AlertOwl

Data Processing Agreement (DPA)

Version 2.0 | March 2026
Friday Surprise LLC
Launch Markets: Germany, UAE, UK, USA
CONFIDENTIAL

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Terms of Service between Friday Surprise LLC, operating as AlertOwl ("Processor", "we", "us"), and the entity agreeing to these terms ("Controller", "Customer", "you").

This DPA applies to the extent that AlertOwl processes Personal Data on behalf of the Customer in the course of providing the AlertOwl service. This DPA is designed to comply with the EU General Data Protection Regulation (GDPR), the UK General Data Protection Regulation and Data Protection Act 2018 (UK GDPR), the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021, "PDPL"), and applicable US state privacy laws including the California Consumer Privacy Act as amended by the CPRA ("CCPA").

1. Definitions

- "Personal Data" means any information relating to an identified or identifiable natural person, as defined under applicable Data Protection Law.
- "Processing" means any operation performed on Personal Data, including collection, storage, classification, transfer, and deletion.
- "Sub-processor" means any third party engaged by AlertOwl to process Personal Data on behalf of the Customer.
- "Data Subject" means the individual to whom the Personal Data relates.
- "Data Protection Law" means, as applicable to the processing: (a) EU GDPR (Regulation 2016/679); (b) UK GDPR and the Data Protection Act 2018; (c) UAE PDPL (Federal Decree-Law No. 45/2021); (d) CCPA/CPRA (California Civil Code 1798.100 et seq.); and (e) any other applicable data protection legislation.
- "Supervisory Authority" means any competent data protection authority, including the relevant EU Member State authority, the UK Information Commissioner's Office (ICO), the UAE Data Office, and the California Attorney General.

2. Scope of Processing

2.1 Subject Matter

AlertOwl processes email messages and metadata from the Customer's connected email accounts (Gmail, Outlook) for the purpose of AI-powered classification and alert delivery via WhatsApp.

2.2 Categories of Data Subjects

- Persons who send emails to the Customer's connected email accounts
- The Customer's employees or agents who use AlertOwl

2.3 Types of Personal Data

- Email metadata: sender address, recipient address, subject line, timestamps
- Email content: message body text (processed transiently for classification, then permanently masked)

- Contact information: Customer's email address, WhatsApp phone number
- Account data: name, timezone, language preference
- Billing data: processed by Stripe (AlertOwl does not store payment card details)

2.4 Purpose and Legal Basis

Processing is performed solely to provide the AlertOwl service. The legal basis for processing is:

- EU/UK GDPR: Performance of a contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f))
- UAE PDPL: Performance of a contract and explicit consent obtained during onboarding
- CCPA: Business purpose (service provision) as defined in Cal. Civ. Code 1798.140(e)

3. Processor Obligations

1. Process Personal Data only on documented instructions from the Controller (i.e., the service agreement and this DPA)
2. Ensure personnel with access to Personal Data are bound by confidentiality obligations
3. Implement appropriate technical and organizational security measures (see Section 6)
4. Assist the Controller in responding to Data Subject rights requests under any applicable jurisdiction
5. Delete or return all Personal Data upon termination of the service, at the Controller's choice
6. Make available all information necessary to demonstrate compliance and allow for audits
7. Notify the Controller without undue delay upon becoming aware of a Personal Data breach
8. Conduct Data Protection Impact Assessments where required by applicable law (see Section 8)

4. Sub-processors

The Customer authorizes the use of the following sub-processors:

Sub-processor	Purpose	Location	Data Processed	Certifications
Supabase Inc.	Database hosting	USA (AWS)	All stored data	SOC 2, HIPAA-ready
DigitalOcean LLC	Server hosting	Germany (FRA1)	Email data in transit	SOC 2, ISO 27001
Twilio Inc.	WhatsApp delivery	USA	Phone numbers, alert content	SOC 2, ISO 27001
Anthropic PBC	AI classification	USA	Email content (transient, zero retention)	SOC 2

Resend Inc.	Email delivery	USA	Email addresses, digest content	SOC 2
Stripe Inc.	Payment processing	USA	Billing information	PCI DSS L1, SOC 2
Cloudflare Inc.	DNS and CDN	Global	Routing metadata	SOC 2, ISO 27001

AlertOwl will notify the Customer at least 14 days before engaging any new sub-processor, providing the Customer an opportunity to object. If the Customer objects on reasonable data protection grounds, AlertOwl will work with the Customer to find an alternative or the Customer may terminate the affected service.

5. International Data Transfers

5.1 EU/EEA Transfers

Where Personal Data is transferred from the EU/EEA to the United States, AlertOwl relies on:

- The EU-US Data Privacy Framework (DPF) for certified sub-processors
- Standard Contractual Clauses (SCCs) as adopted by the European Commission (Decision 2021/914) as a fallback safeguard

The SCCs are incorporated by reference into this DPA and shall apply to all transfers not covered by an adequacy decision.

5.2 UK Transfers

For transfers from the UK, AlertOwl relies on:

- The UK adequacy decision for the EU/EEA (renewed through December 2031)
- The UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs for transfers to the USA

5.3 UAE Transfers

For transfers from the UAE, AlertOwl relies on:

- Contractual safeguards modelled on international standards (as the UAE Data Office has not yet published standard contractual clauses or an adequacy list)
- The Customer's explicit consent to cross-border transfer obtained during onboarding
- The necessity of transfer for the performance of the contract between AlertOwl and the Customer

AlertOwl documents the legal basis for each cross-border data flow and maintains these records for audit purposes, in accordance with Articles 22-23 of the PDPL.

5.4 US Transfers

For processing of Personal Data of US residents, AlertOwl complies with applicable state privacy laws. AlertOwl does not sell Personal Data and does not share Personal Data for cross-context behavioral advertising.

6. Security Measures

AlertOwl implements the following technical and organizational measures across all jurisdictions:

- Encryption in transit: TLS 1.2+ on all connections
- Encryption at rest: AES-256 on database storage (managed by Supabase)
- Access control: Row-Level Security (RLS) on all database tables ensuring tenant isolation
- Authentication: OAuth 2.0 for email connections, bcrypt-hashed passwords for accounts
- Data minimization: email content is permanently masked immediately after AI classification
- Retention controls: configurable per customer (default 30 days), with automatic purge
- Audit logging: all significant actions logged with timestamps in audit_logs table
- Monitoring: real-time error tracking via Sentry
- Backup: automated daily database backups with 7-day retention (Supabase Pro)
- Incident response: documented Incident Response Plan with defined severity levels and notification procedures

7. Data Subject Rights

7.1 Universal Rights

AlertOwl assists the Customer in fulfilling Data Subject requests. Under all applicable laws, data subjects may exercise rights including access, rectification, erasure, and data portability. Customers can exercise these rights via the AlertOwl dashboard or by contacting privacy@alertowl.ai.

7.2 Jurisdiction-Specific Rights

EU/UK GDPR:

- Right to access, rectification, erasure, restriction, portability, and objection
- Right not to be subject to automated decision-making (AlertOwl's AI classification is advisory, not automated decision-making with legal effects)
- Response time: within 30 days of verified request

UAE PDPL:

- Right to access, correct, erase, restrict, and object to processing
- Right to data portability
- Right to withdraw consent at any time
- Response time: as specified by the UAE Data Office (expected within 30 days)

CCPA/CPRA (California):

- Right to know what Personal Information is collected, used, and disclosed
- Right to delete Personal Information

- Right to opt-out of the sale or sharing of Personal Information (AlertOwl does not sell or share)
- Right to non-discrimination for exercising privacy rights
- Response time: within 45 days of verified request

8. Data Protection Impact Assessment (DPIA)

AlertOwl has conducted a Data Protection Impact Assessment covering its core processing activities. This DPIA is available upon request and covers:

- The nature, scope, context, and purposes of processing
- Necessity and proportionality assessment
- Risks to the rights and freedoms of data subjects
- Measures to address identified risks

This DPIA satisfies requirements under EU GDPR Article 35, UK GDPR Article 35, and UAE PDPL DPIA requirements. It is reviewed annually or upon any significant change in processing activities.

9. Breach Notification

9.1 Notification to Customer

AlertOwl will notify the Customer without undue delay (and in any event within 48 hours) after becoming aware of a Personal Data breach. Notification will include:

- The nature of the breach, including categories and approximate number of data subjects affected
- The likely consequences of the breach
- Measures taken or proposed to address the breach
- Contact details for further information

9.2 Regulatory Notification (Customer Responsibility)

The Customer, as data controller, is responsible for notifying the relevant Supervisory Authority where required:

- EU GDPR: relevant supervisory authority within 72 hours (Article 33)
- UK GDPR: ICO within 72 hours (Article 33 UK GDPR)
- UAE PDPL: UAE Data Office immediately (interpreted as within 72 hours)
- CCPA: California Attorney General where required by law

AlertOwl will provide all necessary information and assistance to enable the Customer to fulfill these notification obligations.

10. Data Retention and Deletion

- Email content: permanently masked immediately after AI classification (replaced with "[Content removed for privacy]")
- Email metadata and classification results: retained per Customer setting (default 30 days)
- Account data: retained for the duration of the service agreement
- Upon termination: all Customer data deleted within 30 days unless retention is required by applicable law
- Account deletion: available via dashboard. Soft delete with 7-day grace period, followed by permanent cascading deletion of all customer data including OAuth tokens, messages, settings, and rules

11. Audit Rights

The Customer may, upon reasonable notice and at the Customer's expense, audit AlertOwl's compliance with this DPA. AlertOwl will cooperate with such audits and provide access to relevant documentation, systems, and personnel. Where possible, AlertOwl will satisfy audit requests through the provision of compliance reports and certifications rather than on-site audits.

12. Term and Termination

This DPA is effective for the duration of the service agreement. Upon termination, AlertOwl will delete all Customer Personal Data within 30 days, unless retention is required by applicable law. The Customer may request a data export before termination.

13. Governing Law

This DPA is governed by:

- For EU data subjects: the laws of the Federal Republic of Germany
- For UK data subjects: the laws of England and Wales
- For UAE data subjects: the laws of the United Arab Emirates
- For US data subjects: the laws of the State of Delaware, USA

Where a conflict exists between this DPA and the Terms of Service, this DPA shall prevail with respect to data protection matters.

By using the AlertOwl service, the Customer acknowledges and agrees to this Data Processing Agreement.

Friday Surprise LLC, operating as AlertOwl

Contact: privacy@alertowl.ai

Website: https://alertowl.ai/legal.html

Document Control

Version	Date	Author	Changes
1.0	February 2026	Ali Munir	Initial version (GDPR only)
2.0	March 2026	Ali Munir	Multi-jurisdiction: added UK GDPR, UAE PDPL, CCPA. Added DPIA reference, cross-border transfer mechanisms, jurisdiction-specific rights.