

## CHECKLIST

# GDPR Review Checklist for AI Voice Calls

GDPR review checklist for brokerage AI voice campaigns: lawful basis, call-time transparency, DPIA, processor contracts, retention and data subject rights.

### WHO IT IS FOR

Broker ops leads, DPOs and compliance officers preparing an AI voice campaign that calls EU or UK residents.

### TIME TO COMPLETE

60 minutes plus a DPO review

This checklist walks a brokerage team through the GDPR questions an AI voice campaign raises before the first dormant trader is dialed. It covers the six areas a data protection officer will ask about: why you may call, what the trader is told, whether a DPIA is needed, who processes the audio, how long recordings live and how a trader exercises their rights. Work through it with your DPO or compliance officer and you'll finish with a written record of every decision, not a set of assumptions nobody can defend later.

## 1 Lawful basis for the call and the data

Every record on the list needs a stated reason you may process it for an outbound call, and that reason has to hold when an AI agent makes the call, the same as it would for a human dialer. This section tells you what to review; the conclusion belongs to your DPO or counsel.

### ☐ Write down the lawful basis you rely on for calling each segment: consent, legitimate interests or contract.

A funded client with an open account, a KYC-pending registration and a demo-only lead usually don't sit on the same basis. Record one per segment, not one for the whole list.

### ☐ Pull the consent record for every segment that relies on consent: date, wording, form and whether phone marketing was named.

A registration checkbox that mentions email and doesn't mention calls is the most common gap. If the wording isn't retrievable, treat the record as not consented until your DPO says otherwise.

### ☐ Complete a legitimate interests assessment for every segment that relies on it, and keep it with the campaign file.

The assessment weighs your interest in reactivating the account against what the trader would reasonably expect. A trader who closed the account two years ago probably doesn't expect a call.

### ☐ Check the ePrivacy and national marketing-call rules for each country on the list, on top of GDPR.

GDPR sets the data rules; direct marketing calls also fall under the ePrivacy rules as transposed in each member state and PECR in the UK, and some countries require prior opt-in for marketing calls. List the countries and note the rule for each.

- ☐ **Confirm whether the campaign's purpose matches what the trader was told when the data was collected.**

Data collected to open and service a trading account being reused for a win-back call is a purpose question. Your DPO decides whether it's compatible or needs fresh notice.

- ☐ **Exclude every record with a marketing objection, a withdrawn consent or an erasure request on file, and log the count.**

An objection to direct marketing has to be honoured without exception. Pull these from the CRM, the support desk and past campaign outcomes, not from one system.

Records excluded: \_\_\_\_\_

- ☐ **Get the lawful-basis decision per segment signed off in writing by the DPO or compliance officer before the list is uploaded.**

Signed by: \_\_\_\_\_ Date: \_\_\_\_\_

## 2 Transparency on the call

The trader has a right to know who is calling, that it's an automated agent, why they're being called and what happens to the recording. Decide the exact words before the campaign, not after a complaint.

- ☐ **Draft the opening line so it names the brokerage, states the reason for the call and says the call is handled by an AI agent.**

Keep it short enough that the disclosure lands before the trader can hang up on a robot they weren't told about.

- ☐ **State that the call is recorded and transcribed, and say why, before any account detail is discussed.**

Topcalls records and transcribes every call as part of the per-minute rate, so the notice applies to every campaign you run on it.

- ☐ **Point the trader to the privacy notice and give one plain way to reach it: a URL read out, an SMS or an email sent after the call.**

A notice nobody can find isn't transparency. Choose the channel and test that it works from the agent's flow.

- ☐ **Update the privacy notice to cover automated calls, call recording, transcription and any AI processing of the audio, and record the version date.**

The notice the trader agreed to at registration probably predates AI calls. The updated version needs a date so you can show which one applied on the call day.

Notice version: \_\_\_\_\_

- ☐ **Confirm the disclosure is voiced in the trader's language rather than defaulting to English.**

Topcalls agents run in up to 78 languages. The disclosure text needs a reviewed translation for each language on the list, not a machine draft nobody checked.

- ☐ **Add a clear route to a human on request and a clear route to opt out of further calls, both handled within the call.**

"Press or say 'stop' to be removed" beats "contact support". The opt-out has to write back to the suppression list the same day.

- ☐ **Review the full opening and closing scripts with the DPO and keep the approved version with the campaign file.**

Script version: \_\_\_\_\_ Approved by: \_\_\_\_\_

### **3 Data protection impact assessment**

An AI voice campaign combines automated processing, voice data and, for a brokerage, financial data. That's the kind of combination that often triggers a DPIA. Decide, document the decision either way, and don't skip the screening because the answer looks obvious.

- ☐ **Run a DPIA screening with the DPO and record the outcome: required, not required and why.**

Screen on the factors regulators list: new technology, systematic monitoring, large scale, sensitive or financial data, automated decisions. Two or more usually point to a full DPIA.

- ☐ **Describe the processing end to end: list export, upload to the calling platform, dialing, recording, transcription, AI analysis, CRM write-back and deletion.**

A diagram with every system and every transfer is the fastest way to make the DPIA concrete. Include the telephony carrier and any speech model provider your vendor uses.

- ☐ **Identify every category of personal data on the call: name, phone, account status, deposit history, voice, and anything the trader volunteers.**

Traders volunteer health, family and financial-hardship details on reactivation calls. Decide now how the transcript handles them, because the model can't unhear it.

- ☐ **Assess whether any decision on the call is automated with legal or similarly significant effect on the trader.**

Offering a callback isn't a significant decision. Changing account terms, declining service or scoring creditworthiness on the call would be. Keep those with a human.

- ☐ **List the risks to the trader and the mitigation for each: wrong-person calls, recordings leaked, transcripts used for profiling, calls to vulnerable customers.**

Each risk gets an owner and a control, for example number verification before account details, encryption at rest, retention limits, a vulnerable-customer suppression flag.

- ☐ **Check whether your vendor's own DPIA or security documentation covers the AI voice processing, and file it alongside yours.**

A vendor document doesn't replace your DPIA, but it answers the technical questions you'd otherwise guess at.

- ☐ **Decide whether residual risk is high enough to require prior consultation with the supervisory authority, and record who decided.**

This is a DPO and counsel call. The checklist only makes sure the question was asked before the campaign, not after.

**DPIA decision:** \_\_\_\_\_ **Signed:** \_\_\_\_\_

## 4 Processors, sub-processors and transfers

The AI voice vendor, the telephony carrier, the speech providers and your CRM all touch trader data. Each one needs a contract, a role and a known location.

- ☐ **Sign a data processing agreement with the AI voice vendor that covers recording, transcription, AI analysis and the deletion schedule.**

Ask for the vendor's standard DPA and route it to counsel. It has to state the vendor acts on your instructions and returns or deletes data on request.

- ☐ **Obtain the vendor's sub-processor list: telephony, speech-to-text, text-to-speech, language model, hosting, and the country each runs in.**

An AI voice call passes through several providers in one conversation. If the vendor can't name them, that's your answer about the vendor.

- ☐ **Map every transfer outside the EU or UK and record the transfer mechanism for each: adequacy decision, standard contractual clauses or another approved route.**

Speech and language model providers are often US-hosted. Each hop needs a mechanism and, where required, a transfer risk assessment on file.

- ☐ **Confirm what the vendor and its sub-processors may do with the audio and transcripts beyond your campaign, and get model training and product improvement excluded in writing if that's your policy.**

Voice is personal data. Your DPO decides the position; the contract has to match it.

- ☐ **Confirm the CRM, dialer and any automation tool receiving call outcomes are covered by their own DPAs and listed in your record of processing.**

The Integrations path can push outcomes to many tools. Every destination that gets a phone number or a transcript is a processor or a joint controller.

- ☐ **Set the notification route for a personal data breach at the vendor: contact, deadline and who at the brokerage picks it up.**

GDPR gives controllers a short window to notify the supervisory authority. The vendor's clock has to be shorter than yours.

- ☐ **Update the record of processing activities with the campaign, the processors and the transfers before the first call.**

**Record updated by:** \_\_\_\_\_ **Date:** \_\_\_\_\_

## 5 Retention and deletion

Recordings, transcripts, AI summaries and CRM notes all count. Set a period for each, name who deletes it, and check that it actually happened.

- ☐ **Set a retention period for call recordings and a separate one for transcripts and AI summaries, with the reason for each.**

A recording kept to meet MiFID II record-keeping duties on an investment conversation has a different justification and period from a marketing call summary. Your compliance officer sets both; the checklist just makes sure they're written down.

**Recordings:** \_\_\_\_\_ **Transcripts:** \_\_\_\_\_

- ☐ **Confirm which calls fall under regulatory record-keeping duties and which are marketing only, and store the two classes separately.**

Mixing the two means either deleting something you were required to keep or keeping something you had no basis to hold.

- ☐ **Configure the retention period in the calling platform, in the CRM and in any tool the transcript was pushed to.**

Retention set in one system and forgotten in three others is the most common finding in a data audit.

- ☐ **Define what happens to the uploaded lead list after the campaign closes: deleted from the platform, and the date it happened.**

The list is personal data too. It shouldn't outlive the campaign it was uploaded for.

- ☐ **Set the rule for recordings of wrong-number, wrong-person and non-client calls: delete on a shorter clock.**

You have no relationship with the person who picked up. Their voice shouldn't sit in your archive for years.

- ☐ **Assign an owner for deletion runs and schedule a check that the run happened, with a sample of records verified as gone.**

A policy without a verified deletion is a promise. Keep the verification log with the campaign file.

**Deletion owner:** \_\_\_\_\_ **Next check:** \_\_\_\_\_

- ☐ **Document the retention decisions in the privacy notice and the record of processing so a trader's access request gets a consistent answer.**

## 6 Data subject rights during and after the campaign

Traders will ask for their recording, ask you to stop calling and ask you to delete them. Each request has a route, an owner and a deadline before the campaign starts.

- ☐ **Set the process for an access request that includes a call recording and transcript: where to find them, how to export them and who reviews for third-party data before release.**

Your calling platform should let you pull a recording and transcript by phone number or CRM ID in minutes.

Test it on one record before you need it.

- ☐ **Set the process for an objection to direct marketing raised on the call, by email or through support, and the deadline to stop calling.**

The objection is absolute for marketing. The number goes to the suppression list before the next batch dials, and the CRM flag follows on the same day.

- ☐ **Set the process for erasure requests, including recordings held at the vendor and copies pushed to other tools.**

Erasure has to reach every processor on the list from the processors section. Keep exceptions, such as regulatory record-keeping, documented per case.

- ☐ **Set the process for a rectification request when the agent had the wrong name, balance or account status.**

Wrong data on a call is also a signal that the source list needs fixing. Route the correction back to the CRM as well as the calling platform.

- ☐ **Confirm how a trader can reach a human to contest anything decided on the call, and how that route is stated on the call.**

GDPR gives people a right not to be subject to solely automated decisions with significant effects. Even where no such decision is made, the human route makes the position easy to show.

- ☐ **Train the support team on what an AI call is, what was recorded and where the recording lives, so requests aren't bounced between teams.**

The first access request after an AI campaign usually lands with someone who didn't know the campaign ran.

- ☐ **Log every rights request tied to the campaign with the date received, the date closed and the action taken.**

Requests logged: \_\_\_\_\_

## **7 Security controls and audit trail**

What you can show afterwards is what counts. Keep the evidence in one place and check the controls before the campaign, not during the audit.

- ☐ **Confirm recordings and transcripts are encrypted in transit and at rest at the vendor, and note the evidence you received.**

Ask for the vendor's security documentation or certification rather than a sentence in a sales deck.

- ☐ **Restrict access to recordings, transcripts and the lead list to named roles, and review the user list in the calling platform before launch.**

A campaign built by an agency or a contractor often leaves their accounts active for months. Remove them the day the work ends.

- ☐ **Verify the callee before the agent reads out any account detail: name check, and a further check before deposit or balance figures.**

Numbers change hands. A reactivation call that reads a balance to the wrong person is a personal data breach, not a bad call.

- ☐ **Check that the number shown to the trader belongs to the brokerage and matches the name given on the call.**

A spoofed or unregistered number turns a lawful call into something that looks like fraud to the trader and the regulator.

- ☐ **Keep one campaign file with the lawful-basis sign-off, the approved script, the DPIA decision, the DPA and sub-processor list, the retention settings and the rights log.**

If a supervisory authority or a complainant asks, the answer is a folder, not a search through email.

- ☐ **Schedule a review of this checklist before any change to the list, the script, the vendor's sub-processors or the countries called.**

Each of those changes can move the lawful basis, the DPIA outcome or the transfer map. A checklist done once is a snapshot.

Next review: \_\_\_\_\_

### How to use this checklist

1. Book an hour with your DPO or compliance officer and go through the sections in order: lawful basis, transparency, DPIA, processors, retention, rights, security.
2. Answer every item with evidence you can file, not a verbal yes. Where the evidence doesn't exist yet, write the owner and the date it will.
3. Fill the blanks as you go so the campaign file carries the sign-offs and the versions on paper.
4. Hold the campaign until the lawful-basis, script and DPIA sign-offs are in. The remaining sections can run alongside list preparation.
5. Re-run the checklist whenever the list, the script, the vendor's sub-processors or the target countries change.

### Book a 30-minute call with a Topcalls co-founder

We'll map your dormant book and CRM flow against this checklist, show where recording, retention and opt-outs are configured in Topcalls, and scope a pilot your DPO can sign off.

[topcalls.ai/book](https://topcalls.ai/book)