

PRIVACY POLICY

Website, business-contact, recruiting, public-sector, and commercial privacy notice

Version	Version 1.0
Company	EdgeByte Solutions LLC
Website	https://www.edgebyte.us
Contact	info@edgebyte.us

SCOPE NOTICE

This Privacy Policy governs personal information handled through EdgeByte Solutions LLC public websites, forms, business development activities, recruiting interactions, and similar general business communications. Customer, government, partner, employee, or project data processed under a separate contract, statement of work, data processing agreement, nondisclosure agreement, government contract, order, or other written instrument is governed by that instrument to the extent of any conflict.

Important restricted-data notice. Do not submit classified information, Controlled Unclassified Information (CUI), Federal Contract Information (FCI), source-selection information, procurement-sensitive information, export-controlled technical data, protected health information, payment-card data, Social Security numbers, passwords, private keys, authentication secrets, or other regulated/sensitive information through ordinary website forms or email unless EdgeByte has expressly authorized a suitable secure channel in writing.

Table of Contents

1. Purpose and Scope	4
2. Who We Are	4
3. Categories of Personal Information We May Collect	4
4. Sensitive Personal Information and Data We Do Not Intend to Collect	5
5. Government, Defense, and Public-Sector Restricted Information	5
6. Sources of Personal Information	5
7. Purposes for Which We Use Personal Information	5
8. Legal Bases and Permission to Process	6
9. Cookies, Analytics, and Similar Technologies	6
10. Marketing and Business Communications	7
11. Disclosure of Personal Information	7
12. Sale, Sharing, Targeted Advertising, and Cross-Context Behavioral Advertising	7
13. Public Records, FOIA, and Government Communications	8
14. Customer, Government Contract, and Project Data	8
15. Applicant and Recruiting Information	8
16. Retention	8
17. Security	8
18. Security Incidents and Breach Response	9
19. Your Privacy Rights - General	9
20. California Privacy Notice	9
21. Colorado and Other Universal Opt-Out Rights	9



22. Texas, Virginia, Florida, and Other U.S. State Rights	9
23. How to Submit a Privacy Request	10
24. Children and Minors	10
25. International Visitors	10
26. Third-Party Websites, Social Media, and External Services	10
27. Corporate Transactions and Successors	10
28. Changes to This Policy	11
29. Contact Us	11
Appendix A - Website Notice at Collection	12
Appendix B - U.S. State Privacy Rights Summary	12

1. Purpose and Scope

EdgeByte Solutions LLC ("EdgeByte," "we," "us," or "our") respects the privacy of website visitors, customers and prospective customers, government and public-sector contacts, partners, suppliers, job applicants, and other individuals who interact with us. This Policy describes the categories of personal information we may collect, the sources and purposes of collection, how information may be disclosed, how long information may be retained, and the privacy choices and rights that may be available under applicable law.

This Policy applies to information collected through edgebyte.us and other EdgeByte-controlled webpages that link to this Policy, through online forms, requests for information, requests for quote, RFP/RFI submissions, event or partner communications, recruiting interactions, and similar business communications. It does not automatically apply to third-party websites, products, or services, even when linked from our website.

If a separate customer agreement, government contract, task order, purchase order, data processing agreement, nondisclosure agreement, or other written contract applies to particular information, that agreement controls to the extent it contains more specific or conflicting privacy or security terms.

2. Who We Are

EdgeByte Solutions LLC is a technology integrator serving federal, defense, state and local government, small and midsize businesses, and commercial enterprises. Our principal business contact information is: EdgeByte Solutions LLC, ; info@edgebyte.us.

For purposes of privacy laws that use terms such as "business," "controller," or "data controller," EdgeByte may act in that capacity for information described in this Policy. For customer or project data handled solely on behalf of a customer, EdgeByte may instead act as a processor, service provider, contractor, or similar role, and the governing customer agreement will define the parties' respective obligations.

3. Categories of Personal Information We May Collect

Depending on how you interact with us, we may collect the following categories of personal information:

- **Identifiers and contact information:** name, business email address, personal email address if voluntarily provided, telephone number, postal address, account or profile identifiers, and similar contact information.
- **Professional and business information:** employer, agency, department, business unit, job title, role, professional affiliations, contracting role, procurement interests, business contact history, and information included in business cards, signatures, resumes, capability discussions, or correspondence.
- **Commercial and transaction information:** products or services of interest, quote or proposal requests, purchase or procurement needs, contract or opportunity references, renewal information, partner/OEM interests, transaction history, and related business records.
- **Communications and submission content:** messages, form entries, RFP/RFI materials, attachments, comments, feedback, meeting requests, support inquiries, and other information you choose to provide.
- **Recruiting and applicant information:** resume/CV, employment and education history, qualifications, professional references, work authorization information, compensation expectations, and other job-application information voluntarily submitted.
- **Internet, device, and usage information:** IP address, browser type, operating system, device type, language, referring URL, pages viewed, links clicked, timestamps, session information, cookie or similar identifiers, and diagnostic/security logs.

- **Approximate location information:** coarse location inferred from IP address or device/network information. We do not intend to collect precise geolocation through the ordinary public website unless clearly disclosed.
- **Security and fraud-prevention information:** authentication or anti-abuse signals, suspicious activity indicators, logs, and information reasonably necessary to protect the website, users, EdgeByte, customers, or third parties.
- **Publicly available and business-source information:** information from government records, professional directories, company websites, public profiles, partner referrals, event lists, and other lawful sources.
- **Inferences:** limited business inferences about likely technology interests, customer segment, or service needs derived from the information above, where lawful and reasonably necessary for business development or service improvement.

4. Sensitive Personal Information and Data We Do Not Intend to Collect

EdgeByte does not seek to collect sensitive personal information through ordinary public website forms except where reasonably necessary and lawfully provided. You should not use the public website or ordinary email to transmit government identifiers, Social Security numbers, driver's-license numbers, financial-account credentials, payment-card security codes, biometric identifiers, genetic information, precise geolocation, health information, information revealing racial or ethnic origin, religious beliefs, sexual orientation, union membership, passwords, cryptographic keys, or similarly sensitive data unless EdgeByte has specifically requested the information and provided an appropriate collection method.

If sensitive information is submitted without authorization, EdgeByte may delete, quarantine, restrict access to, or otherwise handle the submission as reasonably necessary for security, compliance, legal obligations, or incident response.

5. Government, Defense, and Public-Sector Restricted Information

The public website and ordinary contact channels are not approved systems for classified information, CUI, FCI, source-selection information, procurement-sensitive information, law-enforcement-sensitive information, export-controlled technical data, or other information requiring a controlled environment unless EdgeByte expressly states otherwise in writing for a specific channel or engagement.

Government personnel, prime contractors, subcontractors, and other public-sector users are responsible for following applicable agency, contract, handling, marking, safeguarding, dissemination, and transmission requirements before sending information to EdgeByte. If you are uncertain whether information may be transmitted through a public website or ordinary email, contact EdgeByte first and request an approved channel.

6. Sources of Personal Information

We may obtain personal information directly from you; automatically from your device or browser; from your employer, agency, organization, or colleagues; from customers, partners, OEMs, distributors, subcontractors, event organizers, and referral sources; from publicly available sources; and from service providers that assist with website operation, security, analytics, recruiting, communications, or business administration.

7. Purposes for Which We Use Personal Information

We may use personal information for one or more of the following legitimate business and legal purposes:

- Operate, maintain, secure, troubleshoot, and improve our websites, forms, and digital services.
- Respond to inquiries, requests for information, requests for quote, RFPs/RFIs, procurement requests, meeting requests, partner inquiries, and support questions.

- Prepare proposals, quotations, bills of material, statements of work, estimates, renewals, licensing options, procurement recommendations, and similar business materials.
- Establish, administer, and manage customer, supplier, partner, OEM, subcontractor, and government relationships.
- Communicate about products, services, events, renewals, security notices, service updates, and other business matters.
- Conduct recruiting, candidate evaluation, background or reference processes where lawful, workforce planning, and related human-resources administration.
- Perform analytics, measure website performance, understand usage, improve user experience, and evaluate business-development effectiveness.
- Detect, prevent, investigate, and respond to security incidents, fraud, abuse, malicious activity, and legal or policy violations.
- Protect our rights, property, systems, personnel, customers, users, and third parties; enforce agreements; establish, exercise, or defend legal claims.
- Comply with laws, regulations, subpoenas, court orders, government requests, contractual obligations, audit requirements, recordkeeping obligations, export-control requirements, and applicable public-sector procurement requirements.
- Support corporate transactions such as financing, reorganization, merger, acquisition, divestiture, due diligence, or sale of assets, subject to applicable confidentiality and legal protections.
- Create aggregated, deidentified, or statistical information that is not reasonably linkable to an identified individual, and use such information for lawful business purposes.

8. Legal Bases and Permission to Process

Where a privacy law requires a legal basis, we process personal information as necessary to perform or prepare for a contract; based on our legitimate interests in operating, securing, and developing our business; to comply with legal obligations; to protect vital or legal interests; and/or based on consent where consent is required. Consent may be withdrawn where applicable, without affecting processing lawfully performed before withdrawal.

9. Cookies, Analytics, and Similar Technologies

We and service providers may use cookies, pixels, scripts, local storage, server logs, and similar technologies to operate and secure the website, remember preferences, measure performance, understand traffic, and improve content. Depending on configuration, analytics or advertising technologies may collect device, browser, IP address, referral, interaction, and similar data.

You may control certain cookies through browser settings and, where provided, consent or preference tools. Disabling cookies may affect site functionality. EdgeByte does not promise that every browser "Do Not Track" signal will be recognized because there is no single universally accepted DNT standard. Where applicable law requires recognition of a qualifying universal opt-out mechanism, including Global Privacy Control (GPC), EdgeByte will honor such signals for the applicable browser/device and processing activity.

10. Marketing and Business Communications

We may send business communications to customers, prospects, government and commercial contacts, partners, and other individuals where permitted by law. Commercial email will be managed in accordance with applicable requirements, including honoring legally required unsubscribe requests. Transactional, security, legal, contract, procurement, and service-related communications may continue even if a recipient opts out of marketing messages.

We do not use this Policy as consent for marketing activities where affirmative consent is required by law. Any telephone or text-message marketing that requires separate consent will be subject to the applicable consent mechanism and records.

11. Disclosure of Personal Information

We may disclose personal information to the following categories of recipients, only as reasonably necessary and subject to applicable law and contractual safeguards:

- **Service providers and processors:** website hosting, content delivery, security, cloud, email, communications, analytics, CRM, file storage, recruiting, professional services, and administrative vendors.
- **OEMs, distributors, technology partners, subcontractors, and suppliers:** when needed to evaluate requirements, obtain pricing, provide technical or licensing information, fulfill a request, or support a customer opportunity.
- **Customers, prime contractors, teaming partners, and public-sector organizations:** when relevant to a proposal, teaming effort, service delivery, compliance requirement, or business relationship.
- **Professional advisers:** attorneys, accountants, auditors, insurers, consultants, and financial advisers subject to appropriate confidentiality duties.
- **Government, regulators, law enforcement, and legal process recipients:** when required or permitted by law, subpoena, court order, regulatory request, national-security requirement, contract requirement, or to protect rights and safety.
- **Corporate transaction parties:** prospective or actual purchasers, investors, lenders, successors, and advisers in connection with a merger, acquisition, financing, restructuring, bankruptcy, sale, or transfer of business/assets.
- **Others with your direction or consent:** when you ask us to disclose information or otherwise authorize the disclosure.

12. Sale, Sharing, Targeted Advertising, and Cross-Context Behavioral Advertising

EdgeByte does not sell personal information for monetary consideration as a business model. Depending on the definitions in a particular state privacy law, some disclosures involving analytics, advertising, or similar technologies could potentially be characterized as a "sale," "sharing," or processing for targeted advertising even when no money changes hands. Where EdgeByte engages in processing that triggers an applicable opt-out right, EdgeByte will provide the legally required notice and opt-out mechanism and will honor qualifying universal opt-out signals where required.

We do not knowingly sell or share the personal information of children or minors in circumstances requiring opt-in authorization.

13. Public Records, FOIA, and Government Communications

Communications involving federal, state, local, tribal, territorial, or other governmental entities may be subject to the Freedom of Information Act, state public-records laws, sunshine laws, records-retention requirements, discovery obligations, audits, or other disclosure regimes. EdgeByte cannot guarantee that information sent to or through a government entity will remain confidential merely because the sender considers it confidential.

Government and contractor users should follow applicable marking, proprietary-data, procurement, source-selection, and records-handling requirements. Confidentiality rights may depend on applicable law, contract terms, protective markings, and the circumstances of submission.

14. Customer, Government Contract, and Project Data

Personal information and other data received in connection with contracted services may be subject to customer-specific or government-specific requirements, including contract clauses, agency security requirements, data processing terms, nondisclosure obligations, records schedules, incident-reporting requirements, cybersecurity requirements, and flow-down clauses. Those terms supplement or supersede this Policy for the covered data.

Nothing in this Policy expands EdgeByte's authority to use customer or government data beyond the authority granted by an applicable contract, order, statement of work, law, or written instruction.

15. Applicant and Recruiting Information

If you apply for employment or otherwise pursue an opportunity with EdgeByte, we may use applicant information to evaluate qualifications, communicate regarding opportunities, verify information, conduct lawful background/reference processes, maintain recruiting records, comply with equal-employment and recordkeeping obligations, and establish or defend legal claims. Additional notices may apply to background checks, biometrics, or jurisdiction-specific employment data.

16. Retention

We retain personal information only for as long as reasonably necessary for the purposes described in this Policy, including to provide services, manage customer and partner relationships, maintain procurement and proposal records, comply with legal/contractual/audit obligations, resolve disputes, enforce agreements, preserve evidence, support security, and maintain appropriate business records.

Retention periods vary based on the type of information, sensitivity, legal and contractual requirements, customer or agency instructions, applicable statutes of limitation, litigation holds, security needs, and whether the information is required for an ongoing relationship. When information is no longer reasonably required, we may delete, anonymize, aggregate, or securely dispose of it, subject to technical limitations and lawful backup/archival practices.

17. Security

EdgeByte uses administrative, technical, and physical safeguards reasonably designed to protect personal information against unauthorized access, acquisition, disclosure, alteration, destruction, or misuse, taking into account the nature of the information and the context of processing. Measures may include access controls, least-privilege practices, authentication, encryption or secure transport where appropriate, logging, monitoring, vendor management, security training, vulnerability management, incident response, and secure disposal practices.

No website, network, transmission, or storage system can be guaranteed to be completely secure. You are responsible for using appropriate security practices on your devices and networks and for avoiding transmission of restricted data through unapproved channels.

18. Security Incidents and Breach Response

If EdgeByte identifies a security incident affecting personal information, EdgeByte may investigate, contain, remediate, preserve evidence, coordinate with affected customers or authorities, and provide notices as required by applicable law or contract. Notice timing, content, and recipients will depend on the facts, applicable breach-notification laws, contractual obligations, government requirements, and law-enforcement considerations.

19. Your Privacy Rights - General

Depending on your state of residence and whether the relevant law applies to EdgeByte and the particular data, you may have rights to: confirm whether we process your personal information; access or obtain a copy; correct inaccuracies; delete certain information; obtain portable data; opt out of sale, sharing, targeted advertising, or certain profiling; limit certain uses of sensitive information; withdraw consent; appeal a denied request; and exercise rights without unlawful discrimination or retaliation.

Privacy rights are subject to statutory definitions, thresholds, exemptions, authentication requirements, and exceptions. Certain laws exclude or limit rights for business-to-business contacts, employees, job applicants, government records, data regulated by other laws, deidentified data, or information processed in a purely commercial or employment context.

20. California Privacy Notice

To the extent the California Consumer Privacy Act (CCPA), as amended, applies to EdgeByte and the information at issue, California residents may have rights to know/access, delete, correct, opt out of sale or sharing, limit certain uses/disclosures of sensitive personal information, use an authorized agent, and receive non-discriminatory treatment for exercising rights.

EdgeByte does not sell personal information for money. If EdgeByte engages in activity deemed a "sale" or "sharing" under the CCPA, legally required opt-out mechanisms will be provided, and qualifying Global Privacy Control signals will be honored as required. We do not offer financial incentives in exchange for personal information unless separately disclosed with legally required terms.

For CCPA disclosure purposes, the categories we may collect include identifiers; customer records/contact data; protected-class information if voluntarily provided in employment/recruiting contexts; commercial information; internet/network activity; approximate geolocation; professional/employment information; and inferences. The business purposes and categories of recipients are described elsewhere in this Policy.

21. Colorado and Other Universal Opt-Out Rights

Where the Colorado Privacy Act or another applicable law requires recognition of a universal opt-out mechanism, EdgeByte will process qualifying signals for the browser/device and covered processing activity in accordance with applicable law. Applicable residents may also have rights to access, correct, delete, portability, opt out of targeted advertising or sale, and appeal certain decisions.

22. Texas, Virginia, Florida, and Other U.S. State Rights

Residents of Texas, Virginia, Florida, Connecticut, Oregon, Montana, Delaware, Iowa, Indiana, Tennessee, New Jersey, New Hampshire, Nebraska, Minnesota, Maryland, Kentucky, Rhode Island, and other states with comprehensive privacy laws may have some combination of access/confirmation, correction, deletion, portability, opt-out, consent, appeal, and non-discrimination rights if the applicable statute covers EdgeByte and the processing activity.

State laws differ materially in thresholds, definitions, exemptions, cure periods, business-to-business and employment exclusions, sensitive-data requirements, universal opt-out obligations, and enforcement. EdgeByte will apply the rights and

procedures required by the law applicable to the requesting individual and data.

23. How to Submit a Privacy Request

You may submit a privacy request by emailing info@edgebyte.us with the subject line "Privacy Request" or by using the Contact Us form available through edgebyte.us. Please describe the right you wish to exercise and provide enough information for us to identify the relevant records.

We may need to authenticate your request using information reasonably related to the records at issue. We will not request more personal information than reasonably necessary for verification. If an authorized agent submits a request, we may require proof of authority and, where permitted, direct verification or confirmation from the individual.

If an applicable law provides a right to appeal a denied request, you may appeal by replying to the denial or emailing info@edgebyte.us with the subject line "Privacy Appeal." We will process appeals within the period required by applicable law.

24. Children and Minors

The EdgeByte website and services are directed to business, professional, governmental, and institutional audiences and are not directed to children under 13. We do not knowingly collect personal information online from children under 13 through the general website. If we learn that we collected such information in circumstances requiring parental consent, we will take reasonable steps to delete or otherwise address it in accordance with applicable law.

Minors should not submit resumes, procurement materials, sensitive information, or other personal data through the website without appropriate authorization.

25. International Visitors

EdgeByte is based in the United States. If you access the website from outside the United States, your information may be processed in the United States and other locations where service providers operate, subject to applicable law. Where the EU General Data Protection Regulation, UK GDPR, or similar law applies, individuals may have rights including access, correction, erasure, restriction, portability, objection, withdrawal of consent, and complaint to a supervisory authority. EdgeByte will apply such rights when legally required.

Cross-border transfers will be handled using a legally recognized mechanism where required. This Policy does not represent that EdgeByte actively targets or offers regulated services in every jurisdiction from which the website may be accessible.

26. Third-Party Websites, Social Media, and External Services

Our website may link to OEMs, partners, government sites, social-media services, documentation, event platforms, and other third-party websites. EdgeByte does not control their privacy practices. A third party's collection and use of information is governed by its own terms and privacy notices. Links do not necessarily constitute endorsement, sponsorship, or responsibility for third-party privacy or security practices.

27. Corporate Transactions and Successors

Personal information may be reviewed or transferred as part of a merger, acquisition, financing, reorganization, bankruptcy, sale of business/assets, due diligence process, or similar transaction, subject to applicable law and reasonable confidentiality protections. A successor may continue to process information consistent with this Policy unless another notice is provided where required.

28. Changes to This Policy

We may update this Policy from time to time to reflect changes in law, technology, services, business practices, or processing activities. If required by law, we will provide additional notice or obtain consent before a material change applies to previously collected information.

29. Contact Us

Questions, complaints, or privacy requests may be directed to: **EdgeByte Solutions LLC**,
; **info@edgebyte.us** . Please do not include sensitive authentication credentials, classified information, CUI, FCI, export-controlled technical data, or other restricted information in an ordinary privacy inquiry.

Appendix A - Website Notice at Collection

This summary is designed to support a short notice placed at or near website forms. It does not replace the full Privacy Policy.

Category	Examples	Primary purposes
Identifiers / contact	Name, email, phone, company, title	Respond to inquiries; proposals; customer/partner communications
Professional / business	Employer, agency, role, business interests	Business development; procurement; relationship management
Submission content	Messages, attachments, RFP/RFI or quote details	Evaluate and respond to requests; prepare proposals/quotes
Device / usage	IP, browser, pages viewed, logs	Operate, secure, measure, and improve the website
Applicant information	Resume, work history, qualifications	Recruiting and candidate evaluation

Restricted data: Do not use public website forms for classified information, CUI, FCI, source-selection information, procurement-sensitive information, export-controlled technical data, PHI, payment-card data, SSNs, passwords, private keys, or other restricted data. Contact EdgeByte for an approved secure channel when needed.

Appendix B - U.S. State Privacy Rights Summary

Right / issue	General treatment under this Policy
Access / confirmation	Available where required; authenticated request may be required.
Correction	Available where required, considering the nature and purpose of the data.
Deletion	Available where required, subject to legal, security, contract, and recordkeeping exceptions.
Portability	Available where required and technically feasible in a usable format.
Sale / sharing / targeted advertising	EdgeByte does not sell personal information for money; applicable opt-outs will be honored if covered processing occurs.
Sensitive data	Not intentionally collected through ordinary website channels; consent or other protections applied where legally required.
Universal opt-out / GPC	Honored for covered processing where applicable law requires it.
Appeal	Available where applicable state law provides an appeal right.
Non-discrimination	EdgeByte will not unlawfully discriminate for exercising applicable privacy rights.

State privacy laws change frequently. This Policy is intended to provide a broad rights framework while preserving statutory definitions, thresholds, exemptions, and jurisdiction-specific procedures. Where a more specific legally required notice applies, that notice controls.