



Call-Recording und KI: Wo rechtliche Risiken beginnen

Gesprächsaufzeichnungen gehören in vielen Unternehmen längst zum Alltag – ob zur Dokumentation, Qualitätssicherung oder KI-gestützten Analyse. Doch wer Telefonate mitschneidet oder transkribiert, bewegt sich schnell im Spannungsfeld zwischen Strafrecht, DSGVO und Informationspflichten. Worauf Vermittler und Beratungsunternehmen achten sollten, hat Felix Pflüger (peoplefon) im Gastbeitrag zusammengestellt.

Wer ein Telefonat heimlich mitschneidet, macht sich strafbar – das ist der Ausgangspunkt jeder Diskussion rund ums Aufzeichnen von Telefonaten. Doch dieses Problem lässt sich schneller aus dem Weg räumen, als viele vermuten. 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: 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. Was das 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.

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 Datenschutzsphäre 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.

5. Verantwortlichkeiten regeln

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

Über den Autor: Felix Pflüger ist Geschäftsführer von Peoplefone Deutschland. Er berät Unternehmen – darunter viele Versicherungsbüros – bei der digitalen Transformation ihrer Telefonie- und Kommunikationsstrukturen.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4949792/Call-Recording-und-KI-Wo-rechtliche-Risiken-beginnen/>