Security & Privacy Disclosure, Final Report

Her.AI - Funny Chat Friend for Android (com.mohie.herai)

An AI chat app with more than 500,000 downloads fires an attribution event before its consent request, sends chats to a US cloud and states four different minimum ages.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	Developer account MohamedGMohie, store panel PCRS LLC, California (Her.AI)
Versions Audited	2.3.5 / 44 (audit of 2026-08-21). The listing shows an update on 9 September 2026, not analysed.
Notice / Publication	2026-08-21 / 2026-11-19 (90 days)
Findings	6: 5 Medium, 1 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 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Findings 6

5.1 M1: A live Adjust event, Google Mobile Ads initialisation and Firebase Messaging setup run before the only consent request 6

5.2 M2: Chat and image requests go to a US cloud backend and the policy offers one sentence on transfers 7

5.3 M3: Four different age statements, no verification, and a store rating of 18 against terms that admit users from 13 8

5.4 M4: Data safety label, listing text and privacy policy disagree on encryption, deletion, location and chat history 9

5.5 M5: Operator is an individual developer account with a limited company on the store panel, a personal Gmail contact and an unfilled governing law 10

5.6 L1: Firebase key and SDK identifiers ship in the application resources 11

6 Impact Analysis 11

7 The Complete Chain 12

8 Child Protection & Age Assurance 12

9 Data Protection: Article by Article 13

10 Consumer Protection & Deceptive Design 13

11 Platform Accountability & the DSA 14

12 Regulatory & Legal Landscape 14

13 Indicators of Compromise & Reproducible Evidence 14

14 Disclosure Timeline & Outcome 15

15 What the Operator Documents State Clearly 15

16 Residual Risk & Recommendations 15

Executive Summary

Her.AI - Funny Chat Friend is an AI chat app with more than 200 characters, user-made characters and picture creation. Google Play shows more than 500,000 downloads, a PEGI 18 rating with the descriptors Users Interact and Shares Location, the marker Contains ads and in-app purchases. The developer account is named MohamedGMohie, and the developer panel lists PCRS LLC of Oakland, California.

RFI-IRFOS analysed version 2.3.5 with root level code analysis and sent the findings under REF HERAI-2026-R1. The notice was delivered on 21 August 2026 at 15:41 UTC to the only contact in the operator's documents, with the Austrian data protection authority in copy. A follow-up of 28 August and a reminder of 17 October 2026 went to the same address. No reply and no delivery failure for that address is recorded.

The start-up code fires a live Adjust event and initialises Google Mobile Ads and Firebase Messaging before the only consent request (M1). The chat backend runs on AWS in the United States, and the policy offers one sentence on transfers (M2). The policy, the agreement, the in-app screen and the store rating state four different minimum ages (M3). The Data safety label says data is not encrypted and cannot be deleted, which the policy contradicts (M4). The agreement contains two unfilled template clauses, and the only contact is a personal Gmail address (M5).

The notice rated its first item as critical. This report rates the same point MEDIUM under CVSS v4.0 and lists the change item by item. The description of the operator as an individual without a company is withdrawn, because the developer panel names PCRS LLC. The comparison of the intimacy mechanic with another target is not carried as a finding.

Scope: Root level code analysis of the Google Play release 2.3.5 (versionCode 44, base.apk, audit of 2026-08-21 from a test device): manifest, resources, network security configuration, string tables of all three dex files, and smali of the classes3.dex package code. Passive DNS and IP registry data for the hostnames found. Public pages read by plain HTTP GET on 14 November 2026: the Google Play listing and Data safety page, the privacy policy and the user agreement at herai.top. No runtime tracing, no emulator, no backend call, no account. Findings that need runtime behaviour are marked UNVERIFIED.

ID	Severity	Title
M1	MEDIUM	A live Adjust event, Google Mobile Ads initialisation and Firebase Messaging setup run before the only consent request
M2	MEDIUM	Chat and image requests go to a US cloud backend and the policy offers one sentence on transfers
M3	MEDIUM	Four different age statements, no verification, and a store rating of 18 against terms that admit users from 13
M4	MEDIUM	Data safety label, listing text and privacy policy disagree on encryption, deletion, location and chat history
M5	MEDIUM	Operator is an individual developer account with a limited company on the store panel, a personal Gmail contact and an unfilled governing law
L1	LOW	Firebase key and SDK identifiers ship in the application resources

Finding Status at a Glance

ID	Notice item	This report	Status on 14 November 2026
M1	F1 (pre-consent SDKs, CRITICAL)	MEDIUM	Open. Control flow established for the files read, runtime effect UNVERIFIED.
M2	F4 (AWS backend, in the notice summary)	MEDIUM	Open. Hosting by passive DNS, content flow inferred from endpoint names.
M3	F2 (three minimum ages, HIGH)	MEDIUM	Open. A fourth statement, the store rating, is added.
M4	New	MEDIUM	Open. Label, listing text and policy disagree.
M5	F3 (no registered entity, HIGH)	MEDIUM	Restated. The panel names PCRS LLC, so the no-company description is withdrawn.
L1	F6 (identifiers)	LOW	Reassessed. Values printed in full.
-	F5 (intimacy mechanic)	not carried as a finding	A product observation without a privacy consequence of its own, described under consumer protection.

Subject & Operator Analysis

The Google Play developer account is named MohamedGMohie. The developer panel lists PCRS LLC, 2001 42nd Ave, Oakland, CA 94601, the telephone +44 7879 503476 and the address mohamedgamalmohie@gmail.com. The privacy policy and the user agreement at herai.top name no company and list the same Gmail address as their only contact. The domain herai.top is registered through NameSilo with the registrant redacted.

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

Architecture & Data Flow

The app is a native Android build, package com.mohie.herai, version 2.3.5, minimum SDK 24, target SDK 35, with the Java namespace com.herai.mobile. The backend api.herai.top serves the chat and group role endpoints from AWS in the United States. Advertising and measurement run through Google Mobile Ads, Adjust for attribution, the Facebook SDK and Firebase. Google Play Billing handles purchases. A local Room database holds messages, group caches, profiles and voice entries, with an intimacy value that gates image unlocks.

The manifest declares no microphone, camera, location or biometric permission. The voice feature plays server-generated audio and records nothing. The Google User Messaging Platform library is present with working code and is called from MainActivity. No network security override exists, so the platform default blocks cleartext traffic at target SDK 35.

Findings

M1: A live Adjust event, Google Mobile Ads initialisation and Firebase Messaging setup run before the only consent request

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 version 2.3.5 the App Startup initialiser AppInitializer.create calls MobileAds.initialize and sets up FirebaseMessaging with no consent-status branch. It runs during ContentProvider attach, before Application.onCreate. MyApplication.onCreate then builds the Adjust configuration (app token xb2kzzkfim80, production) and fires the Adjust event b77sdy. The only consent request found, Google User Messaging Platform requestConsentInfoUpdate, sits in MainActivity, which starts after the launcher activity SplashActivity.

```
smali3/com/herai/mobile/init/AppInitializer.smali   create(Context)    registered as
    androidx.startup initialiser
  SharedPreferences "refers" read
  MobileAds.initialize(context)              line 163
  FirebaseMessaging.getInstance(...)         line 188
smali3/com/herai/mobile/init/MyApplication.smali   onCreate()   line 7746
  AdjustConfig(app token xb2kzzkfim80, "production")   Adjust.onCreate
  AdjustEvent("b77sdy")                                Adjust.trackEvent   fired at
    launch
smali3/com/herai/mobile/activity/MainActivity.smali   requestConsentInfoUpdate (Google
     UMP)   reached after SplashActivity
```

The finding rests on the control flow of the classes that were read as smali. The file classes3.dex holds 1,469 of about 1,541 references to the app's own package. The files classes.dex and classes2.dex were reviewed by string search only, so a consent step in code that was not disassembled is possible and UNVERIFIED. Firebase also initialises automatically in many builds, so the Adjust event is the clearest instance. Whether any SDK transmits before the consent form has been answered needs a runtime trace.

Section 165(3) TKG 2021 requires consent for storing or reading information on the terminal equipment of a user, unless strictly necessary for a service the user requested. An attribution event is not strictly necessary for chat. The app does carry a working consent mechanism, so the defect is the order of calls.

Impact: Each person who installs the app is registered with an attribution service at the first launch, before the form that asks them about advertising appears.

Fix: Move the consent request ahead of every advertising and attribution call, start those SDKs after a recorded choice and fire attribution events only with consent.

M2: Chat and image requests go to a US cloud backend and the policy offers one sentence on transfers

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B)

The app talks to api.herai.top, with the endpoints /honey/bot/chat_new, /honey/bot/chat_stream_refresh, /honey/group_role/chat and /honey/group_role/chat_refresh. Public DNS resolves the host to 3.220.89.10 and 35.173.94.195, which belong to Amazon Technologies Inc. (AWS us-east-1, Northern Virginia). The privacy policy states "Your data may be transferred across borders. We ensure such transfers are conducted with the necessary legal safeguards." It names no provider, no country and no safeguard.

```
api.herai.top  ->  3.220.89.10, 35.173.94.195   OrgName Amazon Technologies Inc.,
    NetName AMAZON-IAD
herai.top: registrar NameSilo, registrant redacted
Policy, International Data Transfers: "Your data may be transferred across borders."
Policy, Interaction Data: "We may log your chat history to enhance AI performance"
Policy, Sharing: "third-party providers to assist with analytics, cloud storage, and
    payment processing"
```

Hosting by a US provider can be lawful. Art. 46 or an adequacy decision under Art. 45 then has to carry the transfer, and Art. 13(1)(f) requires the policy to say which one. The backend was not called and no request content was observed. That the chat text goes to this host is inferred from the endpoint names. The geography rests on passive DNS and IP registry data alone.

Impact: People who talk to the chat characters and generate pictures are told only that data may cross borders. They cannot learn which company stores their chat history or where.

Fix: Name the hosting provider and region, state the Art. 45 or Art. 46 basis, conclude a processor contract under Art. 28 and state the retention period for chat history.

M3: Four different age statements, no verification, and a store rating of 18 against terms that admit users from 13

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 privacy policy states that the application is not designed for users under 13. The user agreement states that users must be at least 13 and that parental or guardian consent is required under 18. The first-run string limit_title reads ”You must be 18+ to use Her AI”. Google Play rates the app PEGI 18 with the descriptors Users Interact and Shares Location. A search of the resources and all three dex files found no date of birth field and no verification step.

```
Privacy policy, Children's Privacy    "not designed for users under 13"
User agreement 2.1 Eligibility        "at least 13 years old. If under 18, parental or
     guardian consent is required."
Build string limit_title              "You must be 18+ to use Her AI"   (one-tap click
    -through)
Google Play listing                   PEGI 18, Users Interact, Shares Location (14
    November 2026)
```

Art. 8(1) GDPR sets the age for valid consent to information society services in Austria at 14 under section 4(4) DSG. A user under 14 needs the consent of a parent, and no document describes how the operator obtains or checks it. The three documents of the operator disagree with each other, so users cannot tell which rule applies. Whether the server applies an age or content rule was not observed and is UNVERIFIED. No minor was observed using the app.

Impact: A twelve or thirteen year old reads a policy that excludes them below 13, an agreement that admits them from 13 and a store page that says 18, and a single tap decides. The operator cannot know who is a child.

Fix: Choose one minimum age, align the policy, the agreement, the in-app screen and the store rating, and publish the age assurance method together with the parental consent step for any user below the chosen age.

M4: Data safety label, listing text and privacy policy disagree on encryption, deletion, location and chat history

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 label of 14 November 2026 states that data is not encrypted in transit and that the developer provides no way to request deletion. The policy offers deletion on request and promises security measures, and the listing text promises "SECURE & PRIVATE". The label declares approximate and precise location as collected and shared for analytics and advertising, while the manifest declares no location permission. The label lists no chat content among collected data, while the policy says that chat history may be logged.

```
Shared: device or other IDs (App functionality, Analytics, Advertising), approximate
    and precise location
        (Analytics, Advertising for precise), crash logs, diagnostics, app
    interactions
Collected: device IDs, approximate and precise location, crash logs, diagnostics,
    photos (optional), name, email address (optional)
Security: "Data isn't encrypted"  "Data can't be deleted"
```

```
Listing text         "SECURE & PRIVATE: Your privacy is our top priority."
Policy, Your Rights  "You may request the deletion of your data at any time"
Policy, Interaction  "We may log your chat history to enhance AI performance"
Manifest             no ACCESS_FINE_LOCATION, no ACCESS_COARSE_LOCATION; no network
    security override, so cleartext is blocked at target SDK 35
```

The label can be wrong in either direction. It may overstate a risk, as for location and encryption, or understate it, as for chat history. 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 descriptor Shares Location on the listing falls under the same open question.

Impact: A person who reads the label is told that their data travels unencrypted and cannot be deleted. The policy and the listing text say the opposite, and neither mentions that chats are logged in the label.

Fix: Align the Data safety declaration with the policy and the build: declare chat content, remove location entries the app cannot collect, and state the encryption and deletion practice that applies.

M5: Operator is an individual developer account with a limited company on the store panel, a personal Gmail contact and an unfilled governing law

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 Google Play developer account is named MohamedGMohie. The developer panel lists PCRS LLC, 2001 42nd Ave, Oakland, CA 94601, United States, telephone +44 7879 503476 and the contact mohamedgamalmohie@gmail.com. The policy and the user agreement name no company, no postal address and no registration number, and give the same Gmail address as the only contact. Section 10 of the user agreement reads ”governed by the laws of [Your Jurisdiction]” and ”arbitration in accordance with the rules of [Arbitration Institution]”. Neither document names a representative in the Union, a legal basis per purpose or a retention period.

```
Google Play developer account   "MohamedGMohie"
Google Play developer panel     PCRS LLC, 2001 42nd Ave, Oakland, CA 94601, +44 7879
    503476
Contact in policy, agreement, listing   mohamedgamalmohie@gmail.com
user-policy.html 10.1   "[Your Jurisdiction]"     10.2   "[Arbitration Institution]"
EU representative: none   DPO: none   Legal bases: none   Retention: "only as long as
    necessary"
```

The notice of 21 August 2026 described the operator as an individual with no registered company. The developer panel of 14 November 2026 names PCRS LLC. Whether PCRS LLC is registered, and how it relates to the developer account, was not checked against a company register and is UNVERIFIED. The description of the operator as an individual without a company is withdrawn.

The app is offered in Austria, so Art. 3(2) GDPR applies to a controller established in the United States, and Art. 27(1) requires a representative in the Union. None is stated. At least three unrelated products carry similar names (Her AI: Virtual Companion with package com.herai.aiboychat, HeraHeavenAI and Hera AI), so every reference must use the package com.mohie.herai and the title ”Her.AI - Funny Chat Friend”.

Impact: A user in Austria who wants to see or delete their chat history has a personal Gmail address and a US address on the store panel, and the agreement they accepted contains two blank clauses.

Fix: Name the controller with its address and registration number in the documents, appoint an Art. 27 representative, state the legal bases and retention, and fill or remove the governing law and arbitration clauses.

L1: Firebase key and SDK identifiers 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 AIzaSyAQBi07uLSDo4-PEpH_ROP2GA54BGFuR6g, project herai-db0da, sender 963459246842, Facebook app id 647494194385139 with client token 076d7dd06442f67d803594420c29faba, the AdMob application id ca-app-pub-2516504098892498~4269075857 and the Adjust app token xb2kzzkfim80. These values ship in every build by design. Restrictions on the key and the security rules of the Firebase project were not tested, because no request was sent to any vendor endpoint.

The notice of 21 August 2026 described these values as publicly shipped identifiers. The finding is limited to the open question of key restrictions and project rules. Rated LOW.

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

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

Impact Analysis

The people affected are users of an AI chat app that presents itself as a funny chat friend. The audience includes teenagers, because the documents admit users from 13 and the app is easy to join in guest mode. Users bring conversations, pictures they create and purchases into the app.

Three points carry the weight. The device is registered with an attribution service before the consent form (M1). The age rules contradict each other and one tap decides (M3). The store label tells users that their data is unencrypted and cannot be deleted while the policy says the opposite (M4).

The remaining findings concern the transfer to a US host (M2), the identity of the operator (M5) and a hygiene item (L1).

The Complete Chain

Step 1, the store page: a user sees PEGI 18, Contains ads and a label that says data is not encrypted and cannot be deleted (M4). The listing promises ”SECURE & PRIVATE”.

Step 2, first launch: the start-up code sets up Google Mobile Ads and Firebase Messaging and fires an Adjust event (M1).

Step 3, age: a first-run screen says 18+, the agreement says 13, the policy says under 13 is excluded, and one tap decides (M3).

Step 4, conversation: chat and image requests go to api.herai.top at AWS in the United States (M2).

Step 5, rights: a user who wants access or deletion finds a personal Gmail address and an agreement with blank governing law and arbitration clauses (M5).

The operator has not answered any of these points.

Child Protection & Age Assurance

The operator states a minimum age of 13 in the policy and the agreement, requires parental consent under 18, shows an 18+ screen in the app and carries a store rating of PEGI 18. The build has no date of birth field and no verification step. The 18+ screen is a click-through. Art. 8 GDPR sets the age for valid consent to information society services in Austria at 14 under section 4(4) DSG, so a user of 13 who follows the agreement is below it.

The store rating of 18 says that the app is meant for adults, and the agreement invites thirteen year olds. The listing text offers a humour chat and picture creation, which appeals to young users. Whether the server applies any rule was not observed and is UNVERIFIED. The question put to the operator on 21 August 2026 about a documented assessment under Art. 35 stays unanswered.

Data Protection: Article by Article

Article 5(1)(a), transparency: engaged by M2, M4 and M5.

Article 6(1)(a), Article 7 and Article 4(11), consent: engaged by M1. The order of calls in the start-up code shows the consent request after the attribution event.

Article 8, Article 24 and Article 25: engaged by M3 and M1.

Article 12(1) and Article 13(1)(a), (b), (c), (e) and (f), Article 13(2)(a): engaged by M2, M4 and M5.

Article 17: engaged by M4. The label says deletion is not possible, and the policy says it is.

Article 27(1) and Article 3(2): engaged by M5. No representative is named.

Article 28(1): engaged by M2 for the hosting provider.

Article 32(1)(a) and (b): engaged by M4 and L1.

Article 35(3)(b): engaged by M3.

Articles 44 to 46: engaged by M2. The policy names no safeguard.

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

Consumer Protection & Deceptive Design

The build contains a monetised intimacy mechanic. The local Room database carries an intimacy_value column in the CacheMessage, GroupCache, Profile and Producer tables and a pricing function GeneratePhotoPrice(intimacy). The string intimacy_vip_save reads ”Pro Can Unlock All Images Using Chat Intimacy Value”. The subscription is therefore sold as a way to unlock content that is gated by an engagement score built up through chat. The design is common for the product category. It was not scored, and its effect on users was not measured. The Unfair Commercial Practices Directive 2005/29/EC applies to the commercial use of such mechanics, and the audience question under M3 makes it more relevant.

The listing text states ”AI Unpredictability” and the agreement states that not all offensive material may be removed at once. Those statements are specific. Their accuracy was not tested.

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 contradiction with the developer's own policy and listing text. 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

The operator has no establishment in the Union in the documents read. Every supervisory authority where users are affected is competent, and the Austrian authority holds the first notice.

HerAI belongs to a group of AI companion 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.mohie.herai
Version       2.3.5 / versionCode 44   minSdk 24, targetSdk 35
Firebase      project herai-db0da   sender 963459246842
Backend       api.herai.top (3.220.89.10, 35.173.94.195)
Adjust        app token xb2kzzkfim80   launch event b77sdy
AdMob         ca-app-pub-2516504098892498~4269075857
Start-up      smali3/com/herai/mobile/init/AppInitializer.smali, MyApplication.smali
    onCreate, MainActivity.smali (consent)
```

```
Google Play listing and Data safety   playstore_snapshot_2026-11-14.txt
herai.top/privacy-policy.html         herai_privacy_policy_2026-11-14.txt
herai.top/user-policy.html            herai_user_agreement_2026-11-14.txt
```

Reproduction for M1: open AppInitializer.create and MyApplication.onCreate and compare their order with the call in MainActivity. Reproduction for M3: open the three documents and the Play listing. Reproduction for M4: compare the Data safety page with the privacy policy. The SHA-256 of the pulled base APK is not recorded in the case folder.

Disclosure Timeline & Outcome

2026-08-21 15:41 UTC Delivery of the notice REF HERAI-2026-R1 to mohamedgamalmohie@gmail.com, the only contact in the policy and the agreement, copy to dsb@dsb.gv.at and edps@europa.eu. The copy to edps@europa.eu was returned as unknown, so the European Data Protection Supervisor did not receive this notice. The 90 day embargo runs from the delivery.

2026-08-28 First follow-up to the same address. No delivery failure was returned.

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

2026-11-14 No reply of any kind is recorded. Listing, Data safety page, privacy policy and user agreement read on this date.

The description of the operator as an individual without a registered company is withdrawn.

What the Operator Documents State Clearly

The app carries a working consent mechanism with the Google User Messaging Platform and the standard IAB TCF keys. The permission set is small, with no microphone, camera, location or biometric access, and the voice feature only plays audio. No custom component is exported, and no cleartext endpoint was found. The policy offers access, correction and deletion and discloses that chat history may be logged. The listing carries the PEGI 18 rating and discloses unpredictable AI output.

Residual Risk & Recommendations

Open on 14 November 2026: all six findings, because the operator has not replied. The runtime questions stay open. They are whether any SDK transmits before the consent form is answered, whether code in classes.dex or classes2.dex calls a consent flow, what the server enforces on age and content, and whether PCRS LLC is the registered operator. Builds since 2.3.5 were not analysed.

Recommendations: ask for consent before any advertising or attribution call. Choose one minimum age and verify it. Name the hosting provider, region and safeguard. Correct the Data safety declaration. Name the controller, appoint an Art. 27 representative and fill the governing law clause.

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 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 HERAI-2026-R1.