Trade Secrets, Data-Driven Contracting, Cross-Border Information Flow and SCOMET

1. Basic Theme of the PPTs

The two PPTs deal with one common issue: **how sensitive technology, data and know-how should be protected when they are shared across persons, organisations or countries**.

Earlier, technology transfer mostly meant transfer of physical goods, machines, documents or samples. Today, technology can be transferred through **email, cloud servers, online meetings, source code, algorithms, APIs, datasets, AI models, training data, technical drawings and oral explanations**. Therefore, modern law has to look not only at physical export but also at **intangible technology transfer**.

The first PPT focuses on **SCOMET and export-control regulation in India**. The second PPT focuses on **trade secrets in data-driven contracts**, especially **Data Use Agreements (DUAs)** and **Data Transfer Agreements (DTAs)**. The PPTs specifically show that sharing sensitive technical data by email, cloud server or oral presentation may raise export-control issues, and MoUs or agreements must be checked for possible dual-use outcomes before they are signed.

PART I — IMPORTANT TOPIC 1: SCOMET

2. Meaning of SCOMET

SCOMET stands for **Special Chemicals, Organisms, Materials, Equipment and Technologies**.

It is India's **National Export Control List** for sensitive and dual-use items. It covers **dual-use goods, munitions, nuclear-related items, software and technology**. The PPT states that the SCOMET list contains **9 categories**, and export licence/authorisation is required for exporting items falling in those categories.

The DGFT official SCOMET page also shows that India periodically updates the SCOMET list, including an **Updated SCOMET List 2025 as on 23.09.2025**. (DGFT)

Simple meaning

SCOMET controls export of sensitive items and technologies which may look civilian but can also be used for military, nuclear, chemical, biological, missile or strategic purposes.

Example

A chemical may be used in agriculture or pharmaceuticals, but the same chemical may also be used for making chemical weapons. Similarly, a drone, sensor, algorithm or high-strength material may have both industrial and military uses.

---

3. What is Dual-Use?

Dual-use means an item, material, technology or software has both:

1. **Civilian use**, and
2. **Military or strategic use**.

For example:

Civilian use	Possible military/strategic use
Drone for agriculture	Drone for surveillance
Chemical for pharma	Chemical weapon precursor
AI algorithm for manufacturing	Defence targeting/surveillance
Composite material for aircraft	Missile/aerospace application
Biological organism for research	Biosecurity/bioweapon risk

The purpose of SCOMET is to ensure that India does not unknowingly allow export of sensitive goods or know-how that may be misused for weapons, military purposes or proliferation.

---

4. Strategic Trade Controls

Strategic Trade Controls (STC) are laws and regulations that manage the flow of **dual-use goods, services and technologies across national borders**. India's strategic trade control system is connected with its commitment to prevent proliferation of sensitive goods, technologies and know-how.

The PPT mentions three important multilateral export-control regimes:

Regime	Main focus
MTCR — Missile Technology Control Regime	Missiles, delivery systems and related dual-use items
Wassenaar Arrangement	Munitions, military items and dual-use goods/technologies
Australia Group	Dual-use chemicals, biological items, equipment and technologies

India is a member of these regimes. This shows that SCOMET is not only a domestic trade rule; it is part of India's international non-proliferation responsibility.

---

5. Categories Covered Under SCOMET

The PPT explains the components of SCOMET as follows:

A. Special Chemicals

These are chemicals that may have normal industrial, agricultural or pharmaceutical uses but may also be used for chemical weapons or military purposes.

Example: A chemical used in pharma production may also be misused as a chemical weapon precursor.

B. Organisms

This includes biological agents and organisms. They may be useful for medicine, agriculture or industry, but they may also create risks of biological weapons or bioterrorism.

C. Materials

This includes metals, alloys, composites and special materials having civilian and military applications.

Example: A composite material may be used in aircraft manufacturing but may also be used in missiles.

D. Equipment

This includes machinery, devices and systems that may have strategic or dual-use capability.

Example: High-precision testing equipment, aerospace equipment, nuclear-related equipment or defence-grade machines.

E. Technologies

This includes technical knowledge and information used in research, development and manufacturing. Technology is dangerous from a compliance perspective because it can be transferred without physical movement.

The PPT specifically states that technology includes knowledge and information used in research, development and manufacturing, where such technology may have military or WMD use.

---

6. Technical Data and Technical Assistance

This is very important for exams.

SCOMET does not apply only to physical goods. It may also apply to **technical data** and **technical assistance**.

Technical data includes:

- Blueprints
- Plans
- Diagrams
- Models

- Formulae
- Algorithms
- Tables
- Engineering designs
- Specifications
- Manuals
- Instructions
- Data recorded on media or devices

Technical assistance includes:

- Instruction
- Skills
- Training
- Working knowledge
- Consulting services

The PPT clearly states that **intangible technology transfer related to SCOMET is subject to regulation**.

Exam sentence

SCOMET applies not only to export of physical goods but also to intangible transfer of controlled technical data, software, algorithms, designs, manuals, know-how and technical assistance.

---

7. Intangible Technology Transfer

Intangible technology transfer means transfer of technology or know-how without physical shipment.

It may happen through:

1. Emailing technical drawings.
2. Uploading source code to cloud servers.
3. Giving foreign collaborators access to technical databases.
4. Explaining controlled technology in an online meeting.
5. Sharing algorithms, formulae or design specifications.
6. Providing technical training to foreign nationals.
7. Allowing foreign contractors access to controlled data.
8. Joint research or MoUs involving sensitive technical outcomes.

The PPT gives examples such as sharing sensitive technical data through email, cloud servers or oral presentations, and states that future MoUs must be vetted for dual-use outcomes before signing.

Simple example

If an Indian researcher shares a controlled aerospace design file with a foreign collaborator through Google Drive, it may amount to export of controlled technology even though no physical item left India.

---

8. SCOMET Applies to What and to Whom?

The PPT gives a broad scope of SCOMET application. It may apply to:

1. **New and used goods**
2. **Controlled and non-controlled goods mixed together**
3. **Goods, software and technologies**
4. **Export of items not in the SCOMET list through catch-all control**
5. **Exclusive Economic Zone**
6. **Indian citizens outside India**
7. **Companies registered or incorporated in India**
8. **Ships, aircraft or other means of transport registered in India or outside India**
9. **Foreigners and persons in service of Government of India**, where relevant

---

9. Catch-All Control

Catch-all control means that even if an item is not specifically listed in SCOMET, export may still be restricted if there is a risk that it may be used for prohibited military, WMD, nuclear, missile, chemical or biological purposes.

Simple explanation

A product may not appear directly in the list, but if the exporter knows or has reason to believe that the product may be used in a weapons programme, export-control obligations may arise.

Exam importance

Catch-all control prevents exporters from escaping liability by saying, "This exact item was not listed."

---

10. Licensing and Evaluation of SCOMET Applications

SCOMET export may require licence or authorisation. Applications are evaluated through a risk-based approach. The PPT mentions:

- Inter-Ministerial Working Group
- Pre-licence screening
- End-use credentials
- End-user certificate
- State end-use
- Whether the end-user is involved in the business of the export item
- Risk assessment
- Credential of end-user
- Credibility of end-use declaration
- Integrity of the chain of transmission from supplier to end-user

Main factors considered

1. **Who is the end-user?**
2. **What is the declared end-use?**
3. **Is the end-use credible?**
4. **Can the item be diverted?**
5. **Is the end-user linked to military/WMD-sensitive activity?**
6. **Is the chain of transfer reliable?**
7. **Does the export create national security risk?**

---

11. Post-Export Reporting and Internal Compliance

The PPT mentions post-export reporting, documentary requirements and internal compliance. It also states that industries and academic institutions working on SCOMET categories need internal compliance systems.

Internal compliance should include:

1. Identification of controlled goods, software and technology.
2. Screening of end-users.
3. Screening of end-use.
4. Checking whether licence is required.
5. Vetting MoUs, research collaborations and technology-transfer agreements.
6. Controlling access by foreign nationals.
7. Maintaining export records.
8. Training employees and researchers.
9. Reporting suspected violations.
10. Creating approval systems before sharing technical data.

The MEA official page also links to India's Strategic Trade Controls handbook, the latest SCOMET list and elements of an effective internal compliance programme.

---

12. Voluntary Submission in Case of Non-Compliance

The PPT mentions voluntary submissions in case of non-compliance.

This means that if an exporter or institution discovers that it has made an unauthorised transfer, it should not hide it. It should:

1. Conduct internal investigation.
2. Stop further transfer.
3. Preserve records.
4. Identify the item, end-user and end-use.
5. Consider voluntary disclosure to authorities.
6. Take corrective action.

Voluntary disclosure may show good faith, but it does not automatically remove liability.

PART II — IMPORTANT TOPIC 2: DATA USE AGREEMENT

14. Meaning of Data Use Agreement

A **Data Use Agreement (DUA)** is a contract that controls **how the recipient may use the data**.

Its main function is **use control**.

It answers the question:

What may the recipient do with the data?

The PPT describes a DUA as primarily a **use-control instrument** dealing with permitted use, defined conditions, access controls, duration, termination, confidentiality and trade-secret acknowledgement.

---

15. Purpose of DUA

The purpose of a DUA is to ensure that when one party shares data with another party, the recipient uses it only for the permitted purpose.

A DUA is important because data may be commercially valuable and may qualify as a trade secret. If the data is freely used, copied, mixed, trained into AI models or converted into derivative outputs, its secrecy and commercial value may be lost.

Simple example

Company A gives machine-performance data to Company B only for testing the efficiency of one component. If Company B uses that data to train its own AI model or improve products for other clients, that is misuse unless expressly allowed.

---

16. DUA and Trade Secret Protection

A DUA helps prove **reasonable measures** for trade-secret protection.

Under trade-secret law, the owner must show:

1. The data has economic value.
2. The data is secret.
3. The owner took reasonable measures to keep it secret.

The PPT's trade-secret test applies these three requirements to data: economic value, secrecy and reasonable measures such as NDAs, DUAs, DTAs, encryption, access logs and need-to-know policies.

A DUA is therefore not only a commercial contract. It is also evidence that the owner treated the data as confidential and controlled its use.

---

17. Essential Clauses in a DUA

A good DUA should include the following clauses:

1. Definition of Data

The agreement must clearly define what data is being shared. It should include raw data, datasets, database contents, metadata, data streams, API outputs, logs, processed data and derivatives where necessary.

2. Permitted Purpose
The DUA must say exactly why the recipient may use the data.
Weak language:
“Data may be used for project purposes.”
Strong language:
“Data may be used only for testing Component X under Statement of Work No. 3.”
3. Use Restriction
The recipient must not use the data for any purpose other than the permitted purpose.
4. Processing Restriction
The agreement should control whether the recipient can clean, aggregate, analyse, transform, benchmark or process the data.
5. No Derivative Data Clause
The recipient should not create derivative datasets, summaries, embeddings, statistical outputs or analytics products unless expressly allowed.
6. No AI/ML Training Clause
The recipient should not use the data for training, fine-tuning, validating or testing AI/ML models unless expressly permitted.
7. Access Control Clause
Only authorised persons and systems should access the data.
8. Commingling Prohibition
The recipient should not mix the data with other datasets or put it into a general data lake without permission.
9. Security Measures
The DUA should require encryption, access logs, password control, secure storage, need-to-know access and monitoring.
10. Audit Rights
The disclosing party should have the right to verify compliance through logs, records and audits.
11. Confidentiality and Trade Secret Acknowledgement
The recipient should acknowledge that the data is confidential and may constitute trade-secret information.
12. Return and Destruction
After completion of the purpose, the data should be returned or securely destroyed, including copies, backups, derivatives and subprocessor copies.
13. Breach Notification
The recipient must immediately notify the disclosing party in case of unauthorised access, use or disclosure.
14. Term and Survival
Confidentiality, non-use and destruction obligations should survive termination.
15. Remedies
The agreement may provide injunctive relief, damages and indemnity for breach.

---

18. DUA Failure Points
The PPT identifies five major DUA failure points.
A. Overbroad purpose clause
If the purpose clause is vague, the recipient may argue that broad analytics, benchmarking or model training was allowed.
B. No restriction on derivative data
If derivative data is not controlled, the recipient may extract commercial value without copying the original dataset.
C. Inadequate access control
If access is not limited, many employees, systems or automated tools may access the data.

D. No commingling restriction
If the data is mixed with other datasets in a data lake, it becomes difficult to separate and protect.
E. Weak termination clause
If return/destruction obligations are weak, data may remain in backups, archives, cloud systems and AI models.

PART III — IMPORTANT TOPIC 3: DATA TRANSFER AGREEMENT

20. Meaning of Data Transfer Agreement
A **Data Transfer Agreement (DTA)** is a contract that controls **movement of data**.
Its main function is **movement control**.
It answers the question:
Where may the data go and how may it be transferred?
The PPT explains that a DTA is a movement-control instrument, dealing with transfer mechanism, destination controls, jurisdictional awareness, receiving party obligations and regulatory compliance.

---

21. Purpose of DTA
A DTA is used when data moves:

1. From one organisation to another.
2. From one system to another.
3. From one country to another.
4. To a cloud server.
5. To a subcontractor or vendor.
6. To a joint venture partner.
7. To a foreign affiliate.
8. Through remote access by foreign personnel.

A DTA is especially important in cross-border data transfers because the data may move into a jurisdiction where trade-secret protection is weaker or enforcement is difficult.

---

22. DTA and Trade Secret Protection
A DTA helps maintain the **secrecy chain** across jurisdictions.
The PPT compares DUAs and DTAs by stating that a DUA establishes reasonable measures through use restrictions, while a DTA maintains the reasonable-measures chain across jurisdictions.
This means that when data moves from India to another country, the owner must ensure that the recipient and destination jurisdiction provide adequate protection.

---

23. Essential Clauses in a DTA
A good DTA should include:
1. Description of Data
The agreement must identify what data is being transferred.
2. Transfer Mechanism
It should mention how the data will be transferred: secure portal, encrypted email, API, cloud access, physical storage device or secure file transfer.
3. Permitted Destination
The DTA should state where the data may be stored or accessed.
4. Server Location Clause
If cloud systems are used, the agreement should specify permitted server locations.
5. Remote Access Restriction
The agreement should clarify whether persons outside the permitted jurisdiction can access the data remotely.

6. Onward Transfer Restriction
The recipient should not further transfer the data to affiliates, vendors, subcontractors or third parties without prior written consent.
7. Back-to-Back Obligations
Any downstream recipient must be bound by obligations equal to or stricter than the original DTA.
8. Jurisdictional Compliance
The recipient must comply with applicable trade-secret, data-protection, export-control and sectoral laws.
9. Export-Control Clause
The DTA should check SCOMET, EAR, EU dual-use rules or other export-control requirements where applicable.
10. Security Safeguards
The DTA should require encryption, secure storage, access logs, monitoring and breach safeguards.
11. Audit and Traceability
The disclosing party should be able to verify who accessed the data, from where and for what purpose.
12. Return/Destruction
At the end of the transfer purpose, data should be returned or destroyed from all systems and jurisdictions.
13. Liability for Downstream Breach
The original recipient should remain liable for breach by subcontractors or downstream recipients.
14. Governing Law and Forum
The agreement should mention governing law and dispute resolution forum.

---

24. Cross-Border Transfer and Jurisdictional Dilution
The PPT discusses **jurisdictional dilution of secrecy**. This means that when data moves across borders, trade-secret protection may become weaker because:

1. The foreign jurisdiction may have weaker trade-secret law.
2. Enforcement may be slow or difficult.
3. Interim injunctions may not be easily available.
4. Evidence may be located abroad.
5. Foreign judgments may be difficult to enforce.
6. Subcontractors may further transfer the data.

The PPT compares the US, EU and India. It states that the US has DTSA and state UTSA, the EU has the Trade Secrets Directive, and India has no standalone trade-secret statute but protects trade secrets through common law, contract and equity.

---

25. DTA and SCOMET
DTA and SCOMET are connected when the transferred data includes controlled technical data, design specifications, process know-how, software or algorithms.
The PPT explains that under India's SCOMET framework, technical data, design specifications and process know-how falling within SCOMET categories may be subject to export licensing, including where data is shared digitally and not physically.
Important point
A good DTA may protect trade secrecy, but it does not automatically satisfy export-control law. Similarly, export-control compliance does not automatically preserve trade-secret protection.
Exam sentence
Export-control compliance and trade-secret protection are complementary but independent obligations.

PART IV — DUA vs DTA

27. Difference Between DUA and DTA

Point	DUA	DTA
Full form	Data Use Agreement	Data Transfer Agreement
Main function	Use control	Movement control
Main question	What can the recipient do with the data?	Where can the data go and how?
Focus	Permitted use, processing, access, derivatives	Transfer mechanism, destination, onward transfer, jurisdiction
Trade-secret role	Shows reasonable measures through use restrictions	Maintains secrecy chain across jurisdictions
Trigger	Project data sharing, vendor analysis, research use	Cross-border transfer, cloud transfer, subcontractor access
Key clauses	Purpose limitation, no training, no derivative data, access control, audit	Destination control, onward transfer, export control, server location, remote access
Failure mode	Data is overused	Data moves to weak-protection jurisdiction
Example	Vendor may use data only for Component X analysis	Data cannot be stored outside India without consent

One-line answer

DUA controls use; DTA controls movement. Both are necessary for protecting trade secrets in modern data-sharing arrangements.

PART V — REMAINING TOPICS FROM THE PPT

28. Data as the New Trade Secret Battlefield

Data is now a major competitive asset. The PPT mentions proprietary datasets, training corpora, sensor data, process optimisation logs and algorithmic outputs as important sources of enterprise value.

In modern business, the most valuable information may not be a document or formula but a dataset showing patterns, correlations, customer behaviour, machine performance or process efficiency.

Example

A company's manufacturing data showing how pressure, temperature and timing affect product quality may be a trade secret because competitors cannot easily recreate it.

---

29. Trade Secret Tri-Part Test Applied to Data

To qualify as a trade secret, data must satisfy three requirements:

1. Economic Value

The data must have commercial value because it is not generally known.

Example: A curated AI training dataset gives competitive advantage.

2. Secrecy

The data must not be publicly available or easily ascertainable.

Example: Access is restricted to authorised employees only.

3. Reasonable Measures

The owner must take reasonable steps to protect secrecy.

Examples:

- NDA

- DUA
- DTA
- Encryption
- Access logs
- Need-to-know access
- Data classification
- Audit rights

Exam sentence

Data becomes a trade secret only when it has economic value, remains secret, and is protected through reasonable contractual, technical and organisational measures.

---

30. Raw Data → Confidential Information → Trade Secret

Not every raw data point is a trade secret.

The PPT gives a spectrum:

Raw Data → Confidential Information → Trade Secret

Data becomes more protectable when it is:

1. Aggregated
2. Processed
3. Structured
4. Cleaned
5. Labelled
6. Contextualised
7. Combined with business know-how

Example

A single machine temperature reading may not be a trade secret. But thousands of machine readings linked with production output, failure rate and efficiency may become valuable trade-secret data.

---

31. Types of Data in Engineering Companies

The PPT identifies several categories of potentially protectable data.

Data category	Example	Trade-secret likelihood
Process optimisation data	Manufacturing parameters, yield correlation	High
Sensor/telemetry data	Equipment performance over time	Medium to high
Customer usage data	Product usage patterns	Medium
Algorithm training data	Curated labelled datasets	High
Test and validation data	Failure modes, quality metrics	High
Supply chain data	Vendor pricing, logistics models	Medium to high

---

32. Static Trade Secret Doctrine

Traditional trade-secret law assumes:

1. Identifiable information.
2. Controlled disclosure.
3. Static storage.
4. Clear boundaries.

This model worked for documents, formulas, drawings and customer lists. But it struggles with modern data because data moves, changes and gets transformed.

---

33. Legal Frameworks for Trade Secrets

United States

The PPT refers to DTSA 2016 and UTSA. Misappropriation includes acquisition by improper means or disclosure/use in breach of duty.

European Union

The EU has the Trade Secrets Directive 2016/943, which harmonises trade-secret protection and requires secrecy, commercial value and reasonable steps.

India

India has no standalone trade-secret statute. Protection is based on:

1. Contract law
2. Equity
3. Breach of confidence
4. Common law principles
5. Related statutory principles

The PPT mentions Indian cases such as **John Richard Brady**, **American Express v Priya Puri**, and **Zee Telefilms v Sundial Communications**.

---

34. Important Indian Case Laws

A. John Richard Brady v Chemical Process Equipments

This case supports protection of confidential technical information, drawings and know-how. If technical information is shared in confidence, the recipient cannot misuse it.

B. American Express Bank Ltd. v Priya Puri

This case shows that not every business information automatically becomes a trade secret. Information that is public or part of an employee's general skill may not be protected in the same way.

C. Zee Telefilms v Sundial Communications

This case supports the principle that confidential ideas or concepts disclosed in confidence may be protected against unauthorised use.

Exam use

Use these cases to show that India protects trade secrets through breach of confidence and contract, even without a specific trade-secret statute.

---

35. Problem When Data Moves

The PPT says that when data moves, doctrine struggles because:

1. Data is not a document.
2. Disclosure is continuous, not episodic.
3. Transformation creates ambiguity.
4. Boundaries are blurred.
5. Access controls are technical, not merely contractual.

Simple explanation

Earlier, the question was: "Was the confidential document disclosed?"
Now the question is: "Who accessed the data, from where, through which system, for what purpose, and what outputs were created from it?"

---

36. Why Classic Confidentiality Clauses Fail

A traditional clause usually says:
"Receiving party shall keep confidential information confidential and shall not disclose it to third parties."
This is not enough for modern data environments because it does not answer:

1. Can data be put in a data lake?
2. Can it be used for AI training?
3. Can derivative data be created?
4. Can APIs continuously access it?
5. Can it be mixed with other datasets?
6. Can model outputs retain the data's value?
7. Can subcontractors access it?

8. Can it be stored in foreign servers?

The PPT clearly states that classic confidentiality language does not address the actual data environment and may not qualify as a reasonable measure.

---

37. Data Lake Problem

A **data lake** is a large storage environment where different types of data are stored together.

The problem is that if trade-secret data is placed into a general data lake:

1. It may be mixed with other data.
2. Access may become broad.
3. Separation becomes difficult.
4. Derivative outputs may be created.
5. It may be impossible to prove who used what.

Exam sentence

A data lake can destroy practical secrecy if the contract does not control access, commingling, processing and derivative use.

---

38. APIs and Analytics Platforms

API access is continuous and programmatic. Each API call may return different data. The PPT states that the scope of access is often defined by API configuration, not merely by the contract.

Analytics platforms also transform data. They may:

1. Aggregate data.
2. Sample data.
3. Featurise data.
4. Train models.
5. Generate outputs that do not look like the original data.

AI/ML risk

A model trained on trade-secret data may retain patterns, correlations or values even after the original data is deleted.

---

39. Cross-Border Transfers and Enforcement Problems

Cross-border transfer creates practical and legal difficulties:

1. Different countries have different trade-secret laws.
2. Injunctions may be harder to obtain.
3. Evidence may be located abroad.
4. Foreign judgments may be difficult to enforce.
5. Data may move to subcontractors.
6. Secrecy may be diluted.

The PPT compares the US, EU and India and notes that India has no standalone trade-secret statute, unlike the US and EU frameworks.

---

40. SCOMET / Deemed Export Logic Extended to Data

The PPT connects export-control compliance and trade-secret protection.

Under the US deemed export doctrine, release of controlled technology or source code to a foreign national may be treated as export. The PPT extends this logic to proprietary technical data and explains that access by foreign-national employees, contractors or JV partners may trigger licensing requirements.

In India, technical data, design specifications and process know-how falling under SCOMET categories may require export-control review even if shared digitally.

Key exam distinction

Trade-secret law protects private commercial secrecy. SCOMET protects national security and export-control interests. Both must be checked separately.

---

41. Enforcement Challenges

The PPT lists four enforcement challenges:

A. Identifying misappropriation

It may be difficult to prove whether the recipient copied the data, trained a model on it, created derivative data or extracted patterns.

B. Obtaining interim relief

Trade-secret matters need quick injunctions because once secrecy is lost, later damages may not be enough.

C. Evidence preservation and discovery

Logs, metadata, access records, API records and audit trails are necessary.

D. Damages and remedies

It is difficult to calculate damages where the value is captured in a model, derivative dataset or statistical output.

---

42. Modern Clause Architecture

The PPT gives seven layers of modern protective drafting.

1. Reworked confidentiality definition

The definition should include data, data streams, APIs, derivatives, model outputs, metadata and analytics outputs.

2. Purpose limitation clause

Use must be limited to a specific defined purpose.

3. No-derivative / no-training clause

The recipient must not create derivative datasets or train AI models unless allowed.

4. Residual knowledge clause

The recipient should not claim that specific trade-secret information is free to use because employees remember it.

5. Audit and traceability clause

The disclosing party should be able to inspect access logs and compliance records.

6. Data return/destruction clause

The data should not remain in active systems, backups, archives or subcontractor systems.

7. Cross-border transfer restriction

The agreement must control where data may go and what protections apply in the destination jurisdiction.

---

43. Purpose Limitation Clause

Purpose limitation is the heart of a DUA.

Weak clause:

“Data may be used for project purposes.”

Strong clause:

“Data may be used only for finite element analysis of Component X under Statement of Work No. 3.”

A strong clause should prohibit:

1. Other commercial use.
2. AI training.
3. Benchmarking.
4. Reverse engineering.
5. Derivative dataset creation.
6. Aggregation.
7. Use beyond the agreed project.

---

44. No-Derivative / No-Training Clause

This clause prevents the recipient from using data to create new value for itself.

It should prohibit:

1. Training AI models.
2. Fine-tuning models.
3. Validating/testing AI systems.
4. Creating embeddings or vectors.
5. Creating statistical summaries.
6. Creating derivative datasets.
7. Extracting correlations or patterns.
8. Reverse engineering underlying methodology.

Exam point

A recipient can misuse trade-secret data without disclosing it, by using it internally to train models or create derivative products.

---

45. Residual Knowledge Clause

Residual knowledge means knowledge retained in human memory after working with confidential information.

A broad residual knowledge clause is risky because it may allow the recipient's personnel to use remembered patterns, values or insights.

A good clause should exclude:

1. Specific data values.
2. Measurements.
3. Parameters.
4. Correlations.
5. Statistical relationships.
6. Predictive insights.
7. Information that can reconstruct the dataset.

---

46. Audit and Traceability Clause

Audit rights are necessary because without evidence, trade-secret protection is weak.

A good audit clause should require records of:

1. Who accessed the data.
2. Date and time of access.
3. Duration of access.
4. Systems that accessed data.
5. Processing operations performed.
6. Transfers to subcontractors.
7. Storage location.

Exam sentence

Audit clauses convert confidentiality promises into verifiable evidence.

---

47. Data Return and Destruction Clause

A weak clause only says "return or destroy confidential information."

A strong clause should include:

1. Original data.
2. Copies.
3. Derivative data.
4. Backups.
5. Archived storage.
6. Disaster recovery systems.
7. Subprocessor systems.
8. Officer-level certification.
9. Specific timeline.
10. Audit survival after termination.

48. Cross-Border Transfer Restriction Clause

A strong cross-border clause should prohibit transfer, access, storage, mirroring, replication, caching or remote access outside permitted jurisdictions without consent.

It should also require:

1. Prior written consent.
2. DTA with downstream recipient.
3. Equivalent protection in destination jurisdiction.
4. Export-control compliance.
5. Notice of destination and recipient.
6. Liability for downstream breach.

---

49. Reworked Confidentiality Definition

Old definitions often cover only marked documents. That is insufficient.

Modern confidentiality definition should include:

1. Data and datasets.
2. Data streams and feeds.
3. API data.
4. Cloud data.
5. Metadata.
6. Query logs.
7. Access patterns.
8. Model weights.
9. Model outputs.
10. Predictions.
11. Correlations.
12. Statistical summaries.
13. Derivative works.
14. Information generated from the original data.

---

50. SRA-Based Protection

The PPT gives an SRA framework:

S — Secrecy

Secrecy must be maintained at every stage: collection, storage, processing, transfer, derivation, retention and destruction.

R — Reasonableness

Reasonable measures must match the data architecture. A paper-file confidentiality clause is not enough for a data lake or API environment.

A — Asset Value

Value may exist not only in raw data but also in trained models, summaries and derivative datasets.

Exam sentence

SRA means secrecy is continuous, reasonableness is technology-specific, and asset value includes derivative value.

---

51. Integrating DUAs, DTAs and Trade Secret Strategy

The PPT gives a four-layer strategy:

Layer 1 — Internal classification and governance

Classify data before sharing.

Layer 2 — Contractual architecture

Use NDA, DUA, DTA, purpose limitation, no-training, audit and destruction clauses.

Layer 3 — Technical implementation

Use encryption, access control, logging, data segregation and monitoring.

Layer 4 — Enforcement readiness
Maintain records, logs, audit trails, jurisdiction clauses and remedies.

---

52. Common Mistakes and How to Avoid Them

Mistake	Consequence	Avoidance
Treating all data as equally sensitive	Weakens secrecy claim	Classify data
Generic confidentiality clause	Does not fit modern data environments	Use modern definitions
Vague purpose clause	Broad use argument by recipient	Define specific permitted purpose
Ignoring derivative data	Value extracted through transformation	Add no-derivative clause
Broad residual knowledge clause	Trade secret walks away with personnel	Narrow the clause
No audit right	Cannot prove misuse	Add audit and access records
Vague destruction clause	Data remains in systems	Specify method and certification
No cross-border restriction	Jurisdictional dilution	Add DTA and destination control
Ignoring export control	Regulatory liability	Check SCOMET/EAR
Contract-tech mismatch	Practical failure	Align legal and technical controls

---

53. Negotiation Priorities

Tier 1 — Non-negotiable

1. Specific purpose limitation.
2. No AI/ML training and no derivative data.
3. Audit rights.
4. Return/destruction with certification.
5. Cross-border transfer consent.

Tier 2 — Strongly preferred

1. Narrow residual knowledge clause.
2. Survival of audit rights.
3. Data segregation/commingling prohibition.
4. Trade-secret acknowledgement.
5. Forum selection clause.

Tier 3 — Desirable

1. Liquidated damages.
2. Injunctive relief clause.
3. Consent before subprocessors.
4. Data lineage tracking.
5. Encrypted storage and key control.

---

54. Case Study: Analytics Vendor Leak

Facts-style example

A company shares manufacturing data with an analytics vendor. The vendor is allowed to analyse the data only for improving one machine process. But the vendor also uses the data to train its own AI tool for future clients.

Issues

1. Was the data a trade secret?
2. Was the permitted purpose specific?
3. Was AI training prohibited?
4. Was derivative data controlled?
5. Were audit logs available?
6. Was there misappropriation through use?

Lesson

Trade-secret leakage may happen through unauthorised use, not only through direct disclosure.

---

55. Case Study: Cross-Border JV Data Leak

Facts-style example

An Indian company shares technical process data with a foreign joint venture partner. The foreign partner stores it on a foreign cloud server and allows its overseas engineers to access it.

Issues

1. Was there a DTA?
2. Was cross-border transfer permitted?
3. Was SCOMET review done?
4. Was onward transfer restricted?
5. Was the destination jurisdiction safe?
6. Were audit records available?
7. Was trade-secret protection diluted?

Lesson

Cross-border movement of data is itself a trade-secret and export-control risk event.