

Neben ihren ausführlicheren Praxishilfen erstellt die GDD regelmäßig Kurzpapiere, um zentrale praxisrelevante Fragestellungen des Datenschutzes kompakt aufzubereiten. Ziel ist es, häufige Praxisszenarien verständlich zu vermitteln und Hinweise für die praktische Umsetzung der Datenschutzvorgaben zu geben. Anlass für GDD-Kurzpapiere können etwa wiederkehrende Fragen aus dem Kreis der GDD-Mitglieder bilden oder aktuelle Gerichtsentscheidungen, die mit Blick auf den Handlungsbedarf für die Datenschutzpraxis entsprechend erläutert werden.

Gesprächstranskription

1. Einleitung

Die Transkription von Telefon- und Videokonferenzen ist ein zunehmend eingesetztes Mittel in Unternehmen. Sie dient der Dokumentation von Gesprächsinhalten, der Qualitätssicherung, der Schulung von Beschäftigten oder der Beweissicherung. Technisch erfolgt die Transkription durch eine Zwischenspeicherung des Audiosignals, das anschließend von einer Software in Text umgewandelt wird. Bereits diese Zwischenspeicherung stellt eine Verarbeitung personenbezogener Daten dar, da Sprache unmittelbar mit einer identifizierbaren Person verknüpft ist. Damit greifen sowohl die Vorgaben der DS-GVO als auch strafrechtliche Schutzmechanismen. Die Herausforderung liegt darin, dass die Transkription nicht nur eine organisatorische Hilfestellung darstellt, sondern eine rechtlich relevante Datenverarbeitung, die einer klaren Rechtsgrundlage und strengen Schutzmaßnahmen bedarf. Hinzu kommt, dass die Aufzeichnung des nicht öffentlich gesprochenen Wortes strafrechtlich besonders geschützt

ist (§ 201 StGB), so dass Unternehmen doppelte Anforderungen beachten müssen.

2. Rechtsgrundlage für die Datenverarbeitung

2.1. Art. 6 Abs. 1 lit. a) DS-GVO - Einwilligung

Die Einwilligung ist in der Praxis eine der wichtigsten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Damit sie wirksam ist, muss sie freiwillig, informiert und jederzeit widerruflich erfolgen.¹ Eine gültige Einwilligung setzt voraus, dass die betroffene Person durch eine **aktive Handlung** eine eindeutige Zustimmung erteilt, etwa durch das ausdrückliche Bestätigen einer Schaltfläche oder eine andere klar erkennbare Willensbekundung. Bloßes Stillschweigen, voreingestellte Optionen oder automatisch aktivierte Funktionen (z.B. Konferenztools) reichen hierfür nicht aus.²

¹ Schwartmann/Jaspers/Thüsing/Kugelman/Schwartmann/Klein, 3. Aufl. 2024, Art. 6 DS-GVO Rn. 16 ff.

² Taeger/Gabel-Taeger, 5. Aufl. 2026, Art. 6 DS-GVO Rn. 51 f.

Vor der Erteilung der Einwilligung müssen die betroffenen Personen umfassend über alle relevanten Aspekte der Verarbeitung informiert werden. Dazu gehören insbesondere der Zweck und der Umfang der Datenverarbeitung, die vorgesehene Speicherdauer, die Kategorien möglicher Empfänger sowie die eingesetzten Systeme. Ebenso wesentlich ist der Hinweis auf die jederzeitige Widerrufsmöglichkeit. Ein Widerruf muss ohne Angabe von Gründen möglich sein und wirkt stets für die Zukunft.³

Besondere Bedeutung kommt der Frage der **Freiwilligkeit im Beschäftigungskontext** zu.⁴ Aufgrund des bestehenden Abhängigkeitsverhältnisses zwischen Arbeitgeber und Beschäftigten kann eine Einwilligung hier im Einzelfall als nicht freiwillig angesehen werden. Um die Verarbeitung dennoch rechtssicher zu gestalten, bietet sich häufig der Abschluss einer Betriebsvereinbarung an, die die betreffenden Verarbeitungsvorgänge kollektivrechtlich absichert.

2.2. Art. 6 Abs. 1 lit. b) DS-GVO - Vertragserfüllung

Die Rechtsgrundlage der Vertragserfüllung nach Art. 6 Abs. 1 lit. b) DS-GVO kommt nur dann in Betracht, wenn die Erstellung einer Transkription tatsächlich zwingend erforderlich ist, um einen bestehenden Vertrag zu erfüllen oder vorbereitende Maßnahmen auf Wunsch der betroffenen Person durchzuführen. Dies kann beispielsweise der Fall sein, wenn Schulungen oder andere Leistungen vertraglich zugesichert wurden und deren Durchführung eine Aufzeichnung oder Transkription zwingend voraussetzt. Ebenso kann eine Verarbeitung auf dieser Grundlage beruhen, wenn die Dokumentation

von Vertragsverhandlungen ausdrücklich Bestandteil der vertraglichen Vereinbarung ist. In der praktischen Anwendung ist diese Rechtsgrundlage jedoch nur selten einschlägig. In der Regel lassen sich Gespräche, Verhandlungen oder Schulungen auch ohne eine Transkription ordnungsgemäß durchführen, sodass die Erforderlichkeit i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO meist nicht gegeben ist.

2.3. Art. 6 Abs. 1 lit. c) DS-GVO - Gesetzliche Pflicht

Eine gesetzliche Pflicht zur Aufzeichnung und Transkription besteht für Unternehmen grundsätzlich nicht. Die spezialgesetzlichen Aufzeichnungspflichten (z.B. im Wertpapierhandelsgesetz oder der Finanzvermittlungsverordnung) beziehen sich dabei nicht auf die Transkription der Gespräche.⁵ Daher stellt Art. 6 Abs. 1 lit. c) DS-GVO in aller Regel keine taugliche Rechtsgrundlage für die Durchführung von Gesprächstranskription dar.

2.4. Art. 6 Abs. 1 lit. f) DS-GVO - Berechtigtes Interesse

Die Verarbeitung auf Grundlage des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f) DS-GVO ist besonders flexibel und kann insbesondere bei internen Besprechungen oder Schulungen eine Rolle spielen. Voraussetzung ist jedoch stets eine sorgfältige und nachvollziehbare **Interessenabwägung**. Zunächst muss geprüft werden, ob die Transkription zur Erreichung des verfolgten Zwecks tatsächlich **erforderlich** ist. Sie darf nur eingesetzt werden, wenn kein mildereres, gleich effektives Mittel zur

³ Schwartmann/Jaspers/Thüsing/Kugelman/Schwartmann/Klein, 3. Aufl. 2024, Art. 6 DS-GVO Rn. 14 ff.

⁴ Siehe ausf. dazu Schwartmann/Jaspers/Thüsing/Kugelman/Schmidt/Thüsing, 3. Aufl. 2024, Art. 88 DS-GVO/§ 26 BDSG Rn. 40 ff.

⁵ Moers, DSRITB 2024, 751 (758).

Verfügung steht. Ist etwa die Erstellung eines manuellen Protokolls ausreichend, fehlt es an der Erforderlichkeit.

Im nächsten Schritt sind die **Interessen** des Unternehmens den schutzwürdigen Interessen der Betroffenen **gegenüberzustellen**. Dabei müssen insbesondere Aspekte wie Vertraulichkeit, potenzielle Nachteile durch die Aufzeichnung sowie das Risiko einer Leistungs- oder Verhaltenskontrolle berücksichtigt werden. Die Verarbeitung ist nur zulässig, wenn die Interessen des Verantwortlichen überwiegen und die Rechte der Betroffenen nicht unverhältnismäßig beeinträchtigt werden.

Schließlich ist eine **transparente Dokumentation** der durchgeführten Abwägung erforderlich, um die Entscheidung im Streitfall nachvollziehbar begründen zu können.⁶ Im Beschäftigungskontext ist die Anwendung dieser Rechtsgrundlage jedoch nur eingeschränkt möglich, da das bestehende Abhängigkeitsverhältnis regelmäßig zu Lasten der Beschäftigten wirkt. Zur rechtssicheren Gestaltung bietet sich daher oft der Abschluss einer Betriebsvereinbarung an, die die Interessenabwägung kollektivrechtlich absichert.

2.5. Betriebsvereinbarung

Eine Betriebsvereinbarung nach Art. 88 DS-GVO i.V.m. § 26 BDSG kann die Rechtsgrundlage für die Verarbeitung im Beschäftigtenkontext bilden. Voraussetzung ist, dass sie klar und verbindlich regelt, unter welchen Umständen Gespräche aufgezeichnet und transkribiert werden dürfen. Dabei müssen insbesondere der **konkrete Zweck** der Verarbeitung, deren Grenzen sowie die Rahmenbedingungen des Einsatzes der verwendeten Systeme eindeutig festgelegt werden. Ebenso ist sicherzustellen, dass gegenüber den Beschäftigten vollständige **Transparenz** besteht und sie nach-

vollziehen können, in welchen Situationen und zu welchen Zwecken eine Verarbeitung erfolgt. Die **Mitbestimmungsrechte des Betriebsrats** sind dabei zwingend zu berücksichtigen.

3. Datenschutzrechtliche Maßnahmen

3.1. Informationspflichten

Vor der Aufzeichnung und Transkription von Gesprächen müssen alle Teilnehmerinnen und Teilnehmer umfassend über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Die Information muss insbesondere den Zweck der Verarbeitung, den Umfang der Aufzeichnung und Transkription, die Speicherdauer, mögliche Empfänger sowie die eingesetzten Systeme (z.B. KI-gestützte Transkriptionsssoftware) umfassen.

Die Information sollte bereits mit der Einladung zum Meeting erfolgen und kann durch Pop-ups oder Ansagen ergänzt werden. Bei Telefonkonferenzen empfiehlt sich eine kurze Ansage zu Beginn, bei Videokonferenzen ein Hinweis im Tool oder ein Link zur Datenschutzinformation.

3.2. Interventionsrechte

Betroffene Personen verfügen über verschiedene Rechte, um die Verarbeitung ihrer Daten zu kontrollieren und gegebenenfalls zu begrenzen. Sie können ihre Einwilligung jederzeit **widerrufen** und damit die weitere Verarbeitung auf dieser Grundlage stoppen. Darüber hinaus haben sie das Recht, der Verarbeitung, die auf einem berechtigten Interesse beruht, zu **widersprechen**. Ebenso können sie jederzeit **Zugang** zu bestehenden Aufzeichnungen und Tran-

⁶ Moers, DSRITB 2024, 751 (759).

skripten verlangen, um die über sie gespeicherten Daten einzusehen.

Wird ein Widerruf oder Widerspruch erklärt, ist die weitere Nutzung der betreffenden Aufzeichnungen oder Transkripte untersagt. Gleichzeitig müssen diese Daten unverzüglich gelöscht werden, um den Rechten der betroffenen Personen Rechnung zu tragen. Damit wird sichergestellt, dass die Verarbeitung jederzeit transparent bleibt und die Selbstbestimmung der Betroffenen gewahrt wird.

3.3. Löschkonzept

Ein strukturiertes Löschkonzept ist für die datenschutzkonforme Verarbeitung von Aufzeichnungen und Transkripten zwingend erforderlich. Es sollte klar regeln, welche Speicherdauer für unterschiedliche Zwecke gilt und dabei sowohl gesetzliche Vorgaben als auch betriebliche Anforderungen berücksichtigen. Automatisierte Löschroutinen sind empfehlenswert, um die Einhaltung der festgelegten Fristen zuverlässig sicherzustellen. Insbesondere sollten Audioaufzeichnungen nach der Fertigstellung des Transkripts gelöscht werden, sofern keine weiteren legitimen Zwecke für deren Aufbewahrung bestehen. Ein solches Löschkonzept trägt wesentlich dazu bei, Transparenz zu gewährleisten und die datenschutzrechtlichen Pflichten gegenüber den Betroffenen einzuhalten.

3.4. Technische und organisatorische Maßnahmen

Die Verarbeitung muss durch geeignete technische und organisatorische Maßnahmen abgesichert werden. Dazu gehört u.a.:

- **Privacy by design:** Systeme müssen so gestaltet sein, dass Datenschutz von Anfang an berücksichtigt wird.
- **Privacy by default:** Voreinstellungen müssen datenschutzfreundlich sein (z.B. keine automatische Aufzeichnung).
- **Zugriffskontrollen:** Nur berechtigte Personen dürfen Zugriff auf Aufzeichnungen und Transkripte haben.
- **Verschlüsselung:** Audio- und Textdateien sollten verschlüsselt gespeichert und übertragen werden.
- **Schulung:** Beschäftigte müssen im Umgang mit Aufzeichnungen und Transkripten geschult werden.

3.5. Drittlandübermittlung

Viele cloudbasierte Konferenztools speichern Daten auf Servern außerhalb der EU. In diesen Fällen müssen besondere Maßnahmen ergriffen werden, um den Anforderungen der Datenschutz-Grundverordnung zu genügen. Zunächst ist sicherzustellen, dass mit den Anbietern entsprechende **Auftragsverarbeitungsverträge** nach Art. 28 DS-GVO abgeschlossen werden. Darüber hinaus müssen geeignete Garantien für den Schutz der Daten im Drittland implementiert sein, etwa in Form von **Standardvertragsklauseln** oder vergleichbaren vertraglichen Sicherungen. Schließlich ist eine **Prüfung der tatsächlichen Schutzmaßnahmen** im Drittland erforderlich, um sicherzustellen, dass das Datenschutzniveau im Drittland den europäischen Anforderungen entspricht und die Rechte der Betroffenen wirksam gewahrt bleiben.

3.6. Einsatz von KI-Systemen

Werden KI-Systeme zur Transkription eingesetzt, sind zusätzlich die Vorgaben der EU-KI-Verordnung zu beachten. Systeme, die Emotionen oder Stimmungen erkennen sollen, können nach Art. 5 KI-VO verboten sein. Je nach Einsatzkontext kann ein Transkriptionssystem als Hochrisiko-KI eingestuft werden. Dadurch entstehen erhöhte Anforderungen an Risikobewertung, Dokumentation, Transparenz und menschliche Aufsicht.

4. Strafbarkeit nach § 201 StGB

§ 201 StGB stellt die unbefugte Aufnahme des nicht öffentlich gesprochenen Wortes unter Strafe. Da die meisten Transkriptionstools eine Zwischenspeicherung des Audiosignals vornehmen, liegt technisch regelmäßig eine Aufnahme vor.⁷ Ohne Einwilligung aller Beteiligten ist dies strafbar.

4.1. Das Merkmal „unbefugt“

„Unbefugt“ bedeutet, dass keine rechtfertigende Befugnis vorliegt. Eine Befugnis kann sich aus Einwilligung, gesetzlicher Erlaubnisnorm oder besonderen Rechtfertigungsgründen ergeben. Im Kontext von Transkriptionen ist die Einwilligung der Gesprächsteilnehmer/-innen der praktisch wichtigste Rechtfertigungsgrund.

4.2. Verhältnis zur DS-GVO

Eine datenschutzrechtlich wirksame Einwilligung nach Art. 6 Abs. 1 lit. a) DS-GVO ist freiwillig, informiert und jederzeit widerruflich.

⁷ Moers, DSRITB 2024, 751 (764 f.).

Liegt eine solche Einwilligung vor, ist die Datenverarbeitung rechtmäßig. Zugleich entfällt die Strafbarkeit nach § 201 StGB, da die Aufnahme nicht „unbefugt“ erfolgt. Umgekehrt reicht eine bloß konkludente Zustimmung, die strafrechtlich als Befugnis gewertet werden könnte,⁸ datenschutzrechtlich nicht aus. Das bedeutet: Strafrechtlich genügt eine konkludente Zustimmung (z.B. Weiterreden trotz Hinweis auf Aufzeichnung), während datenschutzrechtlich eine ausdrückliche, dokumentierte Einwilligung erforderlich ist.⁹

4.3. Konsequenzen und Bewertung für die Praxis

Das Zusammenspiel von Strafrecht und Datenschutzrecht führt zu den folgenden Ergebnissen bei der Bewertung von Aufzeichnungen und Transkriptionen.

- >> Liegt eine Einwilligung vor, die sowohl den Anforderungen der DS-GVO als auch den strafrechtlichen Vorgaben entspricht, ist die Aufnahme unproblematisch und sowohl datenschutzrechtlich als auch strafrechtlich zulässig.
- >> Liegt hingegen lediglich eine strafrechtlich ausreichende, aber datenschutzrechtlich mangelhafte Einwilligung vor, entfällt zwar die Strafbarkeit, es liegt jedoch ein Verstoß gegen datenschutzrechtliche Vorschriften vor.

⁸ Fischer-Fischer, 72. Aufl. 2025, § 201 StGB Rn. 10.

⁹ Kindhäuser/Hilgendorf-Kindhäuser/Hilgendorf, 10. Aufl. 2025, § 201 StGB Rn. 22.

5. Fazit

Die Verarbeitung und Transkription von Gesprächen berührt sowohl datenschutzrechtliche als auch strafrechtliche Vorgaben, weshalb eine sorgfältige Planung und Umsetzung unerlässlich ist. Eine wirksame Einwilligung der Betroffenen bleibt die zentrale Rechtsgrundlage, da sie sowohl datenschutzrechtlich als auch strafrechtlich Sicherheit bietet. Alternative Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO, wie Vertragserfüllung, gesetzliche Pflicht oder berechtigtes Interesse sind denkbar, aber nicht der praktische Regelfall.

Unternehmen müssen insbesondere im Beschäftigtenkontext zusätzliche Maßnahmen ergreifen, wie den Abschluss von Betriebsvereinbarungen, die transparente Infor-

mationspflichten, Interventionsrechte und ein strukturiertes Löschkonzept berücksichtigen. Technische und organisatorische Maßnahmen, etwa Zugriffskontrollen, Verschlüsselung und Privacy-by-Design-Prinzipien, sind ebenfalls unverzichtbar, ebenso wie besondere Regelungen bei der Nutzung cloudbasierter Systeme oder KI-gestützter Transkriptionssoftware.

In der Praxis zeigt sich, dass eine datenschutzkonforme und rechtssichere Verarbeitung die Verbindung von organisatorischen, technischen und rechtlichen Maßnahmen erfordert. Die Einwilligung der Betroffenen stellt hierbei den verlässlichsten Weg dar, um die Anforderungen von Datenschutzrecht und Strafrecht gleichermaßen zu erfüllen und Rechtssicherheit zu gewährleisten.

Wer ist die GDD?

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.



Mitglied werden? Mehr Informationen?

<https://www.gdd.de/service/mitglied-werden> oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

- >> Mitglieder-Nachrichten mit aktuellen Fachinformationen in Form eines monatlichen Newsletters
- >> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
- >> Beratung bei konkreten Einzelfragen
- >> Zugriff auf Rechtsprechungs- und Literaturarchiv in der GDDcommunity
- >> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
- >> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
- >> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.600 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

GDD

Herausgeber:

Gesellschaft für Datenschutz und
Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn

Tel.: +49 2 28 96 96 75-00
www.gdd.de
info@gdd.de