Security & Privacy Disclosure, Final Report

blush - Connect & Chat for Android (com.blush.android)

A chat app for meeting strangers, rated PEGI 18, carries chat, voice and video on a NetEase cloud SDK, adds Tencent analytics, starts advertising calls at launch and tells the store that nothing is shared.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026. EMBARGO DATE 19 NOVEMBER 2026 REACHED. NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026.

Target	ZenithLabs Technology Limited, Hong Kong (Blush)
Versions Audited	1.1.1 / 16 (pulled 2026-08-20). The listing shows an update on 1 September 2026, not analysed.
Notice / Publication	2026-08-21 / 2026-11-19 (90 days); embargo date stated in our notice of 15 November: 19 November; published 21 November
Findings	8: 1 High, 5 Medium, 2 Low (reassessed against the notice, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026

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 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Findings 7

5.1 H1: Chat, voice and video run on a NetEase cloud SDK, and neither the privacy policy nor the store label names the processor or the transfer 7

5.2 M1: Advertising ID read and analytics event dispatch run at application start with no consent branch in the start-up code 8

5.3 M2: Two further China-based collectors, Tencent Beacon and Tencent Bugly, are present and the policy names neither 9

5.4 M3: Google Play label says that no data is shared with third parties, the policy and the build point to advertising and attribution recipients 9

5.5 M4: Policy is a short website text without controller address, legal bases, processors, transfers, retention for chat or an EU representative 10

5.6 M5: The word anonymous in the product description and in the policy title does not match the data model of the build 11

5.7 L1: Firebase configuration values ship in the application resources 12

5.8 L2: Permission set includes phone state, biometrics and advertising permissions, the origin of several entries is not established 12

6 Impact Analysis 13

7 The Complete Chain 13

8 Child Protection & Age Assurance 13

9 Data Protection: Article by Article 14

10 Consumer Protection & Deceptive Design 14

11 Platform Accountability & the DSA 15

12 Regulatory & Legal Landscape 15

13 Indicators of Compromise & Reproducible Evidence 15

14 Disclosure Timeline & Outcome 16

15 What the Operator Documents State Clearly 16

16 Residual Risk & Recommendations 17

Executive Summary

Blush is a chat app for discovering people and starting conversations. Google Play shows the name ”blush - Connect & Chat”, the developer ZenithLabs Technology Limited with an office address in Hong Kong, more than 500,000 downloads, a PEGI 18 rating and in-app purchases. The build carries voice and video chat components next to text chat.

RFI-IRFOS analysed version 1.1.1 with root level code analysis and sent the findings under REF BLUSH-2026-R1. The notice reached the developer’s Google Play support address on 21 August 2026. A first copy to blush.android addresses failed on the same morning because that domain does not exist. A follow-up of 28 August and a reminder of 17 October 2026 went to the same address, with the Austrian data protection authority and the European Data Protection Supervisor in copy on the first message. No reply of any kind is recorded.

The build embeds the NetEase instant messaging and real time communication SDK, so chat, voice and video run on a NetEase cloud service (H1). It adds Tencent Beacon and Bugly (M2) and a Western advertising and attribution stack. Its start-up code reads the Google Advertising ID and starts analytics dispatch without a consent branch (M1). The Google Play label of 14 November 2026 says that no data is shared with third parties (M3). The privacy policy is a short website text of February 2025 without controller address, legal bases, processors or transfers (M4). The word anonymous does not match the identifiers the build ties to every session (M5).

The final notice of 15 November 2026 named 19 November 2026 as the publication date. This report is published on 21 November 2026, after that embargo date was reached. Several items of the notice are not carried. The notice described an AI companion with sexual roleplay as its core content. The listing, the policy and the reviews describe a chat between people, so that framing is withdrawn. The statement that all traffic runs on infrastructure in the PRC is replaced by the narrower fact that the backend is a NetEase service whose server location is UNVERIFIED. The Remote Config observation and the permission criticism for microphone, camera and location are withdrawn.

Scope: Root level code analysis of the Google Play release 1.1.1 (versionCode 16, pulled 2026-08-20 from a test device): manifest, resources, smali class inventory and string tables. Public pages read by plain HTTP GET on 14 November 2026: the Google Play listing and Data safety page, and the privacy policy and terms of ZenithLabs Technology Limited (both last updated February 20, 2025) at breezrd.com, the policy linked on Google Play. No runtime tracing, no emulator, no backend call, no account, no request to NetEase, Tencent or Firebase. Findings that need runtime behaviour are marked UNVERIFIED.

ID	Severity	Title
H1	HIGH	Chat, voice and video run on a NetEase cloud SDK, and neither the privacy policy nor the store label names the processor or the transfer
M1	MEDIUM	Advertising ID read and analytics event dispatch run at application start with no consent branch in the start-up code
M2	MEDIUM	Two further China-based collectors, Tencent Beacon and Tencent Bugly, are present and the policy names neither
M3	MEDIUM	Google Play label says that no data is shared with third parties, the policy and the build point to advertising and attribution recipients
M4	MEDIUM	Policy is a short website text without controller address, legal bases, processors, transfers, retention for chat or an EU representative
M5	MEDIUM	The word anonymous in the product description and in the policy title does not match the data model of the build
L1	LOW	Firebase configuration values ship in the application resources
L2	LOW	Permission set includes phone state, biometrics and advertising permissions, the origin of several entries is not established

ID	Notice item	This report	Status on 21 November 2026

Finding Status at a Glance

ID	Notice item	This report	Status on 21 November 2026
H1	Item 1 (NetEase in the PRC, CRITICAL)	HIGH	Open. NetEase chat, voice and video SDK is established. Server location and runtime traffic are UNVERIFIED.
M1	Item 2 (pre-consent start-up, CRITICAL)	MEDIUM	Open. The order of calls is established, the runtime effect is UNVERIFIED.
M2	Item 3 (three PRC SDKs, CRITICAL)	MEDIUM	Restated for Tencent Beacon and Bugly.
M3	New	MEDIUM	Open. Label of 14 November 2026 says no data is shared.
M4	Policy comparison in the notice	MEDIUM	Open. Policy lacks controller address, legal bases, processors and transfers.
M5	Item 6 (anonymity)	MEDIUM	Restated as a gap between the word and the data model. The AI companion framing is not carried.
L1	Item 7 (Firebase key)	LOW	Reassessed. Identifier by design, restrictions untested.
L2	Item 5 (permissions)	LOW	Reassessed. Microphone, camera and location match the product.
-	Item 4 (Remote Config without defaults)	not carried	A design choice with no privacy finding of its own.
-	Sexual roleplay as core content	not carried	Not shown by the listing, the policy or the build.

Subject & Operator Analysis

Google Play lists the developer as ZenithLabs Technology Limited with the address Rm 903C, 9/F, Cameron Commercial Centre, 458-468 Hennessy Road, Causeway Bay, Hong Kong, the telephone +852 6909 7811 and the support address abdelouahedbana12@gmail.com. The privacy policy and the terms are hosted at breezrd.com and linked from the Play page. The policy applies to the application ”Blush - Anonymous Chat” published by ZenithLabs Technology Limited. The terms are governed by English law.

The app is offered in Austria, so Art. 3(2) GDPR applies to a controller established in Hong Kong and Art. 27(1) requires a representative in the Union. No establishment or representative in the Union appears in the documents or on the Play page, so every authority where users are affected is competent. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the first notice in copy.

Architecture & Data Flow

The app is a native Android build, version 1.1.1 with versionCode 16. Chat, voice and video use the NetEase NIM and NERTC SDK family with the endpoints listed under H1. The Firebase project blush-a11d1 provides Analytics, Crashlytics, Remote Config, Realtime and Installations. Attribution and advertising run through the Facebook SDK, AppsFlyer and the Google Ads and Privacy Sandbox components. RevenueCat handles purchases and Google Maps is bundled. Tencent Beacon and Bugly add analytics and crash reporting.

The start-up class BLTransmit initialises Firebase, the analytics dispatcher and the advertising identifier read in one method. Remote Config is present, so live behaviour can differ from the binary, and the live values were not fetched. Play Integrity is present as an integrity control. Consent strings exist in the resources, and the consent screen itself was not observed.

Findings

H1: Chat, voice and video run on a NetEase cloud SDK, and neither the privacy policy nor the store label names the processor or the transfer

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2 (CVSS-B)

The build embeds the NetEase instant messaging and real time communication SDK family (4,997 smali classes, among them com.netease.nim and com.netease.lava.nertc.sdk with its audio and video chat module). The endpoints compiled into it include abt-online.netease.im, change-api.netease.im, lbs.netease.im, yiyong.netease.im, statistic.live.126.net and statistic-overseas.yunxinfw.com. The operator is established in Hong Kong. The privacy policy names no processor, no destination country and no transfer safeguard, and the Google Play label says that no data is shared with third parties.

```
com.netease.nim                      instant messaging SDK
com.netease.lava.nertc.sdk           real time audio and video (NERTC), avchat module
4,997 smali classes in the NetEase family
abt-online.netease.im   change-api.netease.im   lbs.netease.im   yiyong.netease.im
statistic.live.126.net  statistic-overseas.yunxinfw.com   (YunXin is NetEase's
    commercial IM cloud)
```

```
Third parties named: payment services (Apple iTunes, Google Play), advertisers,
    consultants, social sites such as Facebook
Processor for chat, voice or video: none named
Country of processing or transfer mechanism: none stated
Controller address: none stated
```

Runtime transmission was not observed. The report records what the build is configured to use. NetEase is a company of the People's Republic of China. The SDK carries an endpoint named statistic-overseas, so it may route traffic through servers outside the PRC for users in other regions. Which servers actually serve a user in the Union was not established and is UNVERIFIED. The notice of 21 August 2026 stated that every message, voice call and video stream goes to infrastructure operated from the PRC. This report states the narrower fact that the chat backend is a NetEase service and that its server location is unknown.

Whether the content is special category data under Art. 9 depends on what users write, say and show. The notice described the product as sexual roleplay. The store listing describes discovering people, chatting and making friends, so that description is not carried. Art. 9 is not asserted. A review quoted on the Google Play page describes matching with strangers and sharing photos, which makes intimate content plausible and leaves it unproven.

Impact: Adults who chat with strangers on this app, send photos or talk on camera, are told nothing about the company that carries those messages and streams, or about the country where it operates. They cannot weigh that before they speak.

Fix: Name NetEase (or the actual provider) and the region that serves Union users in the privacy policy, state the Art. 46 safeguard or the Art. 45 adequacy basis for each third country,

conclude a processor contract under Art. 28, and correct the Data safety declaration.

M1: Advertising ID read and analytics event dispatch run at application start with no consent branch in the start-up code

---

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)

In com/blush/android/common/startup/BLTransmit.smali the create(Context) method calls FirebaseApp.initializeApp, then BLConfirm.init (analytics event dispatch) and BLDismissAlign.getGoogleAdId (reads the Google Advertising ID) without a consent-state branch in that method. The manifest declares AD_ID and ACCESS_ADSERVICES_AD_ID. Consent strings exist in the resources (consent_screen, consent_state, consent_settings and others).

```
com/blush/android/common/startup/BLTransmit.smali   create(Context)
  FirebaseApp.initializeApp(context)
  BLConfirm.init()                 analytics event dispatch
  BLDismissAlign.getGoogleAdId()   reads the Google Advertising ID
No branch on a consent state inside create(Context)
```

The finding rests on the order of calls in one method. Consent could be enforced elsewhere, for example by Firebase collection switches that are off by default in the manifest, or by a consent step that runs before the first call. Neither was established. Whether the identifier leaves the device before a consent screen is UNVERIFIED and needs a runtime trace. The base64 literal described in the notice as a Firebase bootstrap proof is not carried as evidence.

Section 165(3) TKG 2021 requires consent for storing or reading information on the terminal equipment of a user, unless it is strictly necessary for a service the user requested. Reading an advertising identifier for advertising or attribution is not strictly necessary for chat.

Impact: An adult who opens the app for the first time has no chance to say no before the advertising identifier is read, and the identifier links their use of this app to their use of other apps.

Fix: Gate every analytics, attribution and advertising call behind a stored consent choice, load the SDKs after that choice and ship Firebase collection switches that default to off.

M2: Two further China-based collectors, Tencent Beacon and Tencent Bugly, are present and the policy names neither

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)

The build contains Tencent Beacon analytics with the upload endpoint otheve.beacon.qq.com/analytics/v2_upload and Tencent Bugly crash reporting with the application id 9fddb592b2. The privacy policy states that device type, IP address, browser type, operating system, access times, pages viewed and ads clicked are collected and that Non-PII may be shared with advertisers and consultants. It names no analytics or crash provider and no country.

```
Tencent Beacon    otheve.beacon.qq.com/analytics/v2_upload
Tencent Bugly     bugly_app_id 9fddb592b2
Google Play label: crash logs collected for App functionality and Analytics
```

The label confirms that crash logs and device identifiers are collected for analytics. It names no recipient. Whether Beacon and Bugly are active at runtime, which fields they send and where their servers stand was not observed and is UNVERIFIED. The notice counted the PRC SDKs together with the NetEase service as three collectors. This report counts them separately, because the analytics purpose differs from the chat purpose.

Impact: Device and crash data of every user flows to analytics providers the user cannot find in any document the operator publishes.

Fix: List every analytics and crash provider with its country in the privacy policy, remove collectors without a documented purpose and state the Art. 46 safeguard for each transfer.

M3: Google Play label says that no data is shared with third parties, the policy and the build point to advertising and attribution recipients

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

The Data safety page of 14 November 2026 reads "The developer says this app doesn't share user data with other companies or organizations". The policy states that Non-PII may be shared with advertisers and consultants. The build contains the Facebook SDK, AppsFlyer (privacy-sandbox.appsflyersdk.com), Google Ads (pagead2.googlesyndication.com) and RevenueCat, and the manifest declares AD_ID. The policy also sorts data into PII and Non-PII, although an advertising identifier is personal data under Art. 4(1) and Recital 30.

```
No data shared with third parties
Collected: approximate and precise location (optional), device or other IDs (App
    functionality, Analytics),
           app interactions, installed apps, crash logs, name (optional), user IDs,
    other info (optional)
Data is encrypted in transit. You can request that data be deleted.
```

```
Collected: name, email address, birthdate, username, gender, device type, IP address,
    browser type,
           operating system, access times, pages viewed, ads clicked, photos you
    upload
Shared:    "Non-PII may be shared with third parties, including advertisers and
    consultants"
           "We do not share PII with advertisers"
Not listed: precise location, installed apps, advertising ID, voice, video, processors
    , countries
```

Google's declaration rules treat a service provider that processes data on behalf of the developer differently from a third party that receives data for its own purposes. NetEase and Crashlytics can fall into the first group. Facebook, AppsFlyer and Google Ads receive identifiers for attribution and advertising and are the stronger case for sharing. The label also declares precise location and installed apps, which the policy does not mention. The state of the label on 21 August 2026 was not archived. This report rates the label as it stands on 14 November 2026. The listing does not carry the Contains ads marker, and whether the app shows ads was not observed.

Impact: A person who reads the store label before installing is told that nothing is shared. The policy they find after installing says that data is shared with advertisers and consultants, and it omits location and installed apps.

Fix: Align the Data safety declaration and the policy, declare the attribution and advertising SDKs as recipients and list every data type the label already names.

M4: Policy is a short website text without controller address, legal bases, processors, transfers, retention for chat or an EU representative

---

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)

The policy of February 20, 2025 is addressed to a "Site" and applies to the mobile application "Blush - Anonymous Chat" published by ZenithLabs Technology Limited. It states no postal address, no legal basis per purpose, no data protection officer, no representative in the Union, no processors, no transfers and no retention period for messages. The only contact is an e-mail address for access, correction and deletion. Google Play shows the developer address as a Hong Kong office (Rm 903C, 9/F, Cameron Commercial Centre, 458-468 Hennessy Road, Causeway Bay) and the contact abdelouahedbana12@gmail.com. The terms are governed by English law and cap liability at 20 pounds.

```
Policy and terms       "Blush", footer sentence names ZenithLabs Technology Limited
Google Play developer  ZenithLabs Technology Limited, Hong Kong office address, +852
    6909 7811
Postal address in policy: none   Legal basis: none   DPO: none   EU representative:
    none
```

The app is offered in Austria, so Art. 3(2) GDPR applies to a controller established in Hong Kong, and Art. 27(1) requires a representative in the Union. None is stated. The policy title says "Anonymous Chat" while the Play listing calls the app "blush - Connect & Chat". Which

document the operator keeps current was not established. The retention statement covers profile data (deleted after 24 months of inactivity) and is silent on messages.

Impact: A user in Austria who wants to see or delete their chats has one e-mail address, a Hong Kong office and no representative in the Union.

Fix: Replace the website text with a privacy notice that meets Art. 13, name the controller with its address, state the legal bases, processors, transfers and retention, and appoint an Art. 27 representative.

M5: The word anonymous in the product description and in the policy title does not match the data model of the build

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

The build strings carry ”Enjoy the fun of anonymous” and a ”Private Club” where users ”share private photos and videos”. The policy applies to ”Blush - Anonymous Chat” and collects name, email address, birthdate and gender at registration. The build ties every session to a Firebase installation, a Google Advertising ID and a NetEase account token. A review on the Google Play page, with a developer reply, describes the app as an anonymous chat that matches users with strangers using avatars. The current store description of 14 November 2026 does not use the word anonymous.

```
Build 1.1.1 strings          "Enjoy the fun of anonymous", "Private Club"
Privacy policy title         "Blush - Anonymous Chat"
Store description (14 Nov)   "discover people, chat, make friends", no use of the word
     anonymous
User review with developer reply (Play, 2026)   "chat anonymously using unique avatars
    "
```

Anonymity toward other users and anonymity toward the operator are different claims. Avatars can hide a face from other users while the operator holds an account, a device identifier and an advertising identifier. The build supports the second reading only. Whether the app shows a real name or photo to other users was not observed. The finding is therefore limited to the gap between the word and the data model.

The notice called the product an AI companion. Nothing in the listing, the policy or the reviews read for this report says that the chat partners are AI characters, and the review describes strangers. The AI companion framing is not carried. Whether partners are people or AI characters is UNVERIFIED.

Impact: An adult who chooses the app for its anonymity shares photos and conversations on the assumption that nobody can tie them to a person. The operator holds an account, device and advertising identifiers for every user.

Fix: Describe what anonymous means in the app and in the policy, limited to what other users can see, and state which identifiers the operator holds.

L1: Firebase configuration values ship in the application resources

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B)

The resources carry the Firebase API key (prefix AIzaSyDbABI3Z9oR16Oqx7jRD5 , remainder withheld), project blush-a11d1, sender 439276656983, application id 1: 439276656983:android:0ee5fc13941f6193450612 and the storage bucket blush-a11d1. firebasestorage.app. These values ship in every Android build by design. Whether the key carries application restrictions and whether the security rules of the database and the storage bucket are strict was not tested, because no request was sent to any Google or Firebase endpoint.

The key is an identifier. The notice of 21 August 2026 states the same. The notice also stated that Remote Config has no local defaults. The absence of defaults is a design choice and carries no privacy finding, so that statement is not carried. Rated LOW for the open question of key restrictions and rules.

Impact: The risk reaches users only if the project rules are open, which was not tested.

Fix: Restrict the key to the application package and signing certificate, and review the Firebase security rules of the project.

L2: Permission set includes phone state, biometrics and advertising permissions, the origin of several entries is not established

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B)

The manifest declares RECORD_AUDIO, CAMERA, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, READ_PHONE_STATE, USE_BIOMETRIC, USE_FINGERPRINT, AD_ID, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, BILLING, POST_NOTIFICATIONS and BLUETOOTH_CONNECT. Microphone and camera match the voice and video chat components of the build. Precise and approximate location match the label, which lists both as optional. The notice stated that the set exceeds what an anonymous chat needs. For a voice and video product that statement is withdrawn for microphone, camera and location.

READ_PHONE_STATE, the biometric permissions and the advertising permissions are the open items. Whether they come from the app’s own code or from merged SDK manifests was not established. The build declares no DETECT_SCREEN_CAPTURE permission. Use of any permission at runtime was not observed.

Impact: Users see a permission list with entries that no feature of a chat product obviously needs.

Fix: Remove permissions that no feature uses and state the purpose of each remaining sensitive permission in the policy.

Impact Analysis

The people affected are adults who use a chat app to meet strangers. Such conversations can become intimate. Users send photos, speak by voice and show themselves on camera. The terms state that content is public unless the user moves it to a private folder.

Three points carry the weight. The transport for all of this sits on a NetEase service that no document names (H1). The advertising identifier is read before any visible choice (M1). The store label tells users that nothing is shared (M3).

The remaining findings concern completeness of the documents (M4), the use of the word anonymous (M5) and hygiene items (L1, L2).

The Complete Chain

Step 1, the store page: the user sees PEGI 18, in-app purchases and a Data safety section that says no data is shared (M3). The description speaks of discovering people and chatting.

Step 2, first launch: the start-up code initialises Firebase, analytics dispatch and the advertising identifier read (M1).

Step 3, registration: the policy asks for name, email address, birthdate and gender. It names no legal basis and no processor (M4). Every session binds to a Firebase installation, a Google Advertising ID and a NetEase account token (M5).

Step 4, conversation: messages, photos, voice and video run on the NetEase SDK (H1). Tencent Beacon and Bugly collect analytics and crash data (M2).

Step 5, rights: a user who wants to see or delete data has one e-mail address, a Hong Kong office and no representative in the Union (M4).

The operator has not answered any of these points.

Child Protection & Age Assurance

The terms and the policy state that the app is for users aged 18 and over, and Play rates it PEGI 18. The terms ask users to confirm the age by accessing the platform. The build was not examined for an age check at registration, which is UNVERIFIED. The policy collects a birthdate, so a check is possible. An app that matches strangers for chat and video carries a higher duty of care for age assurance, and the documents describe no method.

Data Protection: Article by Article

Article 5(1)(a), transparency: engaged by H1, M2, M3, M4 and M5. The label, the policy and the build differ from each other.

Article 6(1)(a), Article 7 and Article 4(11), consent: engaged by M1. The order of calls in the start-up code shows no consent gate.

Article 9: engaged only as a contingent point in H1. Content is not known to be special category data.

Article 12(1) and Article 13(1)(a), (b), (c), (e) and (f), Article 13(2)(a): engaged by H1, M2, M3 and M4.

Article 25: engaged by M1, M5 and L2.

Article 27(1) and Article 3(2): engaged by M4. No representative is named.

Article 28(1): engaged by H1 and M2 for the NetEase and Tencent services.

Article 32(1)(b): engaged by L1 as a hygiene point.

Articles 44 to 46: engaged by H1 and M2. The documents name no third country and no safeguard.

Directive 2002/58/EC Article 5(3), implemented in section 165(3) TKG 2021: engaged by M1.

Consumer Protection & Deceptive Design

The Data safety label is the developer’s declaration and reads ”no data shared with third parties”. The developer’s policy and the build point to advertising recipients (M3). The word anonymous appears in the strings and in the policy title, while the build ties sessions to identifiers (M5). The Unfair Commercial Practices Directive 2005/29/EC applies to statements of this kind in commercial communication.

The terms state that unused credits may expire and that the liability of the operator is capped at 20 pounds. Neither statement was tested for validity against Austrian consumer law.

Platform Accountability & the DSA

Google Play presents the Data safety section with the words "The developer says". The declaration remains the developer's statement, and the store page of 14 November 2026 shows the gap to the developer's own policy. The Digital Services Act (Regulation (EU) 2022/2065) applies to the distribution platform. A report of an inaccurate label to the platform is a separate step from this disclosure.

Regulatory & Legal Landscape

ZenithLabs Technology Limited has no establishment in the Union in the documents read. Every supervisory authority where users are affected is competent, and the Austrian authority and the European Data Protection Supervisor hold the first notice. The privacy policy names English law for the terms. The Hong Kong Office of the Privacy Commissioner for Personal Data is the home regulator.

Blush belongs to a group of consumer chat apps that RFI-IRFOS examines with the same method. The method reads the binary, the published documents and the store pages against each other.

Indicators of Compromise & Reproducible Evidence

Every point below is reproducible from the public Google Play build and the public pages named.

```
Package       com.blush.android
Version       1.1.1 / versionCode 16   (pulled 2026-08-20 from a test device)
Firebase      project blush-a11d1   sender 439276656983   bucket blush-a11d1.
    firebasestorage.app
Bugly         9fddb592b2
NetEase       netease.im hosts, 126.net, yunxinfw.com (see H1)
Tencent       otheve.beacon.qq.com/analytics/v2_upload
Start-up      com/blush/android/common/startup/BLTransmit.smali  create(Context)
```

```
Google Play listing and Data safety   playstore_snapshot_2026-11-14.txt
breezrd.com/proto/privacy-policy      blush_privacy_policy_breezrd_2026-11-14.txt
breezrd.com/proto/terms-of-service    blush_terms_breezrd_2026-11-14.txt
```

Reproduction for H1: list the smali packages under com/netease and search the resources for the endpoint hosts. Reproduction for M1: open BLTransmit.smali and read the create method. Reproduction for M3: open the Data safety page of com.blush.android and read the policy at the linked address. The SHA-256 of the pulled base APK is not recorded in the case folder.

Disclosure Timeline & Outcome

2026-08-21 08:25 UTC First message REF BLUSH-2026-R1 to privacy@blush.android, copy to security@blush.android, press@blush.android, dsb@dsb.gv.at and edps@edps.europa.eu. The blush.android addresses returned delivery failure notices within seconds, because the domain does not exist.

2026-08-21 15:15 UTC Delivery of the notice to abdelouahedbana12@gmail.com, the support address on the Google Play page, copy to dsb@dsb.gv.at and edps@edps.europa.eu. The 90 day embargo runs from this delivery.

2026-08-28 First follow-up to the same address.

2026-10-17 Reminder from security@rfi-irfos.com to the same address with the three questions repeated.

2026-11-14 Listing, Data safety page, privacy policy and terms read on this date.

2026-11-15 Final notice from s.kepp@rfi-irfos.com to the same address (12:58 UTC, day 86), titled 4 days to publication. It withdrew two statements of the notice (the AI companion framing and the claim that all traffic runs in the PRC), restated the findings in narrower form, restated three questions with a deadline of 18 November 2026 and named 19 November 2026 as the publication date.

2026-11-19 Embargo date stated in our notice of 15 November 2026 and 90 days after delivery of the notice of 21 August 2026.

2026-11-21 Published. As of this date no reply of any kind is recorded, including no automatic reply.

The description of the app as an AI companion with sexual roleplay as its core content is withdrawn.

What the Operator Documents State Clearly

The policy and the terms state the age limit of 18 in plain words. The policy offers access, correction and deletion by e-mail and by editing the profile, states that profile data is deleted after 24 months of inactivity, and says that credit card data is processed by Apple or Google. The terms offer private folders for content. The consent strings in the resources show that the team knows consent as a concept, and the Data safety page states that data is encrypted in transit and that deletion can be requested.

Residual Risk & Recommendations

Open on 21 November 2026: all eight findings, because the operator has not replied. The runtime questions stay open. They are which NetEase servers serve users in the Union, whether the advertising identifier leaves the device before a consent screen, whether Tencent Beacon and Bugly send data, what Remote Config delivers and whether registration verifies age. Builds since 1.1.1 were not analysed.

Recommendations: name the chat provider and its region and state the transfer safeguard. Gate analytics and advertising behind consent. Correct the Data safety declaration. Replace the website text with a privacy notice that meets Art. 13. Appoint a representative in the Union. Explain what anonymous means.

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

plus public pages read by plain GET. No operator servers, NetEase, Tencent or Firebase endpoints or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF BLUSH-2026-R1.