

SPRINGCAST GUIDES

Compliance in Podcasting

Organize ownership, privacy and access as your podcast activity grows


springcast.io

IN THIS GUIDE

- 01 **Give podcasting a clear owner**

- 02 **Keep oversight across distribution channels**

- 03 **Decide how personal data will be handled**

- 04 **Match internal access to the sensitivity of the audio**

- 05 **Make the approved workflow usable for makers**

- 06 **Build governance into the publishing routine**

- 07 **Discuss your requirements with Springcast**

Organize ownership, privacy and access as your podcast activity grows.

Give podcasting a clear owner

Podcasts can serve internal updates, customer education, recruitment or public conversations about your field. Each use has its own audience, content and publishing route. As more teams start producing audio, agree who is responsible for the decisions that affect privacy, security and the organization's reputation.

A communications team may own the editorial plan, while IT manages access and the privacy team assesses personal-data processing. Make those responsibilities explicit. Someone should be able to explain which shows exist, who can publish them and where recordings are stored. This also makes it easier to support new makers without asking them to invent a process themselves.

Start with an inventory of existing activity. Include public shows, private feeds, recordings on shared drives and episodes distributed by external production partners. Record the intended audience and whether the material includes personal, confidential or commercially sensitive information. A public customer interview and an internal leadership update may need different review routes.

Use the inventory to identify gaps in ownership and decide what needs attention first. A show with unclear publication rights or sensitive material in a broadly shared folder deserves a concrete follow-up. Assign that follow-up to an owner who can resolve it.

Practical steps

- Appoint an owner for podcast governance and name the editorial, privacy and IT contacts.
- List existing shows, storage locations, publishing routes and responsible teams.
- Agree which content needs review before publication and who can approve it.

Keep oversight across distribution channels

One department may publish through Apple Podcasts and Spotify, another through a private feed, and another through a link on the intranet. Each route has different access and distribution behavior. Document those differences rather than assuming that all podcast links work in the same way.

Choose approved tools and explain when teams should use them. A shared management environment can make ownership and permissions easier to oversee, but the workflow also includes recording software, editing partners, file transfers and backups. Include those steps when reviewing how an episode moves from recording to publication.

For public content, check the final title, description, audio and publication destinations. For internal content, confirm that the intended audience can access it and that people outside that audience cannot gain access through the configured route. An unpublished or unlisted URL is not, by itself, an authentication mechanism.

Keep an operational record of account owners and suppliers. When branding changes, a supplier relationship ends or a show is retired, the team should know which accounts and copies require attention. Central oversight can help, but it does not make every external copy disappear.

Practical steps

- Define an approved publishing route for each type of show.
- Include production partners and file transfers in the workflow map.
- Review account ownership when teams, suppliers or publication plans change.

Decide how personal data will be handled

A recording can contain names, recognizable voices, personal experiences or details about colleagues and customers. Review the intended use before recording, including how the episode will be edited, published, promoted and retained. Explain that use to participants in language they can understand.

Agree and document the appropriate legal basis with your privacy team. Consent is not a universal answer: employees may be unable to give it freely because of the employment relationship. Keep participation agreements separate from that assessment. [EDPB guidance](#).

Decide which information is needed for the purpose of the episode. A useful example does not always need a real customer name, an identifiable colleague or detailed personal circumstances. Prepare guests and hosts for topics that should remain outside the recording, and include a review step for unexpected disclosures.

Assess the hosting arrangement alongside processing agreements, access controls, retention and the intended use of recordings. Ask suppliers which services and locations are involved, including any optional tools used for transcription or editing. European hosting is one procurement consideration; it does not replace the review of the wider workflow.

Make retention operational. Identify which original recordings, edited files and associated data you intend to keep, for what purpose and under whose responsibility. Establish a route for handling correction, removal or privacy requests with the appropriate team. Check what happens to copies already distributed through other services.

Practical steps

- Review the information in the recording and the planned publication audience.
- Agree the legal basis, participant information and retention arrangements with the privacy team.
- Check supplier agreements and the actual processing workflow before approving the setup.

Match internal access to the sensitivity of the audio

Internal podcasts can support leadership updates, onboarding and knowledge sharing. The right access model depends on the content. An introduction to the organization may have different requirements from a restricted strategy discussion. Decide the intended audience before choosing the distribution method.

A hidden link can be forwarded. Personal RSS links can also be shared, and downloaded episodes can remain available after access to a service changes. Treat those limits as part of the choice rather than assuming that an internal label provides confidentiality.

Where authentication is required, examine the available sign-in and account-management options. Single sign-on can connect sign-in to an identity provider, but that alone does not establish how every account is created, updated or removed. Confirm the lifecycle controls supported by the selected product and configuration. Test the process for a person joining, changing role and leaving.

Separate maker permissions from listener access. The ability to edit or publish a show is a different permission from the ability to hear it. Give teams the access they need for their work, and appoint someone to review permissions when responsibilities change.

For Springcast, confirm the relevant plan and application before relying on a particular access feature. Discuss private feeds, authenticated listening and identity requirements with the team using a concrete example of the content and audience.

Practical steps

- Choose the access model based on the sensitivity of the content and the intended audience.
- Check sign-in, account lifecycle and downloaded-copy limitations together.
- Test joiner, role-change and leaver access in the configuration you will use.

Make the approved workflow usable for makers

An approved tool is only part of the process. A maker also needs to know where to store recordings, how to invite guests, who reviews the episode and what to do when something is published incorrectly. Put those instructions where the team works and make the responsible contacts easy to find.

Walk a new maker through a realistic episode before their first publication. Cover preparation, recording, transfer, editing, review and distribution. Include common exceptions, such as an external guest, a freelancer helping with editing or a participant requesting a correction. The aim is to let people handle routine work and recognize when help is needed.

Review the tool inventory periodically. Check whether the tools are still used, whether account owners are current and whether the documented workflow matches actual practice. Where tools duplicate each other, consider whether consolidating them would simplify management. Plan any migration before removing accounts or files that teams still need.

Keep the process proportionate to the material. A public interview and a sensitive internal update may warrant different review steps. A short, clear route that people can follow is more useful than a long policy whose practical owner is unknown.

Practical steps

- Give new makers a walkthrough and a concise publication checklist.
- Name the contact for access problems, corrections and suspected incidents.
- Revisit tools, accounts and working practices when the team or scope changes.

Build governance into the publishing routine

Bring Communications, IT, Security and Privacy into the initial setup. Agree the requirements before selecting a tool or making promises about what the podcast will do. Record the decisions so that new projects can reuse the parts that apply to them.

Use a clear review and approval route for publication. Identify who can release an episode, who checks sensitive content and what evidence is kept of approval. Establish how to pause distribution or correct a mistake, including who can contact an external platform or production partner.

Review available audit information within its actual scope. Check which events are logged, who can access them and how long they remain available. Do not assume that a log covers every external platform, downloaded copy or listener action. Analytics can support an editorial review, but it is not proof of compliance or financial return.

Test the parts that matter for the planned setup: the intended audience can listen, access changes work as configured, publication rights are clear and the team can find the response procedure. Revisit those checks when a material part

of the workflow changes. This gives the organization a practical basis for expanding podcast activity.

Practical steps

- Agree requirements with the relevant teams before choosing the setup.
- Document publication approval, access ownership and the correction route.
- Review the configured controls and evidence when the workflow changes.

Discuss your requirements with Springcast

Springcast brings podcast hosting, analytics and distribution together for organizations and creators. Our applications run in the Netherlands, Germany and Finland. On request, a compliance officer takes your team through the security questionnaires.

Bring the intended audience, content sensitivity, access requirements and reporting needs to the discussion. We can review which Springcast setup and plan conditions fit the proposed workflow, and which arrangements your organization needs to make around it.

[Discuss hosting and access requirements](#)