



Managing data retention schedules during M&A, relocations, and bankruptcy

Tuesday, 22 September

11:00-12:00 PDT

14:00-15:00 EDT

20:00-21:00 CEST



Speaker



Wanne Pemmelaar

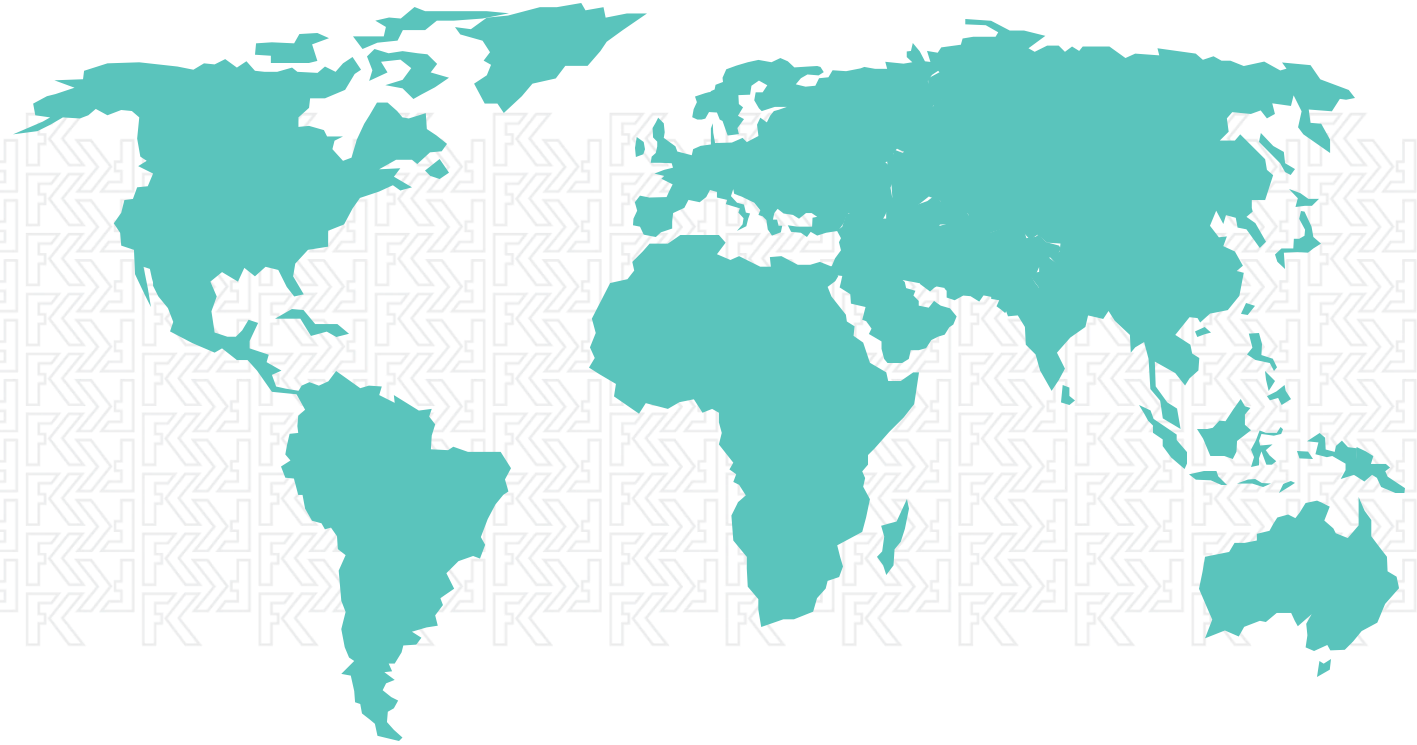
CEO & Co-founder
filerskeepers | Lawstronaut



Wanne is a top-tier data and tech lawyer and 3x entrepreneur who loves building tech solutions to legal problems he has experienced firsthand. Wanne has over a decade of work experience as a legal practitioner. When it comes to developing products, he insists on stellar design and a commitment to user empathy. As a data and tech lawyer, Wanne's passion is assisting companies to navigate the legal landscape against the backdrop of exponential data and tech developments.

www.filerskeepers.co

Introduction to filerskeepers



Founded in 2018

358+

jurisdictions online

363,000+

retention periods

4000+

multinational customers

300+

law firm customers

80+

partners

95

team members



www.filerskeepers.co

How long does it
take to build a data
retention schedule?



Beta

Data class

Data Type

Country

State

Search

Refresh

Download

Settings

Customize

Your Data				Golden Standard					Belgium		
Ref	Data Class	Data Type	Examples	Retention	Period	From	Country Deviation	Considerations	Retention	Period	Ret
HUM01	Human Resources	Prospective candidates	Raise interest, signup for newsletters/notices, chatbot data	2	years	From the date of last interaction		We have based this on the fact that 12 jurisdictions that have an unspecified retention period.	0	days	
HUM02	Human Resources	Non-selected candidate information	Records generated from campus and other recruiting, resumes and other employment histories, contact details, and interview assessments	2	years	From the date on which the vacancy was closed	Netherlands: 4 weeks, United Kingdom: 6 months	We have based this on the fact that 6 jurisdictions that have an unspecified retention period, 3 jurisdictions that have a 2 years retention period, 1 jurisdiction that has a 3 years retention period, 1 jurisdiction that has a 4 weeks retention period, 1 jurisdiction that has a 6 months retention period.	0	days	
HUM04	Human Resources	Job postings	Job title and description, required qualifications, job location, salary and benefits, application instructions, application deadline, records generated from job boards, related administrative and advertising records	5	years	From the date the vacancy was closed	Hong Kong: 6 years, China: 30 years, Japan: 10 years, Netherlands: 20 years	We have based this on the fact that 2 jurisdictions that have a 1 year retention period, 2 jurisdictions that have a 5 years retention period, 2 jurisdictions that have an unspecified retention period, 1 jurisdiction that has a 6 years retention period, 1 jurisdiction that has a 30 years retention period, 1 jurisdiction that has a 10 years retention period, 1 jurisdiction that has a 20 years retention period, 1 jurisdiction that has a 3 years retention period, 1 jurisdiction that has a 2 years retention period.	5	years	
HUM05	Human Resources	Background checks	Records of verification of candidate and employee education and previous	2	years	From the date on which the vacancy was	China: permanent, Netherlands: 4	We have based this on the fact that 4 jurisdictions that have an	0	days	



lawstronaut

A man in a white shirt and tie is sitting at a desk in a dimly lit office at night. He is looking at a laptop screen and smiling, with his right hand resting on his head in a gesture of realization or triumph. The desk is cluttered with papers, a laptop, and a desk lamp. A large stack of papers is visible on the right side of the desk. The background shows a city skyline at night through a window.

The joy of finally figuring it out



• AGENT-READY

Connect your AI to **59,500,000+** laws and court cases!

Lawstronaut is the infrastructure layer that connects AI agents and software to millions of legal documents across 200+ jurisdictions, structured legal data, continuously updated, and ready to use via API and MCP.

Connect your AI agent →

Schedule a meeting

59,500,000+

Legal records

200+

Jurisdictions

1200+

Official portals

430,000+

Governmental institutions

Daily

Legal updates



lawstronaut

JD

John Doe



Hello John Doe, welcome to
Lawstronaut Developers Portal.

Manage your API integrations, explore documentation, and track your developer activity all in one place.



Why Lawstronaut exists

Law isn't built for software: it is scattered across jurisdictions, languages, changing websites, and difficult PDFs.

Making it usable is expensive: crawling, OCR, parsing, translation, and validation demand significant—and increasingly costly—compute.

Everybody gets stuck maintaining the pipeline: websites and formats change, scrapers break, and legal data quickly becomes outdated.

Lawstronaut solves this infrastructure once: delivering structured, current, traceable legal data ready for AI and legaltech products.



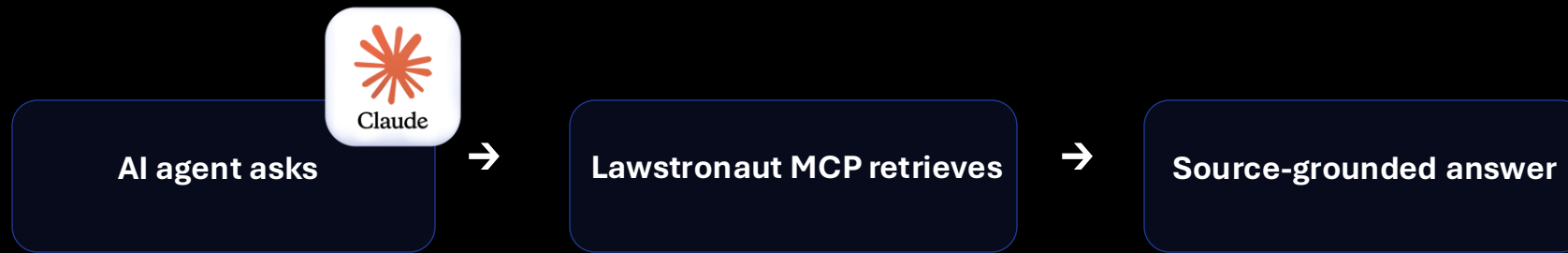
lawstronaut

lawstronaut.com

Plug legal infrastructure into any AI agent.

Lawstronaut MCP gives software a live, structured connection to the legal universe.

“What changed yesterday on AI, privacy or employment law across my key jurisdictions?”



Horizon scanning • cross-jurisdictional research • compliance monitoring • legaltech AI

From “searching the law” to asking your systems what changed — and getting the underlying sources back.

The “pledge” of AI



AI needs records management

- **What does AI need?**
 - High quality, up-to-date data to produce reliable results
 - Compliance and ethical data use
 - Transparency and accountability
 - Efficiency in data handling
- **Without robust records management we risk:**
 - flawed decisions,
 - regulatory violations
 - inefficiencies

...All was well
until the General
Data Protection
Regulation
arrived...

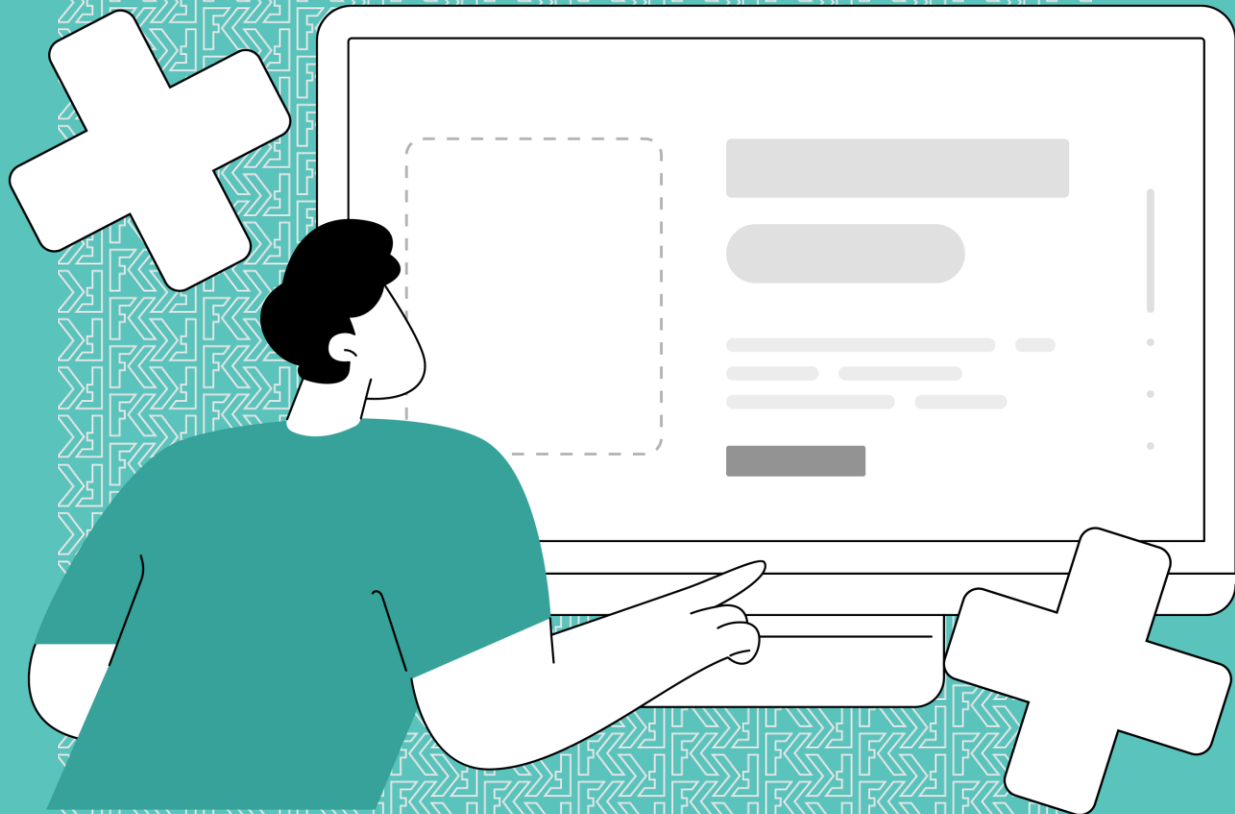




Real compliance!

The three retention issues of any organisation

- Not knowing what the laws say
- Not knowing what to choose
 - Laws are conflicting
 - There are so many
- Not knowing where to start implementation
 - Hardcopy vs digital
 - Global vs local
 - Cloud vs on premise
 - Structured vs unstructured
 - Current vs legacy



What is on
our mind

“Help” may come from unexpected corners

- What if your colleagues suddenly claim to have fixed RIM with AI?
- AI will produce, at this moment, an 80-20 outcome
- 80% fixed what RIM couldn't
- 20% destroyed, impacting the company dearly



You cannot vibe code your way out of records management

- The token economics do not work (yet).
- Retention is a legal-research problem, not merely a coding problem.
- The hard part is the data model.
- Records management requires governance and accountability.



AI changes the question we ask about information

Finding a document is no longer the point. Systems now infer, combine and act on it.

BEFORE

Can we find it?

NOW

**Can we trust what
the machine inferred?**

AI depends on context that rarely sits inside the document itself: origin, authority, version, purpose, relationships and lifecycle status.

Privacy already depends on records management

Privacy sets the obligation. Records management makes it operational.

Purpose limitation

Know why the information exists

Accuracy

Identify the authoritative version

Storage limitation

Apply a lifecycle and defensible disposal

Accountability

Preserve evidence of decisions and actions

Records management supplies the missing context

Five capabilities turn a pool of data into governed information.

01 Provenance Where did this come from, and can we prove it?

02 Ontology What does it mean, and how does it relate to other information?

03 Authority Which source and version should the AI rely on?

04 Lifecycle When may it be used, reviewed, archived or deleted?

05 Evidence Can we reconstruct what the system knew and did?

We are losing the craft when we need it most

AI has renewed the value of records expertise just as the profession is weakening.

UNITED STATES

A golden generation is retiring or being cut.

Their knowledge of provenance, authenticity and lifecycle control often lives in practice rather than policy.

EUROPE

Records management never fully established itself.

Privacy professionals inherited the responsibility, but rarely the full discipline or organisational home.

The risk goes beyond staffing. We may lose the institutional memory that explains how information acquires meaning.

The route to the AI table runs through delivery

Records managers gain influence by solving the problems AI teams already have.

Map

Create an inventory of the sources that feed AI systems

Qualify

Mark authority, provenance, version and permitted use

Structure

Encode business meaning through taxonomy and ontology

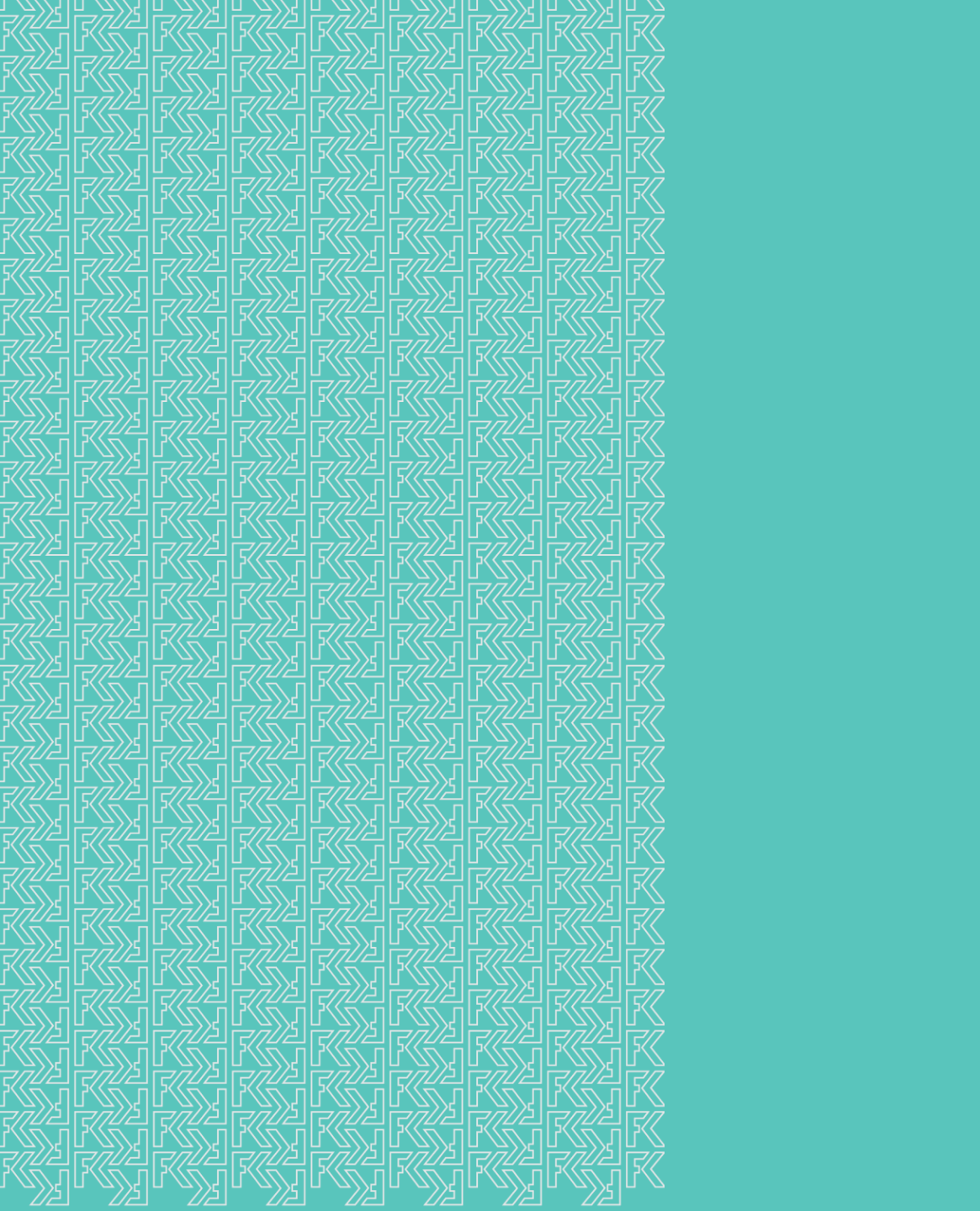
Control

Carry retention, access and deletion into AI pipelines

Prove

Measure traceability, deletion coverage and source quality

Start with one high-value AI use case. Show what changes when the system knows which information deserves trust.



Privacy asks:
May we use it?

Records management asks:
Can we trust it over time?

Together, they give AI memory with
boundaries and knowledge with evidence.

Dedicated to the people who preserve meaning.

What corporate transitions?

- Relocations
- Mergers
- Divestments
- Dissolution
- Bankruptcy



There once was a happy records manager...

Who worked for an organization that:

- Had an up to date retention schedule
- Had information governance/records management policies that people adhered to
- Always asked the records manager for his/her opinion
- Properly labelled all boxes
- Classified its data
- And provided for clear data/record ownership/stewardship



Why This Matters

- Every company will face major transitions — moving, splitting, merging, closing.
- Records are not just “boxes and files.” They are the evidence that proves compliance, supports audits, and protects rights.
- Mismanaging records in a transition can create long-tail risks: litigation losses, fines, reputational damage, and lost business continuity.

Chapter 0: Governance Framework



Governance Framework

- Sponsor: Senior leadership must own records governance during transitions.
- Accountable: Records Manager + Legal/Compliance for retention and legal holds.
- Responsible: IT/InfoSec, business owners, Privacy/DPO.
- Consulted: Internal audit, tax advisors, regulators.
- Informed: Employees, customers, suppliers.
- Key message: governance must be formal, not ad hoc.



Risk Register

- Loss of critical records → mitigate with inventories, custody logs, reconciliation.
- Over-retention of ROT → mitigate with retention screening and destruction.
- Missed legal holds → mitigate with freeze + legal sign-off.
- Metadata corruption → mitigate with migration tools and hash validation.
- Privacy breaches → mitigate with minimization, encryption, privacy reviews.
- Cross-border compliance failures → mitigate with SCCs/BCRs/TIAs.
- Accountability gaps → mitigate with custodian/TSA role assignments.



Records Transition Playbook

- Inventory and classify across all repositories.
- Apply retention + legal hold screening before transfer.
- Use retention/ownership matrices to resolve conflicts.
- Secure physical and digital transfers with custody logs and encryption.
- Document every transfer and destruction.
- Update RoPA, notices, and custodianship arrangements.
- Monitor KPIs and risks as part of governance reporting.



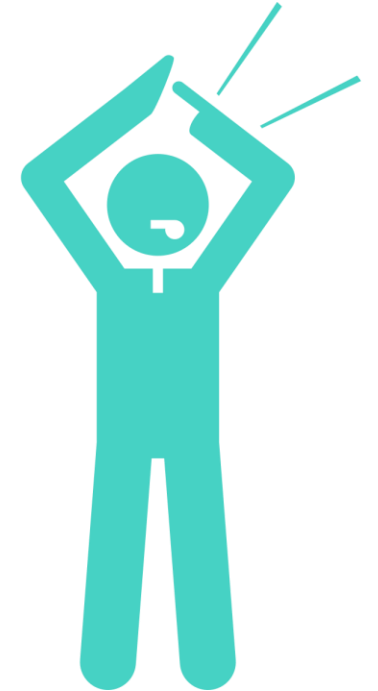
Transition Timeline Model – Phase 1 & 2

- Phase 1 (T-180 → T-120): Inventory all records/data and their locations/sources (physical, digital, SaaS, backups); map retention laws and holds. Engage legal/privacy early.
- Phase 2 (T-90 → T-30): Apply retention screening and purge ROT. Build retention/ownership matrix. Draft TSAs/custodian agreements. Engage regulators if cross-border.



Transition Timeline Model – Phase 3 to 5

- Phase 3 (T-30 → Day 0): Prepare extractions, labels, redactions; secure logistics; freeze access before cutover.
- Phase 4 (Day 0): Execute transfers; document custody and hashes.
- Phase 5 (T+30 → T+180): Reconcile inventories, issue certificates, run validation reports, update retention schedules and RoPA.

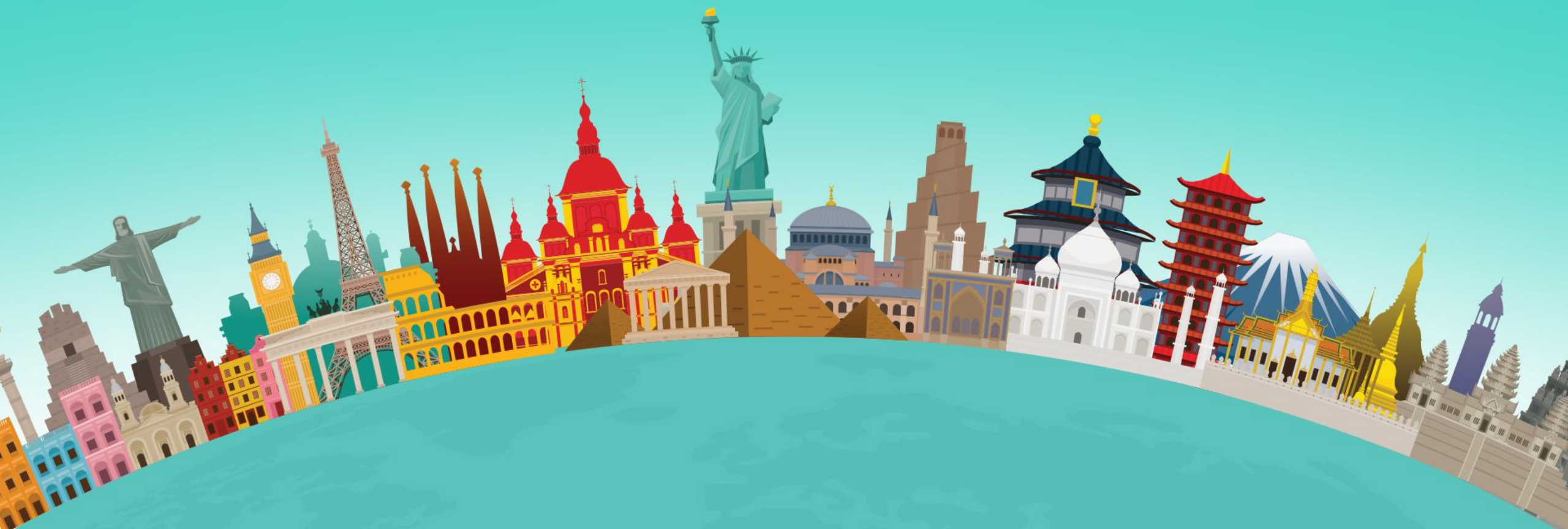


Cross-Scenario KPIs & Acceptance Criteria

- Inventory completeness: 100% of records mapped to a retention rule.
- Retention compliance: 100% expired records destroyed with certificates; 100% in-retention preserved.
- Legal hold compliance: 0 records under hold destroyed.
- Metadata integrity: $\geq 95\%$ metadata preserved during migrations; exceptions documented.
- Access continuity: Critical records accessible on Day 1 with $\leq 2\%$ downtime.
- Privacy compliance: 100% transfers supported by lawful basis, notices updated within 90 days.
- Custodian/TSA roles documented for residual records.
- Audit trail completed within 90 days.



Chapter 1: Relocations



Relocation – Objectives

- Maintain continuous access to records during and after the move.
- Use relocation as an opportunity to purge ROT (redundant, obsolete, trivial records) instead of moving liabilities.
- Preserve chain of custody so records remain legally admissible and confidential.
- Challenge:
 - Do or die deadline
 - Are you truly ready for a project like this? Are you going to make it?
 - Mistakes...



Case Example: Law Firm Relocation

- **Challenge:** A law firm moved 2,000 archive boxes without prior retention screening.
- **Risk:** They transported expired and sensitive data unnecessarily, raising costs and exposure.
- **Outcome:** Storage bills skyrocketed; old client files were misplaced.
- **Lesson:** Always screen, purge, and document destruction before moving.



Relocation – Risks in Relocation

- Physical records can be exposed during transport if boxes are lost or accessed.
- Digital transfers may leak personal data if encryption is not enforced.
- Vendor contracts must include confidentiality clauses and incident notification duties.
- Are you moving records from offsite storage vendors to keep the records near your new office?



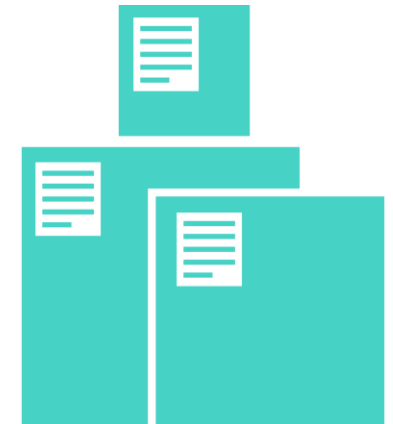
Relocation – Pre-Move Preparation

- Conduct a detailed inventory of all physical and digital records – every file room, archive box, and shared drive.
- Apply retention rules and identify records under legal hold before anything is packed.
- Standardize metadata and labeling: record type, owner, retention rule, confidentiality level, and destination.



Relocation – Packing & Labelling

- Use barcoding and standardized manifests to track every box.
- Seal boxes with tamper-evident tape to prevent unauthorized access.
- Assign clear ownership and custody responsibility for each batch of records.



Relocation – Transport & Security

- Maintain chain-of-custody logs with sign-offs at each handover point.
- Use secure, GPS-tracked vehicles and vetted transport vendors.
- Ensure insurance coverage and clear protocols for overnight storage or delays.



Relocation – Post-Move Reconciliation

- Match delivered boxes and digital data against the pre-move inventory.
- Update file plans and metadata with new physical or digital locations.
- Document any exceptions, missing files, or discrepancies with incident reports.

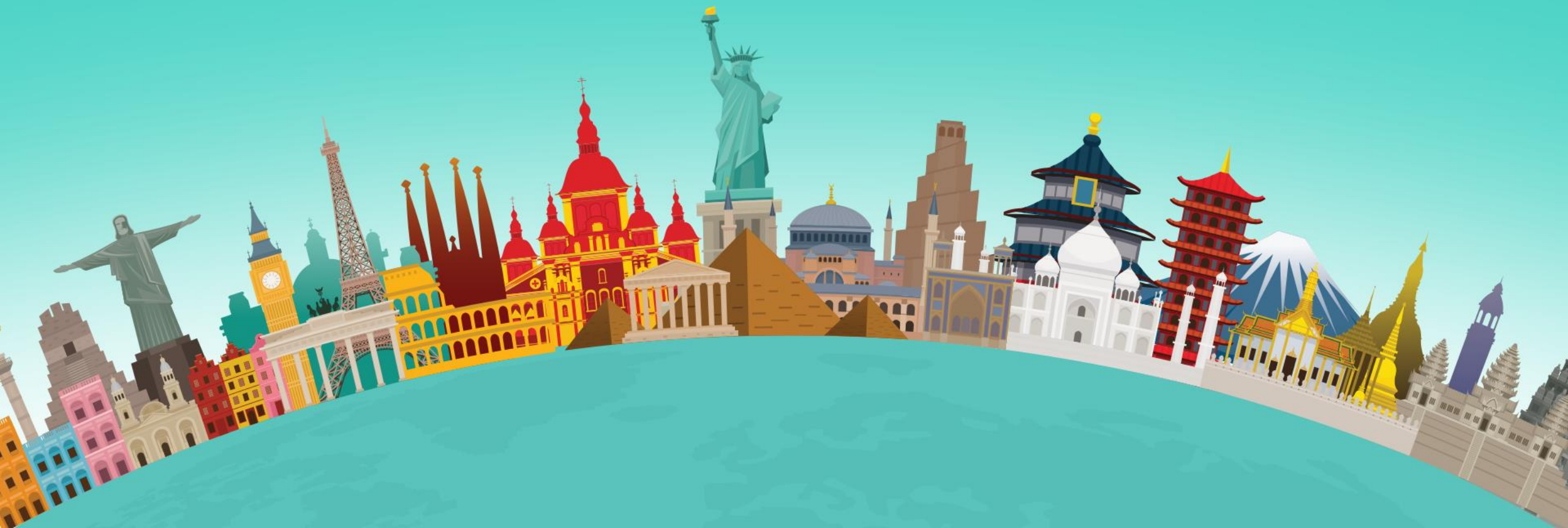


Relocation Summary

- Relocations are logistics-heavy but also prime opportunities to strengthen retention.
- Success depends on preparation, custody controls, and post-move validation.
- Privacy and security risks must be actively managed during the physical move.



Chapter 2: Mergers



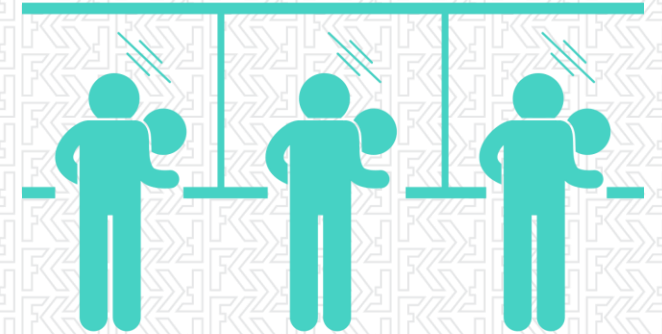
Merger – Objectives

- Harmonize retention schedules across entities.
- Ensure business continuity while integrating systems.
- Prevent ROT explosion by cleaning up redundant data.



Case Example: Bank Merger

- **Challenge:** Two banks merged; one had a 7-year tax retention, the other 10 years.
- **Risk:** Inconsistent retention could undermine audit defense.
- **Outcome:** Adopted 10-year standard across new entity.
- **Lesson:** Use harmonization matrix and retrain staff on unified policy.



Risks in Mergers

- Conflicting retention schedules → risk of over/under-retention.
- Metadata loss making records inadmissible.
- Explosion of ROT if old systems are merged without cleanup.
- Delays in responding to data subject rights requests due to fragmented systems.



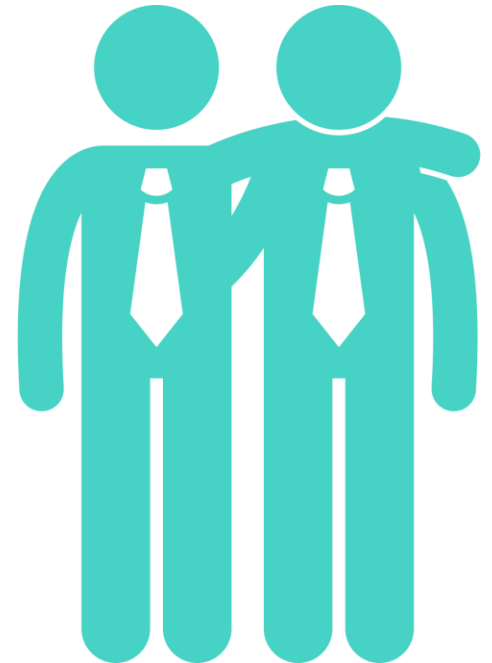
Composite Inventory

- Build a single inventory of both companies' records.
- Normalize metadata and taxonomies for comparability.
- Identify duplicates, overlaps, and gaps.
- Establish which systems will remain and which will be decommissioned.



Retention Harmonization

- Functional scope. We describe it as “A”, while “they” describe it as “AB”
- Conflicts are inevitable (e.g., 7 years vs 10 years for tax records).
- Best practice: apply the stricter or longer requirement for defensibility.
- Document all decisions in a harmonization matrix.
- Create a “golden standard” retention schedule for the merged entity.
- There is time! However, it should follow the actual integration



Legal Holds

- Both entities may have active litigation or regulatory investigations.
- Reconcile all hold lists before destroying anything.
- Freeze overlapping data until approved for release.
- Maintain a unified legal hold register.



Privacy: Minimization

- Avoid merging everything — purge expired or irrelevant data first.
- Minimize the amount of personal data combined into new systems.
- Ensure that data subject rights can be honored across merged repositories.



System Integration & Access

- Plan for metadata preservation during migrations (timestamps, authorship, version history).
- Validate data exports/imports with hash checks and exception reports.
- Implement identity and access management cut-over plans for Day 1.

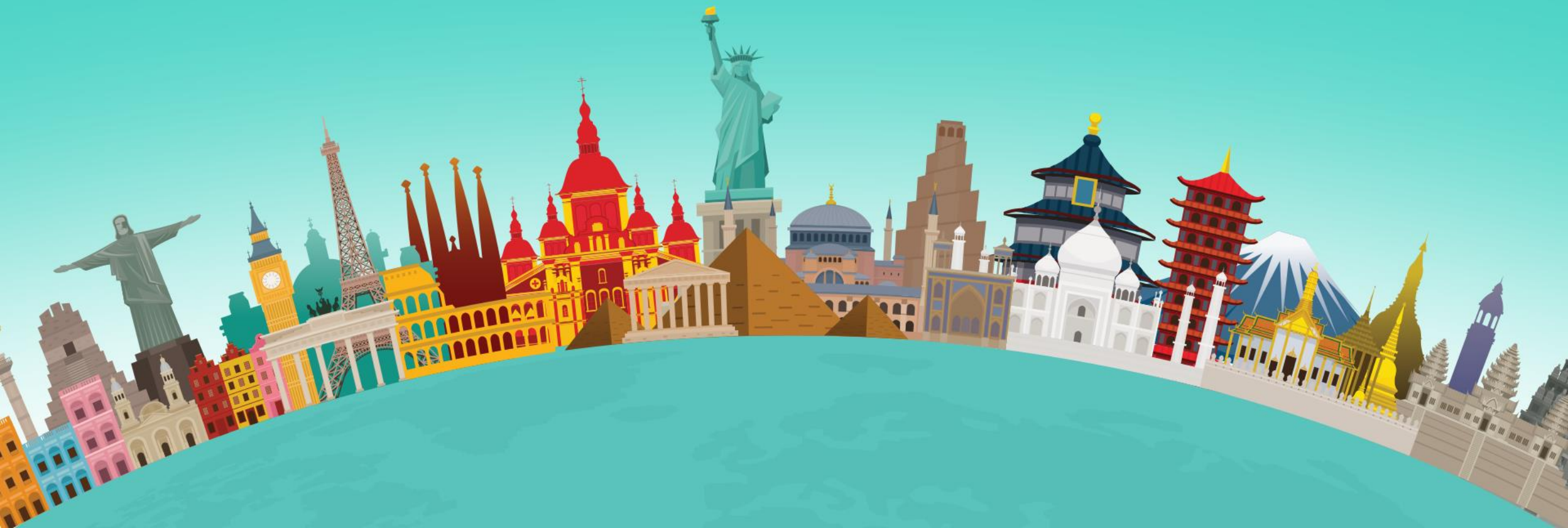


Merger Summary

- Mergers are about unification and harmonization.
- Success requires a composite inventory, a harmonized retention schedule, and strong privacy safeguards.
- Without discipline, merged entities drown in ROT and lose evidential integrity.

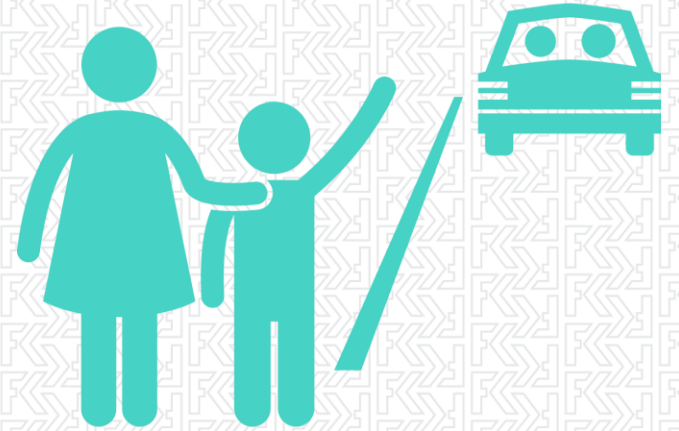


Chapter 3: Divestment



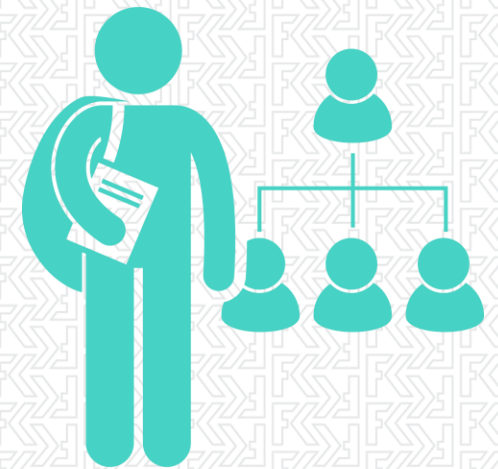
Divestment – Objectives

- Cleanly separate records between Parent, Divested Entity, and Shared.
- Ensure buyer has what it needs to operate and meet compliance.
- Protect the parent's own obligations and sensitive data.



Case Example: HR Data Carve-Out

- **Challenge:** A manufacturing firm sold a division but HR data was in a shared Workday tenant.
- **Risk:** Parent accidentally transferred records of employees who were not part of the sale.
- **Outcome:** Regulator investigation into unlawful data disclosure.
- **Lesson:** Use a retention/ownership matrix, redaction protocols, and TSA privacy appendix.



Risks in Divestments

- Over-disclosure of confidential or personal data to buyer. Breaches of trade secrets/NDAs/IP
- Failure to respect retention or legal hold obligations before transfer.
- Buyer left without necessary records → operational disruption.
- Long-term disputes if transfer/destruction decisions are undocumented.



Segmentation Explained

- Parent-only records: governance, tax, non-divested employee files.
- Divested-only records: operational data, customer files, transferred employees.
- Shared records: contracts, joint systems, historical audit trails, tax, governance — often the hardest to manage.



Inventory & Classification

- Build a complete inventory across all physical and digital repositories.
- Tag each record set as Parent, Buyer, or Shared.
- Capture retention rules, legal holds, and confidentiality status for each record set.
- This forms the basis of the divestment retention/ownership matrix.



Transition Services Agreement (TSA)

- TSA is the “divorce agreement” for data and systems.
- Must define temporary access rights, retrieval SLAs, and fees.
- Must clarify destruction, redaction, and return of data after the TSA ends.
- Include a GDPR/privacy appendix covering lawful processing, minimization, and exit obligations.



Digital Carve-Outs

- SaaS systems: split tenants or provide exports for buyer.
- Shared drives/email: create clean copies with only divested content.
- Backups: typically excluded, but retrieval may be needed under TSA.
- Always preserve audit logs to maintain evidential weight.
- Do you need data discovery tools?
 - Yes, but not just any
 - Without you are error-prone and at risk of over-transfer



Privacy: Minimization & Transparency

- Do not dump entire datasets when only a subset is relevant.
- Inform employees, customers, and suppliers about the transfer and new controller.
- Update privacy notices and provide a DPO contact for questions.

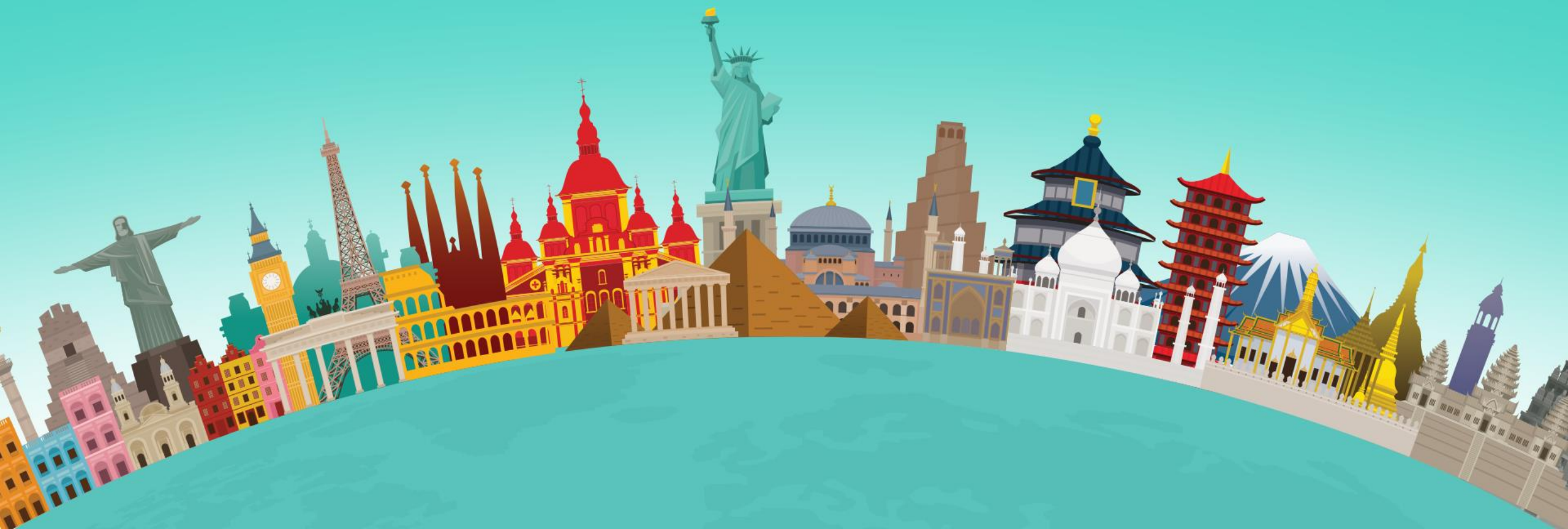


Divestment Summary

- Divestments are about surgical separation.
- Retention and privacy are central — every record must be mapped.
- TSA is the backbone for managing access, responsibilities, and exits.



Chapter 4: Dissolution



Dissolution – Objectives

- Close company records responsibly and legally.
- Retain statutory corporate, financial, and HR records.
- Appoint a custodian for post-dissolution access requests.
- What does dissolution really mean? Is there a surviving legal entity? Did you stop operations or did you dissolve the legal entity?



Case Example: Consultancy Dissolution

- **Challenge:** Consultancy dissolved without assigning custodian.
- **Risk:** Ex-employees later requested HR records that were unavailable.
- **Outcome:** Company faced legal claims it couldn't defend.
- **Lesson:** Always assign a custodian and maintain a retention map.



Risks in Dissolution

- Loss of records needed for tax audits, pensions, or legal inquiries.
- Over-retention of personal data without lawful basis.
- No accountability if no custodian is assigned.
- Metadata loss during system shutdown.



Inventory & Mapping

- Compile a complete inventory of all physical and digital records.
- Map statutory retention requirements by jurisdiction and record type.
- Identify what can be destroyed immediately vs. what must be retained.



Custodianship

- Appoint a custodian (director, notary, third-party archivist).
- Define responsibilities for storing and providing access to records.
- Ensure custodian contact details are published in privacy notices.
- If the legal entity remains: it will be the legal entity!



Privacy: Minimization

- Purge expired personal data (e.g., old marketing databases).
- Retain only what is necessary for statutory or legal obligations.
- Document all destruction with certificates.



Dissolution Summary

- Dissolution is about responsible closure.
- Statutory records must remain accessible; everything else should be defensibly destroyed.
- Custodianship ensures accountability after the company ceases to exist.

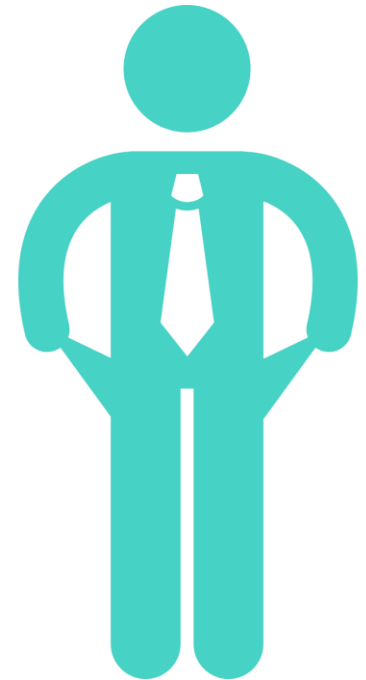


Chapter 5: Bankruptcy



Bankruptcy – Objectives

- Preserve records for courts, regulators, and creditors.
- Meet statutory retention obligations (tax, HR, governance).
- Prevent improper destruction or unauthorized disclosures.
- But who is going to do this?



Case Example: Retailer Database Sale

- **Challenge:** Retailer went bankrupt and auctioned its customer list.
- **Risk:** Regulator intervened due to unlawful transfer of personal data.
- **Outcome:** Sale delayed until customers were re-notified; sensitive data excluded.
- **Lesson:** Privacy review is mandatory before asset sales.



Risks in Bankruptcy

- Premature destruction of records required for investigations or audits or over-retention where there is no legal basis anymore.
 - Does the parent/group still exist or not?
- Data breaches during liquidation sales.
- Loss of SaaS/cloud access if subscriptions lapse.
- Gaps in documenting what was destroyed or transferred.



Inventory & Freeze

- Identify all corporate, financial, HR, customer, and product records.
- Apply immediate freezes to litigation-relevant material.
- Document chain of custody and storage arrangements.



Trustee Oversight

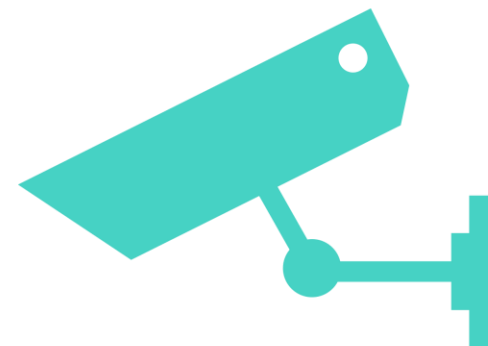
- Trustee or administrator becomes the legal controller of records.
- All transfers, destructions, or sales require trustee approval.
- Court may mandate retention periods for accounting and governance files.



Special Records

- Financial ledgers and tax returns (7–10 years).
- Payroll and employee records (statutory requirements).
- Board minutes, shareholder registers, governance documents.
- Product liability, safety, and IP documentation.



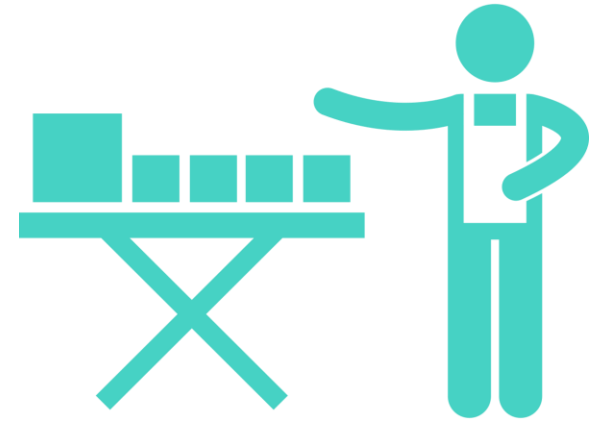


Privacy: Lawful Basis

- Bankruptcy justifies retention under legal obligation and legitimate interests.
- Over-retention without basis remains unlawful.
- Trustee must update privacy notices to reflect new controller status.

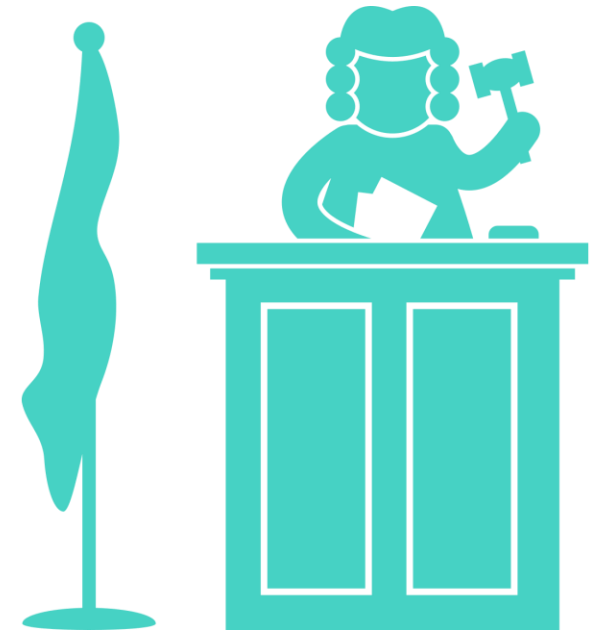
Privacy: Asset Sales

- Customer databases cannot be treated like physical assets.
- Buyers must have lawful basis and often must re-notify individuals.
- Sensitive categories (health, minors) usually excluded from sale.

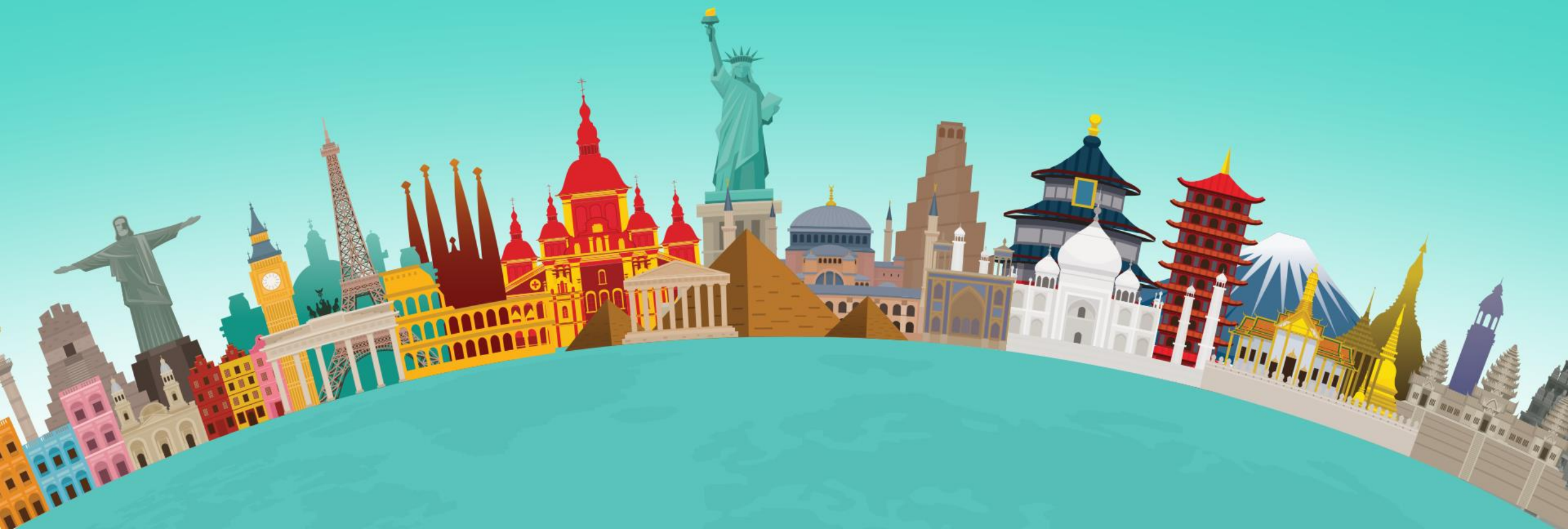


Bankruptcy Summary

- Bankruptcy is about preservation and oversight.
- Trustees act as new controllers, with strict legal obligations.
- Every transfer or destruction must be documented and approved.



Key takeaways & Q&A



And they lived happily ever after...!

- Records management is the foundation of compliance and defensibility in transitions.
- Each scenario is different — but the core principles (inventory, retention, privacy, proof) always apply.
- Transitions are opportunities: clean up ROT, strengthen governance, and future-proof compliance.
- Prepare now, be ready later



Closing & Q&A

“Every corporate transition tells a story. Records management ensures that story remains complete, compliant, and defensible — protecting both the business and the people whose data it holds.”

Questions?



Thank You!

Contact **filerskeepers**

Email: anything@filerskeepers.co

Contact **Lawstronaut**

Email: anything@lawstronaut.com

Scan here!



filerskeepers.co



lawstronaut.com