

SPRINGCAST LEITFÄDEN

Compliance beim Podcasting

Regeln Sie Zuständigkeit, Datenschutz und Zugang, wenn Ihre Podcastaktivitäten wachsen



springcast.io

IN DIESEM LEITFADEN

- 01 **Legen Sie klare Zuständigkeiten fest**

- 02 **Behalten Sie die Verbreitungswege im Blick**

- 03 **Regeln Sie den Umgang mit personenbezogenen Daten**

- 04 **Passen Sie den internen Zugang an die Sensibilität der Inhalte an**

- 05 **Machen Sie den freigegebenen Ablauf praktikabel**

- 06 **Verankern Sie Governance in der Veröffentlichungsroutine**

- 07 **Besprechen Sie Ihre Anforderungen mit Springcast**

Regeln Sie Zuständigkeit, Datenschutz und Zugang, wenn Ihre Podcastaktivitäten wachsen.

Legen Sie klare Zuständigkeiten fest

Podcasts können internen Updates, Kundeninformation, Personalgewinnung oder öffentlichen Gesprächen über Ihr Fachgebiet dienen. Jede Anwendung hat eine eigene Zielgruppe, eigene Inhalte und einen eigenen Veröffentlichungsweg. Wenn weitere Teams Audio produzieren, klären Sie, wer die Entscheidungen zu Datenschutz, Sicherheit und dem Ruf der Organisation verantwortet.

Das Kommunikationsteam kann den Redaktionsplan betreuen, während die IT den Zugang verwaltet und das Datenschutzteam die Verarbeitung personenbezogener Daten bewertet. Machen Sie diese Aufgaben ausdrücklich sichtbar. Es sollte klar sein, welche Sendungen existieren, wer sie veröffentlichen darf und wo Aufnahmen gespeichert werden. So können Sie neue Produzierende unterstützen, ohne dass diese selbst einen Ablauf erfinden müssen.

Beginnen Sie mit einer Bestandsaufnahme. Berücksichtigen Sie öffentliche Sendungen, private Feeds, Aufnahmen auf gemeinsam genutzten Laufwerken und Folgen, die externe Produktionspartner verbreiten. Dokumentieren Sie die vorgesehene Zielgruppe und ob das Material personenbezogene, vertrauliche oder geschäftlich sensible Informationen enthält. Ein öffentliches Kundeninterview und ein internes Update der Geschäftsleitung können unterschiedliche Prüfwege benötigen.

Erkennen Sie anhand der Bestandsaufnahme Lücken in der Zuständigkeit und legen Sie Prioritäten fest. Eine Sendung mit unklaren Veröffentlichungsrechten oder sensibles Material in einem breit geteilten Ordner braucht eine konkrete Folgemaßnahme. Weisen Sie diese einer Person zu, die das Problem lösen kann.

Praktische Schritte

- Benennen Sie eine verantwortliche Person für die Podcast-Governance sowie Kontakte für Redaktion, Datenschutz und IT.
- Erfassen Sie bestehende Sendungen, Speicherorte, Veröffentlichungswege und verantwortliche Teams.
- Legen Sie fest, welche Inhalte vor der Veröffentlichung geprüft werden und wer sie freigeben darf.

Behalten Sie die Verbreitungswege im Blick

Eine Abteilung veröffentlicht möglicherweise über Apple Podcasts und Spotify, eine andere über einen privaten Feed und eine weitere über einen Intranetlink. Diese Wege unterscheiden sich im Zugangs- und Verbreitungsverhalten. Dokumentieren Sie die Unterschiede, statt davon auszugehen, dass alle Podcastlinks gleich funktionieren.

Wählen Sie freigegebene Werkzeuge und erklären Sie, wann Teams sie einsetzen sollen. Eine gemeinsame Verwaltungsumgebung kann helfen, Zuständigkeiten und Berechtigungen zu überblicken. Der Ablauf umfasst jedoch auch Aufnahmesoftware, Schnittdienstleister, Dateiübertragungen und Sicherungskopien. Beziehen Sie diese Schritte ein, wenn Sie den Weg von der Aufnahme bis zur Veröffentlichung prüfen.

Kontrollieren Sie bei öffentlichen Inhalten den endgültigen Titel, die Beschreibung, die Audiodatei und die Veröffentlichungsziele. Prüfen Sie bei internen Inhalten, ob die vorgesehene Zielgruppe Zugang hat und ob Personen außerhalb dieser Gruppe über den eingerichteten Weg ausgeschlossen bleiben. Eine unveröffentlichte oder nicht gelistete URL ist für sich allein kein Authentifizierungsverfahren.

Führen Sie eine betriebliche Übersicht über Kontoverantwortliche und Dienstleister. Bei einem Markenwechsel, dem Ende einer Dienstleisterbeziehung oder der Einstellung einer Sendung sollte das Team wissen, welche Konten und Kopien betroffen sind. Eine zentrale Übersicht kann helfen, lässt aber nicht jede externe Kopie verschwinden.

Praktische Schritte

- Definieren Sie für jede Art von Sendung einen freigegebenen Veröffentlichungsweg.
- Nehmen Sie Produktionspartner und Dateiübertragungen in die Ablaufübersicht auf.
- Prüfen Sie Kontoverantwortlichkeiten, wenn sich Teams, Dienstleister oder Veröffentlichungspläne ändern.

Regeln Sie den Umgang mit personenbezogenen Daten

Eine Aufnahme kann Namen, erkennbare Stimmen, persönliche Erfahrungen oder Angaben über Beschäftigte und Kunden enthalten. Prüfen Sie die geplante Nutzung bereits vor der Aufnahme. Dazu gehört, wie Sie die Folge bearbeiten, veröffentlichen, bewerben und aufbewahren möchten. Erklären Sie den Teilnehmenden diese Nutzung verständlich.

Stimmen Sie die passende Rechtsgrundlage mit Ihrem Datenschutzteam ab und dokumentieren Sie sie. Eine Einwilligung ist keine allgemeingültige Lösung: Aufgrund des Beschäftigungsverhältnisses können Beschäftigte sie möglicherweise nicht freiwillig erteilen. Trennen Sie Teilnahmevereinbarungen von dieser Bewertung. [Hinweise des Europäischen Datenschutzausschusses](#).

Entscheiden Sie, welche Informationen für den Zweck der Folge erforderlich sind. Ein hilfreiches Beispiel braucht nicht immer einen echten Kundennamen, eine identifizierbare Person oder detaillierte persönliche Umstände. Bereiten Sie Gäste und Moderierende darauf vor, welche Themen nicht in die Aufnahme gehören. Sehen Sie eine Prüfung für unerwartet genannte Informationen vor.

Bewerten Sie Hosting, Auftragsverarbeitungsvereinbarungen, Zugangskontrollen, Aufbewahrung und den vorgesehenen Einsatz der Aufnahmen gemeinsam. Fragen Sie Dienstleister, welche Dienste und Standorte beteiligt sind, einschließlich optionaler Werkzeuge für Transkription oder Bearbeitung. Europäisches Hosting ist ein Beschaffungskriterium. Es ersetzt nicht die Prüfung des gesamten Ablaufs.

Machen Sie die Aufbewahrung praktisch umsetzbar. Bestimmen Sie, welche Originalaufnahmen, bearbeiteten Dateien und zugehörigen Daten Sie behalten möchten, zu welchem Zweck und unter wessen Verantwortung. Legen Sie mit dem zuständigen Team einen Weg für Berichtigungs-, Löschungs- oder Datenschutzanfragen fest. Prüfen Sie, was mit Kopien geschieht, die bereits über andere Dienste verbreitet wurden.

Praktische Schritte

- Prüfen Sie die Informationen in der Aufnahme und die vorgesehene Zielgruppe der Veröffentlichung.
- Klären Sie Rechtsgrundlage, Teilnehmerinformation und Aufbewahrung mit dem Datenschutzteam.

- Prüfen Sie Dienstleistervereinbarungen und den tatsächlichen Verarbeitungsablauf, bevor Sie die Einrichtung freigeben.

Passen Sie den internen Zugang an die Sensibilität der Inhalte an

Interne Podcasts können Updates der Geschäftsleitung, Onboarding und Wissensaustausch unterstützen. Das passende Zugangsmodell hängt vom Inhalt ab. Eine Einführung in die Organisation kann andere Anforderungen haben als ein vertrauliches Strategiegespräch. Bestimmen Sie die Zielgruppe, bevor Sie den Verbreitungsweg wählen.

Ein verborgener Link kann weitergeleitet werden. Auch persönliche RSS-Links lassen sich teilen. Heruntergeladene Folgen können verfügbar bleiben, nachdem sich der Zugang zu einem Dienst geändert hat. Berücksichtigen Sie diese Grenzen bei Ihrer Entscheidung, statt aus der Bezeichnung „intern“ automatisch auf Vertraulichkeit zu schließen.

Wenn eine Authentifizierung erforderlich ist, prüfen Sie die verfügbaren Anmelde- und Kontoverwaltungsoptionen. Single Sign-on kann die Anmeldung mit einem Identitätsanbieter verbinden. Daraus folgt jedoch noch nicht, wie jedes Konto angelegt, aktualisiert oder entfernt wird. Klären Sie, welche Kontolebenszyklusfunktionen das gewählte Produkt und die Einrichtung unterstützen. Testen Sie den Ablauf für Eintritt, Rollenwechsel und Austritt.

Trennen Sie Produktionsberechtigungen vom Hörzugang. Eine Sendung bearbeiten oder veröffentlichen zu dürfen ist eine andere Berechtigung als sie anhören zu dürfen. Geben Sie Teams den Zugang, den sie für ihre Arbeit benötigen. Benennen Sie eine Person, die Berechtigungen bei veränderten Aufgaben prüft.

Klären Sie bei Springcast den jeweiligen Tarif und die Anwendung, bevor Sie sich auf eine bestimmte Zugangsfunktion verlassen. Besprechen Sie private Feeds, authentifiziertes Hören und Identitätsanforderungen anhand eines konkreten Beispiels für Inhalt und Zielgruppe mit dem Team.

Praktische Schritte

- Wählen Sie das Zugangsmodell nach der Sensibilität der Inhalte und der vorgesehenen Zielgruppe.

- Prüfen Sie Anmeldung, Kontolebenszyklus und die Grenzen bei heruntergeladenen Kopien gemeinsam.
- Testen Sie Eintritt, Rollenwechsel und Austritt in der Einrichtung, die Sie tatsächlich verwenden werden.

Machen Sie den freigegebenen Ablauf praktikabel

Ein freigegebenes Werkzeug ist nur ein Teil des Prozesses. Produzierende müssen auch wissen, wo sie Aufnahmen speichern, wie sie Gäste einladen, wer eine Folge prüft und was bei einer fehlerhaften Veröffentlichung zu tun ist. Stellen Sie diese Informationen dort bereit, wo das Team arbeitet, und machen Sie die zuständigen Kontakte leicht auffindbar.

Gehen Sie mit neuen Produzierenden vor der ersten Veröffentlichung eine realistische Folge durch. Behandeln Sie Vorbereitung, Aufnahme, Übertragung, Schnitt, Prüfung und Verbreitung. Berücksichtigen Sie häufige Ausnahmen, etwa einen externen Gast, freie Mitarbeit beim Schnitt oder eine Person, die eine Korrektur verlangt. Menschen sollen Routineaufgaben selbstständig erledigen und erkennen können, wann Unterstützung nötig ist.

Prüfen Sie die Werkzeugübersicht regelmäßig. Werden die Werkzeuge noch genutzt? Sind die Kontoverantwortlichen aktuell? Entspricht der dokumentierte Ablauf der Praxis? Wenn sich Werkzeuge überschneiden, prüfen Sie, ob eine Zusammenführung die Verwaltung vereinfachen würde. Planen Sie einen Umzug, bevor Sie Konten oder Dateien entfernen, die Teams noch benötigen.

Halten Sie den Prozess dem Material angemessen. Ein öffentliches Interview und ein sensibles internes Update können unterschiedliche Prüfschritte rechtfertigen. Ein kurzer, klarer Weg, den Menschen einhalten können, ist hilfreicher als eine lange Richtlinie ohne erkennbare praktische Zuständigkeit.

Praktische Schritte

- Geben Sie neuen Produzierenden eine Einführung und eine kurze Veröffentlichungsscheckliste.
- Benennen Sie Kontakte für Zugangsprobleme, Korrekturen und vermutete Vorfälle.
- Prüfen Sie Werkzeuge, Konten und Arbeitsweisen erneut, wenn sich Team oder Umfang ändern.

Verankern Sie Governance in der Veröffentlichungsroutine

Beziehen Sie Kommunikation, IT, Informationssicherheit und Datenschutz in die erste Einrichtung ein. Vereinbaren Sie Anforderungen, bevor Sie ein Werkzeug auswählen oder Zusagen über die Wirkung des Podcasts machen. Halten Sie Entscheidungen fest, damit neue Projekte passende Teile übernehmen können.

Nutzen Sie einen klaren Prüf- und Freigabeweg für Veröffentlichungen. Legen Sie fest, wer eine Folge freigeben darf, wer sensible Inhalte prüft und welcher Freigabenachweis aufbewahrt wird. Regeln Sie, wie sich die Verbreitung unterbrechen oder ein Fehler korrigieren lässt. Dazu gehört auch, wer eine externe Plattform oder einen Produktionspartner kontaktieren darf.

Bewerten Sie verfügbare Auditinformationen innerhalb ihres tatsächlichen Umfangs. Prüfen Sie, welche Ereignisse protokolliert werden, wer darauf zugreifen kann und wie lange die Informationen verfügbar bleiben. Gehen Sie nicht davon aus, dass ein Protokoll jede externe Plattform, heruntergeladene Kopie oder Hörerhandlung erfasst. Analytics kann eine redaktionelle Auswertung unterstützen, ist aber kein Nachweis für Compliance oder finanziellen Ertrag.

Testen Sie die für die geplante Einrichtung entscheidenden Punkte: Die Zielgruppe kann zuhören, Zugangsänderungen funktionieren wie konfiguriert, Veröffentlichungsrechte sind klar und das Team findet das Verfahren für Vorfälle. Prüfen Sie diese Punkte erneut, wenn sich ein wesentlicher Teil des Ablaufs ändert. So erhält die Organisation eine praktische Grundlage für den Ausbau ihrer Podcastaktivitäten.

Praktische Schritte

- Stimmen Sie Anforderungen mit den zuständigen Teams ab, bevor Sie die Einrichtung auswählen.
- Dokumentieren Sie Veröffentlichungsfreigabe, Zugangsverantwortung und Korrekturweg.
- Prüfen Sie die eingerichteten Kontrollen und Nachweise bei Änderungen am Ablauf.

Besprechen Sie Ihre Anforderungen mit Springcast

Springcast verbindet Podcast-Hosting, Analytics und Distribution für Organisationen und Podcaster. Unsere Anwendungen laufen in den Niederlanden, Deutschland und Finnland. Auf Anfrage begleitet ein Compliance Officer Ihr Team durch die Sicherheitsfragebögen.

Bringen Sie die vorgesehene Zielgruppe, die Sensibilität der Inhalte sowie Zugangs- und Berichtsanforderungen in das Gespräch ein. Gemeinsam können wir prüfen, welche Springcast-Einrichtung und Tarifbedingungen zum geplanten Ablauf passen und welche begleitenden Regelungen Ihre Organisation treffen muss.

[Besprechen Sie Hosting und Zugangsanforderungen](#)