

Puzzel Robocall Mitigation Program (RMP)

Effective Date: May 30, 2025

Version: 1.0

Introduction and Purpose

This Robocall Mitigation Program (RMP) outlines the policies, procedures, and technological measures implemented by Puzzel AS, a voice service provider based in Denmark, Finland, Netherland, Norway (HQ), Sweden and United Kingdom to prevent, detect, and mitigate the origination and transmission of illegal robocall traffic, particularly to U.S. telephone numbers.

The primary rule governing this filer's compliance obligation is 47 CFR § 64.6305(g)(2), along with associated FCC orders (e.g., FCC 22-37, the Sixth Report and Order regarding the Call Authentication Trust Anchor).

Explanation of Exemption and Applicability:

Puzzel is exempt from the direct implementation of the STIR/SHAKEN call authentication framework as mandated for U.S.-based voice service providers. This exemption applies because:

1. **Foreign Domicile:** Puzzel AS is a foreign voice service provider operating entirely outside the United States and the North American Numbering Plan (NANP) numbering scheme for purposes of obtaining STIR/SHAKEN certificates.
2. **Technical Infeasibility:** As a foreign entity, Puzzel lacks the technical and legal access to the necessary components of the STIR/SHAKEN framework,

specifically a Service Provider Code (SPC) token and a digital certificate from a U.S. Policy Administrator (STI-PA), which are essential for directly signing calls with STIR/SHAKEN attestations.

3. **Alternative Compliance:** In recognition of this technical limitation, 47 CFR § 64.6305(g)(2) permits foreign voice service providers that utilize U.S. NANP resources in the caller ID field when sending voice traffic to the United States to fulfill their robocall mitigation obligations by submitting a comprehensive Robocall Mitigation Plan (RMP) to the FCC's Robocall Mitigation Database. This RMP details the reasonable steps taken by the filer to prevent illegal robocalls and commits to robust cooperation with U.S. traceback efforts.

Therefore, Puzzel AS complies with the FCC's robocall mitigation requirements through the submission and rigorous adherence to its detailed Robocall Mitigation Program, as permitted by the aforementioned rule, rather than through direct STIR/SHAKEN implementation.

Scope and Application

This RMP applies to all voice communication services provided by Puzzel that involve the transmission of calls utilizing North American Numbering Plan (NANP) resources (i.e., U.S. telephone numbers) in the Caller ID field, regardless of the originating or terminating jurisdiction, as long as these calls are destined for or transit through the United States. This includes, but is not limited to, VoIP services, voice termination and call center solutions.

"Know Your Customer" (KYC) Procedures

Puzzel implements stringent "Know Your Customer" (KYC) procedures to ensure that our customers and upstream providers are legitimate entities and do not engage in illegal robocalling. No customer is onboarded automatically through self service. Our KYC process includes:

- **Customer Onboarding and Vetting:**
 - **Identity Verification:** All new customers undergo a robust identity verification process. This includes, but is not limited to, collecting:
 - Full legal business name and "Doing Business As" (DBA) names.

- Business registration documents and numbers (e.g., company registration extract).
- Physical business address.
- Primary contact person(s) name, title, and contact information (phone, email).
- Tax identification number or equivalent for the relevant jurisdiction.
- **Review of Prior History:** Checking for any public records or industry alerts regarding the customer's involvement in illegal robocalling, fraud, or other illicit activities.
- **Reputation Screening:** Utilizing internal and/or external tools to assess the reputation of potential customers and their compliance within all aspects of their business.
- **Website/Online Presence Review:** Examining customer websites and online presence for legitimacy and consistency with stated use cases.
- **Contractual Provisions:** Our service agreements with customers explicitly prohibit the use of our services for illegal, abusive, or fraudulent robocalling, spoofing, or any activity that violates applicable laws. Contracts include provisions for immediate suspension or termination of services in the event of non-compliance or identified illegal activity.

Ongoing Monitoring: Regularly reviewing customer activity and maintaining records of customer interactions related to service use and compliance.

- **Traffic Monitoring and Analytics**

Puzzel employs proactive measures to monitor and analyze call traffic flowing through its network to identify and mitigate potential illegal robocall activity. Our monitoring capabilities include:

- **Real-time and Near Real-time Monitoring:** Puzzel is utilizing AudioCodes [One Voice Operations Center \(OVOC\)](#) and [AudioCodes Routing Manager \(ARM\)](#) to analyze call patterns, volumes, durations, and other metadata for suspicious activity.
- **Anomaly Detection:** Detecting unusual spikes in call volume, sudden changes in call patterns (e.g., high volumes of short-duration calls,

sequential dialing), rapid call setup/tear-down, and calls to unassigned or invalid numbers.

- **Capacity and Quality Monitoring:** Ensuring our network capacity and call quality are maintained to avoid inadvertently impacting legitimate traffic while detecting anomalies.

Response to Identified Illegal Traffic

Upon detection or notification of suspected or confirmed illegal robocall traffic, Puzzel takes immediate and appropriate action, which may include:

- **Investigation:** Promptly investigating suspicious activity by analyzing Call Detail Records (CDRs), customer accounts, and relevant logs to identify the source and nature of the traffic.
- **Customer Communication:** Notifying the originating customer or upstream provider of the identified suspicious activity, requesting an explanation and proof of legitimate use.
- **Traffic Blocking:** Implementing immediate and effective blocking of identified illegal robocall traffic. This can occur at various points in our network based on:
 - Specific identified numbers (Caller ID or called numbers).
 - Identified call patterns indicative of illegal robocalling.
 - Direct notification from the FCC, law enforcement, or the ITG.
- **Service Suspension/Termination:** If illegal robocalling is confirmed and the customer or upstream provider fails to provide a legitimate explanation or rectify the issue, Puzzel will suspend or terminate their service.
- **Information Sharing:** Collaborating with other voice service providers, industry partners, and analytics vendors to share information on identified illegal robocall campaigns where legally permissible.

Cooperation with Traceback Requests

Puzzel is fully committed to cooperating with traceback requests from the U.S. Federal Communications Commission (FCC), U.S. law enforcement agencies, and the industry traceback consortium (currently the Industry Traceback Group – ITG).

- **Designated Point of Contact:** We have designated a dedicated point of contact responsible for receiving, processing, and responding to traceback requests.
 - **Name:** [Name of Contact Person]
 - **Title:** [Title of Contact Person]
 - **Department:** [Department, e.g., Legal / Operations / Compliance]
 - **Email:** [Dedicated Traceback Email Address]
 - **Telephone:** [Dedicated Traceback Phone Number, including international dialing code]
- **Response Time:** Puzzel commits to providing a full and timely response to all traceback requests within **24 hours** of receipt, including weekends and holidays.
- **Information Provision:** We will provide all available and relevant information to assist in identifying the source of illegal robocalls, including:
 - Call Detail Records (CDRs) for the specified calls.
 - Information about the immediate upstream provider.
 - Customer contact information related to the traffic.
 - Any other relevant data that can aid the investigation.
- **Secure Communication:** We utilize secure and verifiable communication channels for exchanging sensitive information related to traceback requests.

Compliance and Auditing

Puzzel is committed to maintaining compliance with all applicable laws and regulations regarding robocalling and spoofing, including those of Denmark, Finland, Netherland, Norway, Sweden, United Kingdom and the United States (e.g., the TCPA and TRACED Act).

- **Internal Compliance Team:** Puzzel AS has Voice Team responsible for overseeing this RMP and ensuring adherence to its provisions.
- **Record Keeping:** We maintain comprehensive records related to our robocall mitigation efforts, including:
 - Customer KYC documentation.

- Call monitoring logs and analytics reports.
- Records of identified illegal traffic and actions taken.
- Traceback requests received, and responses provided.
- **Regular Review and Updates:** This RMP will be reviewed and updated at least annually, or more frequently as needed to adapt to evolving robocall tactics, technological advancements, industry best practices, and changes in regulatory requirements. Material changes to this plan will be promptly updated in the FCC's Robocall Mitigation Database.
- **Employee Training:** All relevant personnel involved in network operations, customer service, and compliance are trained on the provisions of this RMP and their roles in preventing and mitigating illegal robocalls.

8. Disclaimer

While Puzzel AS implements robust measures to mitigate illegal robocall traffic, we cannot guarantee the complete elimination of all illegal calls from our network or from traffic we transit, given the persistent and adaptive nature of illegal robocallers. However, we are fully committed to continuously improving our mitigation efforts and cooperating with regulatory and law enforcement agencies to protect consumers.