Security & Privacy Disclosure, Final Report

Lovense Remote, companion app for internet-connected intimate devices, Android (com.lovense.wear)

A link that lets a stranger control a device worn on the body, behind a self-declared age gate.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO OF 20 NOVEMBER 2026 REACHED. PUBLISHED TOGETHER WITH THE OPERATOR'S RESPONSE OF 18 NOVEMBER 2026 AND CORRECTED ON ITS REQUEST.

Target	HYTTO PTE. LTD., Singapore, UEN 201926411M, publisher of Lovense Remote
Versions Audited	8.5.0 / versionCode 574, analysed 2026-08-22, and 8.7.0 / versionCode 579, checked 2026-09-21
Notice / Publication	2026-08-22 / 2026-11-20 (90 days), published 2026-11-21
Findings	7: 1 Critical, 1 High, 5 Medium
Status	OPERATOR REPLIED ON 10, 21 AND 29 SEPTEMBER AND ON 18 NOVEMBER 2026. PUBLISHED TOGETHER WITH THE OPERATOR'S RESPONSE AND CORRECTED ON ITS REQUEST. C1 OPEN.
SHA-256 (base APK)	`7782f6e9696277cfbbac016c907fd2b8d74063748aad175b6b954afe37a1e62c`

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 5

6 Findings 7

6.1 C1: Control Link lets an anonymous stranger take live control of a body-worn device, and the age gate is self-declared . . . 7

6.2 H1: Firebase and Huawei AGConnect started before any consent screen, and no consent management platform existed in version 8.5.0 . . . 9

6.3 H2: A NotificationListenerService with an untranslated Chinese label could read the notifications of every app . . . 10

6.4 H3: A Firebase key and a Realtime Database URL are hardcoded in a project named appslog-7821c . . . 11

6.5 H4: The signing certificate declares Guangzhou, China, and the package carried Huawei HMS services including an advertising identifier service . . . 12

6.6 M1: No certificate pinning for any endpoint, including the domains that carry device control and chat . . . 13

6.7 M2: Advertising identifiers of two vendors were present in an intimate-use app, and no ad network was found . . . 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Intimate Data and Control Link 16

10 Data Protection: Article by Article 16

11 Platform Disclosures: Google Play 17

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 17

14 Disclosure Timeline & Outcome 18

15 Operator response 19

16 What Lovense Got Right 20

17 Residual Risk & Recommendations 20

Executive Summary

Lovense Remote is the control app for the internet-connected intimate devices of Lovense, with more than five million installs on Google Play and a Mature 17+ rating. The publisher is HYTTO PTE. LTD. of Singapore. On 22 August 2026 RFI-IRFOS disclosed findings from a root level code analysis of version 8.5.0 under REF LOVENSEREMOTE-2026-R1.

The lead finding is architectural. The Control Link feature generates a link for anonymous device control that the creator can publish on a public feed and that gives whoever opens it live control of a device worn on the body, plus a chat with the account holder. In the versions analysed the only access element in the flow is a checkbox that reads I am over 18 and agree (C1). Lovense answered that single use and non-public sharing are its defaults and that links expire. The strings agree that the public and unlimited options are choices of the creator. A pull of version 8.7.0 on 21 September 2026 still showed the checkbox as the only gate for the person who opens the link. Lovense wrote on 18 November 2026 that since 21 October 2026 the person who opens a link must also enter a year of birth on the web page, that a link is valid for 24 hours only and that since 18 November 2026 an under-18 entry triggers a two-hour block on repeat attempts. RFI-IRFOS states this correction at the operator's request and has not verified it.

Several findings were fixed after the notice. The pre-consent start of Firebase and Huawei AGConnect (H1) and the NotificationListenerService (H2) are removed from the manifest of version 8.7.0. The Huawei services (H4) are gone and the Article 27 representatives are now named in the privacy policy. Lovense also named a Data Protection Impact Assessment for Control Link. We could confirm the manifest changes from the package. The operator states that the Huawei components were never used, and nothing in the package contradicts that or proves it.

Lovense replied in writing on 10, 21 and 29 September and on 18 November 2026. On 29 September it said that the matter is closed on its side. On 18 November 2026 it wrote again after our notice of 15 November and stated that its Impact Assessment concluded that the risks of a stranger misusing a Control Link and of a minor gaining access are addressed by the layered controls. The assessment itself stays internal. Lovense also asked that its reply be published together with this report and that the statement of a checkbox as the only gate be updated. Published together with the operator's response and corrected on the operator's request of 18 November 2026. The embargo date of 20 November 2026 has been reached.

Scope: Root level code analysis of the Google Play release 8.5.0 (versionCode 574), base APK of 141.3 MB extracted from a 473.6 MB XAPK bundle: manifest, resources, network security config, the signing certificate and the string pool of nine classes*.dex files. A package check of version 8.7.0 (versionCode 579) on 21 September 2026 covered the manifest, the Huawei namespace and the Control Link entry flow. No Lovense server was called, no Bluetooth protocol was tested and no traffic was captured. The Google Play listing was read on 22 August 2026. The privacy policy at lovense.com/privacy-policy was read on 21 September 2026. Items that need a runtime test are marked as not shown.

ID	Severity	Title
C1	CRITICAL	Control Link lets an anonymous stranger take live control of a body-worn device, and the age gate is self-declared
H1	HIGH	Firebase and Huawei AGConnect started before any consent screen, and no consent management platform existed in version 8.5.0
H2	MEDIUM	A NotificationListenerService with an untranslated Chinese label could read the notifications of every app
H3	MEDIUM	A Firebase key and a Realtime Database URL are hardcoded in a project named appslog-7821c
H4	MEDIUM	The signing certificate declares Guangzhou, China, and the package carried Huawei HMS services including an advertising identifier service
M1	MEDIUM	No certificate pinning for any endpoint, including the domains that carry device control and chat
M2	MEDIUM	Advertising identifiers of two vendors were present in an intimate-use app, and no ad network was found

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	CRITICAL	Open. Operator disputes the characterisation and states a year of birth step since 21 October 2026, a 24-hour link validity and a two-hour block since 18 November 2026. Not verified.
H1	HIGH	HIGH	Resolved in 8.7.0 at manifest level.
H2	HIGH	MEDIUM	Resolved in 8.7.0 at manifest level.
H3	HIGH	MEDIUM	Operator reports no change required. Not re-checked.
H4	HIGH	MEDIUM	Huawei part resolved in 8.7.0. Representative named.
M1	MEDIUM	MEDIUM	Not addressed in correspondence.
M2	MEDIUM	MEDIUM	Huawei part resolved in 8.7.0. Google part not re-checked.

Subject & Operator Analysis

Google Play lists the developer as Lovense and the legal publisher as HYTTO PTE. LTD., a Singapore private company with UEN 201926411M, incorporated on 13 August 2019, registered at 152 Beach Road #11-05 Gateway East, Singapore 189721, according to public registry data. The listing shows 5M+ installs, 19,900 reviews at 4.4 stars, a Mature 17+ rating for sexual content, user interaction and shared location, and a last update on 20 August 2026.

The APK signing certificate declares the organisation hytto with locality GZ, province GD and country CN. Lovense states that these fields reflect historical build and signing workflows. The publisher confirmed in its letter of 10 September 2026 that HYTTO PTE. LTD. is publisher and operator. The privacy policy of lovense.com names Prighter EU Rep GmbH, Vienna, and Prighter Ltd, London, as representatives under Article 27 of the GDPR and the UK GDPR. We read that text on 21 September 2026. No EU main establishment is known, so each concerned supervisory authority is competent. The Österreichische Datenschutzbehörde is the authority for a matter that starts in Austria.

Architecture & Data Flow

The app is a Java and Kotlin application with nine multidex dex files of about 70 MB, an embedded Unity engine in a separate process and a Cordova module. It controls the devices over Bluetooth LE. The Control Link feature talks to the domains c.lovense-api.com and c.lovense.com and offers device control, chat and media exchange between the creator and the person who opens the link. Firebase provides analytics, messaging, remote configuration and authentication. Version 8.5.0 also carried Huawei AppGallery Connect and HMS services. The release network security config blocks cleartext traffic. A Toy PIN feature lets users protect their own device, and Control Link has a reporting and evidence flow with an automatic timeout of 30 and 45 seconds when a link is not used.

Engagement Summary

The notice REF LOVENSEREMOTE-2026-R1 was sent on 22 August 2026 at 12:54 UTC to support@service.lovense.com, with the Österreichische Datenschutzbehörde and the European Data Protection Supervisor in copy. It stated one critical finding, four high findings and two medium findings, set out three questions and asked for a written answer within 30 days. On 25 August 2026 the Lovense support team acknowledged the matter under ticket FK24141 and said that it was under internal review.

On 10 September 2026 the Lovense Remote app team lead answered with a consolidated response. It reported fixes for H1, H2 and the Huawei components, reviewed the Firebase values and the IABTCF constants, described Control Link as updated and under ongoing review, named a risk assessment for Control Link and said that representative information would appear in an updated privacy policy. It asked for a review of factual matters before publication.

On 11 September 2026 RFI-IRFOS confirmed H1 and H2 as closed against version 8.7.0, asked for a named Impact Assessment and for the representative, and accepted a fact-check request for any named sentence.

On 21 September 2026 Lovense named an Impact Assessment under Article 35 for the app and the PC client that expressly includes Control Link, said that the Huawei component

was never used or invoked and showed the representative entry of its privacy policy. RFI-IRFOS pulled version 8.7.0 on the same day and confirmed the Huawei removal, the manifest changes and the representative text. It asked what the assessment concluded about the Control Link risk, with a reply date of 5 October 2026.

On 29 September 2026 Lovense wrote that Control Link has controls that operate independently of the age confirmation, that a date of birth entry by those opening a link is being taken forward, that the assessment is internal and available to a supervisory authority on request, that the removed components were removed in code maintenance, and that its response is complete and its file is closed. RFI-IRFOS replied the same day. It stated that the date of birth step is not in the current build and that the embargo of 20 November 2026 is unchanged.

The support desk issued automatic ticket acknowledgements on 11 September, 21 September and 29 September 2026. On 15 November 2026 RFI-IRFOS sent a notice five days before the embargo date. It listed the verified fixes, restated C1 as open and asked two questions: what the Impact Assessment concluded about a stranger controlling a body-worn device, and whether the date of birth step is live in a released build and from which version.

On 18 November 2026 the Remote App team leader of Lovense replied, copying the support desk. The reply states that since 21 October 2026 a year of birth is entered each time a Control Link is opened, that links are valid for 24 hours, that a two-hour block on repeat attempts applies since 18 November 2026, that the Impact Assessment concluded that stranger misuse and minor access are addressed by the layered controls, and that the position on the other findings is as set out in earlier letters. It asks for publication of the reply together with this report and for an update of the statement that the only gate is a checkbox. No further message from Lovense is on record.

Findings

C1: Control Link lets an anonymous stranger take live control of a body-worn device, and the age gate is self-declared

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 7.1 (CVSS-B), disclosed as CRITICAL on 22 August 2026, open, operator states a year of birth step since 21 October 2026 (not verified), rated CRITICAL by blast-radius escalation

The onboarding strings of Control Link describe a link for ”anonymous toy control” with ”no personal data shown at all” that lets anyone control the toy without downloading the app and chat anonymously. The creator can choose ”Share publicly”, which lists the link on the Vibe Now tab of the Tophy app, and can choose ”Unlimited”, which reactivates the link after each session. The strings also show that the controller can operate the toy before the account holder has joined the chat room. In the versions analysed the only age related element in the flow is a click-through checkbox, ”I’m over 18 and agree”. A search of all string resources found no date of birth, age verification or COPPA token anywhere else in the package, including SignUpActivity and LoginActivity. Lovense states that single use and non-public sharing are the defaults, that the creator sets the scope and can withdraw it at any time, and that links expire automatically. The strings are consistent with both statements, because the public and unlimited options exist and are chosen by the creator. A fresh pull of version 8.7.0 on 21 September 2026 showed the checkbox as the only access control for the person who opens the link. Lovense wrote on 29 September 2026 that entry of a date of birth by those opening a link is a measure ”presently being taken forward”. On 18 November 2026 Lovense wrote that since 21 October 2026, each time a Control Link is opened, the person opening it must enter a year of birth in addition to confirming that they are over 18, that an entry under 18 cannot proceed and that a Control Link is valid for 24 hours only. It added that since 18 November 2026 an under-18 entry triggers a two-hour block on repeat attempts to open that link, and that these steps apply on the web page through which Control Links are opened and depend on no app version. Lovense asked that the statement of a checkbox as the only gate be updated. This report makes that correction: the checkbox was the only gate in the package versions analysed, and according to the operator the gate has included a year of birth entry since 21 October 2026. The statements are the operator’s and are not verified by RFI-IRFOS, because the web page was not tested. A year of birth entered by the person who opens the link is a self-declaration, like the checkbox. No live call was made and server side enforcement was not tested. RFI-IRFOS blast-radius escalation: raised from HIGH/7.1 to CRITICAL because the harm is physical actuation of an intimate device on a person’s body by an anonymous member of the public, the data relates to sex life under Article 9, and the gate for a minor is a self-declaration, a ticked box in the analysed versions and, according to the operator, also an entered year of birth since 21 October 2026. The CVSS vector scores only the integrity of device control with a user action by the account holder.

```
<string name="control_link_onbording_des1">Generate a link for anonymous toy control</
    string>
<string name="control_link_onbording_des4">Anonymous</string>
<string name="control_link_onbording_des5">no personal data shown at all</string>
<string name="control_link_onbording_txt2">Let anyone control your toy(s) without
    downloading the app, chat anonymously, and more!</string>
<string name="control_link_share_publicly">Share publicly</string>
<string name="control_link_share_publicly_des">Link will be shown on the Vibe Now tab
    of the Tophy app.</string>
<string name="control_link_auto_reactivate">Unlimited</string>
<string name="control_link_auto_reactivate_des">Automatically reactivate after each
    session.</string>
<string name="control_link_enter_pop_tip1">This link may contain adult content. Please
     verify your age below and protect your personal info during this session.</string
    >
<string name="control_link_enter_pop_agree">I'm over 18 and agree</string>
<string name="control_link_hasnt_join_chat2">The other user hasn't joined this room
    yet. You can still control their toy(s).</string>
```

Search for date of birth, age verification and COPPA tokens (birthdate, birth_date, date_of_birth, age_verif, over18, coppa) in all string resources: zero results outside the Control Link checkbox. Control Link domains in the package: c.lovense-api.com and c.lovense.com.

Impact: The person who suffers the harm is the account holder, an adult who wears an intimate device and whose link is opened by someone they do not know. That stranger can drive the device against the holder’s body and enter a chat with them. When the link sits on a public feed, the population that can reach it is the general public, and the barrier for a minor is a self-declaration, a checkbox in the analysed versions and, according to the operator, an entered year of birth since 21 October 2026.

Fix: Verify the age and the identity of the person who opens a link before device control starts, make the creator confirm each controller before the first command, and publish the outcome of the Art. 35 assessment for this feature to the supervisory authority.

H1: Firebase and Huawei AGConnect started before any consent screen, and no consent management platform existed in version 8.5.0

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 22 August 2026, resolved in 8.7.0 at manifest level, rated HIGH by blast-radius escalation

FirebaseInitProvider (directBootAware true, initOrder 100) and Huawei AGConnectInitializeProvider are ContentProviders, so they start with the process before any Activity and before any consent screen. The service ComponentDiscoveryService registers FirebaseAuth, FirebaseDatabase, FirebaseMessaging, AnalyticsConnector, RemoteConfig, Crashlytics, Sessions, Installations, Abt and Datatransport. No OneTrust, Didomi, Usercentrics, consentmanager or Google User Messaging Platform class was present. IABTCF constant names exist in the dex as strings, and Lovense states that they belong to the TCF reading logic inside Firebase Analytics and that the app writes no TCF string. Lovense reports that both providers are removed from the manifest of version 8.7.0 and that Firebase initialization depends on the recorded consent status. Our fresh pull of 8.7.0 on 21 September 2026 confirmed that FirebaseInitProvider is gone as its own ContentProvider. We did not trace the consent logic that now gates initialization. No traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app is used for intimate purposes by a very large user base, and initialization ran before the user could decide. The CVSS vector scores only the low sensitivity identifier level.

```
<provider android:authorities="com.lovense.wear.firebaseinitprovider" android:
    directBootAware="true"
          android:exported="false" android:initOrder="100"
          android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.lovense.wear.AGCInitializeProvider" android:
    exported="false"
          android:name="com.huawei.agconnect.core.provider.AGConnectInitializeProvider
    "/>
<service android:directBootAware="true" android:exported="false"
         android:name="com.google.firebase.components.ComponentDiscoveryService"/>
```

Impact: Every user of the app, including those who use it for intimate purposes, was profiled at the identifier level before any choice was offered.

Fix: Keep the removal and publish how the consent status gates Firebase Analytics, Messaging and Remote Config in the current version.

H2: A NotificationListenerService with an untranslated Chinese label could read the notifications of every app

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.7 (CVSS-B), disclosed as HIGH on 22 August 2026, resolved in 8.7.0 at manifest level

The service com.wear.backgroundservice.service.MediaControllerService is bound with BIND_NOTIFICATION_LISTENER_SERVICE. Its label is a Chinese string that means Notification Monitoring. After the user grants Notification Access, the Android API exposes every notification of every app, among them banking codes and message previews. The class names point to a Media Sync feature, which drives the toy to the beat of music or video and needs only media session data, for which a narrower Android API exists. Neither the Play description nor the Data Safety label mentions notification access. The package shows the capability and the broader permission, and it does not show that notification content outside media sessions is read or sent. The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the exposure needs an explicit special access grant by the user and the use beyond media is inferred from names. Lovense reports that the service and its label are removed in version 8.7.0 and our pull of 21 September 2026 confirmed that the manifest has no NotificationListenerService.

```
<service android:enabled="true" android:exported="false" android:label="[Simplified
    Chinese, U+901A U+77E5 U+76D1 U+63A7]"
         android:name="com.wear.backgroundservice.service.MediaControllerService"
         android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE"
         android:stopWithTask="true">
    <intent-filter>
        <action android:name="android.service.notification.NotificationListenerService
    "/>
    </intent-filter>
</service>
```

Impact: A user who grants this access to sync a toy to music also grants read access to one time passcodes and private messages on the same phone.

Fix: Keep the service removed and use the media session API if Media Sync needs playback data.

H3: A Firebase key and a Realtime Database URL are hardcoded in a project named appslog-7821c

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as HIGH on 22 August 2026, operator reports no change required

The Firebase key for the project appslog-7821c, with a Realtime Database URL and a storage bucket, sits in clear text in the package. The project name suggests a shared logging project that may serve more than one Lovense product. Google documents Firebase keys as non-secret by design, so this is an availability finding. Whether the Security Rules protect the database and the bucket is not shown by the package and was not tested. Lovense states that the values are not secret keys by design, that anonymous sign-in is disabled and that the referenced storage bucket has never been used. The statements were not verified from outside, and the resources of version 8.7.0 were not compared for this item. The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because only availability is shown and the operator has stated that the main exposure paths are closed.

```
<string name="google_api_key">AIzaSyAMXK76jbagx9AJVMKfJkLhBRq8XNl-B2c</string>
<string name="google_crash_reporting_api_key">AIzaSyAMXK76jbagx9AJVMKfJkLhBRq8XNl-B2c
    </string>
<string name="google_app_id">1:132294203598:android:cfb9ecb028df3cc6</string>
<string name="firebase_database_url">https://appslog-7821c.firebaseio.com</string>
<string name="google_storage_bucket">appslog-7821c.appspot.com</string>
<string name="project_id">appslog-7821c</string>
<string name="gcm_defaultSenderId">132294203598</string>
<string name="default_web_client_id">132294203598-gaichf7o6cvo69vfbcrlelvn3n7nhuf2.
    apps.googleusercontent.com</string>
```

Impact: If the shared project is rate-limited or billed out, logging and configuration for the intimate-device apps that use it can stop.

Fix: Restrict the key by package name and signing certificate, enforce App Check and confirm that the Security Rules deny by default.

H4: The signing certificate declares Guangzhou, China, and the package carried Huawei HMS services including an advertising identifier service

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 22 August 2026, Huawei part resolved in 8.7.0, representative named

The APK signing certificate states Owner CN=wear, OU=hytto, O=hytto, L=GZ, ST=GD, C=CN. Google Play names HYTTO PTE. LTD., Singapore, as publisher. The two facts do not contradict each other, and a Singapore company with an engineering team in China is a common structure. The package also carried the Huawei HMS stack with the ads-identifier service 3.4.62.300, AIPolicyService, DNSService, NetDiagnosisService, ML Kit and ScanKit. The notice of 22 August 2026 described the Huawei backend as live. This report records the services as declared in the manifest. Whether they transmitted data is not shown, and Lovense states that the Huawei components were never used or invoked, were present only as an SDK in the static code, and are removed. Our pull of version 8.7.0 on 21 September 2026 found no com.huawei entry in the manifest and no Huawei package namespace in any of the nine dex files. Lovense also states that the certificate region reflects fields used in historical build and signing workflows. The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the transfer was inferred from declared components, and the operator has removed them.

```
Owner:  CN=wear, OU=hytto, O=hytto, L=GZ, ST=GD, C=CN
Issuer: CN=wear, OU=hytto, O=hytto, L=GZ, ST=GD, C=CN
Serial number: 71c45d6c
Valid from: Mon Oct 12 03:05:27 CEST 2015 until: Fri Oct 05 03:05:27 CEST 2040
SHA-256: 96:3A:E7:1D:F7:7D:35:DD:99:DA:70:B1:6F:EC:00:E1:40:53:61:44:B3:A2:04:DF:B0
    :96:E2:AB:FF:5E:21:4B
```

```
<meta-data android:name="com.huawei.hms.client.service.name:ads-identifier" android:
    value="ads-identifier:3.4.62.300"/>
<meta-data android:name="networkservice_ai" android:value="com.huawei.hms.network.ai.
    AIPolicyService"/>
<meta-data android:name="networkservice_dns" android:value="com.huawei.hms.network.dns
    .DNSService"/>
<meta-data android:name="networkservice_netdiag" android:value="com.huawei.hms.network
    .netdiag.NetDiagnosisService"/>
<provider android:authorities="com.lovense.wear.MLInitializerProvider" android:
    exported="false"
          android:name="com.huawei.hms.mlsdk.common.provider.MLInitializerProvider"/>
```

Impact: For a user on a Huawei device without Google services, an identifier service of a second vendor could have served an app that records intimate use. The operator reports that it never did.

Fix: Keep the Huawei components removed and name the group entities that act for HYTTO PTE. LTD. in the privacy policy.

M1: No certificate pinning for any endpoint, including the domains that carry device control and chat

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as MEDIUM on 22 August 2026, not addressed in correspondence

The release network security config sets cleartextTrafficPermitted to false for the whole app. For targetSdk 24 and higher this overrides the older usesCleartextTraffic attribute that remains on the application element. No domain-config with a pin-set exists, so no host is pinned, including c.lovense-api.com and c.lovense.com, which carry device control commands and chat and media content. A trusted certificate authority installed on the device would allow interception. Cleartext blocking is a real strength. The item was not part of the correspondence after the notice and version 8.7.0 was not checked for it.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="false" />
</network-security-config>
```

Impact: Device control commands and intimate chat travel over a channel that a managed device or a hostile network with an installed certificate could read.

Fix: Add a pin-set for the Control Link and API domains, with a backup pin.

M2: Advertising identifiers of two vendors were present in an intimate-use app, and no ad network was found

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as MEDIUM on 22 August 2026, Huawei part resolved in 8.7.0

The package declares com.google.android.gms.permission.AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID and compiles in Google AdvertisingIdClient. Version 8.5.0 also carried the Huawei ads-identifier service. A search of all nine dex files found no AppLovin, Meta Audience Network, Vungle, Unity Ads, ironSource, InMobi, Fyber, Moloco, Mintegral or Pangle code and no AdMob display units. This test shows that intimate usage data did not reach a monetised ad network through a mediation stack. The Play Data Safety label lists Device or other IDs as shared with third parties. The Huawei part is removed in version 8.7.0 and the Google identifier components were not re-checked in that version. The finding concerns the identifier layer only.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
Lcom/google/android/gms/ads/identifier/AdvertisingIdClient;
com.huawei.hms.client.service.name:ads-identifier:3.4.62.300

Absent from all nine classes*.dex: com/applovin/ com/facebook/ads/ com/vungle/ com/
    unity3d/ads/
com/ironsource/ com/inmobi/ com/fyber/ com/moloco/ com/mbridge/ com/bytedance/sdk/
    openadsdk
```

Impact: The identifier of a phone that is used for intimate purposes is treated like the identifier of any other app, with no extra care for its meaning.

Fix: List each identifier recipient in the privacy policy and limit identifier use to what the product needs.

Impact Analysis

The people affected are adults who use connected intimate devices, among them couples in long-distance relationships and people who use the public feed to find partners, and minors who can pass a self-declared age gate. The data describes sexual activity, which Article 9 treats as data concerning a natural person's sex life.

The central harm in C1 is physical. A stranger can drive a device that is worn on the body of the account holder, and can enter a chat with that person. The account holder chose to publish the link, and a public feed turns that choice into an open invitation to unknown people. The other findings add to a profile of device identifiers, a broad notification grant on the same phone and an unprotected channel for control commands and intimate chat.

The Complete Chain

Step 1, install: the user installs an app rated Mature 17+ from Google Play. The Data Safety label lists Device or other IDs as shared with third parties (M2).

Step 2, process start in version 8.5.0: Firebase and Huawei AGConnect start before any consent screen (H1) and the Huawei HMS identifier service is declared (H4, M2).

Step 3, optional grant: the user grants Notification Access for Media Sync and the service can read every notification (H2).

Step 4, Control Link: the user creates a link, chooses Share publicly and Unlimited and the link appears on the Vibe Now tab of the Tophy app (C1).

Step 5, stranger: someone who opens the link ticks I am over 18 and agree (and, according to the operator, enters a year of birth since 21 October 2026), takes control of the device and enters the chat (C1).

Step 6, transport: control commands and chat travel over c.lovense-api.com and c.lovense.com without certificate pinning (M1).

Step 7, infrastructure: a shared Firebase project named appslog-7821c holds the logging and configuration side (H3).

Intimate Data and Control Link

Control Link is the point where the data category and the physical effect meet. The Intimate Wellness Data Notice for the Kegel feature shows that Lovense knows that frequency, duration and intensity of use are sensitive personal information. The same care is missing at the moment a stranger gets control of the device.

Lovense lists four controls that run independently of the age checkbox: the scope set by the creator, withdrawal at any time, single use and non-public sharing as defaults, and automatic expiry. These controls manage the link, and none of them verifies who opens it. Lovense also reports backend capabilities that restrict users from creating links or remove existing links in case of suspected misuse, and the app contains a report and evidence flow. We did not test any of them. The decisive question was what the Impact Assessment concluded about this exact risk. On 18 November 2026 Lovense answered that the assessment concluded that the risks of a stranger misusing a Control Link and of a minor gaining access are addressed by the layered controls, and that the year of birth step and the two-hour block are the measures in force beyond the checkbox. It adds that text chat in Control Link sessions is subject to content controls. The assessment itself remains internal.

The category of non-events does not apply, because the device acts on the body of a person.

Data Protection: Article by Article

Article 5(1)(a) and 5(2), lawfulness and accountability: engaged by H1.

Article 5(1)(c), data minimisation: engaged by H2 and M2.

Article 6(1) and Article 7(1), lawful basis and consent: engaged by H1, resolved in version 8.7.0 at manifest level.

Article 8, child's consent: engaged by C1.

Article 9, special categories: the data concerns sex life and frames C1.

Article 13(1)(a), (c) and (e), information: engaged by H2, H4 and M2.

Article 25, data protection by design and by default: engaged by C1, H2 and H3.

Article 27, representative: not engaged after 21 September 2026. Prighter EU Rep GmbH and Prighter Ltd are named in the privacy policy.

Article 32(1)(a) and (b), security of processing: engaged by C1, H3 and M1.

Article 35, impact assessment: engaged by C1. Lovense names an assessment that covers Control Link, states on 18 November 2026 that it concluded the risks are addressed by the layered controls and keeps the document internal, available to a supervisory authority on request.

Article 44 and Article 46, transfers: engaged by H4 for the period in which the Huawei services were declared. The operator states that no transfer occurred.

ePrivacy Directive Art. 5(3): engaged by H1.

Platform Disclosures: Google Play

The Google Play listing and Data Safety label are declarations by the developer. The label lists Device or other IDs as shared with third parties. The listing rates the app Mature 17+ for sexual content, user interaction and shared location. This report attributes both to the developer and makes no claim about the platform operator. The label states nothing about notification access, which was the subject of H2 in version 8.5.0. The listing and the label were read in August 2026 and were not archived. They were not fetched again for this report.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 9 for data on sex life, Article 8 for children, Article 25 and Article 32 for design and security and Article 35 for the impact assessment, together with Article 5(3) of the ePrivacy Directive. The operator is established in Singapore and offers its product in the Union, which brings Article 3(2) GDPR into play. The representatives under Article 27 are Prighter EU Rep GmbH in Vienna and Prighter Ltd in London.

No single EU main establishment is known, so each concerned supervisory authority is competent. The Österreichische Datenschutzbehörde (dsb@dsb.gv.at) is the authority for a matter that starts in Austria. The European Data Protection Supervisor (edps@edps.europa.eu) is 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.

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 published package. All values are given in full.

```
Package            com.lovense.wear
Version audited    8.5.0 (versionCode 574), analysed 2026-08-22
Version checked    8.7.0 (versionCode 579), pulled 2026-09-21
minSdk / target    23 / 35 (compileSdk 35)
Base APK size      141.3 MB, from a 473.6 MB XAPK bundle
Base APK SHA-256   7782f6e9696277cfbbac016c907fd2b8d74063748aad175b6b954afe37a1e62c
Signing cert       CN=wear, OU=hytto, O=hytto, L=GZ, ST=GD, C=CN, serial 71c45d6c
Cert SHA-256       96:3A:E7:1D:F7:7D:35:DD:99:DA:70:B1:6F:EC:00:E1:40:53:61:44:B3:A2
    :04:DF:B0:96:E2:AB:FF:5E:21:4B
Firebase project   appslog-7821c
Firebase API key   AIzaSyAMXK76jbagx9AJVMKfJkLhBRq8XNl-B2c (google_api_key and
    google_crash_reporting_api_key)
Google app ID      1:132294203598:android:cfb9ecb028df3cc6
Database URL       https://appslog-7821c.firebaseio.com
Storage bucket     appslog-7821c.appspot.com
Sender ID          132294203598
Web client ID      132294203598-gaichf7o6cvo69vfbcrlelvn3n7nhuf2.apps.
    googleusercontent.com
Control Link hosts c.lovense-api.com, c.lovense.com
Huawei ads-id      ads-identifier:3.4.62.300
Publisher          HYTTO PTE. LTD., UEN 201926411M, Singapore
```

```
C1  res/values/strings.xml: control_link_* strings. Search of all string resources for
     age tokens
H1  AndroidManifest.xml: FirebaseInitProvider, AGConnectInitializeProvider,
    ComponentDiscoveryService
H2  AndroidManifest.xml: MediaControllerService with
    BIND_NOTIFICATION_LISTENER_SERVICE
H3  res/values/strings.xml: google_api_key, firebase_database_url,
    google_storage_bucket, project_id
H4  META-INF/BNDLTOOL.RSA. AndroidManifest.xml: com.huawei.hms meta-data and providers
M1  res/xml/network_security_config_release.xml: no domain-config and no pin-set
M2  AndroidManifest.xml: AD_ID permissions. classes*.dex: AdvertisingIdClient and ad
    network namespaces
```

Reproduction: obtain com.lovense.wear 8.5.0 and 8.7.0 from Google Play, check the SHA-256 above for 8.5.0, decode the manifest and resources with apktool, extract the dex strings, run keytool -printcert on META-INF/BNDLTOOL.RSA and read the named files. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 Notice REF LOVENSEREMOTE-2026-R1 to support@service.lovense.com, CC dsb@dsb.gv.at and edps@edps.europa.eu, reply requested within 30 days.

2026-08-25 Lovense support acknowledges under ticket FK24141 that the matter is under internal review.

2026-09-10 Consolidated response from the Lovense Remote app team lead. Fixes reported for H1, H2 and Huawei components, risk assessment and layered controls described for Control Link, request for a factual review before publication.

2026-09-11 RFI-IRFOS confirms H1 and H2 as closed against version 8.7.0 and keeps two questions open, reply requested by 25 September 2026. The embargo of 20 November 2026 is restated.

2026-09-21 Lovense names an Impact Assessment under Article 35 covering Control Link, states that the Huawei component was never used and shows its Article 27 representatives. RFI-IRFOS pulls version 8.7.0, confirms the Huawei removal and the representatives, and asks for the conclusion of the assessment on Control Link, reply requested by 5 October 2026.

2026-09-29 Lovense states that a date of birth entry by those opening a link is being taken forward, that the assessment is internal, and that its file is closed. RFI-IRFOS replies the same day, restates the open question and the embargo date.

2026-11-15 RFI-IRFOS sends a notice five days before the embargo date, restates C1 as open and asks two questions on the Impact Assessment conclusion and on the date of birth step.

2026-11-18 Lovense replies. Year of birth entry since 21 October 2026, 24-hour link validity and a two-hour block since 18 November 2026, Impact Assessment conclusion stated, request to publish the reply and to update the checkbox statement.

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

2026-11-21 Publication together with the operator’s response of 18 November 2026.

Operator response

Published together with the operator's response and corrected on the operator's request of 18 November 2026.

On 18 November 2026 at 09:00 UTC the Remote App team leader of Lovense answered our notice of 15 November 2026 and wrote: "We ask that this reply be published together with your report." The core of the reply follows in the words of Lovense, in short quotations, with the order of the reply kept.

Opening: "Your research led directly to the changes in version 8.7.0 that you have verified, and we appreciate it."

Age step: "each time a Control Link is opened, the person opening it must enter a year of birth" in addition to confirming that they are over 18, since 21 October 2026. "an entry indicating an age under 18 cannot proceed." "A Control Link is valid for 24 hours only." "Since 18 November 2026, an under-18 entry also triggers a two-hour block on repeat attempts" to open that link. The step and the block apply on the web page through which Control Links are opened, so that "neither depends on an app version."

Request for correction: our message of 15 November 2026 stated that the only gate is a self-declared checkbox. Lovense wrote: "that does not reflect the current release, and we ask that it be updated."

Impact Assessment: it "assessed the risks of a stranger misusing a Control Link and of a minor gaining access" and "concluded that they are addressed by the layered controls set out in our earlier letters." The year of birth step and the block are the measures in force beyond the checkbox, and "text chat in Control Link sessions is subject to content controls aimed at preventing misuse."

Other findings: "Our position on the other findings is as set out in our earlier letters."

How this report handles the reply. The statement of a checkbox as the only gate is corrected in the executive summary, in C1 and in the chain of events: the checkbox was the only gate in the package versions analysed (8.5.0 and 8.7.0), and according to Lovense a year of birth entry, a 24-hour validity and a two-hour block apply on the Control Link web page. These statements were made by the operator and are not verified by RFI-IRFOS, because the web page was not tested. A year of birth entered by the person who opens a link remains a self-declaration. The severity of C1 stays as assessed, and a change of severity is a decision of RFI-IRFOS after verification.

What Lovense Got Right

The Kegel feature shows an Intimate Wellness Data Notice that names frequency, duration and intensity as sensitive personal information before use. Control Link carries a real report and evidence flow and an automatic timeout, and the warnings before opening a link and in chat are honest about the risk. No display ad mediation SDK is present. Cleartext traffic is blocked for the whole app. A Toy PIN protects a user's own device. Crashlytics collection and the session lifecycle service were disabled in version 8.5.0. After the notice Lovense removed the pre-consent providers, the notification listener and the Huawei components within weeks, replied substantively three times, named an Article 27 representative and an Impact Assessment, and, according to its letter of 18 November 2026, introduced a year of birth step on 21 October 2026 and a two-hour block on repeat attempts on 18 November 2026 for those who open a Control Link. RFI-IRFOS has not verified these steps. Lovense also asked that its reply be published with this report, which the section Operator response does.

Residual Risk & Recommendations

Open at the date of publication: C1 in full. The year of birth step, the 24-hour validity and the two-hour block stated by the operator on 18 November 2026 apply on a web page that RFI-IRFOS has not tested, and a year of birth entered by the person who opens the link is a self-declaration. H3 and M1 are not re-checked in version 8.7.0. The Google identifier components of M2 are not re-checked.

Recommendations: have the Control Link web page and its age gate tested independently, verify the identity and age of the person who opens a Control Link before device control starts and make the creator approve each controller, publish how the consent status gates Firebase, add certificate pins for the Control Link domains, restrict the Firebase key by package and certificate and confirm deny-by-default Security Rules, and keep the notification listener and Huawei components removed.

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 Lovense servers or accounts were probed. Final report, published 21 November 2026, together with the operator's response of 18 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF LOVENSEREMOTE-2026-R1.