

JeoValid Privacy Policy Research and Tailored Draft

Executive summary

Public materials describe JeoValid as a geology and drilling-data application that imports and validates collar, survey, lithology, and assay data; visualizes data in 2D and 3D; offers premium features through in-app purchases; and, importantly, says project files are primarily processed on the device rather than centrally stored by the developer. The official website also says no account is required to start using the app, and that location permission is used to match field coordinates with the device location for QA/QC purposes. ¹

The main compliance issue is not the app's basic privacy posture, which appears relatively conservative, but the fact that JeoValid's public disclosures are not yet fully harmonized. The Google Play listing currently shows "No data collected" and "No data shared," while Google's own Data safety rules require declarations to reflect third-party SDK handling as well, and RevenueCat's official guidance says apps using RevenueCat should disclose purchase history in Google Play and Purchases in App Store Connect. JeoValid's current website privacy page also states more broadly that the app may collect uploaded datasets, device location, and in-app usage statistics, which is broader than the behavior you have now confirmed. ²

A second cleanup point is contact identity. The Play listing names `jeovalid.destek@gmail.com` as the support email, while the official website prominently uses `destek@jeovalid.com`. For privacy rights handling, it is better to publish one canonical support/privacy address and use it consistently in Play, on the website, and inside the policy. ³

The draft below is therefore written to fit the app behavior you confirmed: no end-user account creation, no photo upload, no camera or microphone access, location permission used but location processed only on-device and not sent to your servers, local file access for imports, Google Play Services and RevenueCat use, and no server-side storage of user project data. Where public sources still leave uncertainty, the report flags those items explicitly instead of guessing. ⁴

Public-source findings

The Play listing presents JeoValid as a professional mobile tool for geological and drilling data verification, review, and visualization. It emphasizes dataset import and management, error detection, column matching, 2D/3D visualization, premium access, and on-device processing of user project files. The listing also shows the app was updated on April 20, 2026, includes in-app purchases, and currently declares "No data shared with third parties" and "No data collected." ⁵

The official website expands the feature set further. It says users can load project tables, run automatic validation, visualize results in 3D, export outputs such as DXF, use PRO subscriptions, and cancel subscriptions through the App Store or Google Play. The FAQ states that no account is needed, location permission is used for field coordinate matching and QA/QC, and support is available through `destek@jeovalid.com` or the contact page. The contact page includes a web form collecting name,

email, subject, and message fields, which means the website itself likely processes at least some contact data even if the mobile app does not. ⁶

The website’s current privacy page is legally thin and partly inconsistent with the stricter app behavior you confirmed. It says JeoValid collects limited data including uploaded datasets, device location for quality control, and possible in-app usage statistics; it also says the website may use limited cookies for preferences and traffic analysis. That wording may be defensible for the website or for future analytics, but if JeoValid currently has no analytics/crash SDKs and does not upload project files or location to JeoValid servers, the policy should be narrowed and made much more precise. The Terms page is also effectively still blank as of July 15, 2026. ⁷

There is also a meaningful store-compliance gap around subscriptions. Google requires Data safety declarations to cover data handled through third-party SDKs and states that developers are responsible for complete and accurate disclosures. RevenueCat’s own platform guidance says that apps using RevenueCat must disclose purchase history in Google Play and Purchases in App Store Connect. RevenueCat further explains that, by default, its SDK creates anonymous App User IDs, and that for Apple privacy disclosures purchase history may be marked as not linked to identity if only anonymous IDs are used and there is no separate way to identify the individual user. ⁸

For structure and tone, similar field-mapping and geology-adjacent apps provide useful benchmarks. QField’s privacy policy separately identifies third-party services such as Google Play Services and Sentry and explains log-data handling, while the U.S. Bureau of Land Management’s S1 Mobile policy distinguishes between automatically remembered local app state and analytics, and expressly notes that the app does not inherently collect personally identifiable information. JeoValid’s finished policy should follow that same pattern of separating local device processing, third-party provider processing, website processing, and user rights. ⁹

Data flow summary

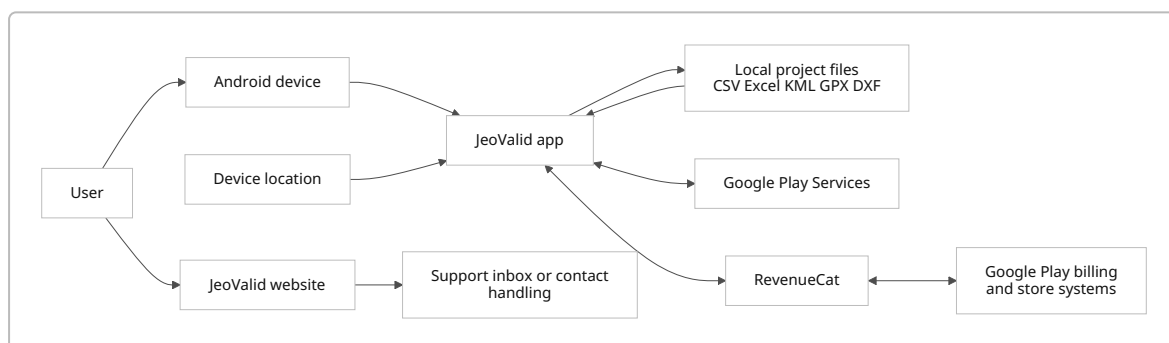
The table below synthesizes what is publicly documented, what is required by platform guidance, and what still needs confirmation before publication.

Data type	Main purpose	Stored on device	Stored on JeoValid server	Possible third parties	Notes
Geological/drilling project files such as collar, survey, lithology, assay tables	Import, validation, visualization, export	Yes	No, according to the Play listing’s on-device processing statement and your confirmed architecture	None identified from public sources	Public sources clearly support CSV/Excel-style table workflows; KML/GPX support was developer-confirmed but is not yet clearly described on the public site. ¹⁰

Data type	Main purpose	Stored on device	Stored on JeoValid server	Possible third parties	Notes
Device location	Field coordinate matching and QA/QC	Yes	No, per your confirmed architecture	Google Play Services may assist with location APIs depending on implementation	Google notes Play services can provide fused location when the app has permission, and in many cases data may be accessed locally without collection off-device. ¹¹
Purchase/subscription history and entitlement status	Unlocking JeoValid PRO, validating purchases, restoring access	Not primary storage location	Not project-data storage, but subscription metadata may be processed by RevenueCat	RevenueCat, Google Play, and on iOS Apple's App Store	This is the clearest disclosure item that should be added to store/privacy materials. ¹²
Anonymous subscription identifier	Identifying the purchaser for entitlement management where no user accounts exist	SDK-generated or app-generated identifier may exist locally	May exist in RevenueCat systems	RevenueCat	RevenueCat says anonymous App User IDs are generated by default if the developer does not provide a custom user ID. ¹³
Website contact details such as name, email, subject, message	Responding to support and sales/contact requests	Browser/session dependent	Likely yes, at least in email inbox or website backend	Hosting/email providers	The current contact page publicly shows a form collecting these fields. ¹⁴

Data type	Main purpose	Stored on device	Stored on JeoValid server	Possible third parties	Notes
Website cookies or similar browser technologies	Site functionality and possibly preferences/traffic analysis	Browser storage	Depends on implementation	Website host and any analytics provider, if enabled	The current public website privacy page says the site may use limited cookies for preferences and traffic analysis, but exact implementation is still unconfirmed.

15



In practical terms, JeoValid appears to be a low-risk app for user project data because the core geology files and live location workflow are designed to remain on the device. The higher-sensitivity processing sits around subscriptions and the website contact channel, not the drilling/project content itself. That distinction should be explicit in the final privacy policy and in store disclosures. 16

Tailored English privacy policy

What follows is a publication-ready long-form draft, written in plain English but with enough legal detail to satisfy the expectations reflected in Google Play's Data safety guidance, Apple's privacy-policy rules, GDPR transparency requirements, and the general principles of Türkiye's Personal Data Protection Law No. 6698. Google requires an accurate privacy policy and accurate Data safety declarations, and Apple requires a privacy-policy link that clearly identifies what data is collected, how it is collected, and how it is used. GDPR and KVKK both require transparency and grant users rights such as access, rectification, erasure, and related request mechanisms. 17

Privacy Policy for JeoValid

Effective Date: July 16, 2026

Who We Are

JeoValid is a mobile application for geological and drilling-data validation, review, and visualization, including local workflows for importing and processing field/project datasets. For purposes of

applicable data-protection laws, the JeoValid developer/publisher is the “controller” of personal data processed through the JeoValid app and website, except where a third party acts as an independent controller under its own privacy terms. RevenueCat states that, in relation to end-user data handled on behalf of the app developer, it acts as a processor. ¹⁸

Scope of This Policy

This Privacy Policy applies to the JeoValid Android app, the JeoValid website, and related support interactions. It is intended to explain what information is processed, how it is used, the legal bases relied on, who may receive it, how long it is kept, and what rights users have. Apple requires apps to make this information easily accessible both in App Store metadata and within the app, while Google Play requires developers to provide accurate privacy and Data safety disclosures. ¹⁹

Core Privacy Position

JeoValid is designed so that geological/project data are primarily processed on the device. Public product materials state that user project files are not centrally stored by the developer, and the public FAQ states that users do not need an account to start using the app. Based on the developer-confirmed configuration used for this draft, JeoValid does not offer end-user account registration, does not use camera or microphone permissions, does not provide photo uploads, and does not send user project files or the app's location-based QA/QC data to JeoValid servers. ¹⁰

Personal Data We Process Through the App

JeoValid may process the following categories of information:

First, **project and file data that you choose to open in the app**, such as geological/drilling datasets used for validation, review, visualization, and export. The Play listing and website describe workflows involving collar, survey, lithology, and assay datasets, including validation and 2D/3D review, and public materials emphasize on-device processing rather than central developer storage. Under the confirmed design assumptions for this draft, these files remain on your device unless you yourself export, share, or back them up using device or third-party tools outside JeoValid. ¹⁰

Second, **device location data**, if you grant location permission. The JeoValid FAQ explains that location permission is requested for matching field/geological coordinates with the device's location and for QA/QC workflows. Under the confirmed app behavior used for this draft, that location processing occurs on-device and is not transmitted to JeoValid's own servers. However, depending on implementation and device settings, Google Play Services may support location functions at the platform level. Google states that Play services can provide location APIs when apps have location permission, and that in many cases data can be accessed locally on the device without being collected off-device. ¹¹

Third, **subscription and purchase-related data** for JeoValid PRO. JeoValid's website states that PRO is sold through in-app purchases via the relevant app store and that payment-card information is not shared with JeoValid. Because JeoValid uses RevenueCat, subscription handling may involve purchase history, entitlement status, and an anonymous or other app user identifier needed to restore and manage paid access. RevenueCat's official guidance says apps using RevenueCat should disclose purchase data in both Google Play and Apple privacy disclosures, and RevenueCat's documentation says its SDK generates anonymous App User IDs by default unless the developer provides a custom identifier. ²⁰

Fourth, **technical network or platform data processed by third-party platform services**. Even where JeoValid itself does not upload project files or live location to its own servers, Google states that Google Play Services collects limited basic information on certified Android devices to support core device

features and developer APIs, such as IP address and other device/service information, with exact collection depending on device settings, installed services, and account configuration. That processing is governed by Google's own privacy terms where applicable. ²¹

Data We Do Not Intend to Collect Through the App

Under the app configuration described in this draft, JeoValid does not require end-user account creation, does not collect profile data for account registration, does not ask users to upload photos, does not use camera or microphone content, and does not store user project files on JeoValid-controlled servers. Public website FAQ content and the Play listing are broadly consistent with an account-free, on-device-workflow model. If any future version introduces analytics, crash reporting, cloud sync, AI APIs, team collaboration, server storage, or account login, this policy and the store disclosures would need to be updated before rollout. ¹⁰

Website Data

If you use the JeoValid website rather than only the mobile app, additional information may be processed. The current website includes a contact form that requests name, email address, subject, and message content. The current website privacy page also says the site may use limited cookies for remembering preferences and analyzing traffic. For legal clarity, the final production site should distinguish essential cookies from optional analytics cookies and, where required by law, obtain consent before setting non-essential cookies. ²²

Why We Process Data

We process data to provide the functions you request, including opening and handling local geological/drilling files; validating and visualizing project datasets; matching field coordinates using on-device location when you grant permission; managing premium access and restoring purchases; responding to support requests submitted through email or the website; maintaining security and preventing misuse; and meeting legal, tax, accounting, and consumer-protection obligations connected to purchases and support. These purposes are consistent with how JeoValid is described in the Play listing and on the official website. ¹

Legal Bases for Processing

Where GDPR applies, JeoValid would generally rely on: performance of a contract or steps taken at your request to provide app functionality and support; your consent where device permissions or optional communications are involved; compliance with legal obligations; and legitimate interests for fraud prevention, service security, and handling support or purchase disputes, insofar as those interests are not overridden by your rights. GDPR recognizes these legal bases and related user rights. ²³

Where Türkiye's KVKK applies, JeoValid would generally rely on the corresponding grounds under Law No. 6698, including explicit consent where required, processing directly related to the establishment or performance of a contract, compliance with legal obligations, the establishment/exercise/protection of a right, and the controller's legitimate interests where such processing does not harm the fundamental rights and freedoms of the data subject. ²⁴

Permissions

JeoValid may request location access for field coordinate matching and QA/QC workflows. It may also require file or storage access, depending on Android version and the specific file-picker or storage framework used, so that users can import local datasets and exports. Based on the confirmed app behavior used for this draft, JeoValid does not request camera access for photo capture, does not request microphone access, and does not require end-user account permissions. Google Play policies also require developers to use sensitive permissions responsibly and accurately explain them. ²⁵

Third-Party Processors and Services

JeoValid currently appears to rely at least on the following third parties:

Google Play Services. Google states that Play services are core system software on certified Android devices and may process limited basic and device-related information to support core functionality and developer APIs. Depending on the APIs JeoValid invokes and the user's settings, Google may process certain technical or location-related information under Google's own privacy framework. JeoValid should not describe such Google-controlled processing as if it were JeoValid's own storage or profiling activity.

21

RevenueCat. RevenueCat is used to manage in-app purchases and subscription entitlements. RevenueCat states that, for end-user personal data handled on behalf of app developers, it is a processor, and its own platform guidance says apps using RevenueCat should disclose purchase data in store privacy disclosures. RevenueCat documentation also explains that anonymous App User IDs are generated by default unless the developer supplies a custom user ID. If JeoValid uses only anonymous RevenueCat IDs and does not link them to names, email addresses, or accounts, Apple's privacy guidance for RevenueCat suggests purchase history may be disclosed as not linked to identity; that should still be verified before the App Store submission is finalized.

26

App Store / Google Play Billing. JeoValid's website states that purchases are processed through the relevant app store and that payment details are not shared with JeoValid. Subscription cancellation is also described as occurring through the store's subscription settings. Because store operators keep their own transaction records, deleting a user's RevenueCat-side subscriber record may not erase the store's own purchase history. RevenueCat's documentation expressly notes that deleting a user from RevenueCat does not delete Apple's purchase history and that restoring purchases can recreate the record. The same principle should be assumed for platform-controlled billing records generally.

27

How Long We Keep Data

For **project files and local working data**, JeoValid's stated design is local, device-based processing. Those files remain on your device until you delete them, remove the app, clear app storage, or move/export them elsewhere using device features or third-party tools. JeoValid does not, under the confirmed architecture used for this draft, keep a server-side copy of your project datasets.

5

For **location data used in QA/QC**, the intended model in this draft is on-device use without server-side retention by JeoValid. If any future version logs or transmits location off-device, the retention section must be updated before release.

28

For **subscription and purchase metadata**, retention may depend on the app store, RevenueCat, accounting obligations, fraud prevention, dispute resolution, and customer-support needs. JeoValid should keep only what is reasonably necessary for entitlement management, refunds/restores, legal compliance, and record-keeping. Because store operators and RevenueCat may retain purchase-related records under their own rules, JeoValid should avoid promising immediate or universal deletion of all billing history across all third parties. RevenueCat documentation specifically warns that deleting the user in RevenueCat does not delete Apple's purchase history and that restored purchases can recreate the record.

29

For **support communications**, JeoValid should retain emails, contact-form submissions, and related support records only for as long as needed to answer the request, maintain a reasonable support history, prevent abuse, and meet legal obligations or defend legal claims. This period should be stated

internally in an operations schedule even if the public policy uses a reasonableness standard. Under KVKK and GDPR, retention should be limited to what is necessary for the stated purposes. ³⁰

International Transfers

If JeoValid or its service providers process personal data outside the country where you are located, such transfers should rely on lawful safeguards. Under the GDPR, international transfers may rely on adequacy decisions, Standard Contractual Clauses, or other recognized safeguards. Under Türkiye's transfer rules, transfer abroad requires compliance with the relevant processing conditions and the applicable cross-border transfer framework. If JeoValid uses RevenueCat, Google, or infrastructure providers located outside Türkiye or the EEA, the final live policy should say so clearly and describe the chosen safeguards in practical terms. ³¹

Security Measures

JeoValid should describe security honestly and modestly. A defensible formulation is that the app uses reasonable technical and organizational measures appropriate to the nature of the data and the architecture of the service. In JeoValid's case, the strongest practical protective measure is that geological project data are processed locally on the device rather than centrally stored by the developer. Additional safeguards may include least-privilege permissions, secure transport for third-party purchase integrations, access control to support channels and admin panels, and regular review of SDKs and dependencies. No internet transmission or electronic storage system can be guaranteed to be perfectly secure. Public benchmark policies for field apps commonly use the same measured approach. ³²

Children's Privacy

JeoValid is a professional geology/productivity app and is not directed to children. JeoValid does not intentionally seek to collect personal data from children. If you believe that a child has submitted personal data through the website contact form or another support channel, JeoValid should be contacted so the information can be reviewed and deleted where appropriate. This is consistent with standard app-policy practice reflected in comparable field-app privacy policies. ³³

Automated Decision-Making

JeoValid provides technical validation, visualization, and analytical support for geological/drilling workflows. The public website presents the product as a tool to support technical evaluation, not as a system that makes legal or similarly significant automated decisions about individuals. Accordingly, the policy should state that JeoValid does not use personal data for solely automated decisions that produce legal effects or similarly significant effects on users. Validation outputs, anomaly flags, and analytical suggestions are decision-support tools and should be reviewed by the user. ³⁴

Your Rights

Where applicable law grants them, you may have the right to request access to your personal data, correction of inaccurate data, deletion or erasure of data, restriction of processing, objection to certain processing, and data portability. GDPR expressly recognizes access, rectification, erasure, portability, and related rights, and Türkiye's Law No. 6698 gives data subjects rights to learn whether their personal data are processed, request information, learn processing purposes and recipients, request correction, request deletion/anonymization where conditions are met, and seek compensation for unlawful processing. ³⁵

Because JeoValid is designed not to hold server-side copies of project files under the confirmed architecture used for this draft, many requests about app project data can be fulfilled most directly by deleting files and app storage on the user's own device. Requests concerning website contact records, subscription-support records, or RevenueCat-side subscriber metadata may still be made to JeoValid,

subject to identity verification, applicable law, and the limits of data that JeoValid actually controls. RevenueCat also states that deletion requests relating to customer data may require contacting RevenueCat. ³⁶

Under GDPR, controllers are generally expected to respond without undue delay and at the latest within one month. Under KVKK, the data controller must conclude the request as soon as possible and at the latest within thirty days, generally free of charge. JeoValid should adopt those timelines in its operational process, while reserving the right to request enough information to verify the requester's identity and understand the scope of the request. ³⁷

How to Request Access, Correction, Deletion, or Portability

JeoValid should offer a simple route such as an email to a dedicated privacy address. For clarity, the policy should say that users may submit requests by emailing the privacy/support contact with enough information to identify the relevant interaction, such as the approximate date of contact or purchase, the platform used, the device platform, and the email address used in contact correspondence if relevant. Türkiye's rules specifically recognize requests to controllers through written or electronic means. ³⁸

Data Deletion Request Procedure

A careful deletion clause for JeoValid should explain the difference between data controlled by JeoValid and data controlled by third parties. JeoValid can delete support emails, website contact records, and any subscriber metadata it controls or can instruct RevenueCat to delete on its behalf where appropriate. JeoValid cannot guarantee deletion of app store billing records held independently by Google or Apple, and deleting RevenueCat's copy may not prevent store-side purchase records from existing or later being restored. RevenueCat's documentation makes that limitation explicit. ²⁹

Sample Data Deletion Request Form Text

Subject: Personal Data Access / Deletion Request

Hello JeoValid Privacy Team,

I am requesting the following action regarding my personal data: access / correction / deletion / portability / objection.

My details:

- Full name (if used in contact with JeoValid): [insert]
- Email address used to contact JeoValid or receive replies: [insert]
- Platform: Android / Website / Other
- Approximate date of purchase or support contact: [insert]
- Description of my request: [insert]

I understand that JeoValid may need additional information to verify my identity and locate the relevant records.

Thank you.

Cookies and Similar Technologies on the Website

For the mobile app itself, traditional browser cookies are generally not relevant. For the website, JeoValid's current public privacy page says limited cookies may be used for preferences and traffic

analysis. The final policy should distinguish essential cookies from analytics or marketing cookies; explain their purpose, duration, and provider where possible; and provide any banner or consent controls required by the user's jurisdiction. If no non-essential cookies are actually used, that section should be simplified accordingly. ¹⁵

Changes to This Policy

JeoValid may update this Privacy Policy from time to time to reflect new features, changed legal requirements, or new service providers. Google Play and Apple both expect app privacy disclosures to stay aligned with actual practices, and Google specifically states that developers are responsible for complete and accurate declarations, including for data handled through third-party SDKs. If JeoValid introduces analytics, crash reporting, cloud sync, team workspaces, external AI services, or any new permissions, the policy and store disclosures should be updated before the relevant version is released.

³⁹

Contact Information

Use one canonical public contact block everywhere. A strong production version would read:

JeoValid Privacy Contact

Email: **privacy@jeovalid.com**

Support: **support@jeovalid.com**

Postal Address: **[Insert legal entity name and address]**

If you do not yet use a dedicated privacy mailbox, `support@jeovalid.com` is preferable to a Gmail address for policy credibility and continuity, but the key task is consistency across the Play listing, website, app, and legal texts. The current public materials already show two different addresses, so this should be fixed before publication. ³

Store metadata snippets

These are short-form notices for store fields or summary boxes. They do not replace the full policy.

Recommended Google Play short notice

JeoValid processes geological project files and location-based QA/QC data primarily on the device to validate and visualize drilling/geology datasets. The developer does not store user project files or live location on its own servers. JeoValid does not require user accounts and does not use camera, microphone, or photo uploads. If JeoValid PRO is purchased, subscription-related purchase history and entitlement data are processed by the app store and RevenueCat to manage paid access. ⁴⁰

Recommended App Store short notice

JeoValid does not require end-user accounts and is designed so project data and field-location workflows remain on-device. No camera, microphone, or photo-upload features are used. If PRO features are purchased, purchase information is processed by the relevant app store and RevenueCat to validate subscriptions and restore entitlements. If only anonymous RevenueCat app user IDs are used and no separate identifier links purchases to a person, JeoValid may be able to disclose Purchases as not linked to identity, but that should be verified before submission. ⁴¹

Finalization checklist

Before publishing the policy and updating store metadata, these items should be confirmed and then frozen in one release checklist.

- **Manifest permissions.** Confirm the exact Android permissions in the shipping build, especially location scope, storage/file access strategy, notification-related permissions, and whether any legacy storage permissions are still present. Public sources do not currently prove the exact manifest. ⁴²
- **Analytics and crash SDKs.** Confirm that no analytics, crash reporting, session replay, advertising, or attribution SDKs are bundled. The current website privacy page mentions possible usage statistics, while the app facts you confirmed assume none. ¹⁵
- **AI feature architecture.** The website markets “AI-supported analysis.” Confirm whether those features run fully on-device or call any external API or cloud model. If external endpoints exist, the privacy policy and Data safety declarations must be expanded before release. ²⁸
- **RevenueCat identity model.** Confirm whether RevenueCat uses only anonymous App User IDs or any custom identifier. This changes Apple privacy labeling and parts of the policy language. ⁴³
- **Canonical contact details.** Choose one privacy/support email and one legal controller name/address. Public materials currently conflict between `jeovalid.destek@gmail.com` and `destek@jeovalid.com`. A dedicated address such as `privacy@jeovalid.com` is recommended for data-rights requests. ⁴⁴
- **Store-side disclosures.** Update Google Play Data safety to reflect any RevenueCat-related purchase-history disclosure if RevenueCat is indeed in the shipping app, because Google requires accurate declarations for third-party SDK handling and RevenueCat explicitly says this data type must be disclosed. Review App Store Connect privacy labels the same way. ⁴⁵
- **Website processing.** Confirm whether the contact form actually stores submissions in a database, sends email only, uses CAPTCHA, sets analytics cookies, or has newsletter subscriptions. The policy should describe the implementation you actually operate, not a template. ²²
- **Server endpoints.** Confirm whether there are any JeoValid-controlled APIs at all for support, subscriptions, updates, remote config, uploads, backups, or moderation. Your current brief says no server-side storage of project data, but the final policy should also say whether any non-project data go to any JeoValid endpoint. ¹⁰

The draft above is strong enough to use as a working production text, but the final release version should only be published after those confirmation points are checked against the actual shipping APK/AAB, the website implementation, and the live SDK inventory. That is exactly the kind of alignment Google Play and Apple expect, and it is also the safest way to stay consistent with GDPR and KVKK transparency duties. ⁴⁶

¹ ² ³ ⁴ ⁵ ¹⁰ ¹⁶ ¹⁸ ³² ³⁴ ³⁶ ⁴⁰ ⁴² ⁴⁴ JeoValid - Apps on Google Play

<https://play.google.com/store/apps/details?id=com.jeovalid.app>

⁶ ¹¹ ²⁵ ²⁸ ⁴¹ JeoValid — Jeolojik Veri Doğrulama ve Analiz Uygulaması

<https://jeovalid.com/>

⁷ ¹⁵ Gizlilik Politikası — JeoValid

<https://jeovalid.com/privacy.html>

- 8 17 39 45 46 **Provide information for Google Play's Data safety section - Play Console Help**
<https://support.google.com/googleplay/android-developer/answer/10787469?hl=en>
- 9 33 **privacy_policy | QField - Efficient field work built for QGIS**
https://qfield.org/privacy_policy/
- 12 20 27 **JeoValid PRO — Fiyatlandırma ve Ayrıcalıklar**
<https://jeovalid.com/Pro>
- 13 43 **Customers in RevenueCat | In-App Subscriptions Made Easy**
https://www.revenuecat.com/docs/customers/user-ids?utm_source=chatgpt.com
- 14 22 **İletişim — JeoValid**
<https://jeovalid.com/Contact>
- 19 **App Review Guidelines - Apple Developer**
<https://developer.apple.com/app-store/review/guidelines/>
- 21 **Learn about Google Play services - Android Help**
<https://support.google.com/android/answer/10546414?hl=en>
- 23 30 **Regulation - 2016/679 - EN - gdpr - EUR-Lex - European Union**
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng?utm_source=chatgpt.com
- 24 **Personal Data Protection Law**
https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law?utm_source=chatgpt.com
- 26 **GDPR | RevenueCat**
<https://www.revenuecat.com/gdpr>
- 29 **Apple App Store & TestFlight | In-App Subscriptions Made ...**
https://www.revenuecat.com/docs/test-and-launch/sandbox/apple-app-store?utm_source=chatgpt.com
- 31 **Standard Contractual Clauses (SCC) - European Commission**
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en?utm_source=chatgpt.com
- 35 37 **Regulation - 2016/679 - EN - gdpr - EUR-Lex - European Union**
https://eur-lex.europa.eu/legal-content/EN-IT/TXT/?uri=CELEX%3A32016R0679&utm_source=chatgpt.com
- 38 **Comminuque On The Principles And Procedures For ...**
https://www.kvkk.gov.tr/Icerik/6638/Comminuque-On-The-Principles-And-Procedures-For-The-Request-To-Data-Controller?utm_source=chatgpt.com