# Security & Privacy Disclosure, Final Report

## Gboard, the Google Keyboard for Android (com.google.android.inputmethod.latin)

A keyboard under every app, with training defaults set to on and a store label that says its data cannot be deleted.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 20 NOVEMBER 2026. ONLY AUTOMATIC REPLIES, NO SUBSTANTIVE REPLY.**

| | |
|---|---|
| **Target** | Google LLC (global) and Google Ireland Limited (controller for EEA and Switzerland) |
| **Versions Audited** | 18.0.3.954559732 / versionCode 175940518, analysed 2026-08-22 |
| **Notice / Publication** | 2026-08-22 / 2026-11-20 (90 days) |
| **Findings** | 7: 1 Critical, 2 High, 2 Medium, 1 Low, 1 observation |
| **Status** | ONLY AUTOMATIC REPLIES, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026 |
| **SHA-256 (base APK)** | `66f93fdd6ca2e53675c725af38e7f47c9474cbb45e80afcefe9782817cec7179` |

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 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 7

6.1 C1: Federated training, usage metrics and personalised dictionaries ship with default value true, wired to a live Federated Compute endpoint . . . 7

6.2 C2: Typed text can be classified as PII and published to the Android Personal Context service for other surfaces on the device . . . 9

6.3 H1: READ_CONTACTS with a wide ContactsContract surface reads data about people who never installed the keyboard . . . 10

6.4 H2: The Data Safety label says data cannot be deleted, and the app offers only a local clear function . . . 11

6.5 M1: allowBackup is true with a custom BackupAgent and no declarative backup rules . . . 12

6.6 M2: GIF search text goes to Tenor, a separately branded Google product, with a key named dev . . . 13

6.7 L1: Firebase and Google API keys are hardcoded in strings.xml, as is usual for a first-party Google app . . . 14

7 Impact Analysis 14

8 The Complete Chain 15

9 Typed Text, Bystanders and Inference 15

10 Data Protection: Article by Article 16

11 Platform Disclosures: Google Play Data Safety and Reporting Channels 16

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 17

14 Disclosure Timeline & Outcome 18

15 What Google Got Right 18

16 Residual Risk & Recommendations 19

## Executive Summary

Gboard is the Google keyboard for Android, published by Google LLC under the package com.google.android.inputmethod.latin with more than ten billion downloads and a PEGI 3 rating. For users in the EEA and Switzerland the controller is Google Ireland Limited, which is an EU main establishment, so the question of an Article 27 representative does not arise. On 22 August 2026 RFI-IRFOS disclosed seven findings from a root level code analysis of version 18.0.3 under REF GBOARD-2026-R1.

A keyboard sees what people type into every other app. Capability alone is not a finding, and this report records no sign of keystroke logging. Its findings concern defaults and a cross-app path. Three keys for federated training, usage metrics and personalised dictionaries ship with a default of true, and the package holds the production endpoint of the Federated Compute service (C1). The package declares the Android Personal Context permissions and lists a suggestion type that its own code calls a PII suggestion (C2). Google's own Data Safety label says that data cannot be deleted, while the app offers to clear local data only (H2). The remaining findings are the contacts permission (H1), backup (M1), GIF search through Tenor (M2) and the hardcoded keys (L1).

The design has real merits. Federated learning is a better architecture than raw text logging, voice donation sits behind an explicit opt-in, cleartext traffic is denied, and no third-party advertising or attribution SDK was found. The findings concern the consent posture around that design and the paths beside it.

The notice of 22 August 2026 went to security@google.com and press@google.com with the Austrian DSB, the EDPS and the Irish Data Protection Commission in copy. Automatic replies arrived the same day. A follow-up on 12 September 2026, a second follow-up on 17 October 2026 and a third follow-up on 15 November 2026 repeated three questions addressed to Google Ireland Limited as controller. The only replies since are two further automatic messages, on 18 October and 15 November 2026. No finding and no question has been answered. This report is published after the embargo date of 20 November 2026 was reached.

**Scope:** Root level code analysis of Gboard 18.0.3.954559732 (versionCode 175940518), pulled from an installed device: manifest, resources, app-restrictions schema and the dex string pool of four classes*.dex files with about 4,800 class descriptors. The package carries platformBuildVersionName DEV, so the device may have been enrolled in a pre-release track. It is treated as equivalent to the public release for these findings. No control-flow analysis was done. The Play Data Safety page and the privacy policy at policies.google.com/privacy were read from the public sites on 22 August 2026. No Google server was called, no traffic was captured and no runtime instrumentation was used. Items the package cannot show are marked UNVERIFIED.

| ID | Severity | Title |
|---|---|---|
| C1 | CRITICAL | Federated training, usage metrics and personalised dictionaries ship with default value true, wired to a live Federated Compute endpoint |
| C2 | HIGH | Typed text can be classified as PII and published to the Android Personal Context service for other surfaces on the device |
| H1 | MEDIUM | READ_CONTACTS with a wide ContactsContract surface reads data about people who never installed the keyboard |
| H2 | HIGH | The Data Safety label says data cannot be deleted, and the app offers only a local clear function |
| M1 | LOW | allowBackup is true with a custom BackupAgent and no declarative backup rules |
| M2 | MEDIUM | GIF search text goes to Tenor, a separately branded Google product, with a key named dev |
| L1 | INFO | Firebase and Google API keys are hardcoded in strings.xml, as is usual for a first-party Google app |

### Finding Status at a Glance

| ID | Disclosed | This report | Status on 21 November 2026 |
|---|---|---|---|
| C1 | CRITICAL | CRITICAL | Open. Question 1 unanswered. |
| C2 | CRITICAL | HIGH | Open. Question 2 unanswered. |
| H1 | HIGH | MEDIUM | Open. No answer received. |
| H2 | HIGH | HIGH | Open. Question 3 unanswered. |
| M1 | MEDIUM | LOW | Open. Scope of the backup agent not read. |
| M2 | MEDIUM | MEDIUM | Open. No answer received. |
| L1 | LOW | INFO | Observation. Keys listed in full. |

## Subject & Operator Analysis

Gboard is published on Google Play by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. The privacy policy at policies.google.com/privacy names Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, as the controller for users in the EEA and Switzerland. Google Ireland Limited is an EU main establishment. The lead supervisory authority is therefore the Irish Data Protection Commission. The Österreichische Datenschutzbehörde and the European Data Protection Supervisor are in copy under the standing practice of the programme.

The Play listing read on 22 August 2026 shows Google LLC as developer, a rating of 4.4 from 18.8 million reviews, more than ten billion downloads, an update of 17 August 2026 and PEGI 3. A system keyboard is a reasonable fit for an all-ages rating and no mismatch is asserted. Google publishes a data protection contact through a troubleshooter page and no direct email address. The app is free and no billing library is present.

## Architecture & Data Flow

The package has four dex files and a base APK of 85 MB with three split APKs. The input method serves every app on the device. It holds an on-device training cache with example stores for speech features and next-word prediction, a federated training result handler that connects to the Federated Compute service, a contacts reader for name spelling, an audio recorder for voice typing with downloadable punctuation and capitalisation models, a GIF search that calls Tenor, and a custom backup agent. Server-side flags arrive through the Phenotype system, which the package wires extensively and which gives the operator control over feature state after installation. The package requests the three Personal Context permissions of the Android framework. Cleartext traffic is denied and the package sets no network security config. No advertising, attribution or session replay SDK was found.

## Engagement Summary

The notice REF GBOARD-2026-R1 was sent on 22 August 2026 at 14:19 UTC to security@google.com and press@google.com, with dsb@dsb.gv.at, edps@edps.europa.eu and info@dataprotection.ie in copy. It listed two critical, two high, two medium and one low finding with evidence, credited the design choices set out below and asked three questions of Google Ireland Limited as controller.

Three automatic replies arrived the same day. The security-noreply@google.com address answered that it is not monitored by humans and refers reporters of security vulnerabilities to Google's own reporting site. The Data Protection Commission mailbox answered that the channel does not accept queries about its market surveillance role, which is a different remit from the supervisory role that this notice engages. According to the follow-up of 12 September 2026 the press address sent its standing acknowledgement. That message is not in the retained thread. None of the three addressed a finding. The matters in this report are consent defaults, a data protection impact assessment and erasure. They are directed to the controller, and a vulnerability reporting programme is not the channel for them.

A follow-up with the three questions went to the same addresses on 12 September 2026, with a deadline of 19 September 2026. A second follow-up from security@rfi-irfos.com followed on 17 October 2026 under the subject line 34 days to publication. The security-noreply@google.com address answered again with the same automatic text on 18 October 2026 at 19:33 UTC. A third follow-up went from security@rfi-irfos.com on 15 November 2026 at 14:06 UTC under the subject line 5 days to publication, and security-noreply@google.com answered with the same automatic text at 14:06 UTC. No message from a person at Google is on record.

## Findings

### C1: Federated training, usage metrics and personalised dictionaries ship with default value true, wired to a live Federated Compute endpoint

**CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, open, rated CRITICAL by blast-radius escalation**

The app-restrictions schema of the package, which managed-configuration consoles read to learn an app's keys and shipped defaults, declares user_enable_federated_training with defaultValue true. It declares enable_user_metrics and pref_key_use_personalized_dicts with defaults that res/values/bools.xml resolves to true. The user-facing strings describe what the keys do: improving typing and voice typing from usage patterns and corrections, patterns that are combined with learnings from other users, and automatic sending of keyboard usage statistics to Google. The manifest declares the training-cache services that consume the data, among them ExampleStoreServiceMultiplexer, a speech precomputed feature store and a next-word-prediction store. The dex string pool of classes2.dex holds the endpoint https://federatedcompute-pa.googleapis.com. Federated learning is built to keep raw text on the device, which is a better design than raw logging. What the package does not show is the first-run flow, the wire payload, or whether data reaches the endpoint for a given user in the Union today. Those items are UNVERIFIED and the notice found no consent screen for these defaults in the string pool. A pre-ticked default is not valid consent under Article 4(11) and Article 7 (CJEU, Planet49, C-673/17). This is a consent and legal-basis finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to CRITICAL because the keyboard sees what people type into every other app, the install base is counted in billions, and typed and spoken text feed the pipeline. The score is zero because no technical vector exists.

```
<restriction android:key="user_enable_federated_training" android:defaultValue="true"
             android:restrictionType="bool" />
<restriction android:key="enable_user_metrics"
             android:defaultValue="@bool/APKTOOL_DUPLICATE_bool_0x7f05006a" .../>
<restriction android:key="pref_key_use_personalized_dicts"
             android:defaultValue="@bool/APKTOOL_DUPLICATE_bool_0x7f050097" .../>

res/values/bools.xml:
<bool name="APKTOOL_DUPLICATE_bool_0x7f05006a">true</bool>   (enable_user_metrics)
<bool name="APKTOOL_DUPLICATE_bool_0x7f050097">true</bool>   (
    pref_key_use_personalized_dicts)
```

```
FederatedResultHandlingService
ExampleStoreServiceMultiplexer (android:process=":train")
SpeechPrecomputedFeatureExampleStoreService  (/speech_precomputed_feature_data)
NWPSanityCheckEvalExampleStoreService         (/nwp_sanity_check_eval_data)
LocalComputationResultHandlingService         (/NEBULAE_LC-.*)

classes2.dex: https://federatedcompute-pa.googleapis.com
```

Strings read in res/values/strings.xml: ”Improve Gboard, Federated learning”, ”Help Google get better at recognizing words and phrases for everyone, based on your Gboard usage patterns on this device. These patterns are combined with learnings from other users”, and ”Automatically send keyboard usage statistics to Google”.

**Impact:** Every person who types or dictates on a phone with this keyboard is a possible contributor to a training pipeline of the operator, by default. The text includes messages, searches and spoken words. The user is not asked first, and the setting is described as an improvement option and not as a consent choice.

**Fix:** Show an upfront, unbundled consent choice for each purpose before the defaults take effect for users in the EEA, and ship the privacy-protective state as the default.

### C2: Typed text can be classified as PII and published to the Android Personal Context service for other surfaces on the device

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, open, rated HIGH by blast-radius escalation**

The manifest declares PERSONAL_CONTEXT_PUBLISH_HINTS, PERSONAL_CONTEXT_RECEIVE_INSIGHTS and PERSONAL_CONTEXT_HOST_INSIGHT_SURFACE. The dex string pool holds the android.service.personalcontext classes (PersonalContextManager, InsightSurfaceClient, ContextHint, ContextInsight and others) and three suggestion types that the keyboard's own code lists: AUGMENTED_AUTO_FILL_PERSONAL_CONTEXT_TEXT_SUGGESTION, AUGMENTED_AUTO_FILL_PERSONAL_CONTEXT_ACTION_SUGGESTION and AUGMENTED_AUTO_FILL_PERSONAL_CONTEXT_TEXT_PII_SUGGESTION. Strings for a PII suggestion tooltip and a PII filter flag for writing tools personalisation show that the engineers treat parts of what is typed as PII. The permissions and names are binary facts. Whether the path runs for a given user, what the classifier counts as PII, and whether any other app receives an insight, are UNVERIFIED because the package gives names and no control flow. The notice of 22 August 2026 rated this finding CRITICAL. This report rates it HIGH, because the package shows the capability and its framing and does not show an exercised flow. This is a capability and legal finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the keyboard sits under every app on the device, including banking, health and dating apps, and the classification of typed text as PII is named in the keyboard's own code. The score is zero because no technical vector exists.

```
<uses-permission android:name="android.permission.PERSONAL_CONTEXT_PUBLISH_HINTS"/>
<uses-permission android:name="android.permission.PERSONAL_CONTEXT_RECEIVE_INSIGHTS"/>
<uses-permission android:name="android.permission.
    PERSONAL_CONTEXT_HOST_INSIGHT_SURFACE"/>

Landroid/service/personalcontext/PersonalContextManager;
Landroid/service/personalcontext/hint/ContextHint;
Landroid/service/personalcontext/insight/ContextInsight;
AUGMENTED_AUTO_FILL_PERSONAL_CONTEXT_TEXT_PII_SUGGESTION
PII_SUGGESTION_TOOLTIP_SHOWN
writing_tools_p13n_enable_pii_filter
```

**Impact:** Text that a person types into a banking app, a health app or a dating app passes through the keyboard. A mechanism that labels such text as PII and hands it to a system service makes it travel beyond the app where the person typed it, without the developer of that app seeing it.

**Fix:** Publish what the Personal Context path does, which text qualifies as PII, who can receive the insights and how a user switches it off. Share the impact assessment for this path.

### H1: READ_CONTACTS with a wide ContactsContract surface reads data about people who never installed the keyboard

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 22 August 2026, open**

The manifest requests READ_CONTACTS. The dex files show the ContactsContract kinds Email, Event, Organization, Phone, StructuredPostal, Contacts, Data and Profile, and the string ”Registering contacts and device user name observers”. The Play string ”Improve voice typing with more accurate name spelling?” states the purpose. Every name, address, employer and number in a contact book belongs to a person who did not install the keyboard and saw no consent screen. The processing rests on the device owner’s permission alone. The scope of structured postal and organisation fields is wide for spelling suggestions. The permission is requested at runtime, and whether those fields enter the personalisation pipeline of C1 is UNVERIFIED. The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the user grants the permission and a purpose prompt exists.

```
<uses-permission android:name="android.permission.READ_CONTACTS"/>

Landroid/provider/ContactsContract$CommonDataKinds$Email;
Landroid/provider/ContactsContract$CommonDataKinds$Event;
Landroid/provider/ContactsContract$CommonDataKinds$Organization;
Landroid/provider/ContactsContract$CommonDataKinds$Phone;
Landroid/provider/ContactsContract$CommonDataKinds$StructuredPostal;
Landroid/provider/ContactsContract$Contacts;
Landroid/provider/ContactsContract$Data;
Landroid/provider/ContactsContract$Profile;
"Registering contacts and device user name observers [SD]"
```

**Impact:** The people in an address book, such as a doctor, a lawyer, a partner or a child’s school, have their names and details read into a keyboard feature without knowing that the keyboard exists on that phone.

**Fix:** Limit the fields read for name spelling to names, document the purpose per field and state whether contact data enters the training pipeline.

### H2: The Data Safety label says data cannot be deleted, and the app offers only a local clear function

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation**

The Data Safety label read live on 22 August 2026 declares collection of Audio, App activity, App info and performance, and Device or other IDs, states that no data is shared with third parties and states: "Data can't be deleted. The developer doesn't provide a way for you to request that your data be deleted." The strings of the package offer to clear on-device data that was saved to improve typing and voice typing, and say that transcripts saved on the device can be deleted by deleting learned words and data. The two statements come from the same company and describe different scopes. Local data can be cleared. For data that has already reached the server side of the training and metrics pipeline in C1, no deletion path is disclosed, and the label says so itself. This is a transparency and rights finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the controller's own public declaration says that no erasure path exists for a service that handles what people type and say. The score is zero because no technical vector exists.

```
Play Data Safety (read 2026-08-22):
  "No data shared with third parties"
  Collected: Audio, App activity, App info and performance, Device or other IDs
  "Data is encrypted in transit"
  "Data can't be deleted - The developer doesn't provide a way for you to request
   that your data be deleted."

res/values/strings.xml:
  "Clear all on-device data that Gboard has saved to improve your typing and voice
    typing experience"
  "Transcripts of what you say and type will be saved on this device. You can delete
    them
   anytime by deleting learned words and data."
```

**Impact:** A person who wants the keyboard to forget what they typed can clear what is on their phone. For anything that has already left the phone, the operator's own label says there is no way to ask.

**Fix:** Describe the erasure path for server-side data in the label and in the app, or correct the label if such a path exists.

### M1: allowBackup is true with a custom BackupAgent and no declarative backup rules

**LOW, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, open**

The application element sets android:allowBackup to true with the backup agent com.google.android.libraries.inputmethod.backup.BackupAgent and restoreAnyVersion true. No android:fullBackupContent or android:dataExtractionRules attribute exists and res/xml holds no rules file. Backup scope is defined in the custom agent's code, which this analysis did not read, so what the agent includes (personal dictionary, learned words, clipboard history) is UNVERIFIED. The notice of 22 August 2026 rated this finding MEDIUM. This report rates it LOW, which is the CVSS band of the exposure that the package shows.

```
<application android:allowBackup="true"
    android:backupAgent="com.google.android.libraries.inputmethod.backup.BackupAgent"
    android:killAfterRestore="false" android:restoreAnyVersion="true" ...>
```

**Impact:** Personalisation data such as learned words may be copied into backup storage, and the user has no list of what that includes.

**Fix:** Document what the BackupAgent includes and exclude sensitive learned data from backup.

### M2: GIF search text goes to Tenor, a separately branded Google product, with a key named dev

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, open, rated MEDIUM by blast-radius escalation**

The strings hold tenor_v2_dev_api_key and the dex files hold the Tenor v2 endpoints https://tenor.googleapis.com/v2/ for autocomplete, categories, featured, posts, registershare, search and trending_terms. Free text that a user types into GIF search can describe mood, relationships or health topics. It goes to a product with its own terms and brand, which a user is unlikely to see as part of the keyboard. A production build that ships a key named dev is a hygiene point. Whether Tenor is disclosed as a separate recipient is a question to the operator. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the query text can reveal mood, relationships or health topics and goes to a recipient that users do not link to the keyboard. The score is zero because no technical vector exists.

```
tenor_v2_dev_api_key: AIzaSyAyimkuYQYF_FXVALexPuGQctUWRURdCYQ

https://tenor.googleapis.com/v2/{autocomplete,categories,featured,posts,registershare,
    search,trending_terms}
```

**Impact:** A person who types a feeling or a health topic into GIF search sends that text to a service they did not choose, under a different product name.

**Fix:** Name Tenor as a recipient in the notice shown for GIF search and use a production key.

### L1: Firebase and Google API keys are hardcoded in strings.xml, as is usual for a first-party Google app

**INFO, no CVSS v4.0 score assigned, disclosed as LOW on 22 August 2026, recorded as an observation**

google_api_key and google_crash_reporting_api_key resolve to the same literal value in res/values/strings.xml. Such client keys are not secrets in Google's own model and are bound by project restrictions. The availability concerns that apply to a small operator's unrestricted key apply with less weight to a project that the platform owner runs itself. The keys are listed in full under the programme's standing rule that every shipped key is a finding. The finding carries no score. No call was made against either key.

```
google_api_key:                AIzaSyDPejeIUWuoRgIrn35eLPSjig2WR8C3jBg
google_crash_reporting_api_key: AIzaSyDPejeIUWuoRgIrn35eLPSjig2WR8C3jBg
```

The notice of 22 August 2026 rated this finding LOW. This report records it as an observation. The key cannot be rotated for installed copies without an app update.

**Impact:** The exposure is small. The point for users is that a key printed in every copy of the app cannot be withdrawn from copies already installed.

**Fix:** Confirm that the key is restricted by package and certificate and that App Check is enforced where it applies.

## Impact Analysis

The people affected are everyone who types or dictates on a phone with this keyboard, and the people whose names and details sit in their contact books. What people type into banking, health and dating apps passes through the keyboard. The sample cases are a banking field with an account number, a health app with a symptom description and a dating app with a phone number.

The findings do not describe a keylogger. The weight lies in two places. The default state of the training and metrics settings is on, so a very large user base takes part unless each person finds the switch (C1). A path exists in the package that treats typed text as PII and offers it to a system service (C2). A user who then asks for deletion reads a label that says there is no way to ask (H2).

## The Complete Chain

Step 1, install and first use: the keyboard is installed or comes with the device, and the user types into other apps. The Play label shows what Google declares (H2).

Step 2, defaults: three settings for federated training, usage statistics and personalised dictionaries are on by default. Their wording is that of improvement options and not of a consent request (C1).

Step 3, contacts: if the user allows contact access for name spelling, the details of people in the contact book are read (H1).

Step 4, personalisation: typed and spoken text feed on-device example stores, and the package holds the endpoint of the Federated Compute service (C1). GIF search queries go to Tenor (M2).

Step 5, cross-app path: text classified as a PII suggestion can be offered to the Personal Context system service for other surfaces (C2).

Step 6, device: a custom backup agent may copy personalisation data into backup storage (M1).

Step 7, erasure: the user can clear local data. For anything already sent, the label says that deletion cannot be requested (H2).

## Typed Text, Bystanders and Inference

The keyboard holds an intermediary position. It sees text before the app that receives it. Two categories of the programme's methodology apply directly.

Bystander data: the people in the contact book give no consent and learn nothing about the processing (H1).

Inference data: a PII suggestion is a derived label that says more than the typed text it came from, because it marks a piece of text as personal information (C2). Control data: the Phenotype system lets the operator change feature state after installation. Which flags are live for a given user is UNVERIFIED.

The categories of non-events, household graph and notification relationships do not apply. The package requests no location or notification listener permission.

## Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H2 and M2.

Article 5(1)(b) and (c), purpose limitation and data minimisation: engaged by C2 and H1.

Article 6(1) and Article 7(1) and (2), legal basis and conditions for consent: engaged by C1 and H1. A pre-ticked default is not valid consent (CJEU, Planet49, C-673/17).

Article 9, special categories: engaged by C2 where classified text comes from health or finance contexts.

Article 12 and Article 17, transparency and erasure: engaged by H2.

Article 13 and Article 14, information: engaged by H1 and M2.

Article 25, data protection by design and by default: engaged by C1, C2 and M1.

Article 32(1)(b), security of processing: engaged by M1 and L1.

Article 35, impact assessment: asked as question 2 in C2.

ePrivacy Directive Art. 5(3): engaged by C1, where storing or reading information on the terminal equipment needs consent unless strictly necessary.

## Platform Disclosures: Google Play Data Safety and Reporting Channels

Google is the operator of the app and the operator of the platform that hosts the Data Safety label. The label is a declaration that the developer completes, and for Gboard the developer is Google LLC. This report attributes the label to the developer and makes no separate claim about the platform.

The label read on 22 August 2026 lists Audio, App activity, App info and performance and Device or other IDs as collected, states that no data is shared with third parties, that data is encrypted in transit and that data cannot be deleted. It also names an independent security review. The statement on deletion is the subject of H2. The page was not archived at the time of reading and should be fetched again before publication.

Google runs its own programme for reports about security vulnerabilities, and its automatic reply points reporters to it. This disclosure is addressed to the controller under the GDPR. It concerns the legal basis for default settings, an impact assessment and erasure, and none of these is a vulnerability in the technical sense. The programme is therefore not the channel used here.

## Regulatory & Legal Landscape

The framework applied is the GDPR with its provisions on consent, the legal basis, erasure and impact assessment, together with Article 5(3) of the ePrivacy Directive for terminal equipment. Google Ireland Limited is the controller for users in the EEA and Switzerland and an EU main establishment, so the Irish Data Protection Commission is the lead supervisory authority and the one-stop-shop applies. The Commission is in copy of the notice at info@dataprotection.ie.

The Österreichische Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) are in copy under the standing practice of the programme. The disclosure follows ISO/IEC 29147 and Art. 17 StGG. No obligation under other digital regulation is asserted in this report.

## Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding from the package. All values are given in full.

```
Package            com.google.android.inputmethod.latin
Version            18.0.3.954559732-release-arm64-v8a (versionCode 175940518),
    analysed 2026-08-22
base.apk SHA-256   66f93fdd6ca2e53675c725af38e7f47c9474cbb45e80afcefe9782817cec7179
base.apk size      89,003,043 bytes (3 split APKs: config.xxhdpi, brella_feature_split
    , tenoranimation_feature_split)
Federated endpoint https://federatedcompute-pa.googleapis.com
Tenor key          AIzaSyAyimkuYQYF_FXVALexPuGQctUWRURdCYQ
Google API key     AIzaSyDPejeIUWuoRgIrn35eLPSjig2WR8C3jBg (google_api_key and
    google_crash_reporting_api_key)
Controller (EEA)   Google Ireland Limited, Gordon House, Barrow Street, Dublin 4
```

```
C1  res/xml/APKTOOL_DUPLICATE_xml_0x7f170002.xml: user_enable_federated_training,
    enable_user_metrics, pref_key_use_personalized_dicts
C1  res/values/bools.xml: two bool values true. AndroidManifest.xml: training cache
    services. classes2.dex: federatedcompute-pa
C2  AndroidManifest.xml: PERSONAL_CONTEXT_* permissions. classes*.dex: android.service
    .personalcontext.*, AUGMENTED_AUTO_FILL_* types
H1  AndroidManifest.xml: READ_CONTACTS. classes*.dex: ContactsContract kinds
H2  https://play.google.com/store/apps/datasafety?id=com.google.android.inputmethod.
    latin (read 2026-08-22). res/values/strings.xml
M1  AndroidManifest.xml: application element, BackupAgent
M2  res/values/strings.xml: tenor_v2_dev_api_key. classes2.dex: tenor.googleapis.com/
    v2
L1  res/values/strings.xml: google_api_key, google_crash_reporting_api_key
```

Reproduction: obtain Gboard 18.0.3.954559732 from Google Play or from the package manager of a device, check the SHA-256 above, decode the manifest and resources with apktool and read the named files. No account or network access is needed for the package findings.

## Disclosure Timeline & Outcome

2026-08-22 Notice REF GBOARD-2026-R1 to security@google.com and press@google.com, CC DSB, EDPS and the Irish Data Protection Commission. Two critical, two high, two medium and one low finding, three questions asked.

2026-08-22 Three automatic replies: security-noreply@google.com (not monitored, refers to Google's own vulnerability reporting site), the Data Protection Commission mailbox (channel does not accept queries about its market surveillance role) and the press address (standing acknowledgement, as recorded in the follow-up of 12 September). No finding addressed.

2026-09-12 Follow-up to the same addresses with the three questions restated, deadline 19 September 2026, embargo named as 20 November 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com, 34 days before the embargo date.

2026-10-18 Automatic reply from security-noreply@google.com, same text as on 22 August. No message from a person.

2026-11-15 Third follow-up from security@rfi-irfos.com at 14:06 UTC, five days before the embargo date.

2026-11-15 Automatic reply from security-noreply@google.com at 14:06 UTC, same text as before. No message from a person.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026.

2026-11-21 No reply from a person and no written position on record.

## What Google Got Right

Cleartext traffic is denied by default. No third-party advertising, attribution or session replay SDK was found, and the package requests no advertising ID permission. No SDK or endpoint from sanctioned or high-risk jurisdictions appears in the string pool. Federated learning keeps raw text on the device and is a materially better design than logging text to a server. The donation of voice audio sits behind an explicit opt-in prompt, which is a more consent-conscious design than the default settings in C1. A PII filter flag exists for a generative personalisation path of writing tools, which shows privacy engineering at work. Google Ireland Limited is a genuine EU main establishment, so users in the Union have a controller with an address in the Union. The Data Safety label states plainly what it declares, including the deletion statement, which made H2 possible to read at all.

## Residual Risk & Recommendations

Open at the date of publication: all seven items, with no written position from the operator as of 21 November 2026. Items that only the operator can close are the consent state in C1, the Personal Context path in C2, the contacts scope in H1, the erasure path in H2, the backup scope in M1, the Tenor disclosure in M2 and the key restrictions in L1.

Recommendations: ship the training, metrics and dictionary settings off until a consent choice is made, publish what the Personal Context path does and who can receive its insights, limit contact fields to what spelling needs, describe or provide an erasure path for server-side data and correct the label, document the backup agent, name Tenor as a recipient and use a production key.

Statements are limited to the package and the public documents named 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 Root level code analysis of the published application.

No Google servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF GBOARD-2026-R1.