

Article9 Privacy Policy

Version v1

This is the published text of this version of the agreement, provided in a form you can store and print as section 27.4 requires. It is not a record of any particular acceptance. The complete text follows this page.

AGREEMENT VERSION	v1
SHA-256 OF THIS TEXT	7fcb0d7e80834ea49a1789cdad313144b18858cf547ed7e825a4e6df8e50336d
PUBLISHED AT	https://article9llc.com/legal/privacy

A superseded version stays published because acceptance records point at it. This copy remains available at <https://article9llc.com/legal/privacy>.

ARTICLE9, LLC PRIVACY POLICY

Version 1. Effective July 30, 2026.

Article9, LLC ("Article9," "we," "us") is a New Hampshire limited liability company with its principal place of business at 27 Whisper Dr, Bedford, New Hampshire 03110. This Policy explains what information we collect, why we hold it, how long we keep it, and who else touches it.

This Policy covers two different things, and the difference matters throughout.

The website is article9llc.com, including the pages describing the platform, the demo and quote forms, and the customer billing portal. Article9 decides what the website collects, and this Policy governs it.

The Platform is the hosted software a licensed labor organization uses to manage its representation work. The information inside it belongs to that organization, not to Article9, and our handling of it is governed by the Article9 License Agreement rather than by our own discretion. Where this Policy describes the Platform, it states what the Agreement already requires and cites the Section that requires it. If this Policy and the Agreement ever conflict, the Agreement controls.

1. WHAT THE WEBSITE COLLECTS

1.1 Information you send us on purpose. When you request a demo or a quote, we collect your name, your organization, your role, your region or local, your electronic mail address, and anything you write in the optional message field. We collect this because you asked us to respond to you, and we use it for that.

1.2 Sign-in information. If your organization has an account, we hold the electronic mail address you sign in with. If you set a password, we store only a salted script hash of it. We never store a password in a form we or anyone else can read, and we cannot tell you what your password is. When you sign in by emailed link, we store a hash of the single-use token and its expiry, not the link itself.

1.3 Session information. Signing in sets one cookie, named `a9_session`. It is signed, marked `httpOnly` so no script can read it, and expires after seven days. It exists to keep you signed in and does nothing else.

1.4 Billing information. For a customer account we hold the organization's legal name, billing address, billing contact address, tier, region, facility code where applicable, and the identifiers, status, and period dates of its Stripe subscription and invoices.

1.5 Records of agreement acceptance. When an Authorized Representative accepts the License Agreement, we record who accepted, the timestamp, the internet protocol address it came from, the version accepted, a cryptographic hash of the exact text accepted, and the facilities or region the acceptance covers. Section 27.5 of the Agreement requires us to keep exactly this and to give it to the organization on request, which we do from the billing portal.

1.6 Abuse prevention. To stop automated abuse of the sign-in and form endpoints we count requests against a salted hash of the requesting address. We keep the hash and not the address, and the hash cannot be reversed to recover it.

2. WHAT THE WEBSITE DOES NOT COLLECT

2.1 No payment details. Card and bank information is entered on pages hosted by Stripe and is never transmitted to or stored on our systems. We hold a Stripe customer identifier and the status of an invoice, and nothing that could be used to charge a card.

2.2 No analytics, advertising, or tracking. The website runs no analytics product, no advertising pixel, no session recorder, and no third-party script of any kind. It sets no cookie other than the session cookie described in Section 1.3, and it does not track you across other websites. There is no "do not track" setting for us to honor because there is nothing doing the tracking.

2.3 No selling of information, ever. We do not sell, rent, lease, or license information about you to anyone, for any purpose, at any price. This is not a preference we may revisit; for information held on the Platform it is a term of the Agreement at Section 5.4.

2.4 No secondary use. We do not use information collected through the website or the Platform for advertising or marketing, and we do not use one organization's information to benefit another.

3. THE PLATFORM: WHOSE INFORMATION IT IS

3.1 The organization owns it. Everything a labor organization or its representatives create or upload on the Platform belongs to that organization, and ownership follows the tier that created it: a facility's records belong to that facility, a region's to that region, a national office's to that national office. Article9 acquires no ownership interest. Agreement Sections 5.1 and 5.2.

3.2 What we may do with it. We hold a narrow license to host, store, transmit, back up, display, and process that information for three purposes only: to provide and support the Platform for the organization, to address technical or security problems, and to comply with law or valid legal process on the terms in Section 4 below. That license ends when our deletion obligations are complete. Agreement Sections 5.3 and 8.6.

3.3 Operational data. We collect data about how the Platform is used, in order to run, secure, and improve it. That data contains no organization records and does not identify any organization, any user, or any bargaining-unit employee. Agreement Section 5.5.

3.4 Member information. Grievance and discipline files describe individual bargaining-unit employees. Inside the Platform, access is scoped to a facility by default, and every consequential action is written to an audit log the region can read. Article9 personnel access an organization's records only as necessary to provide, secure, or support the Platform, and every such access is logged. Agreement Section 11.3.

4. WHO ELSE TOUCHES INFORMATION, AND WHO NEVER DOES

4.1 Service providers. We use a small number of providers to operate the service: a hosting and managed-database provider that runs the application and stores its data, Stripe for payment processing, and a transactional electronic mail provider that delivers sign-in links, invoices, and reminders. Each is bound in writing to confidentiality and security obligations no less protective than those we owe, and we remain fully responsible for their acts and omissions. Agreement Section 11.4.

4.2 Notice before a new provider. Before adding any provider that would process an organization's Platform information, we give that organization at least thirty days' written notice, and we maintain a current list of providers available on request. Agreement Section 11.4.

4.3 The employing agency, never. We will not license the Platform to, or provide substantially similar services for, a federal agency that employs the people an Article9 customer represents, during the Term and for two years after. We will not build or operate anything derived from the Platform to help an agency defend against grievances or other representational actions. We will not disclose an organization's information, or the existence or content of any matter in it, to any agency, agency management official, supervisor, agency contractor, or party adverse to that organization. Agreement Sections 14.1, 14.2, and 14.3.

4.4 Legal process. If we receive a subpoena, court order, discovery request, administrative demand, or other legal process seeking an organization's Platform information, then unless the law forbids it we will notify that organization in writing within two business days and before producing anything, give them a copy of the process, not oppose their efforts to quash or limit it, and produce only the portion we are legally required to produce. We do not respond to informal requests at all. Agreement Section 14.4.

5. HOW LONG WE KEEP THINGS

5.1 Demo and quote submissions. Kept only as long as needed to respond to the request and to maintain a record of the conversation, then deleted.

5.2 Platform information after a subscription ends. The organization may export its information at any time during the Term at no charge. If the subscription is not renewed, within thirty days after expiration we deliver a complete copy in two formats: a machine-readable structured export with all records, fields, metadata, timestamps, and audit-trail entries plus every original file and a manifest, and a human-readable set of Portable Document Format renderings mirroring the Platform's organization. Delivery goes to the officer of record for that tier. Agreement Sections 8.1 through 8.3.

5.3 We will not hold information hostage. Our obligation to return an organization's information is not conditioned on renewal, and we will not withhold, degrade, encrypt against, or delay it as leverage in a commercial negotiation. Agreement Section 8.4.

5.4 Deletion. We keep the information for sixty days after expiration so a replacement or supplemental export can be requested. After that window closes we permanently delete it from production systems, and within a further thirty days from backups, and we provide a written certification of deletion signed by an officer. Agreement Sections 8.5 and 8.6.

5.5 Acceptance records. Records of agreement acceptance are kept for the Term and seven years after, because they are the evidence of what was agreed and when. Agreement Section 27.5.

5.6 Records we must keep. We keep what law requires us to keep, including ordinary business and tax records. Anything retained after a deletion obligation remains subject to the same confidentiality and security duties for as long as we hold it. Agreement Section 8.6.

6. HOW WE PROTECT INFORMATION

6.1 Security program. We maintain a written information security program with administrative, technical, and physical safeguards designed to protect confidentiality, integrity, and availability. Agreement Section 11.1 and Exhibit A.

6.2 Encryption. Information is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 or a stronger algorithm. Agreement Section 11.2.

6.3 Access control. We enforce role-based access control, unique credentials, multi-factor authentication for administrative access, and least privilege. Agreement Section 11.3.

6.4 Testing. We perform, or engage a qualified third party to perform, a vulnerability assessment and a penetration test at least annually, and remediate findings on a risk-prioritized basis. A customer may request a summary of results. Agreement Sections 11.7 and 11.8.

6.5 Backups. We maintain encrypted backups, test restoration at least annually, and maintain a documented business continuity and disaster recovery plan. Agreement Section 11.6.

6.6 No absolute assurance. No security program eliminates risk, and we do not claim otherwise. What we commit to is the specific program above and the notification duties below.

7. IF SOMETHING GOES WRONG

7.1 What counts as an incident. Any unauthorized acquisition of, access to, use of, or disclosure of information in our possession or control, and any unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information within the meaning of RSA 359-C:19. Agreement Section 12.1.

7.2 When we tell you. Without unreasonable delay, and in any event within seventy-two hours after we become aware of it. Notice goes to the Authorized Representative by telephone and in writing. Agreement Section 12.2.

7.3 What the notice says. The nature and scope of the incident, the categories and approximate volume of information affected, the identified or suspected cause, the date or date range, the containment and remedial steps taken and planned, and a point of contact. We supplement the notice as further facts are established. Agreement Section 12.3.

7.4 Statutory notification. Where the affected personal information belongs to a customer, our role under RSA 359-C:20, paragraph I(c) is that of a maintainer, and we notify and cooperate with the owner immediately following discovery. Where the affected information is ours, we make the determination RSA 359-C:20, paragraph I(a) requires and give the notices that statute requires, including to the New Hampshire Attorney General's office. Agreement Section 12.4.

7.5 Cost. Where an incident arose from our breach of our security obligations, or from an act or omission of ours or of a provider we engaged, we bear the cost of notification, credit monitoring where appropriate, and remediation. Agreement Section 12.5.

7.6 Statutory rights are not waived. RSA 359-C:21 provides a private right of action and makes any attempted

waiver of it void. Nothing in this Policy or the Agreement waives or limits any right under it. Agreement Section 12.6.

8. REGULATORY POSITION

8.1 The Privacy Act. The Privacy Act of 1974, 5 U.S.C. 552a, restricts disclosure by federal agencies of records in a system of records, and reaches a contractor only where an agency provides by contract for the operation of a system of records on the agency's behalf. 5 U.S.C. 552a(m)(1). Article9 contracts with labor organizations, not with agencies, and no agency has designated the Platform as a system of records, so Article9 is not a Privacy Act contractor by operation of the Agreement. We nonetheless assume the contractual data protection obligations described in Sections 4, 6, and 7 above. A customer remains responsible for the lawfulness of its receipt of any agency data it uploads. Agreement Section 13.1.

8.2 New Hampshire RSA 507-H. Our present position is that RSA 507-H does not govern this relationship, because its definition of "consumer" excludes an individual acting in an employment or commercial capacity, RSA 507-H:1, paragraph VIII, and because RSA 507-H:3, paragraph I(b) exempts nonprofit organizations. We reassess that position annually and will comply with RSA 507-H if and when it becomes applicable. Agreement Section 13.2.

8.3 Health and financial information are out of scope. The Platform is not designed for and must not be used to process protected health information governed by 45 C.F.R. Parts 160 and 164, or nonpublic personal financial information governed by 15 U.S.C. 6801 through 6809. Where a customer needs the Platform to handle protected health information, a business associate agreement must be executed first, and nothing of that kind may be uploaded before it is. Agreement Section 13.3.

8.4 Accessibility. Section 508 of the Rehabilitation Act binds federal agencies rather than a private vendor selling to a non-federal buyer, but we design the Platform to conform to the Web Content Accessibility Guidelines, Version 2.1, Level AA. Agreement Section 13.5.

9. YOUR CHOICES

9.1 Reaching your own information. A customer organization can export everything it holds on the Platform at any time, from the Platform, at no charge. A signed-in billing contact can see their account details, invoices, and acceptance records in the portal, and download a signed copy of any agreement they accepted.

9.2 Correcting something. Write to us at the address in Section 11 and we will correct inaccurate account or contact information.

9.3 Deleting something. A demo or quote submission can be deleted on request. Platform information is deleted on the schedule in Section 5, or earlier on the organization's instruction, except where law requires us to keep it or where it is evidence of an agreement that was accepted.

9.4 Email you receive from us. Transactional messages, such as sign-in links, invoices, and payment reminders, are part of the service and are not marketing. We do not run marketing email campaigns, so there is no list to unsubscribe from.

10. OTHER MATTERS

10.1 Children. The Platform and the website are for use by labor organizations and their representatives in a professional capacity. They are not directed to children, and we do not knowingly collect information from anyone under sixteen.

10.2 Where information is held. Information is stored and processed in the United States.

10.3 Changes to this Policy. A change is published as a new numbered version of this Policy with its own effective date. A prior version remains available so it is possible to see what was in force at any time. A change that materially reduces the protections in this Policy will be notified to affected customer organizations in writing before it takes effect.

10.4 Relationship to the Agreement. For a licensed organization, the License Agreement governs. This Policy describes our practices and, where it addresses the Platform, restates duties the Agreement already imposes.

It does not reduce any right the Agreement grants, and to the extent of any conflict the Agreement controls.

11. HOW TO REACH US

Questions about this Policy, requests about information we hold, and requests for our current list of service providers should be sent to ops@article9llc.com, or by mail to Article9, LLC, 27 Whisper Dr, Bedford, New Hampshire 03110.

Notices under the License Agreement, including notices about a security incident, follow Section 26 of that Agreement.