

VOICE SERVICES / UNITED STATES

Robocall Mitigation Program

Umbolement UG (haftungsbeschränkt) | Kesru

PROVIDER	PROGRAM CONTROL
FRN 0038971149 Ulmenweg 10, 85221 Dachau, Germany	Version 2.6 4 October 2026 US business receptionist service
info@umbolement.com +49 1556 3047024 kesru.com	Initial RMD program / Activation gates: section 11 Implementation record: section 10

EFFECTIVE PROGRAM / BEFORE AND AFTER ACTIVATION

This policy takes effect immediately and applies before and after service activation. Customer voice traffic is enabled only after identity and number rights are checked, required controls operate, and carrier requirements are met (section 11). The local test record of 4 October 2026 is in section 10.

1. Business activity and scope

Kesru is an AI receptionist for US business end users: incoming calls, business information, messages, appointment requests, authorized callbacks and staff transfers. The initial service is limited to US voice-service operations. It does not offer carrier-to-carrier transit or foreign voice-service origination. Outbound calls to businesses run only under section 6.

The call path is Bulk Solutions (BulkVS), the company's US Asterisk/ARI bridge and the Kesru application; outbound legs return through Bulk. The company serves end users; it is incorporated in Germany without a US office, while the service runs entirely on US-based infrastructure. The assistant identifies the business and its AI role; dynamic speech does not remove calling-permission duties.

2. Accountability and contact

Mirwan Akayguen is the **Authorized Representative and Robocall Mitigation Contact**, acting under a power of attorney. His function is Operations. His business contact details and address are shown above. He administers this program, reviews customer acceptance and number rights, directs incident containment, coordinates provider escalation and authorizes restoration only after the recorded conditions have been met.

Mirwan accepts responsibility for responding to traceback requests within 24 hours of receipt, including weekends and holidays. He is responsible for monitoring the published business email and telephone, arranging a handover when unavailable, coordinating the investigation and ensuring a timely response. Technical work may be delegated; responsibility remains with him.

The FCC certification remains a separate personal declaration subject to its officer-signature rule.

02 / CUSTOMER AND NETWORK ACCESS

Prevent unauthorized calling

3. Customer acceptance procedure

Before allowing a business to originate calls, the reviewer records its legal name, business address, registration details where applicable, website, responsible representative, verified contact information and intended use. The reviewer compares the information with independent business records and resolves inconsistencies with the applicant. Email verification and payment are supporting account checks, not proof of a legitimate calling purpose.

The acceptance record contains the customer identifier, evidence references, reviewer, UTC review time, approved purpose, permitted numbers and initial capacity. Unresolved identity, number rights or use results in no origination approval. Material changes to ownership, numbers, calling purpose or volumes trigger a new review. Credible abuse complaints trigger an immediate risk review rather than automatic expansion.

4. Telephone numbers, caller ID and call permissions

For a number provisioned through Bulk, match the provider assignment to the approved Kesru customer. For an existing external number, require evidence of control and the customer's authorization to use or forward it. Save the evidence reference and review decision. Merely entering a number, recognizing its carrier or passing a format check does not establish rights.

Every enabled callback and transfer route must use the approved customer, purpose and caller ID. Transfer destinations must be approved for that customer. A suspension must block new origination even after retries, new sessions or changed numbers. Any route that cannot enforce these restrictions remains disabled until it passes the corresponding check.

Prohibited uses include illegal robocalling, impersonation, deceptive caller ID, unlawful traffic generation and bypassing a restriction. An existing customer relationship, a dynamic AI voice or an ordinary-looking telephone number is not assumed to provide calling consent.

5. Initial STIR/SHAKEN status and upstream review

Before service activation, retain Bulk's approval of the actual reseller use, contracting entity and relevant RMD record, routing details, operational contacts and authentication arrangements. Record who checked them and when; recheck material provider or route changes. Oracle's published address list places the configured bridge in **us-ashburn-1 (USA)**. The carrier routing is confirmed with Bulk before activation and rechecked after any change.

Initial implementation status: STIR/SHAKEN has not been implemented. The company, a provider directly serving end users, relies on the 47 CFR 64.6304(b) extension for providers incapable of obtaining an SPC token due to Governance Authority policy: as a new provider it does not yet meet the **STI-GA token access policy** (current Form 499-A, assigned OCN, RMD listing). No SPC token, STI certificate or third-party signing arrangement exists.

This filing is the first access step; Form 499-A, OCN, STI-PA registration, its own SPC token and certificate follow. Until then, outbound calls run only through its upstream carrier, which authenticates unsigned calls it receives under its own obligations (47 CFR 64.6302). Foreign incorporation is not claimed as an exemption, and carrier signing is not represented as Umbolement's own implementation. [1,3,4]

03 / TRAFFIC AND INCIDENT HANDLING

Detect, contain and document

6. Practical traffic review

The reviewed implementation contains company-bound inbound routing, request authentication, controlled number assignment, repeated-empty-call protection, customer usage accounting and cost/usage alerts. These are in-house application controls. A dedicated third-party robocall-analytics service is not represented as installed.

During enabled operation, the assigned operator reviews new complaints, provider notices and usage alerts, and checks call records against each customer's approved activity. Investigations consider unusual volume or spend, repeated destinations, unusually short or failed calls, changed caller IDs and unexplained transfers. Volume alone is not proof of abuse; the customer's purpose and other evidence determine the response.

Review at least daily while traffic is enabled, and promptly when an alert or complaint arrives. Record the trigger, affected account, relevant time window and numbers, findings, decision and next review time. Increase capacity only after review. Confirm that alert delivery and the relevant limits actually work before enabling the corresponding route.

Outbound business calls. Kesru's own sales calls pass a server-side check before every dial: a valid US number; a business landline confirmed by carrier lookup (wireless, residential or unconfirmed lines are refused); only states whose law permits such calls to business lines without prior consent; weekdays 9:00-17:00 local time in every time zone of the state; at most two attempts; a permanent internal do-not-call list that also takes verbal opt-outs during the call. Each call opens with the business name, the AI nature of the caller and a callback number. Customer campaigns require documented consent. Sales calls are off by default and have a kill switch.

7. Containment and restoration procedure

STEP	OPERATOR ACTION
Identify	Open a case with a UTC receipt time, source, affected customer and known call identifiers. Verify a requester through an independent trusted channel before disclosing customer information.
Contain	For credible unlawful traffic or compromised access, restrict the affected origination and involve Bulk as needed. Record the actual blocking action and verify that it takes effect. A written decision by itself is not a technical block.
Preserve	Export the minimum relevant call metadata and customer/number-authority evidence into the restricted case folder. Record the evidence period and source; do not copy audio or transcripts merely to establish routing.
Investigate	Compare the complaint with the authorized use, customer identity, assigned numbers and call chain. Obtain missing provider records where necessary; state gaps explicitly.
Restore or close	Restore only after the cause and rights are resolved, restrictions have been tested and management records approval. Close with the result, notifications and a retention review date. No automatic reactivation.

04 / TRACEBACK AND RECORDS

Respond within 24 hours

8. Traceback procedure and commitment

The company commits to respond within **24 hours** to all traceback requests from the FCC, law enforcement and the designated industry traceback consortium, and to cooperate in identifying and stopping unlawful callers using the service. The deadline runs from receipt, including weekends and holidays. A business-hours queue is insufficient. [1]

Mirwan Akayguen is responsible for the published contact channel and arranges a handover when unavailable. The operator opens a case immediately on becoming aware of a request. The local case tool records receipt and the 24-hour deadline; it does not monitor an inbox, wake a person or send a reply. Those duties remain with the assigned contact.

SEQUENCE	REQUIRED CASE CONTENT
1. Receive and verify	Requester, trusted return channel, original receipt timestamp, case reference and exact 24-hour deadline. Request clarification promptly if a call cannot be identified.
2. Locate the call	Search calling/called number and UTC time window or known call ID. Identify the Kesru customer, original call, linked transfer event and available carrier identifiers. Do not substitute an internal call ID for a provider SIP Call-ID.
3. Prepare the response	State the verified customer and call path, evidence source, available timestamps and identifiers, action taken and any missing information. If no match exists, report the search scope and result accurately rather than inventing a match.
4. Respond and follow up	Send the substantive response through the verified channel within the deadline. Retain proof of sending, preserve relevant evidence, cooperate with follow-up requests and record any restriction or remedial action. An unsent draft is not completion.

9. Data minimization and access

The reviewed customer-call store uses a 90-day deletion period. The local traceback journal follows that period and contains routing/event metadata, not audio or transcript copies. It cannot answer from records already deleted. Separate bridge/provider logs may have different availability; no longer period is asserted for them.

An exported incident file is separate from routine call storage. The case tool sets a 30-day retention review. At that review the case owner records a justified deletion date, or the basis and next review date for continued preservation. Case files and their copies require controlled manual deletion; automatic case-file deletion is not claimed.

Only staff handling the case may access the restricted evidence folder. Use verified recipient channels for disclosures. A case hold must identify its basis, scope, owner and review date; it must not silently become permanent retention of all calls.

05 / IMPLEMENTATION AND MAINTENANCE

Evidence and activation conditions

10. Implementation record - 4 October 2026

Offline validation passed 57 initial tests, three targeted follow-ups after review, and 11 independent command-line checks. Synthetic calls exercised actual bridge, authenticated handler and database functions with a simulated carrier. The verified scope and limits follow.

AREA	VERIFIED SCOPE
Customer binding	Call, customer and line binding held. Wrong-customer changes, conflicting replays and invalid bridge signatures were rejected. Existing empty-call protection was exercised.
Call and transfer search	Call ID, customer and number/UTC-window searches passed. Transfer targets match their own event times. Above 500 matches, the operator must narrow the search; incomplete results are not returned.
Case preparation	Deadlines are receipt time plus 24 hours in UTC, tested across a clock change. Search criteria and decision history persist. Drafts and decisions are not recorded as sent or executed.
Record deletion	The existing cleanup removes journal records older than 90 days and records for deleted customers. The journal excludes audio and transcripts.

The complete application/audio stack was not started; the shared ingress decision was a controlled test boundary. No PSTN or successful transfer delivery was tested. A transfer event is not an independent outbound-leg record; general callback correlation remains unverified. Carrier SIP Call-ID is available only if supplied. Deployment, complete route authorization and suspension, alert delivery and signing arrangements remain unverified.

11. Controlled activation and program review

Before live activation, verify customer and number rights, permission and suspension enforcement for every enabled route, monitoring delivery, carrier acceptance and record retrieval across the call lifecycle. Confirm that the responsible contact can retrieve records and respond within 24 hours. Keep origination disabled until these checks pass.

The initial filing describes a direct end-user provider with no STIR/SHAKEN implementation, relying on the 47 CFR 64.6304(b) extension explained in section 5. Company relationships, regulatory-history answers and the personal officer declaration belong to the accompanying filing. RMD listing, SPC eligibility and service activation are distinct steps; an initial filing does not authorize live calls.

Management reviews the program quarterly and after material incidents or service changes; retain versioned changes and approvals. Update required RMD information within 10 business days of a change and recertify annually by the applicable March 1 deadline. [1]

PRIMARY REFERENCES / 47 CFR

- [1] 64.6305 Mitigation and certification
- [2] 64.6300 Provider definitions
- [3] 64.6301 Caller ID authentication
- [4] 64.6304 Extensions and exceptions

06 / CORPORATE PARTICULARS

Company and responsible persons

FILING ENTITY	COMPANY RECORD
Legal name	Umbolement UG (haftungsbeschränkt)
Trading name / product	Kesru kesru.com
FCC Registration Number	0038971149
Commercial register	Amtsgericht München, HRB 313937
Formation	1 April 2026, as recorded in the notarized formation instrument
Business address	Ulmenweg 10 85221 Dachau, Bavaria, Germany

A. Principals and authority

PERSON	DOCUMENTED FUNCTION
Mirwan Akayguen	Sole shareholder at incorporation: the notarized instrument records his subscription for the entire EUR 1,000 share capital, share number 1. Authorized Representative and Robocall Mitigation Contact under the confirmed power of attorney. Function: Operations.
Rislan Aslan-Hamal	Managing Director, as identified in the supplied current commercial register extract dated 20 September 2026.

Umbolement UG (haftungsbeschränkt) is the filing entity and the provider of the Kesru service.

Robocall mitigation contact: Mirwan Akayguen | Operations
info@umbolement.com | +49 1556 3047024 | business address as listed above