

# Privacy Policy

Sift: Product Scanner & Analysis App | Operated by Sift App

Limited Last updated: 12 February 2026 | Effective date: 12 February 2026

## PREAMBLE

Sift App Limited ("Sift", "we", "us", or "our") is committed to protecting your privacy and personal data. This Privacy Policy explains how we collect, use, store, share, and protect your information when you use the Sift mobile application (the "App") and related services.

This Privacy Policy forms an integral part of the Terms and Conditions of Use.

By using the App, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with this Privacy Policy, you must not use the App.

## 1. SCOPE OF THIS PRIVACY POLICY

This Privacy Policy applies to:

- All users of the Sift App, whether accessing free or paid features
- Users located in the United Kingdom, European Union, European Economic Area, United States, and all other jurisdictions where the App is available
- All personal data collected through the App, our website (sift-scanner.com), and related communications

Where local law provides stronger privacy rights than those described in this Policy, those rights shall prevail.

## 2. DATA CONTROLLER

For the purposes of applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), and the Data Protection Act 2018, the data controller is:

**Company Name:** Sift App Limited

**Registered Address:** [INSERT REGISTERED ADDRESS]

**Email:** info@sift-scanner.com

**Country:** United Kingdom

**Data Protection Contact:** info@sift-scanner.com

If you have any questions or concerns about how your personal data is processed, or wish to exercise your data protection rights, please contact us using the details above.

### 3. PERSONAL DATA WE COLLECT

We apply a data minimisation principle and only collect data that is necessary to operate, maintain, and improve the App.

#### 3.1 Information You Provide Directly

When you create an account or use the App, you may provide:

- **Account Information:** Name and email address, provided directly or via third-party authentication (Apple Sign In, Google Sign In)
- **User Content:** Images of products, product names or identifiers entered manually, barcode scans, and search queries
- **Communications:** Any information you provide when contacting us for support or feedback

We do not require users to provide sensitive personal data (also known as special category data).

#### 3.2 Automatically Collected Information

When you use the App, we may automatically collect:

- **Device Information:** Device type, model, operating system version, unique device identifiers
- **App Usage Data:** Features used, interactions, session duration, timestamps, scan frequency
- **Technical and Diagnostic Data:** Crash logs, performance data, error reports
- **Network Information:** Connection type (Wi-Fi, cellular), general network performance metrics

This data is collected solely to ensure functionality, security, performance monitoring, and improvement of the App.

#### 3.3 Payment Information

- Sift does not collect, process, or store payment card details or financial information
- All payments and subscriptions are handled exclusively through Apple In-App Purchases
- Apple acts as an independent data controller for all payment data
- We receive only limited, non-financial confirmation of subscription status (e.g. active, expired, plan tier)

#### 3.4 Information Processed by Third-Party AI Services

When you scan or search for a product, certain information is transmitted to third-party artificial intelligence (AI) services for analysis. This includes:

- Product names and identifiers
- Barcode numbers
- Product category information

**This information is transmitted solely for the purpose of generating product analysis and is not linked to your personal identity or account when sent to AI providers. No images are transmitted to AI services; only text-based product identifiers are shared.**

## 4. DATA WE DO NOT COLLECT

For clarity, Sift does not:

- Collect precise or approximate geolocation data
- Collect biometric identifiers (fingerprints, facial data, voice prints)
- Collect government-issued identification numbers
- Collect health, genetic, or biometric data
- Sell personal data to any third party
- Use personal data for cross-app or cross-website tracking without explicit consent
- Use personal data for targeted advertising or behavioural profiling
- Collect browsing history or data from other apps on your device

## 5. HOW WE USE YOUR DATA

We use personal data solely for legitimate and specified purposes:

### 5.1 Core App Functionality

- Providing and operating the App, including product scanning, search, and rating features
  - Processing product identifiers through AI systems to generate analysis and scores •
- Managing user accounts, authentication, and session management
- Delivering subscription and premium features
  - Maintaining scan history for registered users

### 5.2 App Improvement and Analytics

- Improving App functionality, accuracy, and user experience
- Analysing aggregated and anonymised usage patterns to inform product development
- Monitoring App performance, stability, and error rates
- Generating aggregated trending data based on scanning activity

### 5.3 Security and Compliance

- Maintaining security and preventing misuse, fraud, and abuse
- Enforcing our Terms and Conditions of Use
- Responding to user inquiries and support requests
- Complying with applicable legal obligations

We do not use personal data for purposes unrelated to the App or its improvement.

## 6. IMAGES, SCANS, AND USER CONTENT

### 6.1 Purpose of Processing

Images, scans, and other User Content uploaded to the App are processed solely to:

- Identify products via barcode lookup or image recognition
- Generate informational ratings, scores, and summaries
- Improve the accuracy and performance of the App's identification systems

All processing is automated and performed by software systems without human review of individual User Content.

## 6.2 No Commercial Exploitation

User-uploaded images and scans are:

- Not sold to any third party
- Not licensed to advertisers or marketing companies
- Not used for unrelated commercial purposes
- Not used to build advertising profiles

## 6.3 AI and Automated Processing

Sift uses automated systems, algorithms, and third-party AI/LLM (large language model) services to analyse product identifiers and publicly available information to generate scores, summaries, and recommendations.

No automated processing carried out by the App produces legal, medical, or similarly significant effects on users. Generated scores and summaries reflect opinion-based interpretations of publicly available information and do not constitute verified factual statements.

**Users should not make health, safety, dietary, or medical decisions based on AI-generated Content. All AI outputs may contain inaccuracies, fabrications, or hallucinations.**

## 7. LEGAL BASES FOR PROCESSING (UK & EU GDPR)

We process personal data based on the following legal grounds:

- **Performance of a Contract (Article 6(1)(b)):** Processing necessary to provide the App and its features as described in the Terms and Conditions, including account management, scanning functionality, and subscription delivery
- **Consent (Article 6(1)(a)):** Where required, such as for account creation via third-party authentication and for optional data collection. Consent may be withdrawn at any time without affecting the lawfulness of processing carried out prior to withdrawal
- **Legitimate Interests (Article 6(1)(f)):** App security monitoring, analytics and performance improvement, fraud prevention, and aggregated trend analysis. We conduct balancing tests to ensure our legitimate interests do not override your fundamental rights
- **Legal Obligations (Article 6(1)(c)):** Where processing is necessary to comply with applicable law, including tax, accounting, and regulatory requirements

## 8. APPLE APP STORE & TRACKING COMPLIANCE

In accordance with Apple App Store policies and the Apple Developer Program License Agreement:

- All data collection practices are transparently disclosed in our App Store privacy nutrition labels
- App Tracking Transparency (ATT) consent is requested before any tracking across apps or websites owned by other companies
- We do not track users across apps or websites without explicit opt-in permission
- We do not use device fingerprinting or any covert tracking methodologies
- Users may request access to or deletion of their data at any time
- The App complies with Apple's requirements for apps offering auto-renewable subscriptions

## **9. DATA SHARING AND THIRD-PARTY PROCESSORS**

We may share limited data with the following categories of third-party service providers, each of whom is bound by contractual confidentiality and data protection obligations:

### **9.1 Infrastructure and Database Services**

#### **Google Firebase (Google LLC)**

- Purpose: User authentication, cloud database (Firestore), crash reporting, and analytics
- Data shared: Account information (name, email), scan history, app usage data, crash logs
- Privacy policy: <https://firebase.google.com/support/privacy>
- Data location: Google Cloud infrastructure (US/EU, with appropriate safeguards)

### **9.2 AI and Analysis Services**

#### **xAI (xAI Corp.)**

- Purpose: AI-powered product analysis and scoring via the Grok large language model
- Data shared: Product names, barcode identifiers, product category information (not linked to user identity)
- No personal data (name, email, device ID) is transmitted to xAI
- Privacy policy: <https://x.ai/legal/privacy-policy>

### **9.3 Product Data Services**

#### **Open Food Facts**

- Purpose: Product ingredient and nutritional data lookup
- Data shared: Barcode numbers (not linked to user identity)
- Open Food Facts is an open-source, publicly available database

### **9.4 Payment and Subscription Services**

#### **Apple Inc.**

- Purpose: In-App Purchase processing, subscription management

- Data shared: We receive subscription status confirmation only; Apple processes all payment data independently
- Apple acts as an independent data controller for all payment transactions

## 9.5 Legal and Regulatory Disclosures

We may disclose personal data where required by law, court order, or regulatory authority, or where necessary to protect the rights, property, or safety of Sift App Limited, its users, or the public. We do not sell, rent, lease, or trade personal data to any third party.

## 10. INTERNATIONAL DATA TRANSFERS

Some of our third-party service providers are located outside the United Kingdom and European Economic Area. Where personal data is transferred internationally, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission and/or the UK Information Commissioner's Office
- Adequacy decisions recognising the recipient country as providing an adequate level of data protection
- Appropriate technical and organisational security measures

In particular, data processed by Google Firebase and xAI may be transferred to the United States, where both providers maintain appropriate safeguards under their respective data processing agreements.

## 11. DATA RETENTION

We retain personal data only for as long as necessary to fulfil the purposes described in this Privacy Policy. Specific retention periods are as follows:

- **Account Data (name, email):** Retained for the lifetime of the account, and deleted within 30 days of a valid account deletion request
- **Scan History:** Retained for the lifetime of the account to provide ongoing access to results. Deleted upon account deletion
- **Technical and Diagnostic Data:** Retained for up to 12 months for performance monitoring and debugging purposes
- **App Usage Analytics:** Retained in aggregated and anonymised form indefinitely for trend analysis. Individual-level data is retained for up to 24 months
- **Support Communications:** Retained for up to 24 months following resolution of the inquiry
- **Subscription Records:** Retained for the duration required by applicable tax and accounting laws (typically 6 years in the UK)

Upon expiry of the applicable retention period, personal data will be securely deleted or irreversibly anonymised.

## 12. ACCOUNT DELETION

Users may request deletion of their account and all associated personal data at any time by:

- Using the account deletion feature within the App (Settings > Account > Delete Account)
- Contacting us at [info@sift-scanner.com](mailto:info@sift-scanner.com) with the subject line "Account Deletion Request"

Upon receiving a valid deletion request, we will:

- Verify the identity of the requesting user
- Delete or anonymise all personal data associated with the account within 30 days
- Notify relevant third-party processors to delete associated data where applicable

**Account deletion is permanent and irreversible. Users will lose access to all scan history, credits, subscription benefits, and other data associated with their account.**

Active subscriptions must be cancelled through Apple ID settings prior to or following account deletion. Account deletion does not automatically cancel an active Apple subscription, and the User remains responsible for managing their subscription through Apple.

Certain data may be retained beyond the 30-day period where required by law (e.g. tax records, fraud prevention records, or data subject to ongoing legal proceedings).

## 13. USER RIGHTS

Depending on your location, you may have the following rights regarding your personal data:

### 13.1 UK and EU/EEA Users (UK GDPR / EU GDPR)

- **Right of Access:** Request a copy of the personal data we hold about you
- **Right to Rectification:** Request correction of inaccurate or incomplete data
- **Right to Erasure:** Request deletion of your personal data ("right to be forgotten")
- **Right to Restrict Processing:** Request that we limit how we use your data
- **Right to Object:** Object to processing based on legitimate interests
- **Right to Data Portability:** Receive your data in a structured, commonly used format
- **Right to Withdraw Consent:** Withdraw consent at any time where processing is based on consent
- **Right to Lodge a Complaint:** You may lodge a complaint with the UK Information Commissioner's Office (ICO) at [ico.org.uk](http://ico.org.uk) or your local EU supervisory authority

### 13.2 California Users (CCPA / CPRA)

If you are a California resident, you have the following additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA):

- **Right to Know:** Request disclosure of the categories and specific pieces of personal data collected about you
- **Right to Access:** Obtain a copy of your personal data

- **Right to Correct:** Request correction of inaccurate personal data
- **Right to Delete:** Request deletion of your personal data
- **Right to Opt Out:** Opt out of the sale or sharing of personal data for cross-context behavioural advertising
- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of these rights

**Sift does not sell or share personal data for cross-context behavioural advertising.**

To exercise any of these rights, contact us at [info@sift-scanner.com](mailto:info@sift-scanner.com). We will respond to verifiable requests within 30 days (UK/EU) or 45 days (California), as required by applicable law.

## 14. CHILDREN'S PRIVACY

The App is not intended for children under 13 years of age, or under 16 years of age where required by applicable law (including under the UK Age Appropriate Design Code and EU Digital Services Act).

We do not knowingly collect personal data from children below these age thresholds. If we become aware that we have inadvertently collected personal data from a child, we will take immediate steps to delete that data.

If you believe a child has provided us with personal data, please contact us immediately at [info@sift-scanner.com](mailto:info@sift-scanner.com).

## 15. DATA SECURITY

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure, or destruction, including:

- Encryption of data in transit (TLS/SSL) and at rest
- Secure cloud infrastructure provided by Google Firebase with enterprise-grade security
- Access controls limiting data access to authorised personnel and systems only •

Regular security reviews and monitoring

- Authentication via secure third-party providers (Apple Sign In, Google Sign In, Firebase Authentication)
- Secure API communications between the App and backend services

However, no method of transmission over the internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security.

## 16. DATA BREACH NOTIFICATION

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of users, the Publisher will:

- Notify the UK Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, as required by UK GDPR Article 33

- Notify the relevant EU supervisory authority where the breach affects EU/EEA users
- Notify affected users without undue delay where the breach is likely to result in a high risk to their rights and freedoms, as required by UK GDPR Article 34

Notification to affected users will include, to the extent known:

- The nature of the breach and the categories of data affected
- The approximate number of users affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach and mitigate potential adverse effects
- Contact details for obtaining further information

## 17. COOKIES AND TRACKING TECHNOLOGIES

The Sift App is a native mobile application and does not use browser cookies.

We may use the following mobile tracking and analytics technologies:

- **Firebase Analytics:** Collects anonymised app usage data (screen views, feature interactions, session data) to help us understand how users interact with the App and improve functionality
- **Firebase Crashlytics:** Collects crash reports and diagnostic data to help us identify and fix bugs and stability issues

These technologies do not track users across other apps or websites. Users may limit analytics collection through their device privacy settings.

We do not use any third-party advertising SDKs, tracking pixels, or behavioural targeting technologies.

## 18. DO NOT TRACK SIGNALS

Some browsers and devices transmit "Do Not Track" (DNT) signals. As the App is a native mobile application that does not track users across websites, DNT signals are not applicable. However, we respect all user privacy preferences and do not engage in cross-site or cross-app tracking.

## 19. LIMITATION OF LIABILITY

To the fullest extent permitted by applicable law:

- Sift App Limited is not responsible for unauthorised access to personal data that is beyond our reasonable control
- Users acknowledge that inherent risks exist in internet-based and cloud-based services
- Our total liability for any privacy-related claim shall not exceed the amount set out in Section 17 of the Terms and Conditions of Use

Nothing in this section excludes or limits liability for breaches of data protection law that cannot be excluded or limited under applicable law.

## 20. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors.

For material changes, we will notify users through one or more of the following methods:

- In-App notification
- Email notification to the address associated with your account
- Updated "Last updated" date at the top of this Policy

Continued use of the App after publication of an updated Privacy Policy constitutes acceptance of the revised Policy. If you do not agree with the updated Policy, you must stop using the App and may request account deletion.

## **21. GOVERNING LANGUAGE**

This Privacy Policy is drafted in the English language. If this Policy is translated into any other language, the English language version shall prevail to the extent of any inconsistency.

## **22. CONTACT INFORMATION**

For questions, data protection requests, or privacy-related concerns, contact:

### **Sift App Limited**

Email: [info@sift-scanner.com](mailto:info@sift-scanner.com)

Address: 11 Holloway Drive, GU254SY, Surrey, United Kingdom

Website: <https://sift-scanner.com>

For UK data protection complaints, you may also contact the Information Commissioner's Office

(ICO): Website: <https://ico.org.uk>

Helpline: 0303 123 1113

## **23. ENTIRE AGREEMENT**

This Privacy Policy, together with the Terms and Conditions of Use, constitutes the entire agreement regarding the collection, processing, and protection of personal data in connection with the App.