



Security & Privacy Disclosure, Final Report

Bosch Smart Home Android (com.bosch.sh.ui.android)

A hardcoded Firebase/Google API key and database URL ship inside an otherwise structurally clean smart-home binary, nine messages and 111 days later the one reply received redirected responsibility to a different Bosch-affiliated legal entity than the one this disclosure itself correctly identified as the app's EU-established publisher, and none of the three technical questions asked was ever answered

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28 SEPTEMBER 2026, ONE REPLY RECEIVED, RESPONSIBILITY REDIRECTED TO A DIFFERENT ENTITY, THREE QUESTIONS NEVER ANSWERED

Target	Robert Bosch Smart Home GmbH (Stuttgart) — the EU-established entity RFI-IRFOS's original disclosure identified as this app's publisher. Bosch's own 2026-09-21 reply redirected responsibility to BSH Hausgeraete GmbH, a separate Bosch-affiliated company, without disputing the original identification
Package	com.bosch.sh.ui.android v10.33.4335
Platform Audited	Android, static analysis of the production APK
Initial Disclosure (R1)	2026-06-30, to DPO@bosch.com, BCC Austrian Datenschutzbehoerde and EDPS
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (1 High, 4 Medium, 0 Critical) — the lowest-severity binary in RFI-IRFOS's 2026 smart-home comparison series
Correspondence	9 messages sent by RFI-IRFOS over 111 days (2026-06-30 to 2026-09-12), 1 reply received (2026-09-21, 9 days after the final follow-up and 17 days after the embargo had already passed), redirecting responsibility to a different legal entity, none of the three technical questions answered
Authorities Notified	Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	H1: Hardcoded Firebase/Google API key and Realtime Database URL in the production binary	6
4.2	M1: In-home camera and two-way intercom audio: cloud-recording tier lacks documented Art. 9 lawful basis and retention terms	6
4.3	M2: Foreground presence geofencing implemented without background location, lawful basis undocumented	7
4.4	M3: Vestigial advertising-ID permissions present with no advertising SDK and ads defaulted off	7
4.5	M4: International transfers to Qualtrics and Firebase (United States), and the Security+ alarm-centre flow to Bosch Service Solutions GmbH, not precisely disclosed	7
5	Impact Analysis	8
6	The Complete Chain: Nine Messages, 111 Days, One Reply, Zero Answers	8
7	Data Protection – Article by Article	9
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	11

Executive Summary

Bosch Smart Home is a local-hub smart-home platform app published under `com.bosch.sh.ui.android`. A static analysis of production APK v10.33.4335 (base.apk sha-256 36059d11...faa1d02) found it to be the cleanest binary in RFI-IRFOS's 2026 smart-home comparison series: no Chinese-origin SDKs, no advertising networks, no third-party analytics brokers, cleartext transport disabled globally, telemetry consent-gated and defaulted off, no background location, and an EU-established publisher with a named lead supervisory authority. RFI-IRFOS's original disclosure letter led with this praise before stating its one substantive finding.

That one finding, H1, is a Firebase/Google API key and a Firebase Realtime Database URL hardcoded directly in the binary's string resources (both withheld from this public report; full values were disclosed privately to Bosch in the original R1 letter). An unrestricted key of this kind exposes the project to quota and billing exhaustion, and creates a conditional path to a full database read if the corresponding security rules are not locked to authenticated access. Four further medium-severity notes (M1-M4) covered in-home camera/intercom audio handling, geofencing documentation, vestigial advertising-ID permissions, and undocumented international transfers to Qualtrics and Firebase in the United States.

RFI-IRFOS disclosed these findings on 30 June 2026 to `DPO@bosch.com`, with the Austrian Datenschutzbehörde and the EDPS in BCC per standing practice, stating an embargo date of 28 September 2026. Seven further follow-ups were sent (6 July, 17 July, 23 July, 31 July, 9 August, 21 August, 28 August, 12 September 2026), each restating the finding and three specific yes/no questions, drawing no reply of any kind across that entire 74-day span.

On 21 September 2026, 9 days after the last follow-up and 17 days after the embargo had already passed, `dpo@bosch.com` replied for the first and only time in the correspondence. The reply stated that the mailbox is responsible for Robert Bosch GmbH's information security and data protection, that it is unable to process the matter further because BSH Hausgeraete GmbH is a separate legal entity, and redirected RFI-IRFOS to BSH's own contact channels. The reply did not dispute, correct, or otherwise engage with RFI-IRFOS's original identification of Robert Bosch Smart Home GmbH (Stuttgart) as the app's EU-established publisher, and did not answer any of the three technical questions asked. The embargo of 28 September 2026 has now passed, 19 days overdue, with the one finding that required a technical answer still unanswered on the day this report publishes.

ID	Severity	Title
H1	HIGH	Hardcoded Firebase/Google API key and Realtime Database URL in the production binary
M1	MEDIUM	In-home camera and two-way intercom audio: cloud-recording tier lacks documented Art. 9 lawful basis and retention terms
M2	MEDIUM	Foreground presence geofencing implemented without background location, lawful basis undocumented
M3	MEDIUM	Vestigial advertising-ID permissions present with no advertising SDK and ads defaulted off

ID	Severity	Title
M4	MEDIUM	International transfers to Qualtrics and Firebase (United States), and the Security+ alarm-centre flow to Bosch Service Solutions GmbH, not precisely disclosed

Subject & Operator Context

RFI-IRFOS's original disclosure identified Robert Bosch Smart Home GmbH, Stuttgart, as the EU-established publisher of com.bosch.sh.ui.android, naming the LfDI Baden-Wuerttemberg as the resulting lead supervisory authority and noting that no Art. 27 EU representative was therefore required. The app itself is branded and distributed as a Bosch-branded smart-home product. The one reply received in this correspondence, from dpo@bosch.com, states that the mailbox serves Robert Bosch GmbH and redirects responsibility to BSH Hausgeraete GmbH, a separate Bosch-affiliated company that manufactures household appliances. That reply did not dispute RFI-IRFOS's original identification of the publisher, nor explain the apparent mismatch between the Bosch-branded smart-home app this disclosure concerns and the household-appliance entity it was redirected to. RFI-IRFOS did not pursue a new disclosure to BSH Hausgeraete GmbH, as doing so would open a separate case outside this disclosure's original, never-disputed scope.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to DPO@bosch.com, with the Austrian Datenschutzbehörde and the EDPS in BCC per standing practice, stating an embargo date of 28 September 2026. The letter led with an extended list of what the app got right, before presenting the one HIGH finding (hardcoded Firebase/Google API key and database URL) and four MEDIUM notes, and asking three specific yes/no questions: whether the key is restricted to the production signing certificate and scoped to only the APIs it needs; whether the Firebase Realtime Database security rules are deny-by-default; and whether Bosch's DPO is aware of and has logged the finding internally.

Seven follow-ups were sent at roughly weekly-to-biweekly intervals (6 July, 17 July, 23 July, 31 July, 9 August, 21 August, 28 August, 12 September 2026), each restating the finding and the three questions, each explicitly keeping the collegial tone warranted by an otherwise clean report. The Austrian Datenschutzbehörde was moved into visible CC from the 23 July follow-up onward. None of these eight messages, spanning 74 days from the original disclosure to the last follow-up, drew any reply, not even an acknowledgment of receipt.

On 21 September 2026, dpo@bosch.com replied for the first and only time: the mailbox is responsible for Robert Bosch GmbH's information security and data protection, it cannot process the matter further because BSH Hausgeraete GmbH is a separate legal entity, and RFI-IRFOS should contact BSH directly at its own contact channels. The reply did not address, dispute, or acknowledge any of the three technical questions, and did not explain why a Bosch-branded smart-home app, whose EU-established publisher RFI-IRFOS's own R1 letter had named as Robert Bosch Smart Home GmbH, was now being attributed to a household-appliance manufacturer.

Findings

H1: Hardcoded Firebase/Google API key and Realtime Database URL in the production binary

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.5 — unrestricted key enables quota/billing exhaustion and a conditional database-read path

```
res/values/strings.xml -> google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed  
    privately to Bosch in R1]  
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to Bosch in  
    R1]  
Key reused for: Firebase, Crashlytics, Maps/Geo API  
Reachable by: any party decompiling the published APK
```

Impact: A Firebase/Google API key, serving Firebase, Crashlytics and the Maps Geo API simultaneously, is hardcoded in the production APK's string resources, alongside the Firebase Realtime Database URL it is wired to. Both values are withheld from this public report; full values were disclosed privately to Bosch in the original R1 letter. An unrestricted key of this kind directly enables quota and billing exhaustion against the underlying Google Cloud project, and establishes a conditional full-database-read path if the corresponding Realtime Database security rules are not locked to authenticated, deny-by-default access. This is a confirmed implementation gap, straightforward to remediate by restricting the key to the production signing certificate and verifying the database rules server-side, independent of any further review.

M1: In-home camera and two-way intercom audio: cloud-recording tier lacks documented Art. 9 lawful basis and retention terms

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 — user-initiated, no background capture, flagged for documentation only

Impact: The app supports in-home camera monitoring and two-way intercom audio over RTSP, with an optional cloud-recording tier. Capture is strictly user-initiated: there is no standing CAMERA manifest permission and no background audio or video capture, which is the privacy-respecting design choice. Interior audio and video can nonetheless constitute Art. 9 special-category data by capturing third parties inside the home, so the lawful basis and retention period for the optional cloud-recording tier specifically should be documented in the privacy notice.

M2: Foreground presence geofencing implemented without background location, lawful basis undocumented

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0 — privacy-respecting implementation choice, documentation gap only

Impact: Presence-based automation uses foreground geofencing without requesting background location access, which is itself the privacy-respecting implementation choice and is noted as such. The Art. 6 lawful basis for this foreground location processing is not documented in the available privacy information and should be added.

M3: Vestigial advertising-ID permissions present with no advertising SDK and ads defaulted off

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 4.2 — dead permissions, trivially removable

Impact: The manifest declares AD_ID and ACCESS_AD SERVICES_* permissions although no advertising SDK is present anywhere in the binary and advertising is defaulted off. These are vestigial and inconsistent with the data-minimisation principle of Art. 5(1)(c); they can simply be removed in the next release with no functional impact.

M4: International transfers to Qualtrics and Firebase (United States), and the Security+ alarm-centre flow to Bosch Service Solutions GmbH, not precisely disclosed

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, 5.5 — transfer mechanism and processor relationship not named in available privacy information

Impact: The app sends EU user data to Qualtrics (US) for in-app surveys and to Firebase (US) for core app services, and routes the Security+ alarm-centre and emergency-contact flow to Bosch Service Solutions GmbH as a processor. Neither the specific Art. 46 transfer mechanism for the two US transfers nor the processor relationship for the alarm-centre flow was identified as precisely named in the app's available privacy information, as required by Art. 13(1)(f) and Art. 28.

Impact Analysis

H1 and the four medium notes are routine, fixable engineering and documentation gaps in what RFI-IRFOS's own original letter called the cleanest smart-home binary in its 2026 series, not evidence of systemic disregard for data protection. What sets this case apart procedurally is not the technical substance but the correspondence: 74 days and eight messages of complete silence, followed by a single reply, 9 days after the last follow-up and 17 days after the embargo had already passed, that redirected responsibility to a different legal entity without ever engaging the three technical questions the entire correspondence had been asking.

The Complete Chain: Nine Messages, 111 Days, One Reply, Zero Answers

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings on 30 June 2026 to DPO@bosch.com, with the Austrian Datenschutzbehörde and the EDPS in BCC, stating an embargo of 28 September 2026.

Step 2 – Extended silence: Follow-ups on 6 July, 17 July, 23 July (Austrian Datenschutzbehörde moved to visible CC), and 31 July 2026 restate the finding and the three questions. No reply to any of them.

Step 3 – Continued silence: Further follow-ups on 9 August, 21 August, and 28 August 2026 restate the same finding and questions again. No reply.

Step 4 – Final follow-up: On 12 September 2026, a further nudge is sent, now 74 days since the original disclosure. No reply.

Step 5 – Embargo passes unanswered: 28 September 2026, the stated embargo date, passes with the correspondence still completely unanswered.

Step 6 – The one reply, after the embargo: On 21 September 2026 dpo@bosch.com replies for the first and only time, stating the mailbox serves Robert Bosch GmbH and redirecting RFI-IRFOS to BSH Hausgeraete GmbH, a separate legal entity, without disputing the original identification of Robert Bosch Smart Home GmbH as the app's EU-established publisher and without answering any of the three questions.

Step 7 – Publication: This report publishes 19 days after the embargo, with the full record intact: nine messages sent, one reply received, that reply redirecting responsibility elsewhere rather than answering, and the one finding that required a technical answer still unanswered.

Data Protection – Article by Article

Art. 32(1)(b), Art. 5(1)(f) GDPR – Security of processing, integrity and confidentiality: H1's hardcoded Firebase/Google API key and database URL fall short of the technical measures these provisions require.

Art. 9 GDPR – Special categories of data: M1's in-home camera/intercom audio can capture Art. 9-relevant data of household members and visitors; the cloud-recording tier's lawful basis and retention period are not documented.

Art. 6 GDPR – Lawfulness of processing: M2's foreground geofencing lacks a documented lawful basis, despite its privacy-respecting technical implementation.

Art. 5(1)(c) GDPR – Data minimisation: M3's vestigial advertising-ID permissions are inconsistent with this principle regardless of whether they are ever exercised.

Art. 13(1)(f), Art. 28, Art. 44-49 GDPR – Transfer transparency and processor relationships: M4's transfers to Qualtrics and Firebase (US) and the Security+ processor relationship with Bosch Service Solutions GmbH are not precisely named in the available privacy information.

Regulatory & Legal Landscape

RFI-IRFOS's original disclosure named Robert Bosch Smart Home GmbH (Stuttgart) as the app's EU-established publisher, with the LfDI Baden-Wuerttemberg as the resulting lead supervisory authority. The Austrian Datenschutzbehörde and the EDPS were in BCC on the original disclosure per RFI-IRFOS's standing practice, and the Austrian Datenschutzbehörde was moved into visible CC from 23 July 2026 onward. The one reply received, from dpo@bosch.com on 21 September 2026, did not dispute this entity identification; it redirected responsibility to BSH Hausgeraete GmbH, a separate Bosch-affiliated company, without explaining the relationship between that company and the Bosch-branded smart-home app this disclosure concerns.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 and Art. 5(1)(f) issue in H1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 9, Art. 13, and Art. 44-49 issues in M1 and M4, up to EUR 20,000,000 or 4% of total worldwide annual turnover. A reply that redirects responsibility to a different legal entity rather than answering the underlying technical questions is itself a fact a supervisory authority may find relevant when assessing how the original disclosure was handled internally.

Indicators of Compromise

The following findings were extracted from the production APK via static analysis only. No Bosch servers, accounts, or infrastructure were probed. The hardcoded key and database URL referenced in H1 are withheld from this public report; full values were disclosed privately to Bosch in the original R1 letter.

```
H1 -- Hardcoded Firebase/Google API key + Realtime Database URL,  
res/values/strings.xml, redacted in this public report
```

```
M1-M4 -- camera/intercom cloud tier, foreground geofencing,  
vestigial AD_ID permissions, Qualtrics/Firebase (US) + Bosch  
Service Solutions GmbH transfer disclosure gaps
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to DPO@bosch.com, BCC Austrian Datenschutzbehoerde and EDPS. Embargo stated as 2026-09-28.

2026-07-06 Follow-up sent. No reply.

2026-07-17 Follow-up sent. No reply.

2026-07-23 Follow-up sent, Austrian Datenschutzbehoerde moved to visible CC. No reply.

2026-07-31 Follow-up sent. No reply.

2026-08-09 Follow-up sent. No reply.

2026-08-21 Follow-up sent. No reply.

2026-08-28 Follow-up sent. No reply.

2026-09-12 Follow-up sent, 74 days since original disclosure. No reply.

2026-09-21 dpo@bosch.com replies for the first and only time: redirects responsibility to BSH Hausgeraete GmbH, a separate legal entity, without disputing the original publisher identification and without answering any of the three technical questions.

2026-09-28 Main embargo date reached and passed with the one finding that required a technical answer still unanswered.

2026-10-17 This report published, 19 days after the embargo date. Correspondence record: nine RFI-IRFOS messages, one reply received, zero of three questions answered.

Residual Risk & Recommendations

H1 – Immediate: restrict the hardcoded Firebase/Google API key to the production signing certificate and intended API scope, confirm the Realtime Database security rules are deny-by-default and locked to authenticated access, and rotate the key after disclosure.

M1 – Document the Art. 9 lawful basis and retention period for the optional cloud-recording tier of the in-home camera/intercom feature.

M2 – Document the Art. 6 lawful basis for foreground presence geofencing.

M3 – Remove the vestigial AD_ID and ACCESS_ADSERVICES_* permissions; no advertising SDK depends on them.

M4 – Name the specific Art. 46 transfer mechanism for the Qualtrics and Firebase (US) transfers, and the processor relationship with Bosch Service Solutions GmbH for the Security+ alarm-centre flow, in the app's privacy notice.

Procedural: a reply that redirects responsibility to a different legal entity, without disputing the original entity identification and without answering the specific technical questions on record, does not resolve the one finding that required an answer. RFI-IRFOS remains open to a substantive reply to the three questions, whether from Robert Bosch Smart Home GmbH or BSH Hausgeraete GmbH, at any time; this report will be updated to reflect one if it arrives.

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 All findings derive from static analysis of the pub-

lished application using publicly available tooling. No Bosch servers, accounts, or infrastructure were probed. The hardcoded credential and database URL referenced in finding H1 are withheld from this public report; full values were disclosed privately to Bosch in the original R1 letter and remain available to Bosch or to a supervisory authority on request. Technical evidence is archived under chain of custody. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF BOSCH-2026-R1-001.