Privacy Policy

Risk Data Analytics, Inc.

Last Modified: June 27, 2025

1. Introduction

Risk Data Analytics, Inc. ("RDA," "We," "Us," or "Company") respects your privacy and is committed to protecting it through our compliance with this Privacy Policy. This policy describes the types of information we may collect from you or that you may provide when you access, register with, or use our web portal (the "Portal") at www.riskdataanalytics.com and our mobile applications (the "Apps") (collectively, the "Services"), as well as our practices for collecting, using, maintaining, protecting, and disclosing that information.

This policy applies to information we collect:

- Through the Portal and Apps, including Certlok, Certlok SOS, and LiftAlert Authenticator.
- In email, text, and other electronic communications sent through or in connection with the Services.

For the Certlok SOS App, accounts are created and managed by a third-party licensing company (e.g., your employer or organization) as part of a licensed product. The licensing company owns the account data and is responsible for account management, including deletion requests. Users of Certlok SOS are provided access to the App as a tool by the licensing company, and data deletion requests are handled through the processes described in Section 7. Certain data, such as location information and incident-related data collected via Certlok SOS or LiftAlert, may be retained for legal purposes, as described in Sections 3 and 7.

This policy does not apply to information collected by third parties, who may have their own privacy policies, which we encourage you to review before providing information to them (see Section 6, Third-Party Information Collection).

By accessing, registering with, or using our Services, you consent to this Privacy Policy. Please read it carefully to understand our policies and practices regarding your information. If you do not agree with these policies, do not use our Services. This policy may change over time (see Section 10, Changes to Our Privacy Policy), and your continued use of the Services after such changes indicates your acceptance of the updates.

2. Children Under the Age of 16

Our Services are not intended for children under 16 years of age. We do not knowingly collect personal information from children under 16 without verifiable parental consent. If we learn we have collected such information, we will delete it promptly. If you believe we may have information from or about a child under 16, please contact us at support@riskdataanalytics.com.

3. Information We Collect and How We Collect It

We collect information from and about users of our Services:

- Directly from you when you provide it.
- Automatically as you use the Portal or Apps.

3.1 Information You Provide to Us

When you register with, access, or use the Services, we may collect:

- **Personal Information**: Information by which you may be identified, such as your name, email address, phone number, postal address, or other details necessary for our Services (e.g., credentials or account-related data). For Certlok SOS, this information is typically provided by the licensing company that manages your account.
- **Submitted Content**: Information you upload, such as documents, photos, credential
- **Incident-Related Data**: For Certlok SOS and LiftAlert, data related to incidents (e.g., location information, user details, or data from the Incident Alert or Incident Management applets in Certlok SOS) that is necessary to provide services or required for legal purposes, such as supporting insurance claims or attorney-client privilege, as described in Section 7.
- **Electronic Data Streams**: Part of the Services provided includes the monitoring of your activity through sensors when operating equipment utilizing LiftAlert technology, which may include operational or safety-related data linked to your account. Non-incident-related data may be anonymized upon deletion, as described in Section 7.
- **Correspondence**: Records of your communications with us, including email addresses and phone numbers, when you contact us or report issues.
- **Survey Responses**: Information you provide in surveys we may conduct for research purposes.

This information is collected when you:

- Register for or modify your account (for Certlok and LiftAlert Authenticator) or when the licensing company sets up your account (for Certlok SOS).
- Use forms within the Services.
- Upload content for management, storage, or synchronization.
- Utilize a piece of equipment which has our LiftAlert technology installed.

3.2 Information Collected Automatically

We use technology to automatically collect:

- **Usage Details**: Data about your interaction with the Services, such as log data, accessed resources, and usage patterns.
- **Device Information**: Details about your device, including unique device identifiers, IP address, operating system, browser type, and mobile network information.

- **Stored Information**: Metadata or data associated with files on your device (e.g., photos or contacts), if accessed by the App with your permission.
- **Location Information**: For Certlok SOS and LiftAlert, location data is mandatory to provide services (e.g., incident tracking and safety monitoring). This data may be retained for legal purposes, such as insurance claims or attorney-client privilege, as described in Section 7.

Technologies used include:

- **Cookies**: Small files placed on your device to enhance functionality. You may disable cookies, but this could limit access to certain features.

4. How We Use Your Information

We use the information we collect to:

- Provide, maintain, and improve the Services and their contents.
- Fulfill requests for products, services, or information you seek.
- Carry out obligations and enforce rights from agreements between you and RDA or, for Certlok SOS, the licensing company.
- Notify you of updates to the Services or changes to our offerings.
- Estimate audience size, analyze usage patterns, and personalize your experience.
- Contact you regarding service updates or promotional information (you may opt out of promotional messages, though service-related notices will continue).

5. Disclosure of Your Information

We may disclose:

- **Aggregated or Anonymized Data**: Information that does not identify individuals, without restriction. This includes anonymized LiftAlert sensor data used for safety analytics or equipment performance monitoring, which is not shared with third parties in identifiable form.
- **Personal Information**: For Certlok and LiftAlert Authenticator, with your explicit consent, as managed through the opt-in and opt-out settings in your user profile, we may share your personal information (e.g., name, email, credentials, or uploaded content) with third parties, such as unions, previous employers, or companies, exclusively through our paid CertLok Connect platform. For Certlok SOS, personal information provided by the licensing company may be accessible to third parties (e.g., your employer or union) through CertLok Connect if the licensing company has enabled such sharing and holds a valid license. Third parties must have a valid CertLok Connect license to access your data, which allows them to view or add to your data for purposes such as employment-related services, certification verification, or job opportunity screening. For example, a union you are a member of or a company posting job openings on CertLok Connect may

access your data if sharing is enabled and they have a license. For Certlok and LiftAlert Authenticator, you can modify these sharing preferences at any time in your profile settings within the Apps or Portal, and opting out immediately revokes third-party access to your data. For Certlok SOS, data sharing is managed by the licensing company, and you may contact them to modify sharing preferences. Incident-related data required for legal purposes (e.g., insurance claims, attorney-client privilege) may be retained and shared with relevant parties as required by law, as described in Section 7. We also may disclose personal information:

  - To subsidiaries, affiliates, and trusted contractors or service providers bound by confidentiality obligations, solely for supporting our Services.
  - To a successor entity in the event of a merger, acquisition, bankruptcy, or similar business transition, where your information is among transferred assets.
  - To fulfill the purpose for which you provided it, or with your consent.
  - To comply with legal obligations, court orders, or government requests.
  - To protect the rights, property, or safety of RDA, our users, or others.

We do not sell your personal information to third parties.

6. Third-Party Information Collection

Our Services may involve third-party services (e.g., cloud storage, certification providers, location providers, or the CertLok Connect platform). The CertLok Connect platform facilitates controlled data sharing with third parties (e.g., unions, employers, or, for Certlok SOS, the licensing company) based on your opt-in consent (for Certlok and LiftAlert Authenticator) or the licensing company's settings (for Certlok SOS). Incident-related data required for legal purposes may be shared with relevant parties (e.g., insurance providers, legal counsel) as described in Section 7. These third parties may collect or process information according to their own privacy policies, over which we have no control. We encourage you to review their policies before opting in to data sharing or using Certlok SOS.

7. Accessing, Updating, and Deleting Your Information

- **Access and Updates**: For Certlok and LiftAlert Authenticator, you can review and modify your personal information, including data sharing preferences, by logging into your account on the Portal or Apps and adjusting your profile settings. In your profile settings, you may opt in or opt out of sharing your personal information (e.g., name, email, credentials, or uploaded content) with third parties, such as unions, previous employers, or companies, through the CertLok Connect platform. Only third parties with a valid CertLok Connect license can access your data if you opt in, and opting out immediately revokes their ability to view or add to your data. These preferences can be changed at any time. For Certlok SOS, your account and data sharing preferences are managed by the licensing company (e.g., your

employer or organization). To update your information or modify sharing preferences, contact the licensing company directly or, if directed by them, reach out to us at support@riskdataanalytics.com.

- **Deletion**:
  - **Certlok and LiftAlert Authenticator**: You may request deletion of your account and associated personal data directly within the Apps via the "Delete Account" option in the account settings menu. Alternatively, you can submit a deletion request through our web portal at `www.riskdataanalytics.com/delete-account`. Upon receiving your request, we will verify your identity (e.g., via email or phone confirmation) and process the deletion within 30 days, unless a longer period is required by applicable law. This process includes:
    * Deleting your personal information (e.g., name, email, uploaded content) not related to incidents from our systems and revoking access by third parties through the CertLok Connect platform. We will notify third parties with whom you opted to share data (e.g., unions, employers) to delete your data or confirm that access has been revoked, unless they are legally required to retain it.
    * Anonymizing any personal identifiers linked to non-incident-related LiftAlert sensor data to ensure it cannot be associated with you. Anonymized sensor data may be retained for legitimate business purposes, such as equipment safety analytics or performance monitoring, as permitted by law.
    * Retaining incident-related data (e.g., location information, user details from Incident Alert or Incident Management applets) if required for legal purposes, such as insurance claims or attorney-client privilege. We will inform you of any such retention at the time of your request.
  - **Certlok SOS**: Since your account is created and owned by the licensing company, deletion requests must be initiated through the licensing company, which is responsible for managing your data. You may submit a deletion request within the Certlok SOS App via the "Request Data Deletion" option in the account settings menu, which will direct you to contact the licensing company or submit a request through our web portal at `www.riskdataanalytics.com/delete-account`. We will forward your request to the licensing company for processing within 30 days, unless a longer period is required by law. This process includes:
    * Deleting your personal information not related to incidents from our systems (where applicable) and revoking third-party access via CertLok Connect.
    * Anonymizing personal identifiers linked to non-incident-related LiftAlert sensor data, with anonymized data retained for legitimate business purposes.
    * Retaining incident-related data (e.g., location information, user details from Incident Alert or Incident Management applets) if required for legal purposes, such as insurance claims or attorney-client privilege. The licensing company will be notified to retain

such data as required by law.

You will receive confirmation via email once the deletion and anonymization process is complete, including details of any retained incident-related data, anonymized non-incident data, and the status of third-party access revocation.

If you use Sign in with Apple, we will revoke associated tokens upon deletion. For further assistance, contact us at support@riskdataanalytics.com.

- **Limitations**: We or the licensing company may retain certain information as required by law or for legitimate business purposes (e.g., incident-related data for insurance claims or attorney-client privilege, anonymized LiftAlert sensor data for safety analytics). We will inform you of any such retention at the time of your deletion request.

8. Your State Privacy Rights

Residents of certain states, such as California, may have additional rights under state privacy laws (e.g., California Consumer Privacy Act). Visit `https://oag.ca.gov/privacy/ccpa` for more details.

9. Data Security

We implement industry-standard measures, such as SSL encryption (2048-bit RSA and 256-bit AES), to protect your information from unauthorized access, use, or disclosure during transmission and storage. However, no internet or mobile transmission is entirely secure, and we cannot guarantee absolute security. You are responsible for safeguarding any access codes we provide, and any transmission is at your own risk.

If we detect a security risk (e.g., system vulnerabilities), we may notify you via email or a Portal announcement.

10. Changes to Our Privacy Policy

We may update this Privacy Policy to reflect changes in our Services, business, or legal requirements. Material changes will be posted on the Portal homepage or communicated directly to you. The last modification date appears at the top. Your continued use of the Services after updates signifies acceptance. If you disagree, please discontinue use and request account deletion as described in Section 7.

11. Contact Information

For questions or comments about this Privacy Policy, contact us at:
Risk Data Analytics, Inc.
Email: support@riskdataanalytics.com
Phone: [208-269-3390]