

BERENSON MANSFIELD CONSULTING LLC

Data Privacy, Security & Responsible AI Policy — Version 1.0

Our Commitment

Berenson Mansfield Consulting LLC is committed to protecting client information, maintaining strong security controls, and using artificial intelligence responsibly.

We believe clients should have confidence that their systems, information, and intellectual property are handled with transparency, accountability, and care.

Data Ownership

Clients retain ownership of the information they provide, along with client-specific deliverables produced during an engagement.

Berenson Mansfield retains ownership of its methodologies, frameworks, templates, automation patterns, reusable code, and proprietary consulting processes.

Access Management

Access to client environments is granted only through client authorization. Access methods may include:

- Client-created user accounts
- Temporary consultant access
- Sandbox environments
- Service accounts
- Approved API integrations
- Secure exports

Data Handling Principles

Berenson Mansfield follows several core principles:

- **Purpose Limitation** — Client data is processed only to deliver contracted services.
- **Data Minimization** — Only the information necessary to perform an engagement is accessed.
- **Least-Privilege Access** — Access is limited to authorized personnel and approved systems.
- **Cloud-First Processing** — Client information is processed within approved cloud environments whenever possible.

- **Security by Design** — Privacy and security considerations are incorporated into workflows, automations, integrations, and data architectures.

Security Controls

Security practices include:

- Multi-factor authentication
- Role-based permissions
- Encryption in transit
- Private repositories
- Secure credential management
- Segregated client environments
- Access reviews
- Defined retention schedules
- Controlled sharing permissions
- Secure cloud storage platforms

Responsible AI

Artificial intelligence tools may be used to support:

- Analysis
- Documentation
- Workflow design
- Automation development
- Code generation
- Quality assurance
- Process optimization

AI-generated outputs are reviewed by consultants prior to implementation.

Client data is not sold, shared for advertising purposes, or used to train proprietary models without written consent.

Sensitive credentials, secrets, and prohibited information categories are excluded from AI workflows.

Prohibited Information

Unless explicitly agreed upon in writing, Berenson Mansfield does not knowingly process:

- Protected health information
- Social Security numbers
- Payment card information
- Banking credentials
- Government identification numbers
- Sensitive personal financial information
- Biometric information
- Private encryption keys

Data Retention

Client information is retained only as long as necessary to fulfill engagement obligations, contractual requirements, or support periods.

Temporary working files are deleted after completion of engagements whenever practical.

Clients may request deletion or return of project materials according to contractual terms.

Incident Response

If Berenson Mansfield becomes aware of unauthorized access, disclosure, or loss of client information, we will investigate promptly and notify affected clients in accordance with contractual obligations and applicable laws.

Questions

For questions regarding privacy, security, or responsible AI practices, please contact:

Berenson Mansfield Consulting LLC

info@berensonmansfield.com

www.berensonmansfield.com