Security & Privacy Disclosure, Final Report

Grammarly - AI Writing Assistant for Android (com.grammarly.android.keyboard)

A documentation- and self-disclosure-consistency audit, no binary obtained, no CRITICAL issued, no substantive reply received.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026.

Operator / Controller	Grammarly, Inc. (Play Store developer field) / Superhuman Platform Inc. (data controller per the company's own current privacy policy)
Versions Audited	NOT AVAILABLE, no binary obtained this programme (see Methodology Note); package verified live on Google Play, 50M+ installs, updated 11 Aug 2026
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	5: 0 Critical, 2 High, 2 Medium, 1 Low/Unverified
Status	NO SUBSTANTIVE REPLY as of 14 November 2026. Automated ticket acknowledgments only (12 Sep, 18 Oct 2026); no human response to the original notice, the 20-day follow-up, or the 35-days-to-publication notice.

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 3

2 Methodology Note: Binary Acquisition Failed 4

3 Finding Status at a Glance 5

4 Subject & Operator Analysis 5

5 Architecture & Data Flow (From the Operator's Own Documentation) 5

6 Engagement Summary 6

7 Findings 6

7.1 F1: Default-on, opt-out-per-app Accessibility Service architecture, no self-disclosed sensitive-category exclusion . . . 6

7.2 F2: Play Data Safety declaration omits the core "User content/screen content" category the company's own privacy policy names as collected . . . 7

7.3 F3: Third-party/bystander data self-acknowledged, no separate consent or transparency mechanism described for those individuals . . . 8

7.4 F4: Operator identity at install time does not match the controller named in the linked privacy policy . . . 8

7.5 F5: Dead support link in the app's own Play Store description; AI-training default state not stated . . . 9

8 Impact Analysis 9

9 The Complete Chain 10

10 Data Protection: Article by Article 10

11 Regulatory & Legal Landscape 11

12 Indicators of Compromise & Reproducible Evidence 11

13 Disclosure Timeline & Outcome 12

14 What Grammarly Got Right 12

15 Residual Risk & Recommendations 13

Executive Summary

Grammarly (com.grammarly.android.keyboard, Play Store listing title "Grammarly-AI Writing Assistant") is installed on 50M+ Android devices. This is a documentation- and self-disclosure-consistency audit, not a code-level audit: the audit device was unavailable this session, and the binary could not be obtained from any of the three sanctioned mirrors (APKCombo returned an explicit DMCA removal notice; APKPure and APKMirror returned no matching listing for this developer). Every finding below is sourced to the operator's own dated, first-party, publicly accessible text, with a verbatim excerpt, and no CRITICAL severity is issued, consistent with this programme's standing rule that CRITICAL requires impact demonstrable from the binary.

The product the package name and history describe, a standalone keyboard (IME), has been discontinued by Grammarly's own account. The current app instead uses Android's Accessibility Service to read and process text and on-screen content across every other installed app by default, through a floating widget that activates automatically wherever the user taps a text field. This is a broader access model than the IME commitText model the package name implies, not a narrower one: Accessibility Service exposes the visible node tree of the foreground app generally, not only the text committed to the field being typed into. Exclusion is opt-out, per app, and manual, with no self-disclosed default exclusion for sensitive categories such as banking, health, or dating apps found in the reviewed documentation.

A disclosure-consistency gap recurs three times across the operator's own first-party documents. The Play Store's own mandatory Data Safety declaration lists only personal info, device identifiers, and app performance diagnostics as collected data. It does not list any "User content," "Text," or "Screen content" category. The same company's own privacy policy, one click away from the same install screen, explicitly names "text, screen content, web pages, documents" under "User content" as data the products access and collect. The company's own Trust Center FAQ repeats the omission a third time.

A separate finding concerns operator identity: the Play Store developer field reads "Grammarly, Inc.," while the privacy policy linked from that same listing identifies the data controller as Superhuman Platform Inc., with Grammarly Inc. now listed as one of several subsidiaries. RFI-IRFOS sent the original notice on 23 August 2026, a 20-day follow-up on 12 September 2026, and a 35-days-to-publication notice on 17 October 2026. All three received only automated Zendesk ticket acknowledgments (12 September and 18 October 2026); no human reply of any kind has arrived as of 14 November 2026.

Scope: A documentation- and self-disclosure-consistency audit of the live Google Play listing, the mandatory Play Data Safety declaration, the operator's own privacy policy (grammarly.com/privacy-policy, redirecting to superhuman.com/legal/privacy-policy, effective 2026-07-06), the Grammarly Trust Center FAQ, and official Grammarly support documentation, each fetched live and quoted verbatim. No binary was obtained; no manifest, smali, strings, or network analysis was performed. No dynamic instrumentation, no emulator, no live backend calls, no device installation.

ID	Severity	Title
F1	HIGH	Default-on, opt-out-per-app Accessibility Service architecture, no self-disclosed sensitive-category exclusion
F2	HIGH	Play Data Safety declaration omits the core ”User content/screen content” category the company’s own privacy policy names as collected
F3	MEDIUM	Third-party/bystander data self-acknowledged, no separate consent or transparency mechanism described for those individuals
F4	MEDIUM	Operator identity at install time does not match the controller named in the linked privacy policy
F5	LOW	Dead support link in the app’s own Play Store description; AI-training default state not stated

Methodology Note: Binary Acquisition Failed

The audit device (Vivo, serial 10AD6Y0ZLH001KP) was not connected this session. Per the programme’s fallback protocol, all three sanctioned mirrors were checked: APKCombo’s live fetch tool returned an explicit ”This app has been removed by DMCA” notice for this exact package; APKPure’s site search returned no page for the actual Grammarly, Inc. developer, only unrelated grammar-checker apps from other developers; APKMirror’s developer page for Grammarly Inc. exists but returns ”No uploads found.” This is consistent across all three mirrors and confirmed via an explicit DMCA notice on one of them, not a search-technique failure. Per the programme’s standing rule against untrusted or unlisted sources, no other aggregator was used. The package itself was independently confirmed live and correctly identified on the Play Store before this determination was made. Consequently, every finding below rests on the operator’s own first-party published text rather than decompiled code, and is capped at HIGH severity; where a claim would require binary or runtime confirmation, it is marked UNVERIFIED.

Finding Status at a Glance

ID	Disclosed	This report	Status as of 14 November 2026
F1	HIGH	HIGH	No reply of any kind beyond automated ticket acknowledgments; stands as disclosed.
F2	HIGH	HIGH	Same; stands as disclosed.
F3	MEDIUM	MEDIUM	Same; stands as disclosed.
F4	MEDIUM	MEDIUM	Same; stands as disclosed.
F5	LOW/UNVERIFIED	LOW/UNVERIFIED	Same; stands as disclosed, AI-training default state remains unconfirmed.

Subject & Operator Analysis

The Play Store developer field for this listing reads ”Grammarly, Inc.” Grammarly’s own current privacy policy identifies the data controller as Superhuman Platform Inc. (2261 Market Street, STE 85232, San Francisco, CA 94114), with Grammarly Inc. listed as one of several subsidiaries alongside Coda Project LLC and Superhuman Labs LLC. A concrete EU/UK Art. 27 representative is named (VeraSafe Ireland Ltd, Cork, and VeraSafe United Kingdom Ltd, London), and a named Data Protection Officer is published (Bird & Bird DPO Services SRL, Brussels, dpo.superhuman@twobirds.com), both frequently absent among US-based mobile operators audited in this programme. No EU main establishment has been identified for Superhuman Platform Inc.; an Art. 27 representative does not itself establish the one-stop-shop mechanism, so this Austrian-initiated disclosure routes to the Österreichische Datenschutzbehörde.

Architecture & Data Flow (From the Operator’s Own Documentation)

Grammarly’s own support guide states that once the app is installed and set up, opening any app and tapping any text field makes the floating Grammarly widget appear, and the user can begin typing to receive suggestions immediately. The Play Store listing itself states: ”Accessibility permission is used to process text written in apps and provide you with tailored writing assistance. We also use this permission to turn Grammarly on when you’re typing in apps.” Exclusion is described as manual and reactive: the user holds and drags the widget downward until a block option appears, offering to deactivate Grammarly permanently in that specific app, after having already used it there. No self-disclosed mechanism for automatic exclusion of sensitive input categories, banking, health, dating, or password-manager apps, by default, was found anywhere in the reviewed documentation. Separately, the privacy policy’s ”User content” section states that this content ”may include information about others, such as when you exchange emails with people who don’t use our products,” an explicit first-party acknowledgment of third-party/bystander data within the scope of this programme’s methodology.

Engagement Summary

The original notice went to dpo.superhuman@twobirds.com, privacy@superhuman.com, and support@grammarly.com on 23 August 2026, with the Austrian DSB and the EDPS in copy. A follow-up restating the findings unchanged went out on 12 September 2026, twenty days later, with no reply or acknowledgment of any kind having arrived. A 35-days-to-publication notice went out on 17 October 2026, fifty-seven days without a reply. All three messages produced only automated Zendesk Customer Care ticket-received confirmations (ticket #8942531 on 12 September 2026, ticket #9039064 on 18 October 2026), generic "we've received your message" acknowledgments with no named person and no engagement with any finding. No human reply has arrived as of 14 November 2026.

Findings

F1: Default-on, opt-out-per-app Accessibility Service architecture, no self-disclosed sensitive-category exclusion

HIGH, CVSS scoring does not apply to a self-disclosed default-scope architecture finding; 0.0 (CVSS-B), assessed qualitatively as HIGH given the breadth of access and absence of a default exclusion

Grammarly's own Play Store listing and support guide confirm the Accessibility widget activates on any text field in any app immediately after setup, and that exclusion requires the user to manually locate and drag-to-block each individual app, only after having already used it there once. No self-disclosed mechanism for automatic exclusion of sensitive categories, banking, health, dating, password managers, by default, was found in the reviewed documentation.

```
"With your consent, Grammarly may collect data about app usage and device type.
    Accessibility
permission is used to process text written in apps and provide you with tailored
    writing
assistance. We also use this permission to turn Grammarly on when you're typing in
    apps."

"Once Grammarly for Android is installed and set up on your device, open any app and
    tap on any
text field, the floating Grammarly widget will appear on the screen."
"Hold and drag the Grammarly widget downward until a circle with an X appears...
    offering the
option to block Grammarly permanently."
```

The app usage/device-type collection sentence is explicitly qualified "with your consent"; the Accessibility-permission text-processing sentence that follows it in the same paragraph carries no such qualifier, describing what the permission grant itself enables rather than a separate consent event. No reply addressing this finding has been received; it stands exactly as disclosed.

Impact: The Accessibility widget is active by default over every text field in every installed

app from first setup, including a banking app's PIN entry, a telehealth app's symptom field, or a dating app's messages, until the user notices it there and manually blocks that specific app.

Fix: Open, no reply received.

F2: Play Data Safety declaration omits the core "User content/screen content" category the company's own privacy policy names as collected

---

HIGH, CVSS scoring does not apply to a cross-document disclosure-consistency finding; 0.0 (CVSS-B), assessed qualitatively as HIGH given this is the app's entire reason to exist

The Play Data Safety declaration for this exact listing lists collected data as Personal info (email, user IDs), Device or other IDs, and App info and performance (crash logs, diagnostics) only. No "User content," "Text," or "Screen content" category appears under either collected or shared data. The company's own privacy policy, one click from the same install screen, states under "User content": "We receive the content you upload or enable our products to access, such as emails and drafts, text, screen content, web pages, documents, files, calendars, images."

The same omission repeats a third time in the company's Trust Center FAQ, which answers "What data does Grammarly collect?" with only username, email address, contact and language preferences, again omitting the User content/screen content category the full privacy policy names. All three documents are first-party, dated the same period, for the same product.

Impact: The single Google-mandated disclosure a user sees on the install screen does not list the one data category that constitutes this app's entire reason to exist, the text and on-screen content it reads in order to give writing suggestions, while the company's own privacy policy explicitly names that category one click away from the same screen.

Fix: Open, no reply received.

F3: Third-party/bystander data self-acknowledged, no separate consent or transparency mechanism described for those individuals

MEDIUM, CVSS scoring does not apply to a transparency-gap finding for a self-acknowledged data category; 0.0 (CVSS-B)

The privacy policy states, verbatim: ”Your user content may include information about others, such as when you exchange emails with people who don’t use our products or if you choose to give our products access to your contacts so our editing products make appropriate spelling suggestions. We use the contact information and other information we receive about non-users through user content only to provide our products to you and will not use it to contact, advertise, or market to such individuals.”

Impact: A correspondent who never installed Grammarly, never saw an install screen, and never consented to anything has their name, writing, and communication content processed the moment the account holder’s Accessibility widget is active over an email containing that correspondent’s text, with no retention limit, deletion pathway, or Art. 14 mechanism specific to that non-user named anywhere in the reviewed policy.

Fix: Open, no reply received.

F4: Operator identity at install time does not match the controller named in the linked privacy policy

MEDIUM, CVSS scoring does not apply to a controller-identity transparency finding; 0.0 (CVSS-B)

The Play Store developer field for this listing reads ”Grammarly, Inc.”, the only entity name a user sees before installing. The privacy policy the same listing links opens: ”This Privacy Policy describes how Superhuman Platform Inc. (formerly Grammarly) and our subsidiaries (such as Grammarly Inc., Coda Project LLC, and Superhuman Labs LLC)...” and names the data controller as Superhuman Platform Inc., San Francisco.

Impact: The entity a user is told they are installing software from at the point of install is, per the company’s own current legal documents, a subsidiary of the entity that actually controls the data, a fact not stated anywhere in the Play Store listing itself.

Fix: Open, no reply received.

F5: Dead support link in the app's own Play Store description; AI-training default state not stated

LOW, CVSS scoring does not apply to a documentation-quality and unconfirmed-default finding; 0.0 (CVSS-B)

The Play Store description directs users to a support article about the keyboard's discontinuation at a URL that returns Grammarly's own 404 page. The underlying discontinuation fact is independently confirmed via Grammarly's own support index and public user reports, so only the specific linked article is dead, a minor transparency lapse.

Separately, the privacy policy states a training-opt-out control exists ("You can decide whether Superhuman can use your user content to train our AI models by adjusting the available training control(s) in your account settings") but does not state the default position of that control for a newly created account. This default state is UNVERIFIED: confirming it requires either binary or account-level testing, which this session had no binary to perform and which is correctly out of scope for an R1 regardless.

Impact: A minor self-referenced link failure, and an unconfirmed default for whether a new account's content is used for AI training.

Fix: Open, no reply received.

Impact Analysis

A person who installs Grammarly to improve their emails and social posts has, on the vendor's own documentation, the same Accessibility widget architecture available over their banking app's PIN entry, a telehealth app's symptom field, or a dating app's messages, until they notice it there and drag it into the block list. For the bystander case in F3, a person who has never heard of Grammarly, corresponds by email with someone who has it installed, and writes something sensitive, a health update, a custody detail, a financial figure, has that text pass through the same processing pipeline with no consent screen, no notice, and no distinct retention or deletion path of their own. A correspondent-side bystander is the statistically normal case for anyone who emails, texts, or messages a Grammarly user at all, on a product installed 50M+ times.

The Complete Chain

Point of contact: a user installs Grammarly for writing help and grants the Accessibility Service permission during setup, a single grant rather than a per-app choice. Processing: from that point, the floating widget activates automatically on any text field in any app, reading the screen content of the foreground app generally, not only the text committed to the field being typed into, per Grammarly's own description of the mechanism. Scope creep: because exclusion is manual, per app, and reactive, every app the user has not yet thought to block, a banking app, a health app, a messaging app carrying a bystander's words, is in scope by default. Disclosure gap: the one Google-mandated summary a user actually reads before installing, the Data Safety card, omits the exact category, User content/screen content, that this architecture processes, a gap that repeats in the Trust Center FAQ and is corrected only in the full privacy policy text most users never open. Consequence: both the account holder and any bystander who corresponds with them have their text and on-screen content processed under a scope broader than the install-screen disclosure describes, with the bystander specifically having no notice, no consent screen, and no channel of their own.

Data Protection: Article by Article

- Art. 25(2): data protection by default requires that the scope of processing not exceed what is necessary by default; an Accessibility widget active over every app from first setup, opt-out only after the fact, is the inverse of that default (F1).
- Art. 5(1)(c): data minimization, questioning whether universal default access to every app's screen content is necessary for a writing-assistance purpose (F1).
- Art. 13(1)(c)/(e): the Play Data Safety card's omission of the User content/screen content category misdescribes the scope and purpose of processing to the data subject at the one point most users actually read it (F2).
- Art. 5(1)(a) and Art. 5(2): lawfulness, fairness, transparency, and accountability are all engaged when a controller's own first-party disclosures disagree with each other across three separate documents (F2).
- Art. 14: no evidenced mechanism informs a non-user correspondent, at the point their emailed or messaged content is processed, that Grammarly now holds it (F3).
- Art. 5(1)(b): purpose limitation; the privacy policy's "will not use it to market" commitment toward non-users is a partial, not complete, purpose-limitation statement (F3).
- Art. 13(1)(a) and Art. 4(7): identity and contact details of the controller must be accurately provided; the install-time developer name does not match the privacy-policy-named controller (F4).

Regulatory & Legal Landscape

Superhuman Platform Inc. is a US-incorporated entity (San Francisco). A concrete EU/UK Art. 27 representative is named (VeraSafe Ireland Ltd, Cork, and VeraSafe United Kingdom Ltd, London) and a named Data Protection Officer is published (Bird & Bird DPO Services SRL, Brussels). An Art. 27 representative alone does not establish an EU main establishment or trigger the one-stop-shop mechanism, so this Austrian-initiated disclosure routes to the Österreichische Datenschutzbehörde, with the EDPS in copy per standing practice. No NISG or AI Act citation applies to this target; all GDPR article citations above are exact.

Indicators of Compromise & Reproducible Evidence

Artifact	Value
Package	com.grammarly.android.keyboard
Binary	NOT OBTAINED, see Methodology Note (DMCA removal on APKCombo; no listing on APKPure or APKMirror)
Dead support link cited by the app's own listing	support.grammarly.com/hc/en-us/articles/25038364027661 (returns Grammarly's own 404 page)
Play Data Safety declaration	play.google.com/store/apps/datasafety?id=com.grammarly.android.keyboard
Privacy policy (redirect target)	superhuman.com/legal/privacy-policy, effective 2026-07-06
EU/UK Art. 27 representative	VeraSafe Ireland Ltd, Cork / VeraSafe United Kingdom Ltd, London
DPO contact	dpo.superhuman@twobirds.com (Bird & Bird DPO Services SRL, Brussels)

Disclosure Timeline & Outcome

23 August 2026: original notice to dpo.superhuman@twobirds.com, privacy@superhuman.com, and support@grammarly.com, with the Austrian DSB and EDPS in copy. 12 September 2026: twenty days, no reply or acknowledgment of any kind, RFI-IRFOS restates the findings unchanged; an automated Zendesk Customer Care ticket-received confirmation (#8942531) arrives the same day, with no named person and no engagement with any finding. 17 October 2026: 35-days-to-publication notice, fifty-seven days without a reply; another automated Zendesk ticket-received confirmation (#9039064) arrives on 18 October 2026, again with no human engagement. As of 14 November 2026, no human reply of any kind has arrived at any stage of this correspondence.

What Grammarly Got Right

- A concrete, named EU/UK Art. 27 representative (VeraSafe Ireland Ltd / VeraSafe United Kingdom Ltd), frequently absent among US-based mobile operators audited in this programme.
- A named Data Protection Officer with a direct, functioning contact address (Bird & Bird DPO Services SRL, Brussels).
- EU-U.S., UK, and Swiss Data Privacy Framework certification is claimed and is specific and independently checkable against the official registry, not vague marketing language.
- The privacy policy states plainly that user content is not sold or used for advertising, and that the company's stated revenue model is subscription-based, not content-monetization-based.
- A working, described mechanism exists for users to request personal data deletion, including a self-service "Personal Data Report" tool described in the Trust Center FAQ.
- Grammarly's own "Is Grammarly a keylogger?" FAQ directly engages the exact concern this audit's thesis tests, rather than avoiding the question, even where the underlying scoping question in F1 remains open.
- A user-facing, documented per-app control ("Manage Blocked Apps") exists in plain language, more than many apps of this type offer at all.

Residual Risk & Recommendations

Every finding in this report rests on Grammarly’s own first-party, dated text, not on inference, and stands exactly as disclosed on 23 August 2026. No human reply of any kind has engaged any of the three questions put to the operator across three separate notices spanning fifty-nine days. The binary could not be obtained through any sanctioned channel this programme uses, so no code-level finding, and no CRITICAL severity, is issued for this target; this ceiling is a function of evidence availability, not of a lower actual risk. Should the application again become obtainable through a sanctioned mirror, or should the audit device be reconnected, a code-level follow-up pass is warranted given the scale of self-disclosed Accessibility Service access described above.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria A documentation- and self-disclosure-consistency audit of the operator’s own first-party published text. No binary was obtained; no code-level, manifest, or network analysis was performed. No CRITICAL severity is issued, consistent with this programme’s standing severity discipline. Research conducted under ISO/IEC 29147 and the freedom of scientific research (Art. 17 StGG). REF GRAMMARLYKEYBOARD-2026-R1.