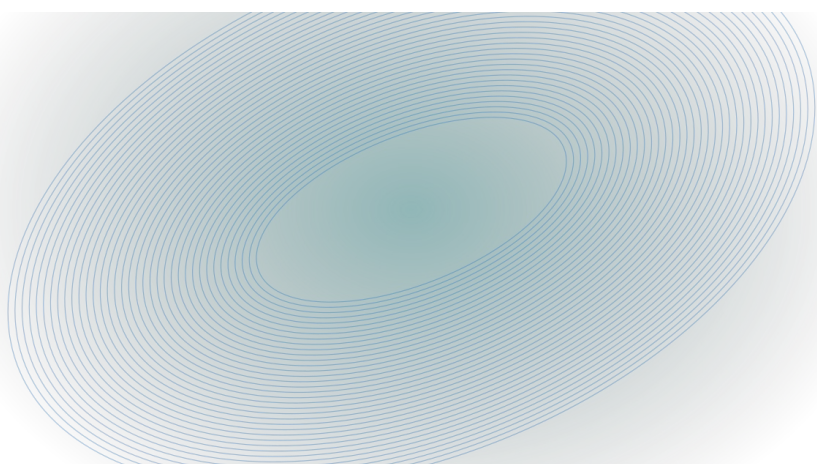




PUBLIC NOTICE / DATA RESPONSIBILITIES

Privacy Notice

Personal information, responsible processing and practical choices.



Metriq PRISM Laboratory

A research laboratory of Metriq Foundation, Inc.

LEG-03 | VERSION 1.2 | 26 SEPTEMBER 2026

PUBLICATION CANDIDATE • LEGAL REVIEW REQUIRED

Business defaults consolidated. No counsel approval or signature is represented.

Responsible organization: Metriq Foundation, Inc., a Florida Not-for-Profit Corporation, acting through Metriq PRISM Laboratory. **Version:** LEG-03 / 1.2. **Effective date:** September 26, 2026. **Postal contact:** 300 South Saturn Ave, Clearwater, FL 33755. **Privacy contact:** prism@metriq.org; put "Privacy request" in the subject and do not attach sensitive records without an approved transfer route.

1. Scope and responsibility

This Notice describes personal information handled for the PRISM website, organization accounts, research inquiries, grant applications, purchasing and project administration. It does not change ownership, confidentiality or permitted use of research data under an executed project agreement. For project personal data we process on a client's instructions, the client generally determines the research purpose and the signed data-processing schedule governs our processing role. For our own account administration, security, procurement and financial records, we determine the relevant operational purposes.

This Notice must describe the services actually enabled on its effective date. Optional research-agent processing, marketing and nonessential analytics are not activated merely by publishing this Notice. A business contact using a work email still has personal-information interests; organization membership does not make all associated information public.

2. Information we receive

Account information includes your name, email, organization, role, verification and membership records, and information needed to establish signing or purchasing authority. Authentication systems process credentials, session information and security events. The Platform may keep encrypted authenticator-factor material, security-key public credentials, challenge/counter records and protected recovery-code records as needed for the enabled MFA design. Do not send us your MFA codes, recovery material or passwords by email. Security-key device biometrics, where used by your device, are not intended to be sent to PRISM as biometric templates.

Application and project information includes contact details, research questions, nonconfidential context, decisions, reviewer assignments, project messages, deliverables and information you are authorized to provide through approved project channels. Payment information includes organization billing details, package and discount selections, transaction references, payment status, refunds and accounting records. Our payment provider may collect payer/bank information needed for its services; PRISM does not require you to give us online-banking credentials.

Technical information can include IP address, browser/device information, timestamps, requested pages, authentication/session identifiers, security logs and error diagnostics. We may receive information from an organization administrator, invited colleagues, service providers, authorized evaluators or public sources relevant to a research inquiry. We do not assume that publicly accessible personal information is unrestricted for every purpose.

3. How we use information

We use information to create and secure accounts; verify authority; maintain organization access; evaluate applications; communicate decisions and project updates; perform agreed research; provide billing, credit and refund records; investigate abuse; meet legal obligations; and resolve disputes. Access and use are limited to a relevant purpose and authorized personnel or providers.

For research, the project agreement defines permitted datasets, methods, recipients and output use. Nonpublic information is not a general license to conduct unrelated research, build unrelated datasets, train or fine-tune

general-purpose models, or improve unrelated services. A separate express authorization and any legally required consent are needed for such a different purpose. We do not use research applicants' information for targeted political advertising or sell access to their confidential proposals.

4. Providers and other recipients

We use service providers to operate PRISM, including providers of website hosting and network security; authentication, databases and private file storage; payment processing and bank-transfer services; and transactional email.

We may also share minimum necessary information with authorized PRISM staff; an organization's administrators and collaborators; project-specific reviewers, contractors and professional advisers who need it for assigned work and are bound by appropriate confidentiality duties; and authorities when legally required. Some providers may process limited information for their own legal, fraud-prevention or security purposes under their own privacy terms.

Provider categories do not themselves authorize access to confidential project material. Before sharing it, we review the provider, data, purpose, location, safeguards, retention, deletion and any required transfer mechanism; the signed project data schedule and necessary permissions control. Computational or AI-assisted services require a written project purpose and remain within its scope. Ask PRISM about recipients relevant to your account or project.

We may disclose information to address a credible security issue or legal claim, or in a legally permitted organizational transaction with continuing safeguards. We do not publish private applications, contact lists or confidential research inputs merely because an application is funded. Public research, organizational acknowledgment and optional promotional material follow separate permissions. We do not sell personal information or share it for cross-context behavioral advertising under this launch policy.

5. AI and automated assistance

Approved tools may help assess completeness, route requests, identify document issues or support scoped computational work. Human reviewers remain responsible for grant decisions and substantive release decisions. Paid research automation must be expressly scoped; fully grant-funded substantive autonomous research is not enabled under the default program policy.

No promise is made that every outside tool has zero retention or universally excludes model training. PRISM must review the relevant provider terms, account settings and project restrictions before sending nonpublic data, and must not use a provider incompatible with the approved schedule. Material AI use and relevant limitations are recorded in project deliverables. You may ask for human review of a consequential application or account decision by contacting PRISM.

6. Cookies, local storage and communications

The Platform uses necessary session, authentication, security and preference technologies. The actual technology inventory must be available with the effective Notice. Nonessential analytics, advertising trackers and marketing pixels remain off unless separately reviewed, accurately disclosed and supported by any required choice mechanism. Browser settings can limit storage but may prevent secure login or other functions.

Account verification, security notices, application decisions, payment and project messages are operational communications. Optional news or marketing subscriptions require a separate choice and may be withdrawn using the unsubscribe route or our contact email. Declining marketing does not affect eligibility, an award or

access to contracted research. We do not put unrelated promotions into a message to disguise its commercial purpose.

7. Retention and deletion

We retain information for the purpose stated and only for the periods below, unless a shorter lawful project instruction, mandatory duty or documented hold applies. The policy is not permission to keep an entire protected dataset merely because a contract or audit record must be kept.

Record category	Default retention / trigger
Unsubmitted application drafts	90 days after last activity; provide notice before routine deletion where practicable.
Declined or withdrawn applications	12 months after final decision or withdrawal.
Ordinary account/profile records	Account life plus 24 months after verified closure, limited to legitimate administration/support; revoke credentials and live access promptly.
Raw confidential project inputs and sensitive derivatives	Return/delete within 90 days after project closeout, or sooner under lawful instructions or a signed data schedule.
Sanitized working project files	2 years after closeout; not a license to retain raw confidential inputs or identifiable sensitive derivatives.
Final deliverables and necessary reproducibility evidence	7 years after closeout, subject to the shorter protected-input rule and specific rights.
Signed contracts, SOWs, changes, assent receipts, credit/payment/refund records	7 years after the relevant project or transaction closes, using the later event needed for that record.
Significant administrative, financial and incident audit evidence	7 years after closeout of the related action or incident.
Routine diagnostic/security logs	12 months from creation; preserve relevant portions for a documented incident or hold.
NDA-only evaluation copies	Return/delete within 30 days of request or end of evaluation under LEG-08, except minimal lawful archive.
Backups after scheduled deletion	Restricted rotation no longer than 90 days after the deletion trigger; no new ordinary use and reapply deletions after restoration.
Public nonpersonal grant/research records	May be retained indefinitely with version/correction history under their valid public licenses.
Lawful holds or shorter mandatory duties	Preserve only covered records while a documented legal hold applies; shorter mandatory deletion duties or controlling law prevail.

Where categories overlap, the stricter confidentiality/personal-data deletion rule governs the underlying content. Prompts, embeddings, caches, traces, extracts, model artifacts and identifiable outputs inherit the relevant input classification unless a documented assessment establishes that a sanitized version no longer exposes it. Keep only necessary sanitized evidence or a minimal access-restricted legal archive after raw data is due for deletion. If exact re-execution then becomes impossible, disclose that limitation.

Legal/incident holds identify their basis, scope, owner and review date. We lift holds and apply overdue deletion when the need ends. Removing a login does not erase an organization's necessary contractual/financial record.

Backup retention is not an authorization to restore deleted information to ordinary use or retain it indefinitely. External providers' actual deletion/backup capabilities must be compatible with the approved processing before the information is sent.

8. Your requests and choices

Contact us for access, correction, deletion, a copy of your information, limits on optional uses or questions about recipients and retention. We verify identity and authority proportionately, without asking for a password or MFA secret. We aim to acknowledge requests within five business days and substantively respond within 30 calendar days, subject to applicable deadlines and lawful extensions. We will explain a denial or limitation, such as protecting another person's information, preserving a legal obligation or acting only on the research client's instructions.

Where applicable law provides additional rights to object, restrict processing, withdraw consent, appeal or complain to a supervisory authority, those rights are preserved. Withdrawal does not retroactively make lawful prior processing unlawful. For information processed only on a client's behalf, we may refer the request to that client and assist as required. We do not retaliate for exercising a privacy right. Mandatory state or country notices and mechanisms must be supplied where their conditions apply.

9. Security and incidents

We use administrative, technical and organizational safeguards appropriate to the approved processing, including access limits, required MFA, private storage and incident procedures where implemented. No system is absolutely secure. Do not infer a certification, specific audit report, guaranteed uptime, U.S.-only processing or a particular encryption implementation unless PRISM expressly supplies current evidence for it.

A suspected account or data incident should be reported promptly to prism@metriq.org with a safe summary. PRISM will follow applicable legal notice duties and contractual incident cooperation obligations. An initial notice may be supplemented as facts become available. We do not wait for perfect information where that would delay a required notification.

10. International access and children

Service providers and authorized personnel may process information in countries other than yours. Before accepting data subject to a transfer restriction, PRISM and the client must identify the locations, appropriate legal mechanism and protective terms. This Notice does not supply executed EU standard contractual clauses, a UK transfer addendum or consent for a restricted transfer. Do not submit such data before the necessary arrangements are complete.

Organization accounts are intended for adults aged 18 or older. We do not knowingly solicit personal information directly from children through public intake. Research involving children's records, health information, special-category data or human-subject information requires a separate approved legal and security review before acceptance, even if a parent or institution offers to submit it.

11. Changes and contact

We will date and archive each version. Material changes will be explained before they take effect where required, with separate consent or another valid basis for new uses when necessary. A revised Notice does not silently expand an existing data agreement. Contact Metriq Foundation, Inc., through prism@metriq.org or the postal address above. A privacy acknowledgment is not a testimonial, marketing opt-in or publication license.