

Checkpunkte für rechtskonforme Call-Recordings

# Telefoniert und mitgeschnitten – rechtlich okay?

🕒 21. April 2026 📖 5 Minuten Lesezeit



Felix Krüger, Geschäftsführer Peoplefone Deutschland: „Zwischen strafrechtlicher Unbedenklichkeit und vollständiger DSGVO-Konformität klafft oft eine Lücke.“ Bild: Peoplefone

Anzeige



**Call-Recording ist kein rechtliches Minenfeld, erfordert aber Sorgfalt. Strafrechtlich müssen sich Unternehmen keine Sorgen machen, solange das Aufzeichnen erkennbar ist. Doch der Datenschutz verlangt eine informierte Einwilligung. So zumindest ist die Behördensicht. „Die lässt sich niedrigschwellig gestalten“, weiß Dr. Carsten Ulbricht, IT-Rechtsanwalt in Stuttgart.**

» *Michael Sudahl, Fachjournalist in Schorndorf*

Wer als Berater ein Telefonat heimlich mitschneidet, macht sich strafbar. Das ist der Ausgangspunkt jeder Diskussion rund ums Aufzeichnen von Telefonaten. Doch dieses Problem lässt sich schnell aus dem Weg räumen. Ulbricht erklärt: „In dem Moment, in dem der Anrufer davon in Kenntnis gesetzt wird, liegt keine unbefugte Aufzeichnung vor.“ Entscheidend ist insofern nicht die aktive Zustimmung, sondern deren Kenntnis. Das kann etwa über eine Ansage vor Gesprächsbeginn geschehen.

Schwieriger wird es beim Datenschutz. Dieser setzt höhere Hürden. Felix Pflüger, Geschäftsführer von [Peoplefone Deutschland](#), einem auf VoIP und virtuelle Telefonanlagen spezialisierten Anbieter aus Fellbach, kennt die Unsicherheiten aus der täglichen Praxis: „Viele Unternehmen glauben, sie seien mit einem kurzen Hinweis am Anfang des Gesprächs auf der sicheren Seite. Doch zwischen strafrechtlicher Unbedenklichkeit und vollständiger DSGVO-Konformität klafft oft eine Lücke, die unterschätzt wird.“

Ob Telekommunikationsgesetz (TKG) oder DSGVO – beide Regelwerke verlangen für den Mitschnitt eine Einwilligung. Und diese muss auf einer aktiven Handlung beruhen, nicht bloß auf Schweigen oder Nicht-Auflegen. „Ein Opt-out reicht nicht. Das Weitersprechen ist keine aktive Handlung“, stellt der Jurist klar [zu Opt-in und Opt-out siehe untenstehendes Glossar]. Was dies konkret bedeutet, zeigen die Checkpunkte:

## **1. Einwilligung vor der Aufzeichnung**

Ein häufiger Fehler in der Praxis ist es, die Aufnahme bereits laufen zu lassen und die Zustimmung im Nachgang einzuholen. Datenschutzrechtlich ist das grundsätzlich nicht erlaubt. Wer auf Nummer sicher gehen will, baut den Einwilligungsprozess an den Anfang des Gesprächs: zuerst informieren, dann aktiv zustimmen lassen, dann aufzeichnen. Das klingt aufwändiger, als es ist – mit der richtigen technischen Unterstützung lässt es sich in Sekunden abwickeln.

## **2. Die aktive Handlung zählt**

„Bitte legen Sie auf, wenn Sie nicht einverstanden sind“ – diese Formulierung ist zwar weit verbreitet, aber unzureichend. Ein Nicht-Auflegen ist kein Opt-in. Der Anwalt empfiehlt stattdessen ein klares Signal: „Drücken Sie die Eins, wenn Sie mit der Aufzeichnung einverstanden sind.“ Der Anrufer tut aktiv etwas, das ist der

entscheidende Unterschied. Dieser Schritt lässt sich technisch einfach umsetzen und protokollieren, etwa durch den Einsatz einer IVR-Ansage (Interactive Voice Response) zu Beginn des Gesprächs. Pflüger bestätigt das aus technischer Sicht: „Eine rechtssichere IVR-Ansage mit Einwilligungsabfrage ist heute keine Frage des Aufwands mehr. Das lässt sich innerhalb weniger Stunden sauber aufsetzen und automatisch protokollieren – inklusive Zeitstempel und Gesprächs-ID.“

### 3. Zwei-Ebenen-Modell

Der Knackpunkt ist nicht die Einwilligung selbst, es ist die vorgelagerte Informationspflicht. Die DSGVO verlangt eine Fülle von Angaben: Wer verarbeitet die Daten, zu welchem Zweck, wie lange, gibt es Unterauftragsverarbeiter, werden Daten in Drittländer übermittelt, welche Rechte hat der Betroffene? Diese Informationen in einem Telefonat vollständig vorzulesen ist weder realistisch noch zumutbar.

Hier liefert ein Zwei-Ebenen-Modell die Lösung: Auf der ersten Ebene wird im Telefonat eine kurze, prägnante Information gegeben, zum Beispiel: „Dieses Gespräch wird zu Qualitätssicherungszwecken aufgezeichnet. Weitergehende Datenschutzhinweise finden Sie unter [Website].“ Auf der zweiten Ebene steht dann eine abrufbare umfassende Datenschutzerklärung online bereit.

### 4. Transkription ist mehr als Aufzeichnen

Wer Gespräche aufzeichnet und automatisch transkribiert, betritt neues Terrain. Anders als bei der reinen Aufnahme lässt sich ein Text-Transkript indexieren, durchsuchen und für KI-Analysen verwenden. Der Eingriff in die Datenschutzhöhle ist damit weitreichender. Unternehmen, die beide Funktionen einsetzen, sind gut beraten, dies in ihrer Datenschutzerklärung explizit und vollständig auszuweisen.

„Ob der Hinweis auf die Transkription bereits im Call selbst erfolgen muss oder auf die zweite Informationsebene ausgelagert werden kann, ist eine Abwägungsfrage“, so Ulbricht. Die Nennung in der Datenschutzerklärung auf der Website, auf der sich der Anrufer informieren kann, gilt jedoch als Mindeststandard. Pflüger ergänzt: „Wir erleben, dass Transkription und KI-Auswertung stark zunehmen. Umso wichtiger ist es, dass Anbieter nicht nur die Technik liefern, sondern ihre Kunden auch auf die erweiterten Dokumentationspflichten hinweisen.“

### 5. Verantwortlichkeiten regeln

Unabhängig davon, welcher Anbieter die Infrastruktur betreibt, trägt derjenige die datenschutzrechtliche Verantwortung, der Telefongespräche aufzeichnet. Daher müssen Unternehmen mit ihrem Telefonanlagendienstleister einen Auftragsverarbeitungsvertrag (AVV) abschließen und diesen in der Datenschutzerklärung ausweisen. Entscheidend ist dabei laut Pflüger die Wahl des

Partners: „Ein seriöser Anbieter liefert Technik und denkt Compliance von Anfang an mit: von einer rechtssicheren IVR-Ansage über die automatische Protokollierung von Einwilligungen bis hin zu Mustervorlagen für AVV und Datenschutzerklärung“.

Die Vollzugspraxis der deutschen Datenschutzbehörden zeigt: Bußgelder gegen den Mittelstand sind die Ausnahme und setzen nachhaltiges Fehlverhalten voraus. Das ist kein Freifahrtschein für Gleichgültigkeit, aber ein Argument für Verhältnismäßigkeit. „Ich rate dazu, risikobasiert vorzugehen“, so Ulbricht. „Ein tragfähiges Opt-in-Verfahren, kombiniert mit einer vollständigen zweiten Informationsebene, ist ein Konzept, das zu empfehlen ist.“

### Zu den Experten:

Dr. Carsten Ulbricht ist IT-Rechtsanwalt bei Menold Bezler in Stuttgart. Felix Pflüger ist Geschäftsführer der Peoplefone Deutschland GmbH mit Sitz in Fellbach. Das Unternehmen bietet rund 10.000 deutschen Geschäftskunden VoIP-Anschlüsse, virtuelle Telefonanlagen und Kommunikationslösungen.

[www.peoplefone.com](http://www.peoplefone.com)

---

## Glossar

**Opt-in** (Zustimmung) und **Opt-out** (Widerspruch) regeln die Einwilligung zur Datennutzung oder Werbung. Opt-in erfordert eine aktive Einwilligung des Nutzers vor der Verarbeitung (zum Beispiel Newsletter-Anmeldung). Opt-out bedeutet eine automatische Einbeziehung, die der Nutzer aktiv beenden muss. Opt-in ist datenschutzrechtlich (DSGVO) meist zwingend.

**Auslandscalls:** Das Datenschutzrecht richtet sich nach dem Marktortprinzip, also dem Sitz des Betroffenen. Ruft ein deutsches Unternehmen bei einer Person in der Schweiz an, gilt das Schweizer Datenschutzgesetz (DSG). Entscheidend ist also, dass der jeweils Angerufene nach seinem nationalen Recht geschützt wird.

UNSERE WEBINAR-EMPFEHLUNG

---