

FACTCheckDining, Inc. – PRIVACY POLICY

Effective Date: January 3, 2025

Last Updated: January 3, 2025

1. OVERVIEW

This Privacy Policy ("Policy") explains how FACTCheckDining, Inc., a Delaware corporation ("FACTCheckDining," "we," "us," or "our"), collects, uses, stores, discloses, protects, and monetizes personal information obtained through your use of our website, iOS application, Android application (Google Play), and related services (collectively, the "Services").

By accessing or using the Services, you acknowledge and consent to the practices described in this Policy. If you do not agree with this Policy, you must immediately discontinue use of the Services.

Our primary goals in collecting your information are to:

- Deliver a secure, personalized, and allergy-conscious dining experience
- Improve our allergy recognition technology and AI/ML algorithms
- Advance food safety innovation through aggregated insights
- Generate commercial value through data analytics, research, and strategic partnerships

IMPORTANT: We reserve broad rights to use, process, analyze, and commercialize data collected through the Services, subject to the terms outlined in this Policy.

2. INFORMATION WE COLLECT

We collect the following categories of information directly from you, automatically through your interaction with the Services, and from third-party sources:

A. IDENTIFYING INFORMATION

- Full Name (First Name, Last Name)
- Display Name / Username
- Email Address
- Phone Number (optional for enhanced account security)
- Date of Birth or Age Range (e.g., 18-24, 25-34, 35-44, 45-54, 55-64, 65+)
- Gender (male, female, non-binary, prefer not to say, or custom)

- Device identifiers (Apple IDFA, Google Advertising ID, device UUID)
- Account credentials and authentication tokens

B. LOCATION DATA

- Default Location (manually entered address, city, state, ZIP code, country)
- Real-time geolocation data (when location services are enabled on iOS or Android devices)
- Location history and search patterns
- IP address and derived location data
- Proximity to restaurants and affiliate locations

C. AFFILIATE INFORMATION

- Default Institution (name of affiliated organization, e.g., "High School")
- Institution Type (e.g., Collegiate, High School, K-12, Hospital, Senior Living, Corporate)
- Role or affiliation status (e.g., student, employee, patient, resident, visitor)
- Meal plan information (if provided by affiliate or user)
- Cafeteria or dining hall usage patterns

D. REASON FOR JOINING

User-selected reason for using the Services, including:

- "I have food allergies"
- "I manage food allergies for someone else" (caregiver role)
- "I have dietary restrictions"
- "I want to explore dietary options"
- Custom or other reasons

E. HEALTH-RELATED AND DIETARY INFORMATION

1. Food Allergies:

We collect information about your food allergies, including:

- **Common Allergens:** Milk, Egg, Fish, Shellfish, Tree Nuts, Peanuts, Wheat, Soy, Sesame, Gluten
- **Custom Allergens:** User-defined allergens not in the common list (e.g., "Chickpea," "Mustard," "Nightshades," "Corn")
- **Allergy Severity Levels:** For each allergen, you may indicate the severity:
 - **Anaphylaxis** (life-threatening, requires immediate medical attention)
 - **Severe** (serious symptoms requiring medical intervention)
 - **Moderate** (noticeable symptoms causing significant discomfort)
 - **Mild** (minor discomfort or symptoms)
 - **Avoidance** (preference-based avoidance without medical symptoms)
 - **Dietary Choice** (voluntary exclusion for non-medical reasons)

- **Reaction History and Medical Notes:** If you provide additional details about your allergy history, symptoms, or medical recommendations

2. Dietary Restrictions:

We collect information about your dietary restrictions, organized by category:

LIFESTYLE:

- **Pescatarian:** Vegetarian diet that includes fish and seafood
- **Vegan:** No animal products including meat, dairy, eggs, and honey
- **Vegetarian:** No meat or fish, but may include dairy and eggs

RELIGIOUS:

- **Halal:** Follows Islamic dietary laws for permissible foods
- **Hindu:** No beef, often vegetarian. Some traditions avoid onion and garlic.
- **Kosher:** Follows Jewish dietary laws including food preparation

HEALTH:

- **Dairy-Free:** No dairy products including milk, cheese, and butter
- **Gluten-Free:** No gluten-containing grains like wheat, barley, and rye
- **Keto:** Low carbohydrate, high fat diet for ketosis
- **Low-Sodium:** Restricted sodium intake for heart and blood pressure health
- **Paleo:** Whole foods diet based on paleolithic eating patterns

Note: Additional dietary restrictions may be available for selection or may be added based on user feedback and product development.

3. Cross-Reference and Overlap:

We understand that dietary restrictions and food allergies may overlap (e.g., a user with a dairy allergy may also select "Dairy-Free" and "Vegan"). We collect both to:

- Provide comprehensive filtering that accounts for both medical and lifestyle preferences
- Improve accuracy of menu recommendations
- Train AI/ML models to understand the relationship between allergies and dietary choices
- Generate insights on how users manage overlapping dietary needs

F. FAVORITE RESTAURANTS AND USAGE DATA

- Saved or favorited restaurants (name, address, rating, price range)
- Restaurant menu interactions (views, clicks, item selections)

- Restaurant search history and query patterns
- Menu item preferences and selections
- Session duration, frequency of use, and engagement metrics

G. PLATFORM AND USAGE DATA

- Device type, make, model, operating system (iOS version, Android version, web browser)
- Browser type, version, and user agent string
- IP address and network connection type
- App version, build number, and installation identifier
- Click patterns, navigation paths, and feature usage
- Search queries (restaurant names, locations, dietary filters)
- Time zone, language preferences, and regional settings
- Session recordings and interaction heatmaps (via Microsoft Clarity)

H. USER-SUBMITTED CONTENT

- Feedback, reviews, comments, and ratings
- Photos of food, menus, or restaurant environments
- Communications with customer support
- Survey responses and product feedback
- Social media interactions related to the Services

I. THIRD-PARTY AND PUBLICLY AVAILABLE DATA

We may enhance the data we collect by cross-referencing or integrating:

- Publicly available information from social media profiles, directories, or public records
- Data from third-party partners, data brokers, or marketing analytics providers
- Restaurant and affiliate menu data from public sources, APIs, or direct integrations
- Demographic, psychographic, and behavioral data from data enrichment services

3. HOW WE COLLECT INFORMATION

A. DIRECT COLLECTION

Information you provide when you:

- Create an account or complete your profile
- Enter personal information (name, email, display name, age range, gender)
- Select your default location
- Enter affiliate information (default institution, institution type)

- Select your reason for joining
- Add or modify food allergies (including custom allergens and severity levels)
- Select or update dietary restrictions
- Save favorite restaurants
- Search for restaurants or view affiliate menus
- Enable location services on your device
- Contact customer support or submit feedback
- Participate in surveys, promotions, or research studies

B. AUTOMATIC COLLECTION

Information collected automatically through:

1. Cookies and Tracking Technologies:

We use cookies, web beacons, pixel tags, local storage, and similar technologies to track user behavior, preferences, and session data.

2. Analytics Services:

- **Google Analytics:** Web and mobile app analytics, user demographics, behavior flow, conversion tracking, cross-device tracking, and remarketing
- **Microsoft Clarity:** Session recordings, heatmaps, click tracking, scroll depth analysis, and user interaction analysis
- **Cloudflare Analytics:** Performance monitoring, bot detection, traffic analysis, security event logging, and DDoS mitigation

3. Mobile SDKs:

iOS and Android SDKs may collect device information, crash reports, performance metrics, push notification tokens, and usage statistics.

4. Server Logs:

IP addresses, request timestamps, HTTP headers, referrer URLs, request methods, response codes, and error logs.

C. THIRD-PARTY SOURCES

- Data from affiliate partners (e.g., institutional dining providers sharing meal plan or access information)
 - Data from restaurant partners (e.g., menu updates, ingredient changes, promotional offers)
 - Data from third-party APIs (e.g., Google Places, mapping services, nutrition databases)
 - Publicly available data from social media platforms, review sites, or public records
 - Data brokers and marketing analytics providers
-

4. HOW WE USE YOUR INFORMATION

We process personal data for the following purposes:

A. SERVICE DELIVERY AND PERSONALIZATION

- Display safety warnings (e.g., "Very Limited Choices," "Contains: Egg, Mustard, Sesame")
- Provide personalized restaurant and affiliate menu recommendations
- Enable allergy filtering based on your allergen profile (common allergens, custom allergens, severity levels)
- Enable dietary restriction filtering based on your selected preferences (lifestyle, religious, health)
- Maintain your favorite restaurants list across devices
- Customize user experience based on historical behavior, default location, and affiliate information
- Send account notifications, updates, and service announcements
- Synchronize allergen settings and dietary preferences across all devices (iOS, Android, web)

B. RESEARCH, ANALYTICS, AND AI/ML DEVELOPMENT

1. Train and improve machine learning models for:

- Allergy recognition and ingredient analysis
- Custom allergen detection and classification
- Dietary restriction classification and menu parsing
- Natural language processing for user queries
- Predictive modeling for allergen risk assessment
- Severity-based risk scoring (Anaphylaxis, Severe, Moderate, Mild, Avoidance, Dietary Choice)
- Restaurant safety scoring and recommendation algorithms

2. Conduct internal research and product development:

- Test new features, algorithms, and user interfaces
- Analyze usage patterns and feature adoption
- Identify trends in food allergies (including custom allergens) and dietary restrictions
- Benchmark platform performance and reliability
- Evaluate affiliate program effectiveness and institutional engagement

3. Generate aggregated insights:

- Location-based usage trends and demand forecasting
- Demographic analysis of allergy prevalence by age range, gender, and geography
- Dietary preference trends across regions, institutions, or demographics
- Restaurant and affiliate performance metrics
- Custom allergen frequency and emerging allergen trends
- Severity distribution analysis (Anaphylaxis vs. Mild vs. Avoidance)

C. COMMERCIAL USE AND MONETIZATION

We reserve the right to use collected data for commercial purposes, including but not limited to:

1. Data Sales and Licensing:

- Selling anonymized, pseudonymized, or aggregated datasets to third parties, including:
 - Food manufacturers and restaurant chains
 - Pharmaceutical companies and medical device manufacturers
 - Research institutions and universities
 - Market research firms and data analytics companies
 - Insurance companies and healthcare providers
 - Government agencies and public health organizations
- Licensing data for commercial research, product development, or market analysis
- Providing custom data reports and insights to paying clients

2. Advertising and Marketing:

- Targeted advertising based on user profiles, allergen data, dietary restrictions, location, age range, gender, and behavior
- Promotional campaigns and partnerships with restaurants, affiliates, or food brands
- Retargeting users across third-party platforms (e.g., Google Ads, Facebook Ads, programmatic ad networks)
- Building lookalike audiences for customer acquisition campaigns
- Delivering location-based offers and promotions

3. Business Intelligence and Consulting:

- Providing insights to restaurants and affiliates to improve menu offerings, allergen management, and customer satisfaction
- Offering data-driven consulting services to food industry stakeholders
- Benchmarking institutional dining programs against industry standards
- Analyzing favorite restaurant trends and competitive dynamics

D. COMPLIANCE, LEGAL, AND SECURITY

- Comply with legal obligations, subpoenas, court orders, or lawful requests from government agencies
- Enforce these Terms and Conditions and our Privacy Policy
- Investigate and prevent fraud, abuse, security threats, or illegal activity
- Protect the rights, property, and safety of FACTCheckDining, our users, and the public
- Respond to data subject access requests and privacy rights inquiries
- Maintain audit trails and compliance documentation

E. COMMUNICATIONS AND ENGAGEMENT

- Send transactional emails (e.g., account verification, password resets, allergen setting confirmations)
 - Send marketing emails, newsletters, and promotional offers (you may opt out at any time)
 - Conduct surveys, research studies, or user feedback campaigns
 - Provide customer support and respond to inquiries
 - Notify users of menu updates at favorite restaurants
 - Alert users to allergen-related safety recalls or warnings
-

5. INFORMATION SHARING AND DISCLOSURE

We may disclose your information in the following circumstances:

A. SERVICE PROVIDERS AND VENDORS

We share data with third-party service providers who perform functions on our behalf, including:

- **Cloud hosting and infrastructure:** AWS, Google Cloud, Microsoft Azure, Railway
- **Analytics and tracking:** Google Analytics, Microsoft Clarity, Cloudflare
- **Email and communication platforms:** Godaddy, Microsoft Outlook
- **Marketing and advertising platforms:** Google Ads, Facebook Ads, programmatic ad networks
- **Data enrichment and enhancement services**
- **AI/ML model training platforms**

Service providers are contractually obligated to use data only for the purposes we specify and to maintain appropriate security measures. However, we are not responsible for their independent data practices.

B. BUSINESS PARTNERS AND AFFILIATES

1. Restaurant Partners:

We may share aggregated, anonymized, or individual-level data with restaurant partners to:

- Help them understand allergen demand and dietary restriction trends
- Improve menu offerings and allergen disclosures
- Provide insights on customer satisfaction and safety ratings
- Enable targeted marketing and promotional campaigns

2. Affiliate Program Participants:

We may share user data with institutional dining providers (e.g., universities, hospitals, senior living facilities) to:

- Enable menu access and meal plan integration
- Provide usage analytics and engagement metrics
- Support allergen management and dietary accommodation programs

- Facilitate communication about menu changes or safety alerts

3. Corporate Affiliates:

We may share data with parent companies, subsidiaries, or affiliated entities for internal business purposes, including product development, marketing, and research.

C. COMMERCIAL TRANSACTIONS AND ASSET SALES

In connection with any merger, acquisition, asset sale, corporate reorganization, bankruptcy, or business transition:

- **User data (including personally identifiable information, health data, allergen profiles, dietary restrictions, favorite restaurants, location data, and usage data) may be transferred, sold, or assigned as part of the transaction.**
- The acquiring entity will assume the rights and obligations under this Privacy Policy unless you are notified otherwise.
- We may conduct due diligence by sharing data with potential acquirers, investors, or advisors under confidentiality agreements.

D. DATA SALES AND LICENSING

We reserve the right to sell, license, or monetize data in the following forms:

1. Anonymized Data:

Data that has been stripped of direct identifiers (e.g., name, email, phone number) but may still include:

- Age range (e.g., 18-24)
- Gender
- Default location (city, state, ZIP code)
- Allergen profiles (including custom allergens and severity levels)
- Dietary restrictions
- Favorite restaurants and menu interaction patterns
- Affiliate information (institution type, role)
- Reason for joining

2. Pseudonymized Data:

Data linked to a unique identifier (e.g., hashed user ID, device ID) rather than direct personal identifiers.

3. Aggregated Data:

Data combined across multiple users to produce statistical summaries, trends, or insights (e.g., "30% of users aged 18-24 in Ohio have peanut allergies with Anaphylaxis severity").

IMPORTANT: While we take commercially reasonable steps to de-identify or aggregate data before sale or licensing, **there is a risk that data could be re-identified by third parties using advanced**

techniques, external datasets, or by combining multiple data sources. By using the Services, you acknowledge and accept this risk.

Examples of data commercialization include:

- Licensing allergen prevalence datasets to pharmaceutical companies developing allergy treatments
- Selling dietary restriction trend data to food manufacturers for product development
- Providing location-based allergen demand data to restaurant chains for menu planning
- Sharing custom allergen frequency data with research institutions studying emerging allergies

E. ADVERTISING AND MARKETING PARTNERS

We may share data with advertising networks, demand-side platforms (DSPs), and marketing analytics providers to:

- Deliver targeted advertisements based on user profiles, allergen data, dietary restrictions, location, age range, gender, and behavior
- Retarget users across third-party websites and apps
- Measure ad performance, conversion rates, and return on investment (ROI)
- Build lookalike audiences for customer acquisition campaigns
- Enable dynamic creative optimization (DCO) based on allergen profiles

Data shared may include:

- Device identifiers (IDFA, Google Advertising ID)
- Age range and gender
- Default location
- Allergen profiles and dietary restrictions
- Restaurant search and menu interaction patterns
- Favorite restaurants

F. RESEARCH INSTITUTIONS AND ACADEMIC PARTNERS

We may share de-identified, pseudonymized, or aggregated data with universities, research institutions, or public health organizations for:

- Epidemiological research on food allergies and dietary trends
- Development of public health interventions or educational programs
- Academic publications, conferences, or white papers
- Clinical trials or studies on allergen immunotherapy
- Analysis of custom allergen emergence and severity patterns

G. LEGAL AND REGULATORY DISCLOSURES

We may disclose your information to:

- Comply with subpoenas, court orders, legal processes, or lawful government requests
- Enforce our Terms and Conditions or investigate violations
- Protect the rights, property, or safety of FACTCheckDining, our users, or the public
- Respond to emergencies involving imminent harm to persons or property
- Cooperate with law enforcement or regulatory investigations
- Meet data breach notification requirements under applicable laws

H. WITH YOUR CONSENT

We may share your information with third parties for purposes not described in this Policy if we obtain your explicit consent.

6. LEGAL BASIS FOR PROCESSING

Our processing activities are supported by the following legal bases:

A. CONSENT

You provide explicit consent by:

- Creating an account and accepting this Privacy Policy
- Entering allergen information (including custom allergens and severity levels)
- Selecting dietary restrictions
- Saving favorite restaurants
- Enabling location services on your device
- Opting in to marketing communications
- Agreeing to specific data processing activities (e.g., participation in research studies)

You may withdraw consent at any time by contacting us at info@factcheckdining.com. However, withdrawal of consent may limit your ability to use certain features of the Services (e.g., allergy filtering, dietary restriction filtering, personalized recommendations).

B. CONTRACTUAL NECESSITY

Processing is necessary to provide the Services you requested, including:

- Account creation and authentication
- Personalized allergy and dietary filtering
- Restaurant and affiliate menu recommendations
- Synchronization of settings across devices
- Customer support and communications

C. LEGAL OBLIGATIONS

Processing is necessary to comply with applicable laws, regulations, or legal processes, including:

- Tax reporting and financial compliance
- Responding to subpoenas or court orders
- Meeting data breach notification requirements
- Cooperating with law enforcement or regulatory investigations
- Complying with health information privacy laws (where applicable)

D. LEGITIMATE INTERESTS

We process data based on our legitimate interests in:

- Improving the Services and developing new features
- Conducting research and analytics to enhance allergy recognition technology
- Training AI/ML models for allergen detection and dietary classification
- Preventing fraud, abuse, and security threats
- Marketing and promoting the Services
- Generating commercial value through data monetization
- Advancing food safety innovation and public health research

We balance these interests against your privacy rights and do not process data in ways that would be unexpected or harmful to you.

7. SPECIAL CATEGORIES OF INFORMATION (HEALTH DATA)

A. SENSITIVE PERSONAL DATA

Some information you provide qualifies as **sensitive personal data** under applicable privacy laws, including:

- Food allergy information (common allergens, custom allergens, severity levels)
- Medical conditions requiring dietary modifications
- Dietary restrictions related to health conditions (e.g., Gluten-Free for celiac disease, Low-Sodium for hypertension)
- Reason for joining (e.g., "I have food allergies," "I manage food allergies for someone else")

This information is:

- Collected only with your explicit consent

- Used to enhance the allergy-conscious features of our Services
- Protected by heightened technical and administrative safeguards
- May be shared in de-identified, pseudonymized, or aggregated form for commercial purposes, research, or analytics

B. CONSENT TO PROCESS SENSITIVE INFORMATION

By voluntarily submitting health-related or dietary data, you consent to our use of this information for:

- Personalization of recommendations and allergy/dietary filtering
- Reducing allergen risk in food discovery
- Platform performance analytics and user experience optimization
- Research and development in de-identified, pseudonymized, or aggregated form
- Commercial sale or licensing of de-identified or aggregated datasets
- Training AI/ML models for allergen recognition and dietary classification

You understand and acknowledge that:

- Custom allergens you create may be used to improve allergen detection algorithms
- Severity level selections (Anaphylaxis, Severe, Moderate, Mild, Avoidance, Dietary Choice) may be used for risk scoring and research
- Favorite restaurant data may be combined with allergen profiles for trend analysis
- Affiliate information may be linked to allergen and dietary data for institutional insights

You may modify or delete this information by:

- Editing your profile through the Services
- Contacting us at info@factcheckdining.com with the subject line: "Data Request – [Your Full Name]"

C. HIPAA DISCLAIMER

FACTCheckDining is NOT a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act (HIPAA). The Services are not subject to HIPAA regulations, and health information you provide is not protected by HIPAA. By using the Services, you acknowledge that your health-related data is governed solely by this Privacy Policy and applicable consumer privacy laws.

8. LOCATION DATA

A. COLLECTION AND USE

We collect and use location data to:

- Provide regional restaurant and affiliate menu recommendations
- Improve search relevance based on proximity
- Analyze geographic trends in allergy prevalence and dietary preferences
- Deliver location-based advertising and promotions
- Conduct market research and demand forecasting
- Enable real-time navigation and directions to restaurants

B. TYPES OF LOCATION DATA

- **Manual Entry:** Default location you manually enter (address, city, state, ZIP code)
- **Device-Based Geolocation:** Precise GPS coordinates (latitude/longitude) when you enable location services on your iOS or Android device
- **IP-Based Geolocation:** Approximate location derived from your IP address
- **Wi-Fi and Cell Tower Data:** Location inferred from nearby Wi-Fi access points or cell towers

C. LOCATION SHARING AND COMMERCIALIZATION

Location data may be used in aggregated, de-identified, or pseudonymized form for:

- Commercial sale or licensing to third parties (e.g., market research firms, real estate developers, food industry stakeholders, urban planners)
- Demographic research and trend analysis (e.g., "allergen prevalence in Chagrin Falls, OH")
- Advertising targeting and campaign optimization
- Restaurant and affiliate site selection and expansion planning

D. CONTROLLING LOCATION SERVICES

You can control location permissions through your device settings:

- **iOS:** Settings > Privacy & Security > Location Services > FACTCheckDining
- **Android:** Settings > Location > App Permissions > FACTCheckDining

Options:

- **Never:** Disable location access entirely
- **While Using the App:** Allow location access only when the app is open
- **Always:** Allow continuous background location tracking

Disabling location services may limit the functionality of the Services, including restaurant search, proximity-based filtering, and location-based recommendations.

9. TRACKING TECHNOLOGIES AND THIRD-PARTY ANALYTICS

A. COOKIES AND SIMILAR TECHNOLOGIES

We use cookies, web beacons, pixel tags, local storage, and similar technologies to:

- Authenticate users and maintain session state
- Remember user preferences and settings (e.g., allergen profiles, dietary restrictions, favorite restaurants)
- Track user behavior, clicks, and navigation patterns
- Measure ad performance and conversion rates
- Enable retargeting and personalized advertising
- Analyze traffic sources and user demographics

Types of cookies we use:

- **Essential Cookies:** Required for core functionality (e.g., login, session management)
- **Analytics Cookies:** Used to understand user behavior and improve the Services
- **Advertising Cookies:** Used for targeted advertising and retargeting campaigns
- **Third-Party Cookies:** Placed by third-party services (Google Analytics, Microsoft Clarity, Cloudflare, ad networks)

B. THIRD-PARTY ANALYTICS SERVICES

1. Google Analytics:

- **Data Collected:** Page views, session duration, bounce rate, user demographics (age, gender), interests, device type, operating system, browser, location, traffic sources, conversion events
- **Purpose:** Web and mobile app analytics, behavior flow analysis, cross-device tracking, remarketing, lookalike audience building
- **Data Sharing:** Google may use this data for its own purposes, including improving its services and delivering targeted advertising
- **Opt-Out:** <https://tools.google.com/dlpage/gaoptout>

2. Microsoft Clarity:

- **Data Collected:** Session recordings, heatmaps, click tracking, scroll depth, rage clicks, dead clicks, user frustration signals, form interactions, page performance metrics
- **Purpose:** User experience analysis, bug identification, conversion rate optimization, A/B testing insights
- **Data Sharing:** Microsoft may use this data to improve its services
- **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>

3. Cloudflare Analytics:

- **Data Collected:** IP addresses, request metadata, HTTP headers, referrer URLs, bot detection signals, security events (DDoS attacks, malicious traffic), performance metrics (page load times, bandwidth usage)
- **Purpose:** Performance monitoring, bot detection, traffic analysis, security event logging, DDoS mitigation, content delivery optimization
- **Data Sharing:** Cloudflare processes data as a service provider
- **Privacy Policy:** <https://www.cloudflare.com/privacypolicy/>

C. MOBILE SDKs

Our iOS and Android applications may include third-party SDKs that collect:

- Device information (make, model, operating system version)
- App version and build number
- Crash reports and error logs
- Performance metrics (CPU usage, memory usage, battery impact)
- Push notification tokens
- Advertising identifiers (IDFA, Google Advertising ID)
- Usage statistics and event tracking

Third-party SDKs may include:

- Google Firebase (analytics, crash reporting, cloud messaging)
- Facebook SDK (analytics, advertising, login)
- Amplitude (product analytics)
- Segment (customer data platform)

Each SDK has its own privacy policy, and you should review them independently.

D. CONTROLLING COOKIES AND TRACKING

Web Browsers:

- Adjust cookie settings in your browser preferences
- Enable "Do Not Track" signals (note: we do not currently respond to Do Not Track signals)
- Use browser extensions to block trackers (e.g., Privacy Badger, uBlock Origin)

Mobile Devices:

- **iOS:** Settings > Privacy & Security > Tracking > Allow Apps to Request to Track (toggle off)
- **iOS:** Settings > Privacy & Security > Apple Advertising > Personalized Ads (toggle off)
- **Android:** Settings > Google > Ads > Opt out of Ads Personalization

Note: Disabling cookies or tracking may limit the functionality of the Services.

10. DATA SECURITY

A. SECURITY MEASURES

We implement commercially reasonable technical, administrative, and physical safeguards to protect your data, including:

Technical Safeguards:

- Encryption of data in transit using TLS/SSL
- Encryption of sensitive data at rest (e.g., passwords)
- Secure authentication mechanisms (password hashing, multi-factor authentication)
- Regular security audits and vulnerability assessments
- Intrusion detection and prevention systems
- DDoS and Turnstile protection via Cloudflare

Administrative Safeguards:

- Employee training on data protection and privacy
- Role-based access controls and least privilege principles
- Background checks for personnel with access to sensitive data
- Incident response and breach notification procedures

Physical Safeguards:

- Secure data centers with restricted physical access
- Environmental controls (fire suppression, climate control)
- Redundant power and network infrastructure

B. LIMITATIONS OF SECURITY

No system can guarantee 100% security. By using the Services, you acknowledge the inherent risks of online data transmission and storage, including:

- Unauthorized access by hackers or malicious actors
- Data breaches or security incidents
- Interception of data during transmission
- Insider threats or employee misconduct
- Third-party service provider breaches

We are not liable for:

- Security breaches caused by third-party service providers

- Unauthorized access resulting from user negligence (e.g., weak passwords, sharing credentials)
- Data loss or corruption due to force majeure events (natural disasters, cyberattacks, infrastructure failures)

C. DATA BREACH NOTIFICATION

In the event of a data breach involving your personal information, we will:

- Investigate the breach and assess its scope and impact
- Notify affected users via email within the timeframe required by applicable law (typically 72 hours for EU users, varies by U.S. state)
- Provide information about the breach, including:
 - Types of data affected
 - Potential risks and consequences
 - Steps we are taking to mitigate harm
 - Recommendations for protecting yourself (e.g., changing passwords, monitoring accounts)
- Notify regulatory authorities as required by law

We are not liable for damages resulting from data breaches, except as required by applicable law. Our liability is limited as described in Section 8 of our Terms and Conditions.

11. DATA RETENTION

A. RETENTION PERIODS

We retain your personal information as long as needed to fulfill the purposes described in this Policy, unless a longer retention period is required or permitted by law.

Retention guidelines:

- **Account Data:** Retained for the duration of your account plus 90 days after deletion (to accommodate re-activation requests)
- **Allergen and Dietary Data:** Retained for the duration of your account plus 180 days after deletion (for research and analytics)
- **Usage Data:** Retained for up to 2 years for analytics and product improvement
- **Transaction Data:** Retained for 7 years for tax and financial compliance
- **Communications:** Retained for up to 3 years for customer support and legal purposes
- **De-identified or Aggregated Data:** Retained indefinitely for research, analytics, and commercial use

Backup and Archival:

- Backup copies of data may be retained for up to 90 days for disaster recovery purposes
- Anonymized or de-identified versions may be stored indefinitely for auditing, integrity, and security purposes

B. DATA DELETION

Upon account deletion, we will:

- Remove your account from active databases within 90 days
- Delete or anonymize your personal information (name, email, display name)
- **Retain allergen profiles, dietary restrictions, location data, and usage data in de-identified or aggregated form for research and commercial use**

Data that may NOT be deleted upon account deletion:

- Data already sold, licensed, or shared with third parties in de-identified or aggregated form
- Data required for legal, regulatory, or contractual obligations
- Backup or archival copies retained for disaster recovery
- Data involved in ongoing disputes, investigations, or litigation

C. DELETION REQUESTS

To request account deletion or data deletion, contact us at:

Email: info@factcheckdining.com

Subject Line: "Data Deletion Request – [Your Full Name]"

Include:

- Your full name
- Email address associated with your account
- Specific data you wish to delete (if not requesting full account deletion)

We will respond within 30 days and may require identity verification before processing your request.

12. YOUR RIGHTS AND CHOICES

A. ACCESS AND PORTABILITY

You have the right to:

- **Access:** Request a copy of the personal information we hold about you
- **Portability:** Receive your data in a structured, machine-readable format (e.g., JSON, CSV)

To exercise these rights, contact us at:

Email: info@factcheckdining.com

Subject Line: "Data Access Request – [Your Full Name]"

We will provide your data within 30 days, subject to identity verification.

B. CORRECTION AND UPDATE

You may correct or update your information by:

- Editing your profile through the Services (Personal Information, Affiliate Information, Additional Information, Allergies, Dietary Restrictions, Favorite Restaurants)
- Contacting us at info@factcheckdining.com

C. DELETION AND ERASURE

You may request deletion of your account or specific data by contacting us at info@factcheckdining.com. See Section 11(C) for details.

Note: Deletion may not apply to data already sold, licensed, or shared in de-identified or aggregated form.

D. RESTRICTION AND OBJECTION

You may request to:

- **Restrict processing:** Limit how we use your data (e.g., suspend marketing communications)
- **Object to processing:** Object to specific uses of your data (e.g., data sales, targeted advertising)

Contact us at info@factcheckdining.com with your request. We will evaluate your request and respond within 30 days.

Note: Restricting or objecting to processing may limit your ability to use certain features of the Services.

E. WITHDRAW CONSENT

You may withdraw consent at any time by:

- Disabling location services on your device
- Opting out of marketing communications (click "unsubscribe" in emails)
- Deleting your account
- Contacting us at info@factcheckdining.com

Withdrawal of consent does not affect the lawfulness of processing conducted prior to withdrawal.

F. OPT-OUT OF DATA SALES

Under certain U.S. state privacy laws (e.g., California CCPA, Virginia VCDPA), you may have the right to opt out of the "sale" or "sharing" of your personal information.

To opt out, contact us at:

Email: info@factcheckdining.com

Subject Line: "Do Not Sell My Personal Information – [Your Full Name]"

Note: Opting out of data sales may not apply to:

- Data already sold or licensed before your opt-out request
- De-identified or aggregated data that cannot reasonably be linked back to you
- Data shared with service providers for operational purposes (not considered a "sale")

G. CALIFORNIA PRIVACY RIGHTS

California residents have additional rights under the California Consumer Privacy Act (CCPA):

- Right to know what personal information is collected, used, disclosed, or sold
- Right to delete personal information (subject to exceptions)
- Right to opt out of the sale or sharing of personal information
- Right to non-discrimination for exercising privacy rights
- Right to limit use of sensitive personal information

California "Shine the Light" Law:

California residents may request a list of third parties to whom we disclosed personal information for direct marketing purposes in the prior calendar year.

To exercise your California rights, contact us at info@factcheckdining.com.

H. EUROPEAN ECONOMIC AREA (EEA) AND UK RIGHTS

EEA and UK residents have rights under the General Data Protection Regulation (GDPR) and UK GDPR:

- Right of access, rectification, erasure, restriction, and portability
- Right to object to processing based on legitimate interests
- Right to withdraw consent
- Right to lodge a complaint with a supervisory authority (e.g., ICO in the UK)

Data Transfers:

We transfer data from the EEA and UK to the United States and other countries. We rely on:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions (where applicable)
- Your explicit consent

By using the Services, you consent to international data transfers.

13. CHILDREN'S PRIVACY

A. AGE REQUIREMENTS

The Services are not intended for children under **13 years of age**. We do not knowingly collect personal information from children under 13 without verifiable parental consent.

If you are under 18, you may only use the Services with the involvement and consent of a parent or legal guardian.

B. PARENTAL CONSENT

If we learn that we have collected personal information from a child under 13 without verifiable parental consent, we will:

- Delete the information promptly
- Terminate the account
- Notify the parent or guardian (if contact information is available)

Parents or guardians may request access to, correction of, or deletion of their child's information by contacting us at info@factcheckdining.com.

C. VERIFICATION

We may request proof of age or parental consent if we suspect a user is under 13 or using the Services without proper authorization.

14. INTERNATIONAL USERS

A. DATA TRANSFERS

If you are located outside the United States, please be aware that your data will be transferred to, stored in, and processed in the United States and other countries where our service providers operate.

By using our Services, you consent to this transfer and acknowledge that:

- U.S. data protection standards may differ from those in your jurisdiction
- Your data may be subject to U.S. government surveillance or legal processes

- We take commercially reasonable steps to protect your data, but cannot guarantee the same level of protection as in your home country

B. LEGAL BASIS FOR TRANSFERS

We rely on the following mechanisms for international data transfers:

- **Standard Contractual Clauses (SCCs):** Approved by the European Commission for transfers from the EEA to third countries
- **Adequacy Decisions:** Where the European Commission has determined that a country provides adequate data protection
- **Consent:** Your explicit consent to the transfer
- **Performance of Contract:** Where the transfer is necessary to provide the Services

C. EEA AND UK DATA PROTECTION OFFICER

For questions about data protection or to exercise your GDPR rights, contact:

Email: info@factcheckdining.com

Subject Line: "GDPR Inquiry – [Your Full Name]"

15. CHANGES TO THIS POLICY

We reserve the right to modify this Privacy Policy at any time. We will provide notice of material changes by:

- Posting an updated version on our website with a new "Last Updated" date
- Sending an email notification to your registered email address (if applicable)
- Displaying an in-app notification upon your next login

Changes become effective thirty (30) days after notice is provided, except for changes required by law, which may be effective immediately.

Your continued use of the Services after the effective date constitutes acceptance of the revised Policy. If you do not agree to the changes, you must discontinue use of the Services and may request account deletion.

Material changes include:

- Expansion of data collection categories
- Introduction of new uses or disclosures
- Changes to data retention periods
- Changes to your rights or choices

We encourage you to review this Policy periodically to stay informed about our data practices.

16. CONTACT INFORMATION

For questions, privacy requests, or to withdraw consent, please contact:

FACTCheckDining, Inc.

A Delaware Corporation

Email: info@factcheckdining.com

Subject Line: "Privacy Inquiry – [Topic]"

For specific requests, use these subject lines:

- "Data Access Request – [Your Full Name]"
- "Data Deletion Request – [Your Full Name]"
- "Do Not Sell My Personal Information – [Your Full Name]"
- "GDPR Inquiry – [Your Full Name]"
- "COPPA/Parental Consent – [Child's Full Name]"

We will respond to all requests within **30 days** (or as required by applicable law) and may require identity verification before processing your request.

END OF PRIVACY POLICY