

Data Processing and Confidentiality Policy

Free Clear Port Consulting LLC

Effective Date: November 20, 2025

Company Address: 30 N Gould St, Sheridan, WY 82801, United States

Website: <https://fcp-consulting.co>

Email: office@fcp-consulting.co

This Policy explains how Free Clear Port Consulting LLC processes and protects engineering files technical materials project data personal information and all other confidential content shared by clients or collected through professional collaboration. This Policy applies to all clients suppliers and visitors of the website and is aligned with privacy requirements in the United States and the European Union.

1. Purpose of This Policy

The goal of this document is to ensure that all information provided during engineering consulting activities is collected used stored and protected in a secure and responsible manner. This includes technical drawings static calculations design documentation feasibility studies CAD models photos operating parameters and all related material.

2. Types of Data Processed

We process several categories of information depending on the nature of the project.

Personal Contact Data

Name email address phone number job title and company information required for communication.

Project and Technical Data

Engineering documents CAD files material specifications internal diagrams concept designs load data operating conditions measurements reports and similar content necessary for accurate consulting work.

Operational and Business Data

Purchase records payment confirmations invoices commercial agreements and internal project notes.

Website and Communication Data

Messages sent through forms emails interaction records and general usage analytics from website visits.

3. Legal Grounds for Processing Data

For clients located in the European Union we process data under the following legal grounds.

Execution of a Contract

Processing required to deliver engineering consulting services prepare proposals and develop project documentation.

Legitimate Interests

Processing necessary for internal security quality control safe storage of files disaster recovery and improvement of service delivery.

Consent

Processing performed only after you choose to submit forms or voluntarily send documents.

Compliance with Legal Obligations

Processing required for accounting financial reporting or cooperation with official authorities.

4. How We Use Processed Data

Collected information is used strictly for business functions and never for unrelated marketing or the sale of data.

Service Execution

Performing calculations producing CAD models preparing drawings evaluating client specifications and delivering solutions.

Communication

Responding to questions providing status updates scheduling meetings and sending finalized materials.

Project Management

Maintaining internal records quality verification revision history version control and workflow optimization.

Security

Verifying authenticity of access requests reviewing file activity and protecting against unauthorized access.

Compliance and Risk Reduction

Meeting engineering standards ensuring professional responsibility and adhering to mandatory regulations.

5. Confidentiality Obligations

All client information received by Free Clear Port Consulting LLC is treated as confidential.

We do not share or disclose confidential content to any party unless required for project execution under controlled conditions or when legally mandated.

Confidential materials include project files CAD documents technical specifications business strategies internal formulas measurement data and all related engineering content provided by the client or created by us.

Confidentiality remains in force without time limitation and continues after completion of the project or termination of the agreement.

6. Access Control and Security Measures

We apply strict access control policies to ensure that only authorized personnel can view or work with client data.

Key measures include the following practices.

- Secure cloud storage systems with controlled permissions

- Encrypted communication channels for file transfers

- Multi factor authentication for internal access

- Regular backup routines for disaster recovery

- Isolated environments for sensitive engineering work

- Periodic review of access logs

- Internal confidentiality agreements for employees and collaborators

While no system can guarantee perfect protection we consistently maintain high security standards aligned with industry practice for engineering data management.

7. Use of External Software and Service Providers

To deliver engineering consulting services we rely on software platforms and service providers that may process limited data.

Examples include the following.

- CAD collaboration systems for version control

- Cloud storage for file hosting

- Analytic tools that evaluate website performance

Payment processors that verify transactions
Communication systems used for email delivery

These providers operate under their own privacy terms and are selected only when they apply strong security and compliance measures.

We do not authorize these providers to use client data for their purposes beyond what is required for the service they deliver.

8. Sharing Data With Subcontractors

We may collaborate with verified engineering partners when a project requires specialized knowledge or additional capacity.

Subcontractors receive only the information necessary for assigned tasks and must follow confidentiality obligations equal to or stricter than ours.

We do not collaborate with subcontractors that fail to meet strong privacy and security standards.

9. International Transfers

Because clients can be located anywhere in the world data may be stored or processed outside the client region including in the United States.

For data originating from the European Union we apply additional protection such as encrypted storage secure transfer protocols and appropriate contractual safeguards.

10. Data Retention Timeline

Data is stored only as long as needed for legitimate reasons.

Engineering files

Kept for a reasonable period after project completion to support revisions additional consulting or performance review.

Financial documentation

Stored for the duration required by accounting and tax regulations.

Communication records

Retained to maintain project continuity and protect both parties in case of disputes.

Upon request and when legally acceptable certain data may be deleted earlier.

11. Rights of Individuals From the European Union

Clients and visitors within the European Union have the following rights.

Access to data

Review of the personal data we hold.

Correction

Updating inaccurate or outdated data.

Deletion

Request removal of data when legally permissible.

Restriction of processing

Limiting use of data under certain situations.

Transferability

Receiving data in a structured format.

Objection

Challenging processing based on legitimate interests.

Withdrawal of consent

Ending processing where consent was provided.

12. Handling of Sensitive Engineering Files

Engineering data is treated with special protection because it may affect safety performance and business confidentiality.

Such data is used only for project analysis design creation of solutions and related engineering support.

We never use engineering data to develop internal commercial products or for unrelated research.

We never disclose engineering files to external parties without a valid purpose tied to the project.

13. Data Breach Response

If we detect any unauthorized access loss or compromise of data we will take immediate steps to contain the incident notify affected clients and work with relevant authorities if required.

Corrective actions may include password resets termination of suspicious access points secure restoration from backups and further strengthening of protective measures.

14. Right to Refuse Unreasonable Requests

We reserve the right to decline data requests that are abusive repetitive unfounded or contradictory to legal and safety requirements.

15. Updates to This Policy

We may update this document to reflect changes in technology security practice or legal obligations.

The effective date always indicates the latest revision.

Continued use of our services confirms acceptance of the updated version.

16. Contact Information

For questions regarding this Policy your data rights or procedures for managing confidential engineering content contact us at

Email: office@fcp-consulting.co

Address 30 N Gould St Sheridan WY 82801 United States