

QA Enterprises Privacy Policy

Effective Date: August 17, 2025

Last Updated: August 17, 2025

1. Introduction

QA Enterprises, an artificial intelligence consulting firm, is committed to protecting the privacy and security of your personal information. This Privacy Policy explains how we collect, use, share, store, and protect personal information from clients, website users, and others who interact with us. It also outlines your rights regarding your personal information and how to contact us with privacy-related concerns.

This policy applies to all services provided by QA Enterprises, including our website (www.qaenterprises.com) and related platforms. By using our services or website, you agree to the practices described in this policy.

We comply with applicable data protection laws, including but not limited to the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), other US state privacy laws (e.g., those effective in Delaware, Iowa, Nebraska, New Hampshire, New Jersey in 2025), and the EU Data Act.

2. Definitions

- **Personal Information:** Any information that identifies or could reasonably be used to identify an individual, directly or indirectly, such as name, email address, IP address, or payment details.
- **Processing:** Any operation performed on personal information, including collection, storage, use, sharing, or deletion.

3. Information We Collect

We collect personal information in the following categories:

- **Contact Information:** Name, email address, phone number, and mailing address provided voluntarily (e.g., through website forms, client onboarding, or inquiries).
- **Website Usage Data:** IP addresses, browser type, device information, and browsing behavior collected via cookies, web beacons, or analytics tools.
- **Client Data:** Information provided during consulting engagements, such as business contact details or specific project data.
- **Payment Information:** Billing details (e.g., credit card numbers) processed through secure third-party payment providers.

- **Third-Party Data:** Information obtained from public sources or partners, where permitted by law.

We do not intentionally collect sensitive personal information (e.g., health, racial, or political data) unless explicitly required for a specific service and with your consent.

4. How We Collect Information

We collect personal information through:

- **Voluntary Submission:** When you fill out forms, contact us, or sign up for services.
- **Automated Technologies:** Cookies, web beacons, and analytics tools (e.g., Google Analytics) track website usage. You can manage cookie preferences via our cookie banner.
- **Third-Party Sources:** Business partners, public records, or service providers, where legally permitted.

For more details on cookies and tracking, see our **Cookie Policy** on our website.

5. Purposes of Processing Personal Information

We process personal information for the following specific, explicit, and legitimate purposes:

- To provide and manage our consulting services.
- To communicate with you regarding inquiries, updates, or service delivery.
- To process payments securely through third-party providers.
- To improve our website and services through analytics and user feedback.
- To send marketing communications, where you have given consent.
- To comply with legal obligations (e.g., tax reporting or regulatory requirements).
- To protect our business, prevent fraud, and ensure data security.
- To develop and improve AI models and services, using anonymized, pseudonymized, or aggregated data where possible, in compliance with data minimization principles.

We do not use personal information for automated decision-making or profiling that produces legal or significant effects without your explicit consent.

6. AI-Specific Privacy Practices

As an AI consulting firm, we integrate privacy by design and by default into our AI development and services. This includes:

- Conducting data protection impact assessments for high-risk AI processing.
- Minimizing data use in AI training and ensuring anonymization where feasible.
- Providing transparency on AI algorithms and data sources upon request.
- Complying with the EU AI Act for any high-risk AI systems, including risk management, documentation, and human oversight.

7. Legal Basis for Processing (GDPR Compliance)

For users in the European Union, we process personal information based on the following legal grounds:

- **Consent:** For non-essential purposes like marketing or certain cookies (you may withdraw consent at any time).
- **Contract:** To fulfill agreements with clients or respond to inquiries.
- **Legal Obligation:** To comply with applicable laws or regulations.
- **Legitimate Interests:** For improving services, preventing fraud, or ensuring security, provided your rights are not overridden.

8. Sharing of Personal Information

We share personal information only with the following recipients, under strict confidentiality agreements:

- **Service Providers:** Trusted third parties providing hosting, payment processing (e.g., Stripe), or analytics services (e.g., Google Analytics).
- **Business Partners:** When necessary to deliver services (e.g., joint projects or AI tool vendors), with your consent where required.
- **Legal Authorities:** When required by law, such as in response to subpoenas or regulatory requests.

We do not sell, trade, or rent your personal information to third parties for their marketing purposes.

9. International Data Transfers

If you are located outside the United States, your personal information may be transferred to and processed in the United States or other countries where our service

providers operate. We ensure appropriate safeguards, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules, or adequacy decisions, to protect your data in compliance with GDPR (Chapter V), the EU Data Act, and other applicable laws.

10. Data Security

We implement industry-standard measures to protect your personal information, including:

- Encryption (e.g., SSL/TLS) for data transmission and storage.
- Firewalls and secure servers to prevent unauthorized access.
- Regular security audits, vulnerability assessments, and access controls.
- Data governance policies, including regular training for employees and privacy impact assessments.

In the event of a data breach posing a risk to your rights, we will notify you and relevant authorities within 72 hours, as required by GDPR (Article 33) and other applicable laws.

11. Data Retention

We retain personal information only for as long as necessary to fulfill the purposes outlined in this policy or comply with legal requirements. Specific retention periods include:

- **Contact Information:** Up to 5 years after the end of a client relationship or last interaction.
- **Website Usage Data:** Up to 12 months for analytics purposes, unless anonymized.
- **Payment Information:** As required by tax laws (typically 7 years).

When no longer needed, we securely delete or anonymize personal information using industry-standard methods.

12. Your Privacy Rights

Depending on your location, you may have the following rights regarding your personal information:

- **Access:** Request a copy of your personal information.
- **Rectification:** Correct inaccurate or incomplete data.
- **Erasure:** Request deletion of your data, subject to legal obligations.
- **Restriction:** Limit how we process your data in certain circumstances.

- **Data Portability:** Receive your data in a structured, machine-readable format.
- **Object:** Object to processing for marketing or legitimate interests.
- **Withdraw Consent:** Revoke consent for non-essential processing at any time.
- **Opt-Out of Sale/Sharing (CCPA/CPRA):** Request that we do not sell or share your data for targeted advertising (note: we do not currently sell data).
- **Rights under EU Data Act:** Access and portability for data from connected devices, if applicable.

To exercise these rights, contact our Privacy Officer at info@qa-enterprises.com. We will respond within 30 days (GDPR) or 45 days (CCPA), as applicable, without charge unless requests are manifestly unfounded or excessive.

13. Children's Privacy

Our services and website are not directed to children under 13 (or 16 in certain EU jurisdictions). We do not knowingly collect personal information from children. If we learn that a child's data has been collected without verifiable parental consent, we will delete it promptly. If you believe we have collected a child's data, contact us at info@qa-enterprises.com.

14. Third-Party Websites and Services

Our website may contain links to third-party websites or services. We are not responsible for their privacy practices or content. We encourage you to review the privacy policies of those platforms before providing personal information.

15. Data Breach Notification

If a data breach occurs that is likely to result in a high risk to your rights and freedoms, we will notify you and relevant authorities (where required) without undue delay, in accordance with GDPR, CCPA/CPRA, EU Data Act, and other applicable laws.

16. Updates to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices, legal requirements, or emerging regulations. Material changes will be communicated via email (if we have your contact details) or a prominent notice on our website at least 30 days before they take effect. We encourage you to review this policy periodically at www.qaenterprises.com/privacy.

17. Governing Law and Jurisdiction

This Privacy Policy is governed by the laws of the State of Delaware, USA, without regard to its conflict of law principles. Any disputes arising from this policy will be

resolved in the state or federal courts of Delaware, unless otherwise required by applicable law (e.g., GDPR for EU residents).

18. Contact Us

For questions, concerns, or to exercise your privacy rights, please contact our Privacy Officer:

- **Email:** info@qa-enterprises.com
- **Phone:** +1(309) 868-3652

We are committed to resolving privacy concerns promptly and transparently. If you are not satisfied with our response, you may contact your local data protection authority (e.g., an EU supervisory authority or the California Attorney General).

19. Cookie Policy

We use cookies and similar technologies to enhance your website experience. You can manage your preferences through our cookie banner. For details, visit www.qaenterprises.com/cookie-policy.

Conclusion

QA Enterprises is dedicated to safeguarding your personal information and ensuring compliance with global privacy laws. Thank you for trusting us with your data.