



Security & Privacy Disclosure, Final Report

Trade Republic (de.traderepublic.app) v4.2627.3

A securities, SEPA and crypto-custody app with no declared certificate pin, Firebase and ML Kit started before any consent screen, three biometric processors including recurring face re-authentication, and a Junior account product for minors in the same install as an operator-admitted advertising attribution stack

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 4 OCTOBER 2026, ONE TEMPLATE REPLY IN 103 DAYS, NONE OF THE THREE QUESTIONS ANSWERED

Target	Trade Republic Bank GmbH, Brunnenstraße 19-21, 10119 Berlin (BaFin-supervised credit institution). Privacy contact published by the operator: dataprotection@traderepublic.com ; the privacy notice also routes DPO contact by letter or by email request. No named Data Protection Officer was found.
Package	de.traderepublic.app (versionCode 31688), minSdk 32, targetSdk 35
Platform	Android, static analysis (base.apk 167.7 MB, split_config.arm64_v8a.apk 39.4 MB, split_config.xxhdpi.apk 1.0 MB; 17 classes*.dex files; Pairip app-shielding wrapper)
Initial Disclosure (R1)	2026-07-06 (REF de.traderepublic.app, R1). Gmail holds no sent copy of the 6 July message; two automated replies arrived on 6 July and the 26 July message records the 6 July contact.
Disclosure / Embargo Date	2026-10-04
Report Published	2026-10-17
Overall Severity	HIGH
Findings	8 (3 High, 4 Medium, 1 Low) plus 1 negative result on ad-serving and session-replay SDKs
Correspondence	Gmail holds five messages sent by RFI-IRFOS in the case thread (26 July, 9 August, 12 August, 24 August, 3 September 2026), addressed to dataprotection@traderepublic.com and, from 26 July, datenschutz@traderepublic.com , with service@ and presse@traderepublic.com in copy and, on 26 July, 9 August, 12 August and 24 August, the Berlin data protection authority (BlnBDI), the Austrian DSB and the EDPS. The 3 September message was copied to service@ and presse@ only. The 26 July message records four earlier mails from 6 July, none of which is held in the Gmail account, so the written record counts nine sends, five of them verified. Trade Republic responded with seven messages: six identical automated replies from no-reply@traderepublic.com ('Bitte verwende das Hilfe-Center in der App', 6 July twice, 24 July, 25 July twice, 26 July) and one reply from dataprotection@traderepublic.com on 9 August, a customer-support template with an unfilled subject field ('regarding [add topic]') asking RFI-IRFOS to write from an email address registered to a customer account. No reply of any kind arrived after 9 August. No delivery failure was recorded.
Authorities CC'd	Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) at mailbox@datenschutz-berlin.de , Österreichische Datenschutzbehörde (DSB), European Data Protection Supervisor (EDPS)
SHA-256 (base APK)	67a49dbb510ea4ec2c05c0c444d00d0be18c0c47568bf50bacb6331d6392bdd0

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	H1: No declared certificate pin on a securities, SEPA and crypto-custody app: the only network security configuration is a debug-overrides block	6
4.2	H2: Firebase, ML Kit and a boot receiver start before any consent screen; no consent-management implementation and no Consent Mode default	7
4.3	H3: Three biometric and identity processors, including a recurring face re-authentication flow on AWS, in one banking app	8
4.4	M1: Firebase and Google credentials plus a live Firebase Realtime Database URL in plaintext in strings.xml	9
4.5	M2: Adjust, Braze and GrowthBook: an operator-admitted personalized-advertising and influencer attribution stack in a licensed brokerage app	10
4.6	M3: A SharedPreferences store named CARD_CACHE_SHARED_PREFS with a CARD_NUMBER_KEY and no Jetpack Security usage anywhere in the binary	11
4.7	M4: Junior accounts for minors and a Savings Patron data flow for non-customers in the same install as the attribution stack	11
4.8	L1: Debug and developer scaffolding in the production release	12
5	Impact Analysis	13
6	The Complete Chain: Seven Replies, One Template, Zero Answers	13
7	Disclosure Timeline & Outcome	14
8	What Trade Republic Got Right	14
9	Data Protection Article by Article	15
10	Regulatory Landscape & Fine Exposure	15
11	Indicators of Compromise	16
12	Residual Risk & Recommendations	16

Executive Summary

Trade Republic's Android application (de.traderepublic.app v4.2627.3) was analyzed on 6 July 2026 with apktool (no baksmali), raw string extraction across all 17 dex files, an aapt2 cross-check and a native library inventory of the arm64 split. The analysis recorded three HIGH findings, four MEDIUM findings and one LOW finding. It also recorded a negative result: no ad-serving SDK and no named session-replay SDK exists in the binary.

H1: the only network security configuration ships a debug-overrides block that trusts user-installed certificate authorities and declares no base-config, no domain-config and no pin for any Trade Republic domain; OkHttp's CertificatePinner classes are present and no populated sha256/ pin value exists in any of the 17 dex files. H2: FirebaseInitProvider (initOrder 100) and MIKitInitProvider (initOrder 99) are instantiated at process start, a BOOT_COMPLETED receiver fires on device boot, no consent-management implementation exists in the binary and the manifest declares none of the Google Consent Mode default meta-data. H3: identity and biometric checks run through Fourthline, WebID Solutions and AWS Rekognition Face Liveness via AWS Amplify, the last in a package named selfieauth that points to recurring face re-authentication.

M2 rests on the operator's own words. Trade Republic's privacy notice (page 3, section 2.3) says it uses Adjust 'to display (or not display) personalized ads to you' and to 'attribute sign ups or other customers behavior to specific campaigns, affiliate marketing partners or influencers'. The binary matches: Adjust through a Trade Republic branded endpoint, Braze with an EU endpoint, and GrowthBook feature-flag experimentation wrapped in Trade Republic's own package. M4 records that the same install carries the Junior account onboarding flow for minors and a 'Savings Patron' data flow for non-customers.

RFI-IRFOS put three questions to Trade Republic: who the named data protection officer or security lead is for this disclosure; whether the findings were logged internally and assessed against the Art. 33 GDPR notification duty; and whether a substantive technical reply would arrive before or after the Berlin authority or the Austrian DSB made contact. The case thread shows six identical automated redirects to the in-app help center and one customer-support template. No named person, no yes or no on Art. 33 and no technical reply arrived in 103 days. The embargo ended on 4 October 2026.

ID	Severity	Title
H1	HIGH	No declared certificate pin on a securities, SEPA and crypto-custody app: the only network security configuration is a debug-overrides block
H2	HIGH	Firebase, ML Kit and a boot receiver start before any consent screen; no consent-management implementation and no Consent Mode default
H3	HIGH	Three biometric and identity processors, including a recurring face re-authentication flow on AWS, in one banking app
M1	MEDIUM	Firebase and Google credentials plus a live Firebase Realtime Database URL in plaintext in strings.xml

ID	Severity	Title
M2	MEDIUM	Adjust, Braze and GrowthBook: an operator-admitted personalized-advertising and influencer attribution stack in a licensed brokerage app
M3	MEDIUM	A SharedPreferences store named CARD_CACHE_SHARED_PREFS with a CARD_NUMBER_KEY and no Jetpack Security usage anywhere in the binary
M4	MEDIUM	Junior accounts for minors and a Savings Patron data flow for non-customers in the same install as the attribution stack
L1	LOW	Debug and developer scaffolding in the production release

Subject & Operator Context

Trade Republic Bank GmbH is a Berlin credit institution that offers securities trading, SEPA transfers, card products, crypto custody through BitGo Europe GmbH and Junior accounts for minors in one Android application. The privacy notice (Privacy-Website_en-DE.pdf, last updated 2025-06-23, fetched 2026-07-06) names BaFin, the Deutsche Bundesbank, the EBA and the ECB as prudential reporting recipients. BaFin is a banking supervisor and has no GDPR lead-authority role. The company's main establishment is in Berlin, so the Berlin authority (BlnBDI) is the likely lead authority under Art. 56; the privacy notice describes the Art. 77 complaint route to the authority at the company's location without naming BlnBDI, so this report treats BlnBDI as an inference from location. The Austrian DSB acted as the initiating authority. The in-app App Privacy Notice sits behind login and was not accessed; statements about app-side consent gating are limited to what the binary shows.

Engagement Summary

RFI-IRFOS analyzed de.traderepublic.app v4.2627.3 on 6 July 2026 using apktool (manifest, resources and strings without baksmali; host memory was constrained throughout), raw string extraction across classes.dex to classes17.dex, an independent aapt2 and dumpsys check of the runtime target SDK, and an inventory of the arm64 native libraries. No Trade Republic server, account or production system was accessed, no embedded key was used and the Firebase Realtime Database URL was not queried. Findings are classified as observed fact, where the artifact itself shows the behavior, or inference, where a runtime capture (R2) would be needed. Severity labels follow the RFI-IRFOS blast-radius method: the CVSS v4.0 base score is shown in each finding box and a label above the score band is explained in the finding text. CVSS 4.0 scores in this report were assigned from the standard vector pairs used across the 2026 series and were not produced by a calculator.

Findings

H1: No declared certificate pin on a securities, SEPA and crypto-custody app: the only network security configuration is a debug-overrides block

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 - TLS trust rests on the platform default, no pin-set for any Trade Republic domain

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
  <debug-overrides>
    <trust-anchors>
      <certificates src="user" />
    </trust-anchors>
  </debug-overrides>
</network-security-config>
```

```
certificatePinner
Certificate pinning failure!
Certificate pinning requires X509 certificates
pins must start with 'sha256/' or 'sha1/':
provideCertificatePinner
Lokhttp3/CertificatePinner;
Lokhttp3/CertificatePinner$Builder;
```

Impact: AndroidManifest.xml declares android:networkSecurityConfig="@xml/network_security_config". The referenced file contains a debug-overrides block that trusts user-installed certificate authorities and nothing else: no base-config, no domain-config and no pin-set for any traderepublic.com or trade.re domain. OkHttp's CertificatePinner family is linked into the app (certificatePinner, 'Certificate pinning failure!', provideCertificatePinner) and a search for a populated pin (sha256/ followed by 20 or more base64 characters) across all 17 dex files returned no match. Production TLS trust for this release therefore rests on the Android platform default for targetSdk 35: cleartext blocked and every system certificate authority trusted. Observed fact: the shipped configuration declares no pin and no pin value exists in the dex strings. Not observed: runtime behavior against production endpoints, which needs an interception test in R2. RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.6 to HIGH because the channel carries securities orders, SEPA transfers and crypto-custody instructions, so any device with an attacker-controlled trusted root (an enterprise-injected certificate, some security or parental-control software, a compromised device) can read and alter traffic that moves money, a consequence the CVSS vector does not capture.

H2: Firebase, ML Kit and a boot receiver start before any consent screen; no consent-management implementation and no Consent Mode default

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 - two ContentProviders at process start, no CMP, no google_analytics_default_allow meta-data

```
<provider android:authorities="de.traderepublic.app.firebaseinitprovider" android:
  directBootAware="true"
  android:exported="false" android:initOrder="100" android:name="com.google.firebase.
  provider.FirebaseInitProvider"/>
<provider android:authorities="de.traderepublic.app.mlkitinitprovider" android:
  exported="false"
  android:initOrder="99" android:name="com.google.mlkit.common.internal.
  MLKitInitProvider"/>
<receiver android:exported="false" android:name="de.traderepublic.notification.
  broadcasts.PushNotificationRebootReceiver">
  <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></intent
  -filter>
</receiver>
```

Impact: com.google.firebase.provider.FirebaseInitProvider (initOrder 100, directBootAware) and com.google.mlkit.common.internal.MLKitInitProvider (initOrder 99) are ContentProviders that Android instantiates during application process creation, before any Activity and so before any consent interface can render. Firebase's ComponentDiscoveryService registers Analytics, Messaging, Installations and Remote Config at the same point. PushNotificationRebootReceiver listens for BOOT_COMPLETED, so code runs on device boot whether or not the user has ever opened the app. A search for OneTrust, Didomi, Usercentrics, Cookiebot and consentmanager across all 17 dex files found none; the IABTCF_* names that exist are constants inside Google's SDK. The manifest declares none of the google_analytics_default_allow_* Consent Mode meta-data, so no default-deny posture exists either. Observed fact: the providers and receiver are declared as quoted and no consent mechanism exists in the binary. Not observed: the data fields that Firebase transmits in that window, which need a cold-start capture in R2. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the structure applies to every launch of a regulated banking application and a Firebase Installation ID is created before the user can choose, which makes valid consent under Art. 7 structurally impossible for that first processing.

H3: Three biometric and identity processors, including a recurring face re-authentication flow on AWS, in one banking app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 4.5 - Fourthline, WebID Solutions and AWS Rekognition Face Liveness wired into onboarding and re-authentication

```
de.traderepublic.kyc.fourthline.v2.impl.presentation.selfie.FourthlineSelfieActivity
de.webidsolutions.video_ident.plugin.VideoIdentActivity
de.webidsolutions.video_ident.plugin.services.WebIdCameraService (camera|microphone)
de.traderepublic.selfieauth.impl.presentation.liveness.views.TRFaceGuide
com.amplifyframework.ui.liveness.model.
    FaceLivenessDetectionException$SessionTimedOutException
com.amplifyframework.predictions.aws.models.liveness.ClientSessionInformationEvent
de.traderepublic.kyccommon.rekyc.presentation.loading.
    ComposableSingletons$KycProvidersScreenViewKt
imprint_company_name = WebID Solutions GmbH
imprint_company_commercial_register = HRB 146331B
```

Impact: The manifest declares FourthlineSelfieActivity (de.traderepublic.kyc.fourthline.v2) and the WebID Solutions video-identification activity and camera service (foregroundService Type camera|microphone), and WebID Solutions GmbH's own imprint strings (HRB 146331B) ship inside the app. AWS Amplify's Face Liveness SDK (com.amplifyframework.ui.liveness, com.amplifyframework.predictions.aws.models.liveness) is wired into Trade Republic's own de.traderepublic.selfieauth package (TRFaceGuide), and the arm64 split carries libliveness_opengl_renderer_jni.so and libtensorflowlite_jni.so. Separate use cases for registration and re-KYC providers (getGetRegistrationKycProvidersUseCase, getGetReKycProvidersUseCase) show a deliberate multi-vendor design. Facial biometric data used for identification is special-category data under Art. 9 GDPR. AWS is a US company, so Art. 44 to 49 applies to that component. Observed fact: the three vendor integrations and the selfieauth package exist. Not observed: which Amazon region and contract terms apply, and the in-app App Privacy Notice, which sits behind login. RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.5 to HIGH because the selfieauth package points to repeated facial capture for re-authentication and not only a one-time onboarding check, which raises the frequency and volume of special-category processing across three outside processors, a scope the CVSS vector does not capture.

M1: Firebase and Google credentials plus a live Firebase Realtime Database URL in plain-text in strings.xml

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 - API key, OAuth client, project identifiers and a Realtime Database hostname in the public APK

```
default_web_client_id = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade  
    Republic in R1]  
firebase_database_url = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade  
    Republic in R1]  
gcm_defaultSenderId = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade  
    Republic in R1]  
google_api_key = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade Republic  
    in R1]  
google_app_id = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade Republic in  
    R1]  
google_crash_reporting_api_key = [REDACTED IN PUBLIC REPORT -- disclosed privately to  
    Trade Republic in R1]  
project_id = [REDACTED IN PUBLIC REPORT -- disclosed privately to Trade Republic in R1  
    ]
```

Impact: res/values/strings.xml holds default_web_client_id, firebase_database_url, gcm_defaultSenderId, google_api_key, google_app_id, google_crash_reporting_api_key and project_id, extractable with apktool in under a minute. This build ships a Firebase Realtime Database URL. Per RFI-IRFOS methodology the URL was not queried, because that would be live testing of a production endpoint. Google documents Firebase API keys as not secret by design, so the residual risk is quota abuse and, if the database security rules are misconfigured, unauthorized read or write; the rules cannot be judged from static analysis. The exact values are withheld from this public report and were given to Trade Republic in R1: [REDACTED IN PUBLIC REPORT – disclosed privately to Trade Republic in R1].

M2: Adjust, Braze and GrowthBook: an operator-admitted personalized-advertising and influencer attribution stack in a licensed brokerage app

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 - Trade Republic branded Adjust endpoint, Braze with EU endpoint, GrowthBook experimentation, ad-ID permissions

```
https://app.tr.adjust.com
sdk.fra-01.braze.eu
de.traderepublic.remoteconfig.growthbook.usecase.GrowthBookSDKManagerImpl
https://cdn.growthbook.io
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_AD SERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_AD SERVICES_AD_ID"/>
```

Impact: Adjust is integrated through <https://app.tr.adjust.com>, a Trade Republic specific subdomain, with 412 class-string hits. Braze is integrated with 1,276 class-string hits and an EU endpoint (sdk.fra-01.braze.eu) next to the US default. GrowthBook runs through `de.traderepublic.remoteconfig.growthbook.usecase.GrowthBookSDKManagerImpl` against cdn.growthbook.io, a server-controlled experimentation platform whose configured experiments cannot be read from static strings. The manifest requests `AD_ID`, `ACCESS_AD SERVICES_ATTRIBUTION`, `ACCESS_AD SERVICES_AD_ID` and the Play install referrer service, which this integration explains. The operator's privacy notice (page 3, section 2.3) states: 'We use Adjust for marketing purposes; namely in order to track how our campaigns perform and improve them, display (or not display) personalized ads to you, to prevent marketing fraud and to attribute sign ups or other customers behavior to specific campaigns, affiliate marketing partners or influencers.' Observed fact: the integrations exist and the operator describes the purposes in its own words. Not observed: the data fields sent to Adjust and Braze, and which GrowthBook experiments touch order tickets or position screens. No AppLovin, AdMob mediation, Vungle, Unity Ads, ironSource, ContentSquare, GlassBox, Microsoft Clarity, Smartlook or FullStory classpath was found.

M3: A SharedPreferences store named CARD_CACHE_SHARED_PREFS with a CARD_NUMBER_KEY and no Jetpack Security usage anywhere in the binary

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 - card cache key name present, no EncryptedSharedPreferences or SQLCipher match in 17 dex files

```
CARD_CACHE_SHARED_PREFS
CARD_NUMBER_KEY
CARD_SCANNER
```

Impact: The dex strings contain CARD_CACHE_SHARED_PREFS, CARD_NUMBER_KEY and CARD_SCANNER. A search for androidx/security/crypto, EncryptedSharedPreferences, EncryptedFile and SQLCipher across all 17 dex files returned no match; the only AndroidKeyStore strings belong to AWS Amplify's own credential storage. The runtime contents of the store were not extracted, because the audit device holds no real financial data and no live account or card flow was triggered, so the value kept under CARD_NUMBER_KEY (a masked reference or a fuller number) is not established. The finding records a comparison: another payment app in the same 2026 series shows explicit encrypted preferences and a masked-number field name for its card cache, and this binary shows neither. The controller may protect the value with a mechanism that dex strings do not reveal, including a payment SDK with its own encryption.

M4: Junior accounts for minors and a Savings Patron data flow for non-customers in the same install as the attribution stack

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 4.5 - minor onboarding with birthplace, address and guardian consent next to Adjust, Braze and GrowthBook

```
<data android:host="traderepublic.com" android:path="/onboarding/junior/account-setup
"/>
de.traderepublic.junior.impl.domain.SavingsPatronRepositoryImpl
de.traderepublic.junior.impl.presentation.parentalcontrols.
    ParentalControlsTarget$CashControls
de.traderepublic.onboarding.v2.impl.junior.domain.usecase.JuniorDocumentUploadUseCase
de.traderepublic.onboarding.v2.impl.junior.presentation.birthplace.
    JuniorBirthplaceNode
de.traderepublic.onboarding.v2.impl.junior.data.model.
    JuniorGuardianBConsentAcceptanceApiModel
```

Impact: The manifest carries deep links for /onboarding/junior/account-setup and the dex strings contain a complete minor onboarding flow: JuniorOnboardingAddressNode, JuniorBirthplaceNode, JuniorDocumentUploadUseCase, JuniorGuardianBConsentAcceptanceApiModel and ParentalControlsTarget\$CashControls. The operator's privacy notice (page 3 and 4, section 2.7) states: 'We offer Junior Accounts to minors. Custodians of minors (usually

their parents) can invite others to contribute to the savings of the minor (Savings Patrons). Savings Patrons do not need to have a regular customer account with us. If you receive such an invite, you can click on the link and set up a direct debit mandate by entering your name, IBAN and email address (which needs to be verified).’ Observed fact: the minor flow and the Savings Patron description exist in the same binary that carries H2 and M2. Not observed: whether tracking identifiers, GrowthBook experiments or Adjust attribution are kept away from the minor journey, and an app-side disclosure surface for Savings Patrons, who interact through a web link. Recorded as a data-flow observation that the controller should confirm.

L1: Debug and developer scaffolding in the production release

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 3.1 - profileable shell, Amplify DeveloperMenuActivity, Compose PreviewActivity, NetworkDebugActivity

```
<profileable android:shell="true"/>
<activity android:name="com.amplifyframework.devmenu.DeveloperMenuActivity" android:
    theme="@style/OverlayActivity"/>
<activity android:exported="true" android:name="androidx.compose.ui.tooling.
    PreviewActivity"/>
<activity android:exported="false" android:name="de.traderepublic.networkdebug.ui.
    NetworkDebugActivity"/>
```

Impact: The release manifest contains profileable `android:shell="true"`, AWS Amplify’s `DeveloperMenuActivity`, Jetpack Compose’s `PreviewActivity` (`exported=true`, no intent filter) and Trade Republic’s own `NetworkDebugActivity` (not exported). Exploiting profileable or `PreviewActivity` needs local adb access or the ability to launch an explicit intent, which keeps real-world risk low. The finding records unnecessary attack surface and debug tooling in a banking app that otherwise shows careful build hygiene (`allowBackup false`, full backup and transfer exclusion).

Impact Analysis

H1, H2 and H3 describe the app from three sides. H1 leaves the trust of the transport channel to the device's certificate store. H2 starts analytics and ML components before the user can decide anything. H3 collects face data through three processors, one of them a recurring flow on a US cloud. M2 and M4 sit on top: an operator-admitted advertising and influencer attribution stack, and a minor onboarding flow in the same install. M1 and M3 add credentials and a card cache whose protection the binary does not show, and L1 adds debug surface. The negative results matter as much: no ad-serving SDK and no session-replay SDK were found, and several controls are done well (see below).

The Complete Chain: Seven Replies, One Template, Zero Answers

Trade Republic's side of the correspondence consists of seven messages. Six are the same automated text from no-reply@traderepublic.com, 'Bitte verwende das Hilfe-Center in der App': it states that the address is only for data protection and privacy requests, that the request cannot be handled by email, and that the user should send it through the app. They arrived on 6 July (14:12 and 15:48 UTC), 24 July (15:55), 25 July (15:47 and 19:28) and 26 July (14:57). The seventh is a reply from dataprotection@traderepublic.com on 9 August at 08:40 UTC to RFI-IRFOS's follow-up: a customer-support template that opens 'Hello , Thank you for your message regarding [add topic]', states that RFI-IRFOS wrote from an address not associated with a customer account and asks for a new request from the registered address. The subject placeholder was never filled in.

RFI-IRFOS's messages: the 26 July message records the first contact with dataprotection@traderepublic.com on 6 July and three further mails before it; Gmail holds no copy of those four. Gmail holds the case thread from 26 July: on 26 July RFI-IRFOS added datenschutz@traderepublic.com, the DPO contact that Trade Republic publishes, and presse@traderepublic.com, and stated that the response pattern had been published on 25 July, while the technical findings stayed under embargo until 4 October. On 9 August RFI-IRFOS followed up. On 12 August it quoted the unfilled template field and restated the three questions. On 24 August it named a third deflection layer after twelve days without any human reply and repeated that an ongoing internal review does not delay an initial Art. 33(4) GDPR notification. On 3 September it sent a fifth message with a 5 September deadline, copied to service@ and presse@ only. No reply of any kind followed.

The three questions as restated on 12 August and 3 September: (1) who at Trade Republic is the named data protection officer or security lead for this disclosure; (2) whether the findings were logged internally and assessed against the Art. 33 GDPR notification duty, yes or no; (3) whether a substantive technical reply would arrive before or after the Berlin authority or the Austrian DSB made direct contact. None was answered.

The operator's own privacy notice names dataprotection@traderepublic.com for data protection requests and offers a letter to the Data Protection Officer or an email request for a direct contact. A requester without an account, such as a researcher, a journalist or a former customer, cannot use an in-app help center, which is the access path the automated reply prescribes.

Disclosure Timeline & Outcome

2026-07-06 First contact with dataprotection@traderepublic.com (R1), findings and three questions. Two automated replies the same day. Gmail holds no sent copy.

2026-07-24, 2026-07-25 Three further identical automated replies.

2026-07-26 06:20 Case thread message in Gmail: datenschutz@ and presse@traderepublic.com added, BlnBDI, DSB and EDPS in copy, embargo unchanged at 2026-10-04. A sixth identical automated reply follows at 14:57.

2026-08-09 05:38 Follow-up. Reply at 08:40 from dataprotection@traderepublic.com: customer-support template with the unfilled subject field.

2026-08-12 Follow-up quoting the unfilled field and restating the three questions.

2026-08-24 Follow-up naming a third deflection layer after twelve days of silence.

2026-09-03 Fifth message in the thread, 5 September deadline. No reply.

2026-10-04 Embargo date reached. Correspondence record: 9 sends (5 verified in Gmail), 7 replies, 0 questions answered.

2026-10-17 This report published, 13 days after embargo, 103 days after original disclosure.

What Trade Republic Got Right

Real screen-capture protection: DETECT_SCREEN_CAPTURE is backed by code (USE_WINDOW_FLAG_SECURE_IN_ACTIVITIES, a Braze secure-window flag and the Android 14 ScreenCaptureCallback API).

Self-hosted crash reporting with privacy hardening: Sentry runs at sentry.traderepublic.com with screenshot and view-hierarchy attachment switched off, and Crashlytics collection is disabled.

Backup and transfer exclusion: allowBackup is false and data_extraction_rules.xml excludes every domain from cloud backup and device transfer.

Transparent automated-decision disclosure: the privacy notice names the Art. 22 GDPR processing for anti-money-laundering profiling and the right to manual review.

Named, regulated vendors in the KYC, payment and custody chain: Fourthline, WebID Solutions GmbH (with its own imprint in the app), Adyen for 3-D Secure 2 and BitGo Europe GmbH with an explicit in-app custody contract step.

An EU-region endpoint for the Braze SDK (sdk.fra-01.braze.eu).

No ad-serving SDK and no named session-replay SDK, checked by targeted search.

Consistent identity disclosure of Trade Republic Bank GmbH between the binary and the published privacy notice.

Data Protection Article by Article

Art. 32(1)(a) and (b) GDPR: H1 leaves transport security of money-moving traffic to the device's trust store, and M3 raises the question of how a card cache is protected at rest.

Art. 6(1), Art. 7(1) and Art. 5(1)(a) GDPR, ePrivacy Art. 5(3): H2 starts Firebase and ML Kit at process creation without a consent mechanism or a Consent Mode default.

Art. 9 and Art. 35 GDPR: H3 routes face data through three processors, one of them recurring. Whether a DPIA covers the chain is not stated by the operator.

Art. 44 to 49 GDPR: AWS Face Liveness is a US component. The transfer mechanism is not visible in the binary or in the website privacy notice.

Art. 5(1)(c), Art. 13, Art. 14 and Art. 25 GDPR: M2 describes personalized-advertising and influencer attribution in a brokerage app, and the app-side gating of that processing is not shown.

Art. 8 GDPR: M4 puts the minor journey in the same install as the attribution stack.

Art. 12(1) GDPR: the operator must make data protection requests reachable. A reply that points to an in-app help center excludes requesters without an account.

Art. 33(4) GDPR: RFI-IRFOS stated in writing from 12 August that an ongoing internal review delays only the completeness of an initial notification. The supervisory authority copies have had visibility since the first message that copied them.

Art. 5(2) GDPR: for M1 the burden of showing that the key and database rules carry no abuse risk sits with the controller.

Regulatory Landscape & Fine Exposure

Trade Republic Bank GmbH has its main establishment in Berlin, so the Berlin authority (BlnBDI) is the likely lead authority under Art. 56, as an inference from the company's location. BaFin supervises the bank in the prudential sense and is not a GDPR lead authority. The Austrian DSB acted as the initiating authority, and the EDPS received the copies sent to it. The 3 September message was not copied to any authority. Any member-state authority where affected users reside may independently assert competence.

Art. 83(5) GDPR: fines up to EUR 20,000,000 or 4% of worldwide annual turnover apply to violations of Art. 5, 6, 7, 9 and 44 to 49. H2 and H3 implicate this tier.

Art. 83(4) GDPR: fines up to EUR 10,000,000 or 2% of worldwide annual turnover apply to violations of Art. 8, 25, 28, 32 and 35. H1, M1, M3, M4 and L1 implicate this tier.

This report states exposure categories; it does not predict any authority's decision.

Indicators of Compromise

All findings derive from static analysis of de.traderepublic.app v4.2627.3 as installed from Google Play, analyzed 2026-07-06. base.apk SHA-256: 67a49dbb510ea4ec2c05c0c444d00d0be18c0c47568bf50bacb6331d6392bdd0. split_config.arm64_v8a.apk SHA-256: 5f92b70e1d4c68d2e127d41af063c76ed0058ca2c81fdd75b11f21a1db0bf958. split_config.xxhdpi.apk SHA-256: 12754fe376ddddd10f509444f12fcd356dde9fb42c1bdb181efa49831156afe7b. Files of interest: AndroidManifest.xml (providers, receiver, permissions, debug components), res/xml/network_security_config.xml, res/values/strings.xml (Firebase values, withheld here), classes*.dex (pinning strings, Adjust, Braze, GrowthBook, KYC and Junior classes). No Trade Republic servers, accounts or production infrastructure were probed or accessed.

Residual Risk & Recommendations

H1: ship a base-config or domain-config with a pin-set and a backup pin for the Trade Republic API and trading domains, and verify that CertificatePinner is wired to it in the release build.

H2: start Firebase, ML Kit and any non-essential collection only after a consent decision, add a consent-management mechanism, declare the Consent Mode defaults as denied, and document the legal basis for what runs before it, including the BOOT_COMPLETED path.

H3: document an Art. 35 DPIA for the Fourthline, WebID and AWS chain, publish the Art. 44 to 49 mechanism for the AWS component, and state the retention of liveness data.

M1: rotate the key, restrict it to the package name and signing certificate, verify that the Realtime Database rules deny unauthenticated reads and writes, and remove the values from version-controlled resource files.

M2: justify personalized-advertising and influencer attribution in a brokerage app under Art. 5(1)(c), disclose the app-side gating and review GrowthBook experiments for investor-protection effects.

M3: confirm what is stored under CARD_NUMBER_KEY and how it is protected at rest.

M4: confirm that tracking identifiers and experiments are kept away from the Junior journey and disclose the Savings Patron flow in an app-side notice.

L1: remove profileable, DeveloperMenuActivity, PreviewActivity and NetworkDebugActivity from release builds.

Process-level: a privacy mailbox that answers every message with the same in-app redirect, and a customer-support template that treats a coordinated disclosure as an account-recovery request, need an internal route to a person who can read a disclosure addressed to the data protection function. An Art. 12 route for requesters without an account would close the gap.

Open R2 items for RFI-IRFOS: interception test of the production endpoints; cold-start capture of the pre-consent window; the data fields sent to Adjust and Braze; the contents of CARD_NUMBER_KEY under an authorized test account; the Realtime Database rules; the vendor of the two opaque native libraries. A later app version is not covered by this report.

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of de.traderepublic.app as installed from Google Play, analyzed 2026-07-06, using publicly available tools (apktool, aapt2, string extraction). No Trade Republic servers, accounts or production systems were accessed, no embedded key was used and the Realtime Database URL was not queried. Statements about the operator's privacy notice rest on Privacy-Website_en-DE.pdf (last updated 2025-06-23) as fetched on 2026-07-06; the in-app App Privacy Notice sits behind login and was not accessed. Technical evidence is archived under chain of custody and will be provided to the competent supervisory authority on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF TR-2026-R1-001.