



Nexxtra GmbH  
Straße der Pariser Kommune 12-16  
Berlin, 10243  
Germany

Phone: +49 30 20 994 42-0  
Fax: +49 30 20 994 42-99  
Email: [infonexxtra.de](mailto:infonexxtra.de)

Date: 05.06.2025

## **Nexxtra GmbH Robocall Mitigation Plan**

### **1. Introduction and Purpose**

This Robocall Mitigation Program (RMP) outlines the policies, procedures, and technological measures implemented by nexxtra GmbH, a network operator based in Germany 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).

### **2. Explanation of Exemption and Applicability:**

nexxtra GmbH 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:

- (i) **Foreign Domicile:** nexxtra GmbH 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.
- (ii) **Technical Infeasibility:** As a foreign entity, nexxtra GmbH 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.

- (iii) **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, nexxtra GmbH 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.

### **3 "Know Your Customer" (KYC) Procedures**

nexxtra GmbH 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).
- **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.

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

- **Traffic Monitoring and Analytics**

nexxtra GmbH applies proactive measures to monitor and analyse call traffic flowing through its network to identify and mitigate potential illegal robocall activity. Our monitoring capabilities include:

- **CPS Monitoring**

if nexxtra GmbH notices too many calls with **low CPS** (Calls Per Second is a metric used to measure the number of telephone calls completed in one second), nexxtra GmbH will block the calls.

- **ASR Analysis**

**ASR** (Answer to Seizure Ratio is a measure of network quality and call success rates) is checked twice a day to detect malicious or robocalls. Such calls are blocked immediately.

**5. Response to Identified Illegal Traffic**

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

- **Investigation:** Promptly investigating suspicious activity by analysing 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, nexxtra GmbH 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.

## 6. Cooperation with Traceback Requests

nexxtra GmbH 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.

- o **Name:** Thomas REINIG

- o **Title:** Chief Executive Officer (CEO)

- o **Department:** Operations

- o **Email:** thomas.reinig@nexxtra.de

- o **Telephone:** +4930209944210

- **Response Time:** nexxtra GmbH commits to providing a full and timely response to all traceback requests within 24 hours of receipt, excluding weekends and public holidays in Germany.
- **Information Provision:** We will provide all available and relevant information to assist in identifying the source of illegal robocalls, including:
  - o Call Detail Records (CDRs) for the specified calls.
  - o Information about the immediate upstream provider.
  - o Customer contact information related to the traffic.
  - o 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.

## 7. Compliance and Auditing

nexxtra GmbH is committed to maintaining compliance with all applicable laws and regulations regarding robocalling in the United States (e.g., the TCPA and TRACED Act).

- **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.

## 8. Disclaimer

While nexxtra GmbH implements robust measures to mitigate illegal robocall traffic, we cannot guarantee the complete elimination of all illegal calls from our network, 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.