Data Processing Addendum

Last Updated: November 2nd, 2025

This Data Processing Addendum ("DPA") is between your organization ("Customer") and AIncident ("Processor"). This DPA explains how we handle personal data you provide through our incident reporting platform (the "Service") and is part of our Terms of Service agreement.

1. Simple Definitions

- **Personal Data:** Any information about an identified or identifiable person, like names, contact details, voice recordings, location data, and incident report content.
- **Processing:** Any operation we perform on personal data, like collecting, storing, using, or deleting it.
- **Controller:** The entity (you) that decides what personal data to collect and how to use it.
- **Processor:** The entity (us) that handles personal data on your behalf.
- **Subprocessor:** Third-party services we use to help process your data (like AWS for storage or Twilio for voice processing).
- **Data Subject:** An individual person whose personal data is being processed.
- **Security Incident:** Any unauthorized access, loss, or breach of personal data.

2. Our Roles

You Are the Controller

You decide:

- What personal data to collect from your employees and staff
- Why you're collecting it
- How long to keep it
- What to do with it

You're responsible for:

- Making sure you have legal permission to collect the data
- Getting necessary consents from your employees
- Telling employees how their data will be used
- Following privacy laws like CCPA
- Responding to employee requests about their data

We Are the Processor

We handle your data according to your instructions. We will:

- Only use your data to provide the service
- Follow this DPA and applicable laws
- Not use your data for our own purposes
- Not sell or share your data with others

3. How We Use Your Data

You authorize us to process personal data to:

- Operate the incident reporting platform

- Create AI summaries of incident reports
- Process and transcribe voice recordings
- Store incident data and location information
- Send notifications to your designated users
- Provide customer support
- Maintain security and prevent abuse
- Comply with legal obligations

If you give us instructions that we believe violate privacy laws, we'll let you know and won't follow those instructions until the issue is resolved.

4. Security Measures

We protect your data with:

Access Controls:

- Only authorized personnel can access data
- Multi-factor authentication for admin accounts
- Unique login credentials for each user
- Regular access reviews
- Immediate access removal when employees leave

Encryption:

- Data is encrypted when transmitted over the internet
- Data is encrypted when stored on our servers
- Secure key management

Infrastructure Security:

- Secure AWS hosting in U.S. data centers
- Firewalls and intrusion detection
- Regular security testing
- Secure backup procedures

Monitoring:

- Security event monitoring and logging
- Automated threat detection
- Regular security audits

Personnel:

- Background checks for employees with data access (where legal)
- Confidentiality agreements for all staff
- Regular security training
- Clear incident response procedures

SOC 2 Compliance

We maintain SOC 2 Type II certification. You can request a summary of our most recent audit report once per year.

Security Updates

We may update our security measures to respond to new threats. Any updates will maintain at least the same level of protection. If we make changes that reduce security, we'll notify you in advance.

5. Our Subprocessors

We use these trusted partners to process your data:

Partner	What They Do	Location
Amazon Web Services (AWS)	Cloud storage and hosting	United St
Twilio Inc.	Voice call and SMS processing and routing	United St
OpenAI, L.L.C.	AI-powered summaries (zero data retention)	United St
Stripe, Inc.	Payment processing	United St
Google LLC	Website analytics	United St

Our Responsibilities

We ensure that:

- Each subprocessor signs agreements to protect your data
- Subprocessors follow appropriate security standards
- We remain responsible for what our subprocessors do

Changes to Subprocessors

We'll give you 30 days' notice before:

- Adding a new subprocessor
- Replacing an existing subprocessor
- Making major changes to how a subprocessor is used

Notice will be sent to your admin email or shown in your account dashboard.

If You Object

If you have concerns about a new subprocessor based on data protection issues, notify us in writing within 15 days. Include specific reasons related to data protection.

We'll work with you to find a solution, which might include:

- Addressing your concerns with additional safeguards
- Finding an alternative solution
- Allowing you to stop using the specific feature requiring that subprocessor

If we can't resolve your concerns within 30 days, you can terminate the affected part of the service and get a refund for prepaid fees. This is your only remedy for subprocessor objections.

6. Employee Rights Requests

Helping You Respond

We'll help you respond to requests from your employees to:

- Access their personal data
- Correct inaccurate information

- Delete their data
- Restrict how their data is processed
- Get a copy of their data
- Object to certain processing
- Opt out of specific uses

How It Works
If we receive a request directly from one of your employees, we will:

- Forward it to you within 5 business days
- Not respond without your permission
- Help you respond using our service features

Important Note About Data Ownership
Because incident reports belong to your organization (not individual employees), requests from Managers or Users to delete incident reports they created may not be fulfilled. The organization retains ownership of that data.

Tools We Provide
Our service includes features to help you fulfill employee rights:

- Data export functionality
- Account deletion capabilities
- Tools to correct inaccurate information
- Access controls to manage data access

7. Security Incidents

We'll Notify You
If we discover a security incident affecting your personal data, we will:

- Notify you without undue delay after we become aware
- Send notification to your admin contact via email
- Include available information about what happened, what data was affected, how many employees may be impacted, and what we're doing about it

What We'll Do
After a security incident, we will:

- Investigate promptly
- Take steps to fix the cause
- Implement measures to prevent similar incidents
- Cooperate with your reasonable requests for information
- Document the incident and our response

Your Responsibilities
You're responsible for:

- Deciding if you need to notify affected employees

- Deciding if you need to notify government authorities
- Making any required notifications under privacy laws
- Following breach notification requirements

Important
Our notification doesn't mean we admit fault or liability. "Without undue delay" takes into account factors like investigating the incident and restoring security.

8. Data Location

U.S. Storage Only
All personal data is processed and stored in the United States:

- Primary storage in AWS us-west region
- Planned expansion to AWS us-east region
- No international transfers

Future International Transfers
If we ever need to transfer data outside the U.S., we will:

- Notify you in advance
- Put appropriate safeguards in place
- Get your consent if required
- Ensure adequate protection

9. How Long We Keep Data

Active Accounts

- Incident reports and text: 7 years
- Voice recordings: 3 years
- Text transcripts: 7 years
- Account information: While subscription is active
- Payment records: 7 years (legal requirement)

After Termination
When your service ends or you request deletion:

- We stop processing (except for deletion)
- We delete or return data as you direct within 30 days
- Backups are deleted within 7 days
- We provide written confirmation if requested

Legal Holds
We may keep data longer if:

- Required by law
- Needed for legal proceedings
- Subject to government investigation
- Required by regulatory retention rules

Data kept for legal reasons will be isolated and not used for other purposes.

Anonymized Data
We may keep anonymized and aggregated data that doesn't identify individuals after the retention periods. This data isn't considered personal data and may be used for analytics and service improvement.

10. Audits and Compliance

Records We Keep
We maintain records of:

- What categories of data we process
- Why we process it
- Which subprocessors we use
- What security measures we have
- Any data transfers
- Our retention practices

Your Audit Rights
Once per year, you may:

- Request information showing we comply with this DPA
- Review our SOC 2 reports and security documentation
- Conduct audits of our data processing

Audits must:

- Happen during normal business hours
- Have at least 30 days' advance notice
- Include appropriate confidentiality agreements
- Not disrupt our operations
- Be at your expense

Alternative to On-Site Audits
Instead of visiting our facilities, we can provide:

- Recent SOC 2 audit reports
- Security questionnaire responses
- Compliance certifications
- Other documentation showing compliance

This documentation satisfies your audit rights if it adequately demonstrates our compliance.

11. California Consumer Privacy Act (CCPA)

Our CCPA Role and Certification
Under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

- We are a "service provider" as defined under California Civil Code § 1798.140(ag)
- You are a "business" as defined under California Civil Code § 1798.140(d)
- This DPA constitutes your instructions for how we process personal information

Service Provider Certification
We certify and warrant that we understand the restrictions in California Civil Code § 1798.140(ag) and will comply with them. Specifically, we certify that we will not:

1. **Sell or Share Personal Information**
   - We will not "sell" personal information as defined in Cal. Civ. Code § 1798.140(ad)
   - We will not "share" personal information for cross-context behavioral advertising as defined in Cal. Civ. Code § 1798.140(ah)
2. **Limit Use to Business Purpose**
   - We will retain, use, and disclose personal information only for the specific business purpose of performing the services specified in this DPA and our Terms of Service
   - We will not retain, use, or disclose personal information for any commercial purpose other than providing the services to you
   - We will not retain, use, or disclose personal information outside of the direct business relationship between us
3. **No Unauthorized Combination**
   - We will not combine personal information that we receive from or on behalf of you with personal information that we receive from or on behalf of another person or persons, or collect from our own interaction with consumers
   - Exception: We may combine personal information to perform any business purpose as defined in regulations adopted pursuant to Cal. Civ. Code § 1798.185, or as otherwise permitted by the CCPA

Important Legal Notice Regarding Service Provider Status
Ongoing Compliance: This certification is made as of the effective date of this DPA based on our current business practices and understanding of CCPA requirements. We have implemented policies and procedures designed to maintain service provider status under CCPA.

Your Responsibility: As the business, you are responsible for:

- Ensuring your own CCPA compliance
- Verifying that our role as service provider is appropriate for your use case
- Providing any required consumer notices about our processing activities
- Ensuring your instructions to us comply with CCPA requirements

Changes in Law: CCPA regulations continue to evolve through California Attorney General rulemaking and court interpretations. We will make commercially reasonable efforts to maintain compliance with CCPA as it evolves, and we will notify you of any material changes to our practices that could affect our service provider status.

If Our Practices Change: If we make any changes to our data practices that would affect our status as a service provider under CCPA, we will provide you with at least 30 days' advance notice and an opportunity to terminate the affected services.

Legal Review Recommended: Because CCPA interpretation is evolving and your specific circumstances may affect our service provider relationship, we recommend you consult with legal counsel to confirm that our relationship structure meets your CCPA compliance needs.

Supporting Consumer Rights
We'll help you respond to California consumer requests for:

- Information about what data is collected
- Access to personal data
- Deletion of data
- Correction of inaccurate data
- Opt-out of sale or sharing (not applicable since we don't sell)

CCPA Verification
Upon request, we'll provide written confirmation that we're complying with CCPA requirements.

12. Liability

Our Responsibilities
We're responsible for:

- Our own actions in processing your data
- Our subprocessors' actions (as if we did them ourselves)
- Security incidents caused by our failure to maintain proper security

Subject to the liability limits in our Terms of Service.

Your Responsibilities
You acknowledge that you're responsible for:

- Determining if it's legal to collect and process the data
- Getting necessary consents from employees
- Providing accurate and legal data to us
- Following privacy laws in your use of the service
- Responding to employee requests and government inquiries

Liability Limitations
Nothing in this DPA limits liability for:

- Fraud
- Gross negligence or willful misconduct
- Privacy law violations
- Matters that can't be limited under law

Otherwise, liability is subject to the limits in our Terms of Service.

13. Term and Changes

When This DPA Applies
This DPA starts when you begin using the service and continues until:

- Your service ends, or
- All data processing is complete and all data is deleted

Some sections survive termination, including data retention, audits, liability, and general provisions.

Updates to This DPA

We may update this DPA to reflect:

- Changes in privacy laws
- New regulatory requirements
- Industry standards and best practices
- Security improvements

We'll give you at least 30 days' notice of material changes. Continued use after changes take effect means you accept them.

Other Terms

If this DPA conflicts with our Terms of Service, this DPA controls for personal data processing.

This DPA, the Terms of Service, and Privacy Policy make up the complete agreement about data processing.

This DPA is governed by California law (same as our Terms of Service).

14. Contact Information

For questions about this DPA or data processing:

AIncident Privacy Team
Email: privacy@aincident.io
Contact Form: https://aincident.io/contact

Appendix: Details About Data Processing

Who We Process Data About

- Your employees and personnel
- Managers and supervisors
- On-site staff and security personnel
- People who create incident reports
- People mentioned in incident reports

What Personal Data We Process

Identity Information:

- Names
- Employee IDs
- Job titles and roles

Contact Information:

- Email addresses
- Phone numbers

Login Information:

- Account credentials
- Authentication data

Voice and Audio:

- Voice recordings of incident reports
- Audio files

Location Information:

- GPS coordinates
- Location assignments
- Geolocation data

Incident Information:

- Report descriptions
- Narratives and details
- Summaries

Visual Information:

- Photos and images

Technical Information:

- IP addresses
- Device information
- Usage logs

Payment Information:

- Billing details (processed by Stripe)

Sensitive Data

Our service isn't designed to collect sensitive data. However, employees might accidentally include:

- Social Security numbers
- Financial account numbers
- Health information
- Biometric data
- Information about children

You're responsible for instructing users not to include unnecessary sensitive data.

Why We Process Data

- Incident reporting and documentation
- Incident management and tracking
- AI-powered summarization
- Voice recording and transcription
- Location tracking and mapping
- User notifications and alerts
- Multi-location management
- Login and authentication
- Customer support
- Service improvement

- Payment processing
- Legal compliance and security

How We Process Data

- Collecting and recording
- Organizing and storing
- Retrieving and viewing
- Using and analyzing (including AI processing)
- Transmitting and routing
- Restricting and deleting

How Long We Process Data

Personal data is processed for the durations specified in Section 9 (How Long We Keep Data) of this DPA.

Our Subprocessors

See Section 5 (Our Subprocessors) for the complete list.

Your Acknowledgment

By using the service, you acknowledge that you have read, understood, and agree to this Data Processing Addendum. You confirm that:

- You understand your role as the Controller
- You will obtain necessary consents from employees
- You will follow applicable privacy laws
- You understand how we process personal data
- You accept the terms of this DPA