gO Score Privacy Notice

Version 1.8 · In force since 2026-10-11

Text SHA-256 fingerprint: 384df400d81ba4130e7674459cf2e318c59c39ff55673f4b29e4e0eff24e369b

https://goscore-app.com/go-score/en/legal/privacy/v/1.8

1. Data controller

E & F International, Inc. ("E&F," "we"), a corporation organized under the laws of the State of Texas, United States of America (file number 805048008 with the Texas Secretary of State), with its registered office at 8122 Datapoint, Suite 250, San Antonio, Texas 78229, United States, which is also its address for exercising rights, is the controller of personal data collected through the gO Score platform (website and mobile app, the "Platform").

Privacy contact: Privacy Officer, E & F International, Inc. · privacidad@goscore-app.com · 8122 Datapoint, Suite 250, San Antonio, Texas 78229, United States.

This Notice is issued under Mexico's Federal Law on the Protection of Personal Data Held by Private Parties (published in the Official Gazette on March 20, 2025) and applicable United States law. Where a U.S. state law grants you additional rights, Section 13 describes them.

2. Who this Notice covers

This Notice applies to individuals whose data we process, who may be:

- Administrators and Authorized Users of an Organization Account.
- Individuals operating a business (for example, individual growers) who run an Organization Account in their own name.
- Contact persons, legal representatives, partners or employees of an Organization whose data appears in documentation that Organization provides.
- Persons mentioned in public or licensed source information the Platform uses for research, where identifiable (for example, the holder of a public record).
- Website visitors.

Data about legal entities (companies) is not personal data; however, data about the individuals linked to them is, and is governed by this Notice.

3. Personal data we process

We process only the data necessary for the purposes in Section 5. Depending on your relationship with the Platform, the categories are:

Category · Examples · Source

Identity and contact · Name, email, phone, country, language · You; the Organization that onboards you

Role and representation · Title, authority, document evidencing representation · You; the Organization

Business documentation · Articles, powers of attorney, official IDs of representatives, registration certificates · The Organization

Tax information · Tax ID (RFC, EIN or others), tax certificates, tax address · The Organization; public records

Financial and asset information · Financial statements, trade references, transaction proofs the Organization chooses to provide as Evidence · The Organization

Commercial relationships · Counterparties, invitations, relationship confirmations, transaction history

within the Platform · You; your Counterparties

Queries and research · Which Evaluated Subjects you look up, Reports you generate, Links you share · Your Platform activity

Files and Evidence · Documents and their metadata, verification results · You; our verifications

JORIX queries · Questions you ask JORIX within the Platform (not retained as memory) and, if you authorize it, the public context for your welcome (Section 10) · You; public sources

Device and activity · IP address, app or installation identifiers, operating system, access and security logs, usage events · Your device and browser

Payments · Masked payment method, charge history, subscription status, processor transaction identifiers · Payment processors; Apple

Preferences · Notification channels, consents given and their date · You

Data we do not process:

- Biometric data. If you use Face ID, Touch ID or another device biometric method, the check is performed by your device; gO Score does not receive or store biometric data: your phone only stores whether the lock is on.
- Full card numbers. These are received and stored by the payment processor or Apple, not gO Score. We only see masked data and transaction identifiers.
- Sensitive personal data (health, ethnic origin, religion, political opinions, sexual orientation, among others). We do not request it. If it appears incidentally in a provided document, we do not use it for any purpose and you may ask us to suppress it.

Financial and asset data. When you provide financial or asset information about an individual (for example, an individual grower), Mexican law requires that individual's express consent. We request it on the Platform at the time of upload, with a separate, unticked checkbox; without it, the document is not uploaded.

4. Where we obtain data

- Directly from you, when you sign up, use the Platform or contact us.
- From the Organization that onboards you or provides documents in which you appear.
- From other Users, when they confirm a commercial relationship with your Organization or provide Evidence mentioning you (such Evidence is treated as an allegation until verified, per the Evidence Policy).
- From public records and publicly accessible sources, under each source's conditions. The sources connected today are Mexico's National Statistical Directory of Economic Units (INEGI DENUE), the Legal Entity Identifier database (GLEIF), FMCSA open data (U.S.) and the official lists of OFAC (U.S.) and of Mexico's SAT (Articles 69 and 69-B of the Federal Tax Code). The public export of the USDA Organic INTEGRITY database is loaded weekly into the Search catalog and is not queried live. For PACA (USDA), its official releases (sanctions, restrictions, complaints, which are labeled as alleged, and lifted actions) are loaded weekly; the PACA license registry is not machine-read and is checked manually or through a screenshot the Organization provides. If you authorize it in a research request, public web pages are also consulted through a search engine.
- From licensed data providers: today we receive no data from any licensed-data provider. If we contract one (for example, an industry directory), we will identify it here, with its country, before using it.
- From service providers (payments, Apple, analytics), as described in Section 9.

Where we obtain your data from a source other than you and you have no account, we will

inform you of this Notice at our first contact with you or, if there is no contact, keep it publicly available at https://goscore-app.com/go-score/en/legal/privacy and in every Report that mentions you.

5. Purposes of processing

5.1 Necessary purposes (without them we cannot provide the service)

a) Create and manage the Organization Account and authenticate Users.

b) Verify the Organization's existence and its representatives' authority.

c) Host, organize and verify provided documentation and Evidence.

d) Calculate and display the Score, Verification Levels and Badges, and generate Reports and Verification Links, per the Evidence Policy and the audiences you define.

e) Manage commercial relationships and invitations between Organizations.

f) Provide research and market-information services to Users whose Plan includes them.

g) Operate JORIX within the Platform.

h) Process payments, subscriptions, Credits, receipts and invoicing.

i) Send operational communications (security, material changes, charges, corrections).

j) Handle correction, dispute and rights requests.

k) Prevent fraud, impersonation, Score manipulation and prohibited uses; secure the Platform.

l) Comply with legal, tax and accounting obligations and respond to authority requests.

m) Defend our rights in claims.

5.2 Optional purposes (you may decline them without affecting the service)

n) Send you commercial communications about gO Score or gO ecosystem products by email or other channels.

o) Usage analytics: we do not use third-party analytics tools. The Platform only generates its own usage and response-time statistics, aggregated by day and without identifying the User or their Organization, which are kept for 30 days. If we ever used a third-party tool, we would first ask for your separate consent.

p) Model training: we do not use your JORIX conversations or your documents to train or fine-tune artificial intelligence models, and this purpose is not offered. If we ever wished to do so, we will update this Notice and do it only with your specific, separate authorization.

q) Display your Verification Level or Badges in other gO ecosystem products (gO AgroMarket, Goldfield Origin), when that feature exists and you enable it.

You may decline optional purposes at sign-up, from Settings › Privacy in the gO Score app or by writing to privacidad@goscore-app.com.

6. Legal bases and consent

- For necessary purposes (5.1), processing is based on the legal relationship you or your Organization establishes with us by using the Platform, on compliance with legal obligations, and on our legitimate interest in security and fraud prevention. Under Mexican law, your consent is deemed tacitly given when this Notice is made available to you, except for financial and asset data, which require express consent.

- For optional purposes (5.2), we request your consent through a separate affirmative action (an unchecked box or a setting you turn on). You may withdraw it at any time with prospective effect.
- For third-party data an Organization provides, the Organization represents that it has informed those persons and has the necessary legal basis (Terms of Use, Section 12.2).

We do not condition access to the Platform or to paid features on your giving optional consents.

7. Profiling, Score, inferences and automated decisions

7.1 What the Platform does. The Score and Verification Levels are calculated automatically from the information described in the Evidence Policy. Where the Evaluated Subject is an individual operating a business, that calculation constitutes profiling of that individual.

7.2 What we do not do. We do not make decisions producing legal effects on you or similarly significantly affecting you based solely on automated processing. Decisions on account suspension, corrections and disputes are reviewed by a person. The Score is a support tool for other Users, who make their own commercial decisions.

7.3 Your rights. You may: learn the general logic of the calculation (Evidence Policy); request correction of the information it relies on; obtain human review; and object to your data being subject to automated processing intended to evaluate aspects such as your economic situation or professional performance where it produces effects you do not want, under Mexican law. If you exercise this right, we will assess the request and, where appropriate, mark your profile as "not evaluated" instead of showing a Score.

7.4 Inferences. Where the Platform or JORIX generates inferences or estimates about an Evaluated Subject, they are labeled as such and not as verified facts.

8. Audiences: who sees your data within the Platform

Your data and your Organization's data are not public by default. Visibility of each element depends on the audience your Organization's Administrator defines among the available options: your Organization only; Link recipients (with an access code, 1-to-30-day expiry and revocable); and confirmed Counterparties, who see your Passport only if you choose to share it (Terms of Use, Section 11.1). In general:

- Users of your own Organization see the File according to their permissions.
- Counterparties see what your Organization chooses to share when confirming the relationship.
- Recipients of a Report or Verification Link see what is included in that Report or Link, while valid.
- Users with the research feature may see public- or licensed-source information about Evaluated Subjects, with or without an account, within permitted uses.
- Other gO ecosystem products do not receive your private data unless you enable the corresponding feature.

9. Processors, recipients and transfers

9.1 Processors (providers processing data on our behalf)

Provider · Service · Country of processing · Data

Railway · Hosting and infrastructure, databases, backups and logs · United States (Railway region “sfo”) · All Platform data

Anthropic, PBC · Language model to prepare a commercial research report, only if you grant the "Send data to an AI provider" permission · Not stated per request; Anthropic, PBC is a U.S. company · Name of the researched company and searches, your request, documents you attach, what was read in public sources and your transaction history with that company; see 9.3

Brevo · Transactional email (access codes, notices) and bounce handling · European Union: servers in France and Belgium; Brevo GmbH provides support and maintenance from Germany. Some Brevo sub-processors (network and support) may process data in the United States · Email, notification content, delivery status

Apple Push Notification service (APNs) · Push notifications on iPhone · Apple does not state where APNs itself runs. Its general policy says it stores data in the United States and that its affiliates in other countries may access it · Device token, minimal notification content

Meta Platforms (WhatsApp Business Platform), only if you link your number · WhatsApp notifications with your authorization · Meta data centers in several countries · Phone number, template content

Cloudflare, only the internal JORIX vault · Queries by the internal gO team, at the CEO's request, to the Score Control Center and to Score appeals · Global (Cloudflare network) · Score, Level and review status of network Organizations; for each appeal: the Organization, what is appealed, the reason, the evidence submitted, who appealed (name and role), the status and its log

Resend (backup, only if Brevo is not configured) · Backup transactional email · Account data, metadata and logs: United States. Sending goes out from the region configured for the domain in Resend · Email, notification content

Telegram · Internal alerts to the gO team (for example, a deletion request) and, if you linked your Telegram, your access codes · Several countries; Telegram does not specify it for accounts opened outside the UK and the European Economic Area · User and Organization the alert refers to; access code

ipwho.is · Locating the approximate country of each sign-in, for security alerts · Not stated; its policy says it may use servers in several countries · Connection IP address

Brave Search, only if gO turns it on · Internet searches for a commercial research request · Not stated; Brave Software, Inc. is a U.S. company · Name of the researched company and search terms

We do not use third-party analytics tools or external document or identity verification providers.

Processors only process data under our instructions and with contractual confidentiality and security obligations. Under Mexican law they do not require your consent, but we identify them for transparency.

9.2 Recipients processing data on their own behalf

- Apple, for App Store purchases: receives payment and subscription data under its own privacy policy. We receive transaction identifiers and subscription status from Apple, not your payment method.
- Stripe and, when it appears as an option on the payment screen, PayPal, for web purchases: receive your payment data as independent controllers under their own policies; we receive masked data and transaction identifiers.
- Other Platform Users, within the audiences in Section 8.
- Authorities, where there is a legally grounded request.
- Successors in a merger, acquisition or reorganization, with prior notice to you.

9.3 Artificial-intelligence providers

Anthropic, PBC is today the only artificial intelligence provider that receives gO Score data, and only when you grant the "Send data to an AI provider" permission (Settings › Privacy and connections). It is used to prepare the report for a commercial research request you make, and receives: the name of the researched company and the searches, your request, documents you attach, what was read in public sources and your transaction history with that company.

Without that permission nothing is sent to it; if you withdraw it, the research in progress stops. JORIX within the app and the reading of File documents do not use any artificial intelligence model. Country or region of processing, the provider's retention period and whether training of its models is excluded: as set by the commercial terms Anthropic publishes for its API (anthropic.com/legal); if they change, we will update this Notice. We do not state that the provider does not train on the data until the contract confirms it.

We distinguish three uses that are not authorized as a bundle:

1. Service memory: JORIX within gO Score does not retain memory of your conversations (Section 10).
2. Usage analytics: only first-party, aggregated statistics, with no third parties (5.2.o).
3. Model training: not performed or offered (5.2.p); for external providers, see the previous paragraph.

9.4 International transfers

E&F is established in the United States and its providers process data in the countries stated in Section 9.1. If you are in Mexico, your data is transferred to the United States to provide the service. Under Mexican law, transfers to processors and those necessary to perform the contract between you and us do not require your consent. For any other transfer that requires it, we will request it expressly and state the recipient and purpose. If you do not object to the transfers described in this Section that require consent, you will be deemed to accept them; you may object at privacidad@goscore-app.com.

10. JORIX memory

• JORIX within gO Score does not retain memory of your conversations: each answer is built from information you are already authorized to see, and the question is not stored.

• If you turn on "Public context for my JORIX welcome," the Platform queries GLEIF with your company's name and country and reads the public homepage of the website you provide, to suggest topics. That result is kept for up to 7 days and refreshed if your profile changes; it sends no documents, tax data, email or phone, and uses no artificial intelligence models.

• You can withdraw that permission in Settings › Privacy and connections; withdrawing it deletes the context. You may also request it at privacidad@goscore-app.com.

• JORIX conversations are not used to train models without specific authorization (Section 9.3).

11. Security and incidents

We apply reasonable administrative, technical and physical measures proportionate to the nature of the data, including: encrypted connections (HTTPS with HSTS) and security headers (content security policy and framing protection); passwords stored salted with a key-derivation function (scrypt) and one-time access codes; separation of information by Organization and role-based permissions; audit logs; rate limits against abuse; and daily backups. The database and files are not encrypted at rest. No system is invulnerable; we do not guarantee absolute security. If a security breach significantly affects your rights, we will inform you without undue delay through the contact channels we have and, where the law requires, the competent authority, stating the nature of the incident, the data affected, measures taken and recommendations for you.

12. Your rights and how to exercise them

12.1 Rights under Mexican law (ARCO and related). You have the right to access your data, rectify it when inaccurate or incomplete, cancel it (request deletion) when no longer needed for the purposes, and object to its processing for a legitimate cause or where automated processing has the effects described in Section 7.3. You may also revoke consent given and limit the use or disclosure of your data.

12.2 How to request. Send your request to privacidad@goscore-app.com or from the app, in Settings › Privacy and connections ("Download my data" and "Close, leave or delete"); to rectify evaluated information, you may also use the correction form at https://goscore-app.com/go-score/en/correction, stating: (a) your name and a means to communicate the response; (b) documents evidencing your identity or, where applicable, your legal representation; (c) a clear description of the data and the right you wish to exercise; and (d) anything that helps locate the data. Identity verification will be proportional to the sensitivity of the data: for access to or deletion of business documents we will ask for more elements than for changing a notification preference.

12.3 Timeframes. We will communicate our determination within a maximum of 20 days from receipt of the request and, if it proceeds, give it effect within 15 days after the communication. These periods may be extended once for an equal period where circumstances justify it, with notice to you.

12.4 No fee. Exercising rights is free of charge; only justified shipping or reproduction costs may be charged where the law allows.

12.5 Authority. If you believe your rights have been violated, you may apply to the Secretaría Anticorrupción y Buen Gobierno (Mexico), the competent authority under the 2025 LFPDPPP. You may do so through the channels that authority publishes.

12.6 Persons without an account. If you have no account and appear in Platform information, you may exercise the same rights through the channels indicated; the Evidence Policy also describes the correction procedure for evaluated information.

12.7 Deleting your account. If you request deletion of your account in the app (Settings › Privacy and connections › Close, leave or delete), we send you an acknowledgment with the reference number and the deadline, which is no later than 30 calendar days after the request. If no one has resolved it by that date, the system carries it out that day, unless a security incident prevents it; in that case it is carried out as soon as the incident is resolved. When it is carried out, we send a confirmation to the account's email address before removing it. We delete the account and pseudonymize your contact details: your email, phone and username no longer appear in your account or in gO Score, except for what you yourself wrote in support messages, and references to you remain linked to a pseudonym. This is not complete anonymization: we keep the consent history, the log without your contact details, the evidence of transactions and the accounting records, and the name you typed when accepting legal documents, only as a record of that acceptance. That name is kept only in the internal record of acceptances; it is not shown on the platform to other users or other organizations.

13. Additional information for United States residents

13.1 Applicable law. Depending on your state of residence and the volume of data we process, state privacy laws may apply (for example, the California Consumer Privacy Act as amended by the California Privacy Rights Act, and laws of other states).

13.2 Rights we offer. Regardless of whether a state law applies, we offer U.S. residents the rights to know, access, correct, delete and port their personal data, and to opt out of the sale or

sharing of data for advertising. We do not sell your personal data or share it for behavioral advertising.

13.3 Categories. The data categories, sources, purposes and recipients described in Sections 3 through 9 correspond to the categories state laws require to be disclosed. We do not process sensitive personal data under those laws, except tax or financial identifiers the Organization provides, which we use only for necessary purposes.

13.4 Fair Credit Reporting Act. gO Score Reports concern Organizations and their commercial activity and must not be used to decide on an individual's consumer credit, insurance, employment or housing.

13.5 Non-discrimination. We will not treat you differently for exercising your privacy rights.

13.6 Authorized agents. You may designate an authorized agent to exercise your rights; we will require proof of authorization.

13.7 Contact. privacidad@goscore-app.com or from the app (Settings › Privacy and connections). We do not have a telephone number.

14. Retention, blocking, deletion and backups

14.1 Principle. We retain data only as long as necessary for the purposes for which it was collected and to comply with legal obligations. There is no single period for everything: each category has its own period, described in the internal Data Inventory and Retention document and summarized below.

- Category · Retained while… · After account closure
- Account and profile data · the account is active · Blocking for 30 days then deletion, subject to exceptions
- Original File documents · the Organization keeps them · Deletion after the blocking period; only those incorporated into Reports delivered to third parties are kept for 5 years from delivery, or those required by law
- Extracted structured data · the source document exists · Same as the source document
- Score and verification results · current; history kept for traceability for 5 years · Anonymization or deletion
- Third-party evidence and allegations · relevant per the Evidence Policy · Deletion or anonymization depending on review outcome
- Consents and acceptances · the relationship exists and during the limitation period for claims · Retained for the limitation period (10 years)
- Billing and payments · required by tax and accounting law · Retained for the legal period (Mexico: 5 years; U.S.: per federal and state law)
- Public context for the JORIX welcome · up to 7 days from the query, or until you withdraw the permission · Deletion within 7 days
- Security and access logs · 12 months · Deletion when the period ends
- Public-source data on Evaluated Subjects · current and relevant; periodically re-verified · Deletion when no longer relevant or upon a valid request

14.2 Blocking. Upon account closure or fulfillment of the purpose, data enters a blocked state in which it is retained only to address liabilities arising from processing, and is then deleted or anonymized.

14.3 Backups. Deleted data may remain in daily backups for 30 days, until rotation, and in the monthly database archive, which is not rotated; those copies are not used for any active purpose and are restored only in case of an incident.

14.4 Exceptions. We may retain certain data longer where necessary to comply with legal

obligations, respond to authority requests, resolve disputes or defend claims, or where the data forms part of a Report already delivered to a third party per the Terms of Use.

15. Cookies, analytics and communications

15.1 Website. The site only stores in your browser what it needs to work: your language and your cookie choice; the web app also stores your session, language and visual theme. If you choose "Allow minimal analytics," the site counts, by day and language and without identifying you (no IP, device or cookie), clicks on the App Store link; with "Necessary only" nothing is counted. We do not use third-party analytics or advertising cookies, or tracking pixels. You can change your choice with the "Cookie preferences" button at the bottom of every page of the site.

15.2 Mobile app. The app uses the app's device identifier and the Apple push-notification token (up to 5 per person) to send you notices, the approximate country of each sign-in (derived from the IP address) for security alerts, and usage and response-time statistics aggregated by day without identifying you. We do not access the device's advertising identifier or track you across other apps or websites.

15.3 Operational communications. We send notices necessary for the service (Section 5.1.i). They cannot be disabled while you hold an account.

15.4 Marketing. We send commercial communications only if you authorized them. You may withdraw authorization in each message or at Settings › Privacy (“News and promotions”) in the gO Score app.

16. Account closure and data that must remain

When you close your account (available in-app and on the web), we stop processing your data for service purposes and apply the periods in Section 14. Billing and payment data, consent and acceptance records, records needed to handle claims, and Reports already delivered to third parties with their date must remain for the legal periods. We will state this on the closure screen.

17. Minors

The Platform is not directed to persons under 18 and we do not knowingly collect their data. If we detect a minor's data, we will delete it.

18. Changes to this Notice

We will publish changes at https://goscore-app.com/go-score/en/legal with the update date. If a change affects purposes, recipients or your rights, we will notify you by email or on the Platform before it takes effect and, where the law requires, request your consent again.