Google Play Personal Loans Policy: What changed, impact, and mitigations for digital lenders

Audience: Digital lenders, facilitators, EWA providers, and credit-related apps

Table of contents

Executive summary

- Google Play has tightened its Financial Services, Personal Loans policy. Personal-loan apps, lines of credit, facilitators/lead generators, accessory credit apps (calculators/guides), and EWA apps are prohibited from accessing several sensitive permissions (e.g., contacts, photos/videos, precise location, phone numbers, broad app visibility, external storage).

- Expect enforcement during app review and on updates. Non-compliance can lead to rejection or removal.

- Impact on data-driven lending: certain device signals will no longer be available, which can reduce model lift if you relied on them.

- Credolab's view: Compliance first. Predictive performance can be preserved with a tailor-made model that taps our 11M+ engineered features (vs. the ~100 features many clients use today) and focuses on permitted, stable signals.

What changed (at a glance)

Who's in scope

- Personal-loan apps (including lead generators/facilitators and lines of credit)
- Accessory loan/credit apps (e.g., calculators, guides)
- Earned Wage Access (EWA) apps

Prohibited permissions for in-scope apps (examples)

- READ_CONTACTS (no phonebook access)
- READ_MEDIA_IMAGES / READ_MEDIA_VIDEO (no broad photo/video access)
- READ_EXTERNAL_STORAGE / WRITE_EXTERNAL_STORAGE
- ACCESS_FINE_LOCATION (precise location)
- READ_PHONE_NUMBERS
- QUERY_ALL_PACKAGES (no broad installed-app inventory)

Other ongoing requirements (selected)

- App category must be set to "Finance".
- Disclose min/max repayment period, max APR, representative cost example, privacy policy in store listing.
- Short-term personal loans (≤60 days) are not allowed.
- US APR ≥36% is not allowed.
- Country-specific licensing and disclosures apply for India, Indonesia, Philippines, Nigeria, Kenya, Pakistan, and Thailand.

Timing

Enforcement is active. Assume no grace if you newly request a prohibited permission.

What this means for your app and models

The following signals are likely to disappear:

- **Contacts/phonebook**: Referral flows, social-graph heuristics, collections "friend reach" tactics.
- **Photos/videos/external storage**: Any verification or "gallery scan"-type checks.
- **Precise location**: Fine-grained geolocation features.
- **Read phone numbers**: Automatic line detection, some telco-based heuristics.
- **Installed-app inventory (broad)**: Installed apps features via QUERY_ALL_PACKAGES.

Functional impacts

The following features and workflows must be redesigned:

- Referral programs that depend on phonebook access must be re-designed (e.g., user-initiated share sheet without ingesting contacts, typed input).
- Collections workflows cannot scrape contacts. Instead, they should rely on first-party contact details provided by the borrower and compliant messaging flows.
- Fraud/affordability features relying on broad app inventory must be replaced with permitted alternatives (e.g., scoped inter-app intents for payments, not analytics).

The risk of non compliance may cause the following:

- Requesting any prohibited permission can trigger rejection/removal.
- Repeat issues may escalate to Developer account being suspended.

Recommended actions

A. Compliance (immediate)

- **Remove** prohibited permissions from manifest, code, and third-party SDKs.
- **Refresh Data Safety** section and store listing with required lending disclosures.
- **Update Privacy Policy**: Clear, purpose-limited, retention details. Place a clean link in store listing.
- **Country-specific docs**: Upload required licenses/IDs where applicable (e.g., RBI/CBK/FCCPC/SEC).
- **Re-design flows**: Replace contacts/photo/location features with compliant, user-initiated alternatives (e.g., share sheets, system pickers where allowed, manual entry).

B. Model and analytics (within 2-4 weeks)

- **Feature audit**: Map current features to allowed categories. Drop/replace disallowed signals. Emphasize stable device/behavioral metadata that remain in scope.
- **Tailor-made model**: Build a custom score using Credolab's 11M+ features to offset signal loss.
- **Validation plan**: Back-test vs. off-the-shelf model; report AUC/KS/PSI, stability, and bias.
- **Rollout**: Staged A/B with kill-switch; watch approval, default, and fraud deltas.

If your app is flagged or removed (appeal readiness)

Follow the process below should your app be flagged or removed by Google Play:

- In Play Console / Policy Status, open the violation and use Appeal.
- Provide: (a) policy-compliant use case explanations, (b) updated store disclosures and privacy policy excerpts, (c) licenses/registrations, (d) evidence of permission removal, and (e) parity examples (if comparable apps are allowed the same compliant access).
- Do not republish until issues are fixed. Keep one clean, well-documented appeal per action.

How Credolab will support you

- **Compliance pack**: Manifest/SDK audit checklist; Data Safety and privacy-policy guidance.
- **Rapid assessment**: Apply our off-the-shelf model on collected datasets to assess baseline performance.
- **Custom model**: Develop a bespoke score leveraging the most predictive permitted signals from our feature universe. Deliver lift and stability analysis.
- **Implementation**: Integration guidance to improve Google Play disclosures and streamline re-submission.

Draft disclosure snippets (adapt to your policy)

- **Purpose limitation**: "We access only the data needed to deliver lending services (e.g., identity, affordability, risk assessment) and do not access contacts/photos/videos."
- **User control**: "Permissions are optional where feasible and can be revoked in device settings."
- **Security and retention**: "Data is encrypted in transit and at rest and retained only for legal, regulatory, and operational requirements."
- **Collections**: "We use contact details provided by you for collections. We do not read or upload your phonebook."

Appendix - References and resources

- Financial services (Personal loans) policy: scope (personal loans, facilitators/lead-gen, lines of credit, accessory credit apps, EWA), required disclosures, ban on short-term loans (≤60 days), US APR < 36%, and prohibited permissions list (READ_CONTACTS, READ_MEDIA_IMAGES/VIDEOS, ACCESS_FINE_LOCATION, READ/WRITE_EXTERNAL_STORAGE, READ_PHONE_NUMBERS, QUERY_ALL_PACKAGES). Updated Aug 28, 2025.
  https://support.google.com/googleplay/android-developer/answer/9876821

- Permissions policy: Broad package visibility (QUERY_ALL_PACKAGES) — high-risk permission; allowed only when core, user-facing functionality requires broad app visibility.
  https://support.google.com/googleplay/android-developer/answer/10158779

- Data safety section (store listing): What to disclose and how to complete the form in Play Console.
  https://support.google.com/googleplay/android-developer/answer/10787469

- Financial features declaration: Who must file and guidance for completing it in Play Console.
  https://support.google.com/googleplay/android-developer/answer/13849271

- Check policy status and appeal: Where to find violations and how to file an appeal if removed or rejected.
  https://support.google.com/googleplay/android-developer/answer/9842754
  https://support.google.com/googleplay/android-developer/answer/2477981

- Policy announcements: Timelines and clarifications (e.g., July 2025 update noting narrow exceptions for short-term loans in Pakistan only).
  https://support.google.com/googleplay/android-developer/announcements/13412212