

Presentation of Proposed Clause Language for Data Sharing Agreements

OPAI Data Sharing Work Group

April 24, 2026 Meeting

Jacqueline Rosati, EPRI

Jack White, EPRI

Ensuring clear, compliant, and secure data contracts

Agenda Overview

- Parties and Purpose
- Data Description and Scope
- Permitted Use and Restrictions
- Confidentiality and Data Privacy
- Special Data Categories and Controls
- Data Security, Breach, and Audit
- Ownership, Publication, and Retention
- Compliance, Export Control, and Other Clauses

Parties and Purpose

Clause Language and Formal Example

Identification of Parties

Legal names and principal places of business must be clearly identified for all parties involved in the agreement.

Purpose Specification

The purpose should be narrowly tailored to the specific collaboration, governing use of shared data by the receiving party.

Formal Agreement Example

A formal clause example describes the agreement for research on outage prediction using distribution-level grid measurements.



Data Description and Scope

Clause Language and Formal Example

Clause Description

The clause clearly specifies data categories, formats, timeframes, exclusions, and sensitivity levels to ensure precise data sharing terms.

Formal Data Example

A formal example outlines time-synchronized SCADA and PMU data specifications, secure formatting, and exclusion of customer-identifiable information.



Permitted Use and Restrictions

Clause Language and Formal Example

Purpose Limitation

Shared Data must only be used for the stated project purpose and nothing beyond it.

Prohibition on Re-identification

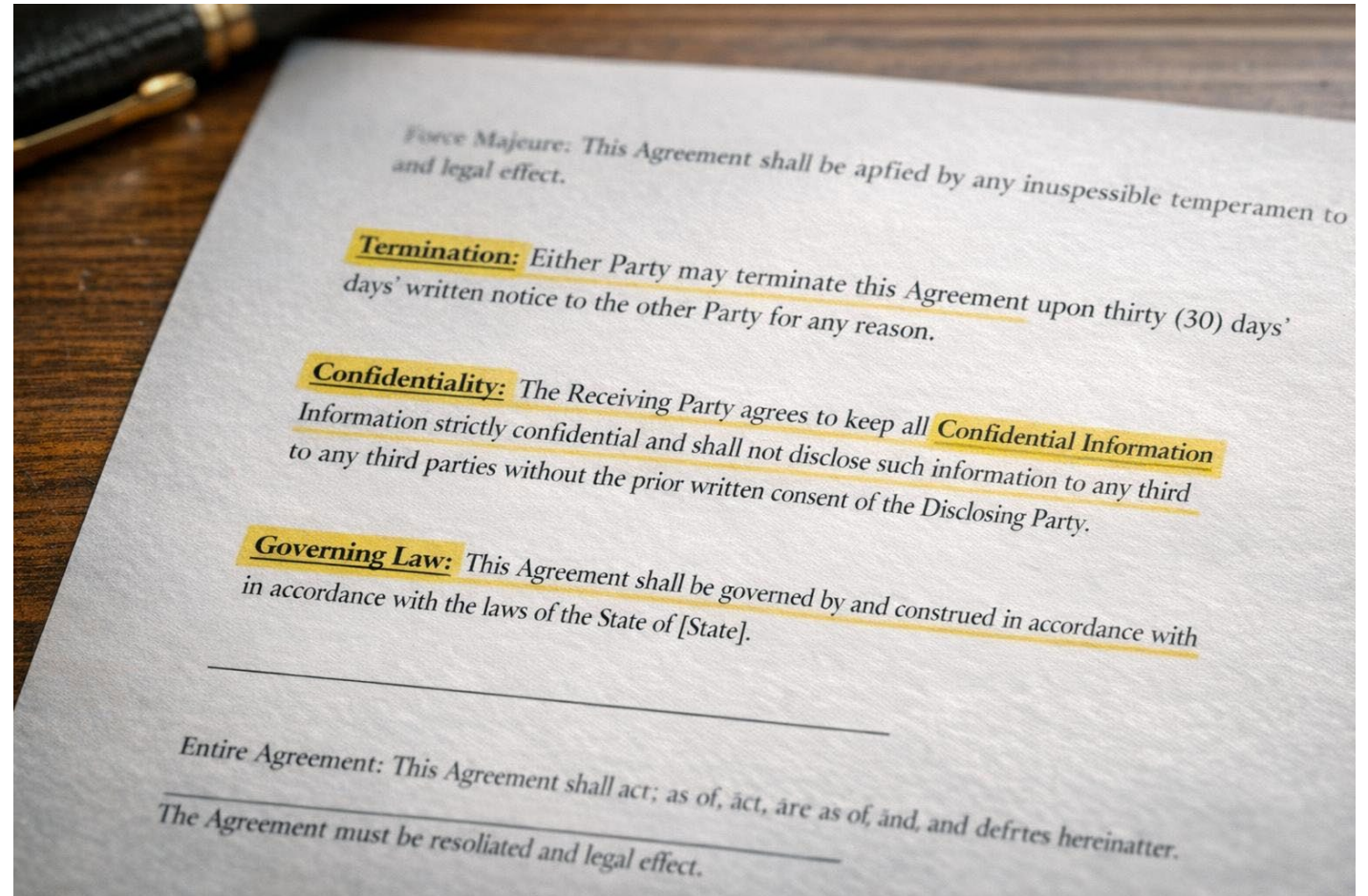
Receiving Party is prohibited from re-identifying anonymized or de-identified data under any circumstance.

Disclosure Restrictions

Data cannot be disclosed to third parties except approved sub-recipients with flow-down obligations.

Commercial Use Prohibition

The data cannot be commercially exploited without a separate license or agreement.



Confidentiality and Data Privacy

Clause Language and Formal Example

Confidentiality Definition

Non-public information must be protected with the same care as the Receiving Party's own confidential data.

Need-to-Know Basis

Confidential information should only be disclosed to individuals who require access to perform the project.

Labeling and Handling Procedures

Deliverables subject to public records requests must be appropriately labeled and handled per applicable regulations.



Special Data Categories and Controls

Personally Identifiable Information (PII)

Compliance with Privacy Laws

Parties must comply with privacy laws when handling PII and implement safeguards based on NIST SP 800-122 standards.

Data Minimization Principle

Minimizing collection of PII reduces risk and enhances data protection effectiveness.

Prohibition on Re-identification

Re-identification of de-identified data is prohibited to maintain confidentiality and privacy.

Role-based Access Controls

Access to PII must be restricted based on user roles to protect sensitive information.



Sensitive Energy Information (SEI)

Definition of SEI

Sensitive Energy Information includes operational grid data linked to critical infrastructure requiring stringent protection controls.

NERC CIP-011 Controls

SEI must be protected under NERC CIP-011, covering access control, handling, storage, transfer, and media sanitization.

Formal SEI Agreement

Parties acknowledge SEI status and implement controls to prevent unauthorized access and define data retention and disposal.

No BCSI to be provided



Controlled Unclassified Information (CUI)

CUI Definition and Scope

CUI refers to unclassified information requiring safeguarding under federal regulation 32 C.F.R. Part 2002 and agency directives.

Compliance Requirements

Parties must follow marking, safeguarding, dissemination, de-controlling, and training requirements for handling CUI.

Restrictions on Information Transfer

Onward transfer of CUI is prohibited without written authorization from the originating federal agency.



Data Security, Breach, and Audit

Data Security Measures

Secure Data Transfer

All data transfers use encrypted, mutually authenticated channels to ensure confidentiality and integrity.

Controlled Data Storage

Data at rest is encrypted and stored in controlled environments with role-based access and logging.

Access Restrictions and Auditing

Access is restricted to authorized personnel using MFA and audit mechanisms ensure compliance.



Breach Notification and Incident Response

Prompt Notification Requirement

Receiving Party must notify Provider within 24 hours of any suspected or confirmed unauthorized access incidents.

Cooperation in Incident Management

Parties collaborate in containment, investigation, notification, and remediation of security breaches.

Record Preservation for Audit

Related records are preserved to support auditing and ensure accountability post-incident.



Audit Rights

Audit Purpose

Audits verify compliance with agreements related to sensitive data protection and export control obligations.

Audit Process

Provider may perform audits with prior notice and protections to avoid unrelated information disclosure.

Confidentiality Measures

Audits are subject to confidentiality to ensure sensitive information is protected during the review.



Ownership, Publication, and Retention

Data Ownership and Intellectual Property

Provider's Data Rights

The Provider retains all rights and ownership of the shared data throughout the engagement.

Receiving Party's License

The Receiving Party obtains a limited license with no rights beyond the agreed terms for using shared data.

Ownership of Derived Results

Receiving Party can own models and analyses created, excluding raw shared data or confidential information.



Publication and Disclosure of Results

Prior Review Periods

A mandatory prior review period of 30 days helps prevent accidental disclosure of confidential information during publication.

Written Notice Requirement

The receiving party must provide at least 30 days' written notice before any proposed publication for review and redaction.

Scientific Independence

Scientific independence is respected despite the review and redaction process to maintain research integrity.



Data Retention and Destruction

Retention Period Limits

Data retention is strictly limited to the project duration or an agreed timeframe to ensure compliance.

Data Destruction Requirements

Upon project end, shared data must be securely deleted or returned, with certification of destruction.

Legal and Audit Exceptions

Archival copies may be retained only if legally required for audit or compliance purposes.



Compliance, Export Control, and Other Clauses

Nuclear Quality Assurance (NQA-1)

Quality Processes for Nuclear Projects

Projects involving nuclear facilities must maintain quality processes aligned with ASME NQA-1 standards to ensure safety and reliability.

Key NQA-1 Requirements

NQA-1 requires document control, configuration control, software quality assurance, audits, and corrective actions for nuclear safety.

Quality Program Implementation

Receiving parties must implement and maintain a documented quality program consistent with NQA-1, accessible for review.



Third-Party Intellectual Property

Compliance with Licenses

Receiving Party must comply with all applicable third-party licenses when using shared data materials.

Restrictions on Use

Modification, sublicensing, or reverse engineering of third-party materials is prohibited without express permission.

Limited Project Use

Use of third-party content is strictly limited to the project scope under applicable terms.



Export Control

Export Administration Regulations

Parties must comply with EAR regulations covering items under Commerce Control List and EAR99 classifications.

EAR99 Classification

Items not on the Commerce Control List are classified as EAR99 but require due diligence on destination and end-use.

DOE Part 810 Authorization

Nuclear technology assistance requires specific authorization under DOE Part 810 before export or transfer.



Compliance with Laws and Regulations

Adherence to Applicable Laws

Parties must comply with laws covering infrastructure protection, privacy, and public records.

Information Protection Standards

Compliance includes NERC CIP controls for grid data and federal information-handling programs.

Export and Assistance Regulations

Parties must follow export controls and nuclear assistance rules where applicable.



Governing Law and Dispute Resolution

Governing Law Specification

Agreements must clearly specify the governing law and jurisdiction to apply in case of disputes.

Tiered Dispute Resolution

Dispute resolution may involve negotiation, mediation, and ultimately litigation or arbitration as structured steps.

Formal Clause Example

A formal clause example includes governing law, negotiation attempts, and court jurisdiction for unresolved disputes.



Term and Termination

Effective Date and Duration

Agreements must specify the start date and length of the term clearly to manage expectations.

Termination for Convenience

Contracts should allow termination upon notice, providing flexibility for parties to end the agreement.

Survivability Clauses

Certain provisions like confidentiality, IP rights, and export controls remain effective even after termination.



Other Standard Clauses

Entire Agreement Clause

This clause confirms the contract and its exhibits constitute the full and complete agreement between the parties.

Amendments and Assignment

Amendments require written consent by both parties and assignment is restricted without prior written approval.

Other Standard Clauses

Clauses like No Waiver, Severability, and Counterparts protect contractual integrity and outline procedural rules.



Conclusion

Comprehensive Clause Coverage

All key proposed clause language sections were covered to ensure thorough data sharing agreements.

Ensuring Compliance

Agreements were designed to be compliant with regulations, protecting all parties involved.

Safeguarding Interests

The agreements aim to safeguard interests and ensure clarity between sharing parties.