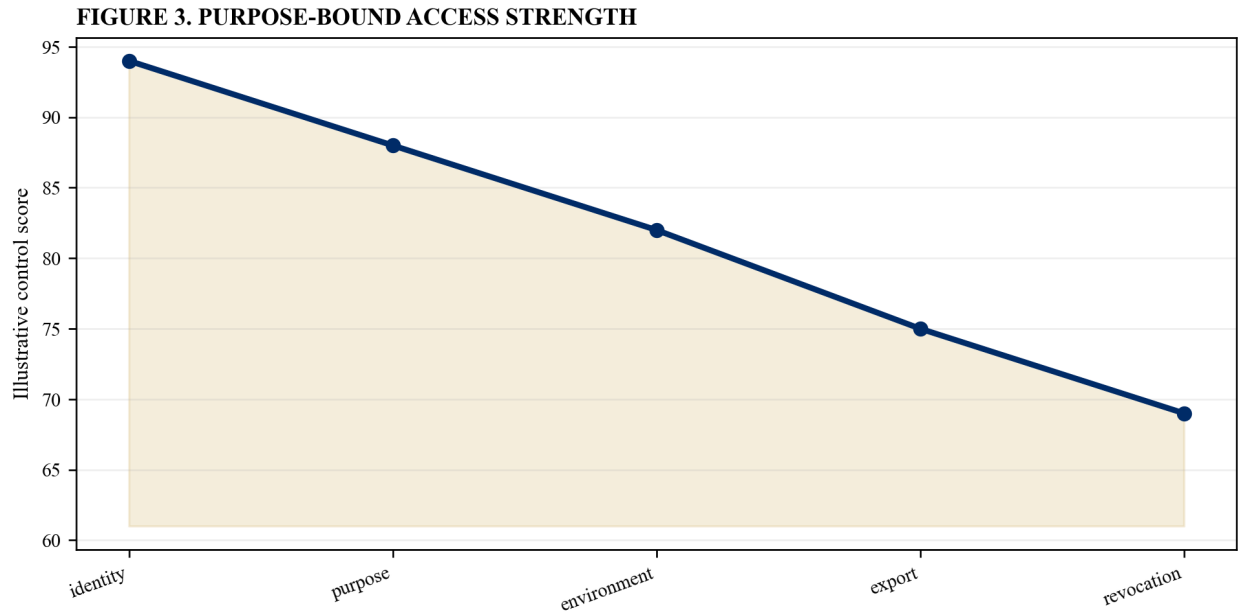
Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

Table 3. Access-control architecture

Layer	Decision	Control
identity	who	role access
purpose	why	policy binding
environment	where	clean room
export	what leaves	approval and logging

Illustrative analytical structure; verified transaction evidence and specialist review govern.

Figure 3. Purpose-bound access strength



Illustrative analytical scenario; verified transaction evidence should replace index values.

21. Use secure collaboration environments

The partners should apply clean rooms, federated learning, confidential computing, aggregation or controlled APIs where appropriate. The required output is a protected-compute design. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [30][32].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that partners can copy raw information when only joint insight is needed. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

22. Control competition-sensitive information

The partners should restrict prices, customers, wages, capacity, pipelines and strategy between competing parents. The required output is a competition clean-team protocol. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [33][34].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the venture can become a conduit for coordination. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

23. Design interoperability and access rights

The partners should map connected-product data, user rights, switching, export formats and third-party access. The required output is a Data Act compliance map. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [35][36].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that technical lock-in can conflict with statutory access or portability. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

24. Govern cross-border transfers

The partners should identify origin, destination, recipient, safeguards, localisation, government-access risk and onward transfer. The required output is a transfer-impact register. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [11][37].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that cloud architecture can move data beyond approved jurisdictions. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

25. Set retention and deletion rules

The partners should define operational need, legal hold, model effects, backups, embeddings, logs and certified deletion. The required output is a lifecycle schedule. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [11][30].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that source deletion can leave recoverable or influential derivatives. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

26. Create security ownership

The partners should allocate identity, encryption, keys, vulnerability, supply chain, monitoring, recovery and assurance. The required output is a shared-security model. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [31][38].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that split responsibility can leave critical controls ownerless. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

27. Classify AI Act roles and systems

The partners should determine provider, deployer, importer, distributor, GPAI and high-risk status for each product and market. The required output is an AI regulatory map. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [3][4].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that branding or modification can shift provider obligations. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

28. Document models for downstream users

The partners should provide capabilities, limitations, inputs, outputs, evaluation, integration, energy and risk information. The required output is a model information pack. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [3][25].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a downstream venture can lack information needed for compliant deployment. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

29. Evaluate performance and risk

The partners should test accuracy, robustness, bias, privacy, security, misuse, drift and human oversight by use case. The required output is an evaluation and acceptance record. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [2][39].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a model can be approved on generic benchmarks unrelated to venture decisions. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

30. Govern model and data changes

The partners should approve new sources, versions, prompts, tools, vendors, thresholds and deployment contexts. The required output is a change-control ledger. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [2][31].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a compliant initial design can drift through routine updates. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

31. Manage vendor concentration

The partners should map cloud, model, data, tooling, licence, continuity, audit, export and replacement dependencies. The required output is a third-party dependency register. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [16][38].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the venture can lack rights to continue after vendor or partner exit. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

32. Value contributed rights

The partners should measure scope, exclusivity, quality, lawful usability, scarcity, useful life, substitution and supporting cost. The required output is a rights valuation. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [40][8].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that data volume can be mistaken for economic value. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

33. Separate ownership from economics

The partners should allocate fees, royalties, revenue shares, compute costs, improvement rights and commercial channels. The required output is a commercial-rights waterfall. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [8][40].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that legal title can receive value twice through ownership and revenue rights. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

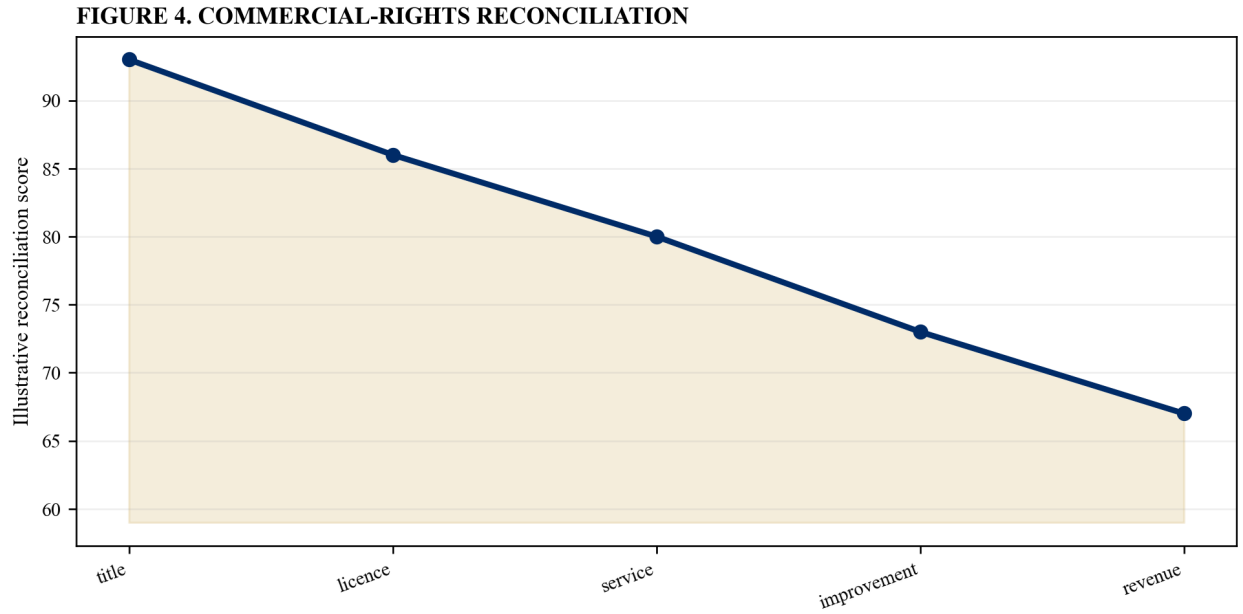
Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

Table 4. Commercial-rights bridge

Right	Economic route	Double-count control
ownership	residual asset value	title schedule
licence	royalty	scope
service	cost-plus or fee	deliverable
improvement	revenue share	foreground map

Illustrative analytical structure; verified transaction evidence and specialist review govern.

Figure 4. Commercial-rights reconciliation



Illustrative analytical scenario; verified transaction evidence should replace index values.

34. Define customer and market use

The partners should specify products, segments, territories, channels, sublicensing, white labelling and parent-company use. The required output is a commercial-use matrix. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [15][35].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that one partner can commercialise joint assets outside the venture perimeter. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

35. Set transfer-pricing discipline

The partners should align legal ownership with functions, assets, risks, development, enhancement, maintenance, protection and exploitation. The required output is a tax-and-rights bridge. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [6][40].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that contractual title can diverge from value-creating activity. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

36. Create auditable telemetry

The partners should log source, user, purpose, model, version, prompt, output, export, approval and incident without over-collecting. The required output is a rights-use audit trail. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [2][31].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the venture can lack evidence of compliance or exceed retention needs. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

37. Prepare incident and claim routes

The partners should coordinate privacy breach, cyber incident, IP claim, harmful output, regulator notice and customer remedy. The required output is an incident-responsibility playbook. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [12][38].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that partners can issue inconsistent responses while harm expands. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

38. Resolve rights deadlock

The partners should route disputes over source, access, training, release, valuation and deletion to defined experts and escalation. The required output is a data-and-AI dispute matrix. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [1][20].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a technical service can stop while the forum is contested. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

39. Engineer exit and portability

The partners should define export, formats, licences, model continuity, transition services, deletion, audit and residual rights. The required output is an exit-rights plan. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [35][36].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that a partner can leave with the only usable copy or operating capability. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

40. Issue the rights certificate

The partners should reconcile assets, provenance, roles, permissions, controls, economics, incidents, exceptions and exit treatment. The required output is an auditable data-and-AI rights certificate. Record the asset, rights holder, legal basis, permitted purpose, users, territory, term, restrictions, technical control, accountable owner and approval [1][2].

Test each permission against source provenance, privacy, intellectual property, confidentiality, competition, security, sector regulation, vendor terms and the venture's operating model. Separate access, use, training, modification, disclosure, commercialisation, portability and deletion rather than relying on a single ownership label.

The principal risk is that the commercial bargain can outlive its evidence and technical enforcement. Compare the proposed right with the narrowest permission needed for the approved use case and define evidence, monitoring, revocation and remedy.

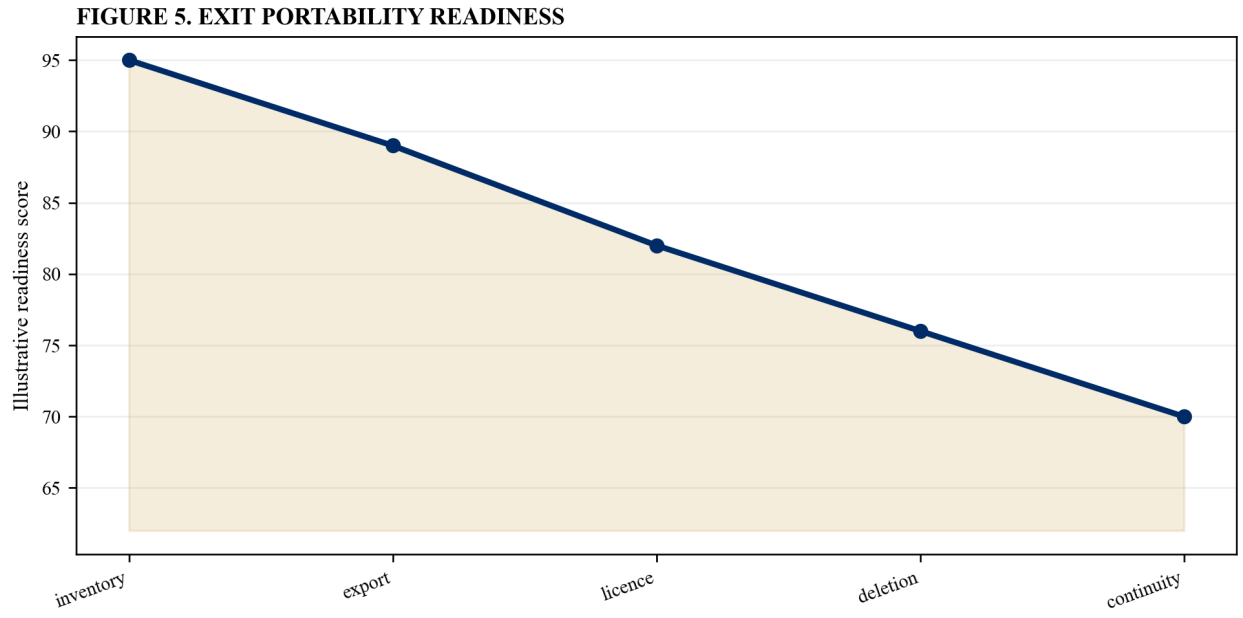
Retain contracts, notices, consents, licences, lineage, model cards, evaluations, access logs, approvals, incidents, changes and exceptions. Refresh the analysis when sources, laws, models, vendors, purposes, jurisdictions or ownership change.

Table 5. Exit rights certificate

Conclusion	Evidence	Acceptance
export	files and formats	technology
licence	continuing permissions	legal
deletion	source and derivatives	privacy
continuity	models and services	operations

Illustrative analytical structure; verified transaction evidence and specialist review govern.

Figure 5. Exit portability readiness



Illustrative analytical scenario; verified transaction evidence should replace index values.

References

[1] OECD, G20/OECD Principles of Corporate Governance 2023, https://www.oecd.org/en/publications/g20-oecd-principles-of-corporate-governance-2023_ed750b30-en.html

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

[3] European Commission, AI Act Regulatory Framework, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[4] European Commission, Guidelines on Obligations for General-Purpose AI Providers, https://digital-strategy.ec.europa.eu/en/faqs/guidelines-obligations-general-purpose-ai-providers

[5] ISO/IEC, ISO IEC 22989 Artificial Intelligence Concepts and Terminology, https://www.iso.org/standard/74296.html

[6] OECD, Transfer Pricing Guidelines 2022, https://www.oecd.org/en/publications/oecd-transfer-pricing-guidelines-for-multinational-enterprises-and-tax-administrations-2022_0e655865-en.html

[7] World Intellectual Property Organization, Intellectual Property for Business, https://www.wipo.int/en/web/business/

[8] International Valuation Standards Council, IVS Standards, https://ivsc.org/standards/

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

[10] World Intellectual Property Organization, IP Due Diligence, https://www.wipo.int/en/web/business/ip-due-diligence

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

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

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

[14] UK Information Commissioner's Office, Special Category Data, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/

[15] World Intellectual Property Organization, IP Licensing, https://www.wipo.int/en/web/business/licensing

[16] NIST, Cybersecurity Supply Chain Risk Management Practices, https://csrc.nist.gov/pubs/sp/800/161/r1/final

[17] European Union, Directive 96/9/EC on Legal Protection of Databases, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31996L0009

[18] UK Government, Database Right Guidance, https://www.gov.uk/guidance/sui-generis-database-rights-after-the-transition-period

[19] World Intellectual Property Organization, Trade Secrets, https://www.wipo.int/tradesecrets/en/

[20] European Union, Trade Secrets Directive, https://eur-lex.europa.eu/eli/dir/2016/943/oj

[21] World Intellectual Property Organization, Copyright and Computer Programs, https://www.wipo.int/copyright/en/

[22] U.S. Copyright Office, Copyright and Artificial Intelligence, https://www.copyright.gov/ai/

[23] European Commission, General-Purpose AI Models Questions and Answers, https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers

[24] NIST, Secure Software Development Framework, https://csrc.nist.gov/Projects/ssdf

[25] European Commission, General-Purpose AI Code of Practice, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

[26] NIST, Generative AI Profile, https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence

[27] U.S. Copyright Office, Copyright and AI Part 2 Copyrightability, https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf

[28] UK Intellectual Property Office, Artificial Intelligence and Intellectual Property, https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence

[29] U.S. Copyright Office, Registration Guidance for Works Containing AI-Generated Material, https://www.copyright.gov/ai/ai_policy_guidance.pdf

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

[31] ISO/IEC, ISO IEC 42001 Artificial Intelligence Management System, https://www.iso.org/standard/81230.html

[32] UK Information Commissioner's Office, Privacy-Enhancing Technologies Guidance, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

[33] UK Competition and Markets Authority, Guidance on Horizontal Agreements, https://www.gov.uk/government/publications/guidance-on-horizontal-agreements

[34] UK Competition and Markets Authority, Collaborating with Other Businesses, https://www.gov.uk/government/publications/collaborating-with-other-businesses/collaborating-with-other-businesses

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

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

[37] UK Government, Data Use and Access Act 2025, https://www.gov.uk/government/collections/data-use-and-access-act-2025

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

[39] NIST, AI 600-1 Generative AI Profile, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[40] World Intellectual Property Organization, Valuing Intellectual Property Assets, https://www.wipo.int/en/web/business/ip-valuation

About the Author

Authored by Chennakeshav Adya, Independent Researcher

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.