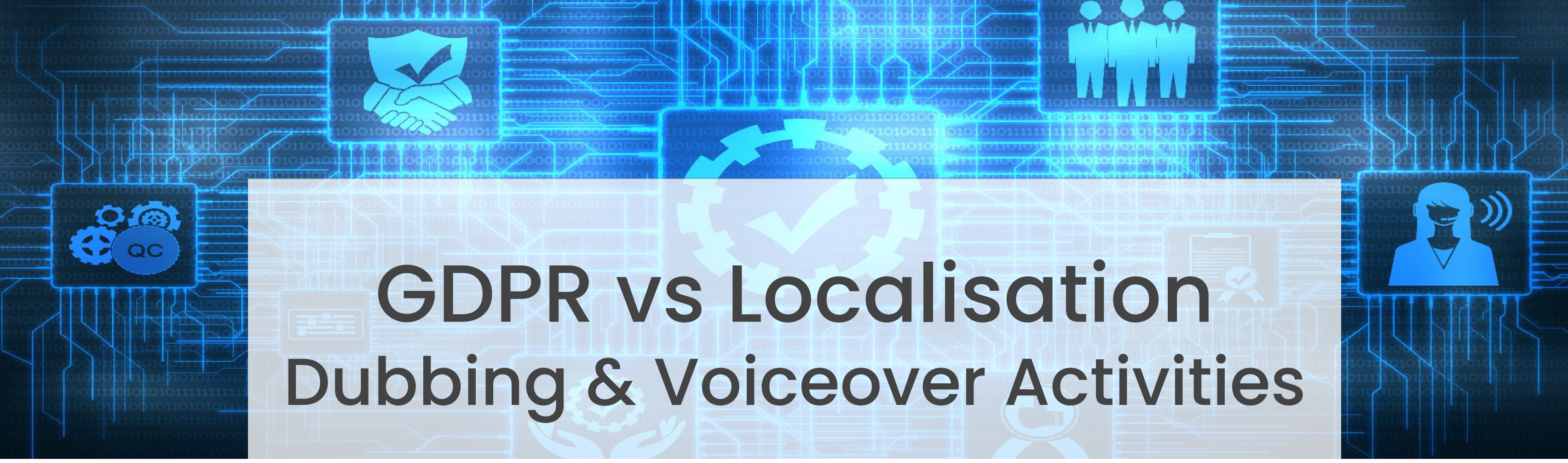
mediartis

Navigating GDPR Compliance in Dubbing & Voiceover Operations

Mediartis | Updated October 2023

Index



GDPR vs Localisation

Dubbing & Voiceover Activities

Voice is a personal data, strictly protected by the European General Data Protection Regulation (GDPR) and most worldwide data protection legislations. The increasingly rapid development and adoption of AI voice generators, AI dubbing and voice cloning technologies in the entertainment industry have made voice data privacy concerns a focal point for European Data Protection Authorities, voice actors and trade unions worldwide.

For localisation professionals with dubbing and voiceover operations, GDPR impacts all workflows that involve the collection, storage and sharing of actors' voice samples. The regulation impacts the industry on multiple levels with two especially high privacy risk areas in production: Voice Casting Database Management and Personal Data Circulation.

Since the arrival of the world's strictest data protection legislation, the GDPR, in 2018, the localisation industry has invested heavily in privacy tools with a strong focus on security, HR, marketing and sales activities. While the industry has been a privacy pioneer in several areas, internal and partner production workflows remain artisanal and do not consistently address voice data compliance or verification of partner compliance, dangerous oversights that should not be underestimated.

Voice localisation resources include a lot of personal data that is subject to very specific processing rules to conform with EU data protection law. Protected data includes EU data originating from and delivered within the EU, EU data transiting to non-EU countries, and non-EU data transiting to or through the EU. Every European country has a Data Protection Authority (DPA), and GDPR legislation accords DPAs the authority to launch compliance audits and issue warnings, reprimands and fines, both locally and internationally.

Service provider selection and compliance monitoring are critical as the GDPR introduces the notion of compliance co-responsibility, meaning that a data breach, anywhere in the supply chain, puts all project stakeholders at risk of **penalties that can reach 20M€ or 4% of global revenues**.

GDPR

General Data Protection Regulation

What is it?

In effect since May 25th, 2018, the European General Data Protection Regulation (GDPR) is the strictest data protection law in the world. It is a legal framework that sets guidelines for the collection, processing and sharing of European citizens and residents personal data.

Personal data is defined by the GDPR as any information relating to an identified or identifiable natural person (referred to as "data subject") and covers a broad scope that includes both directly identifying data and indirectly identifying data. Examples of personal data include name, pseudonym, date of birth, email, telephone number, photos, **voice recordings**, fingerprints, DNA, ethnicity, religion, union status, etc.

Non-compliance risks?

Every European country has a **Data Protection Authority** (DPA), and GDPR legislation accords DPAs the authority to launch compliance audits and issue warnings, reprimands and fines, both **locally and internationally**. Aside from obvious risks such as brand reputation and client confidence, if a Data Protection Authority audits an organisation and deems they have not respected GDPR obligations, they can:

- ➔ Temporarily or permanently **limit data processing**
- ➔ **Delete the data** in question (2019 HMRC conviction – 5M voice recordings deleted)
- ➔ Apply fines of up to 10M€ or 2% of the annual turnover for breaches of "Privacy by Design" or "Privacy by Default" or up to **20M€ or 4% of global revenues** (max of the 2) for any breach of data subject rights
- ➔ Create and make public a **sanction named after the company**

GDPR Risks
Voice Casting Databases

Dubbing and voiceover service providers often keep internal casting databases that include actor details **and voice samples.** These databases are compiled over time, data often includes files and information that was collected pre-contract or contracted for use in a specific project and then added to the casting database for future projects. Original data sources and compliance status are often unknown and **new voice recordings** saved from auditions, live-castings, outsourced creative directors, inbound castings shared by partner studios, agents and voice casting platforms are added on a regular basis.

When preparing casting propositions for clients, project managers and creative directors might include recordings made specifically for the project in question, but will often include voice samples from their own casting databases to support their talent propositions. Shared samples are often saved by recipients for reference in future projects, or inadvertently. Both scenarios fall into the scope of GDPR and require the actors be notified and the voice data be processed in alignment with the regulation's rules.

This is how the industry has always worked, so what's the problem?

Even if it seems obvious that actors want to be referenced in a studio's casting database, personal data processing must adhere with the principles laid out by the GDPR to be compliant with EU data protection law. Some of which include:

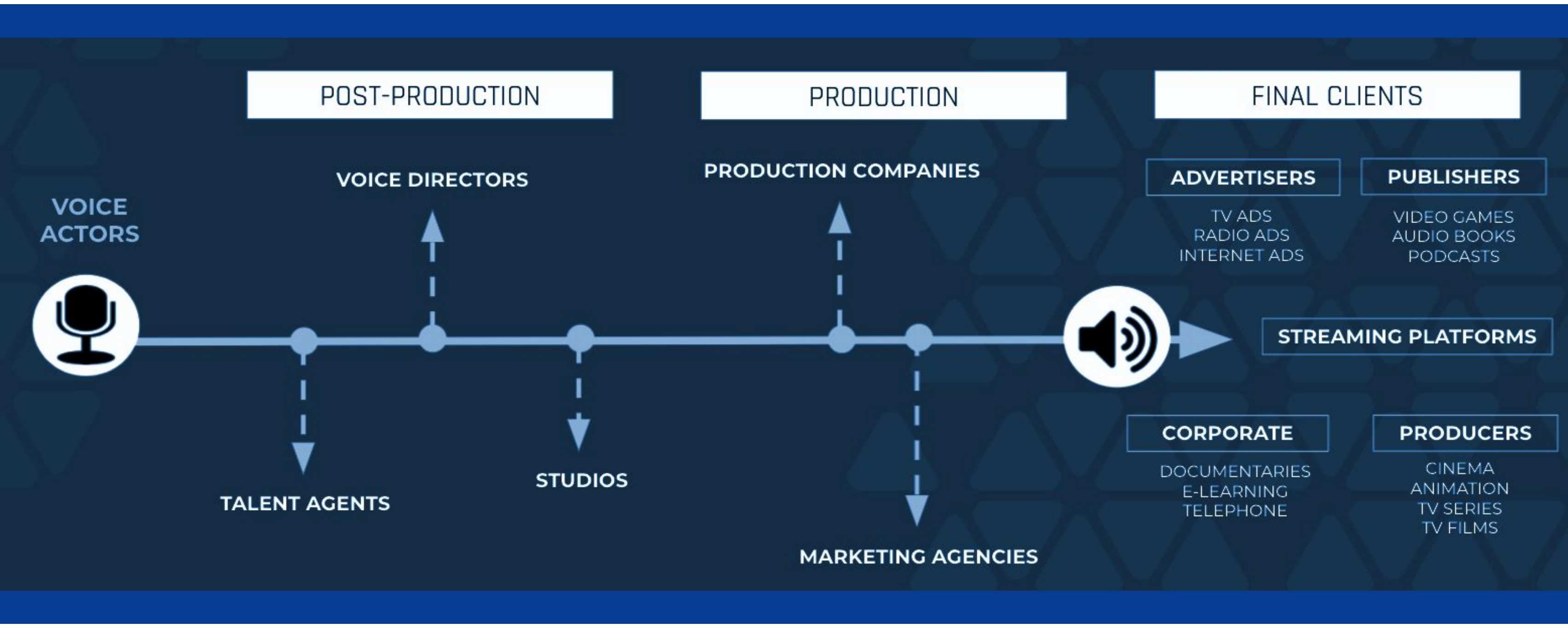
- Alert actors their data is being processed and shared
- Solicit and record actors' explicit opt-in consent of use - 100% independent of work contracts and NDAs
- Renew consent on a regular basis (2 years is standard for voice data)
- Provide access to personal data within 30 days of request
- Process modification and deletion requests within 30 days of request
- Secure the voice data
- Minimise data collection and processing
- Specify purpose and duration of processing
- Clearly communicate with whom the data will be shared

GDPR Risks
Casting Workflows

Data protection strategies tend to focus more on security concerns than privacy risks in localisation production workflows. Leading security and privacy assessors confirm that the majority of the industry’s data protection policies do not address voice data practices in production and that many current industry practices leave organisations open to non-compliance risks.

During the voice casting phase, high volumes of personal data are shared between numerous project stakeholders in a concentrated period of time to find the best voice actors for different characters and languages. When projects are voiced in several languages, the number of service providers increases and partner compliance becomes complex, if not impossible, to verify manually.

Workflows often involve sharing physical files via upload to ftps, private clouds, casting approval portals or via email. Data receivers sometimes conserve resources for future projects or inadvertently forget the personal data in email inboxes or on servers. In addition to sharing voice data with external project stakeholders directly involved in the casting process, actor details and voice recordings are also shared with multiple internal services (audio, marketing, sales, IT) for feedback and validation.



Tips for tightening up your voice data privacy

1. Your organisation contracts service providers to voice your games:

- Identify internal workflows that process personal data
- Define and implement service-specific GDPR compliance processes
- Require proof of voice data GDPR compliance from your voice service providers *and also for their outsourced service providers*
- Look closely at how your partners obtain actor consent - independent of contracts and NDAs?
- Prohibit personnel from receiving and sharing physical voice files. If this is not possible:
    - establish GDPR compliant internal workflows and train your personnel on the GDPR obligations
    - establish GDPR compliant workflows with external service providers
- If your teams save personal data received from service providers after completion of the casting phase see sections 3 & 4

2. Your organisation provides dubbing and voiceover services:

- If outsourcing projects to other service providers, require proof of their GDPR compliance *and also for their outsourced service providers*
- If you maintain a voice casting database see sections 3 & 4
- If you save personal data received from suppliers after completion of the casting phase see section 3
- Prohibit personnel from receiving and sharing physical voice files. If this is not possible:
    - establish GDPR compliant internal workflows and train your personnel on the GDPR obligations
    - establish GDPR compliant workflows with external stakeholders and inform the organisations with whom you share the data of their GDPR obligations

3. Your organisation maintains a voice casting database and wants to manage your voice data GDPR manually:

- Alert referenced talents that your organisation is processing their personal data
- Solicit and record actor’s explicit consent of use of their data - 100% independent of work contracts and NDAs
- Renew actor’s consent every 2 years
- Delete non-authorised samples within a determined time limit
- Process rectification and deletion requests within 30 days upon request
- Provide actors access to their personal data (samples included) within 30 days upon request
- Secure data with “need to access” permissions

4. Your organisation receives castings and/or maintains a casting database and wants to learn about tools that automate voice data GDPR obligations, provide workflow privacy safeguards and visibility of project privacy compliance:

Discover MEDIARTIS and our custom-developed tools that protect the entire supply chain.

Conclusion

GDPR is not only an EU issue and has far reaching impact and implications for Media & Entertainment companies with dubbing and voiceover activities. GDPR concerns organisations located anywhere in the world who create, deliver or receive dubbing or voiceover projects that include EU personal data and are shared with either EU or non-EU companies, and if projects include non-EU personal data and are delivered to EU companies.

The compliance of all service providers engages the final client's GDPR responsibility, just as the client's compliance engages the responsibility of the entire supply chain. If teams are sharing data externally, partners and clients should be informed of their GDPR obligations and their compliance should to be verified. Auditing partner compliance is crucial for ensuring privacy integrity and protecting your organisation and all project stakeholders.

Voice-data security is a fundamental GDPR obligation and organisations should ensure personal data risks are assessed and appropriately addressed with measured controls. Companies should ensure that data access is restricted to specific personnel and departments, that their network is secure and passwords are modified on a regular basis.

Actor databases require ongoing compliance management and often contain outdated personal data. GDPR requires organisations to minimize the data they process, and limit processing to only necessary and pertinent data. Non-compliant data should be deleted across all organisational supports. Companies must be able to justify the purpose and duration of processing.

Actors must be advised their data is being processed, and reminded on a regular basis. Processing consent must be collected 100% independent of work contracts and NDAs. Actors have the right to access their data, samples included, and request rectifications and deletion of data.

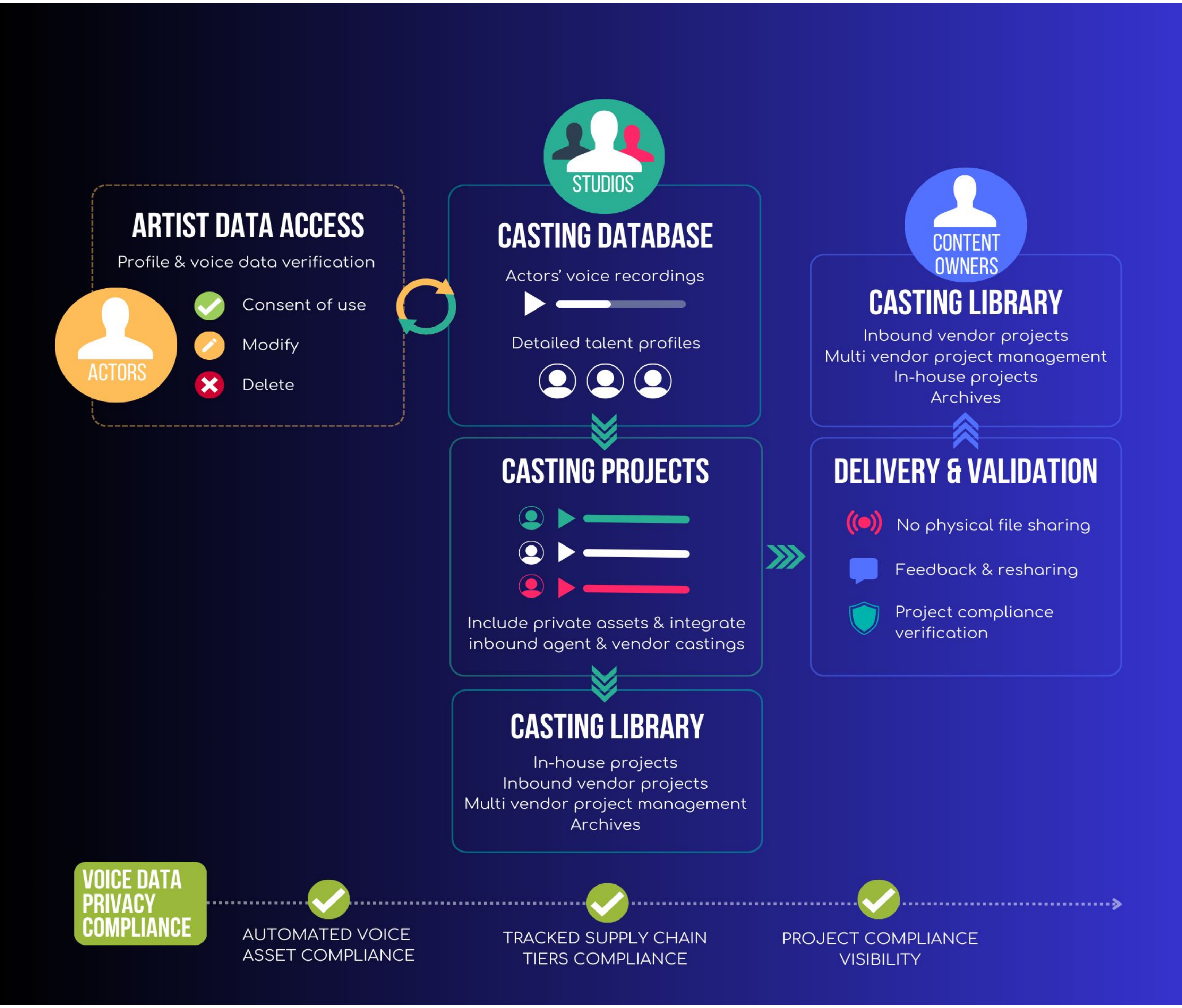
In order to mitigate asset and project GDPR non-compliance risks, service providers and content owners should reassess and adapt their voice data processing and sharing practices, and demand proof of compliance from partners.

mediartis

THE MEDIA & ENTERTAINMENT INDUSTRY'S FIRST VOICE PRIVACY COMPLIANCE SOLUTION

VOICE CASTING GDPR COMPLIANCE BY MEDIARTIS

Mediartis protects Media & Entertainment companies with dubbing and voiceover activities. It automates the initial and ongoing compliance of service providers' voice resources, offers project compliance safeguards and provides organisations with controls to verify inbound voice project privacy compliance.



ACTORS

ARTIST DATA ACCESS

Profile & voice data verification

- ✓ Consent of use
- ✎ Modify
- ✗ Delete

STUDIOS

CASTING DATABASE

Actors' voice recordings

Detailed talent profiles

CASTING PROJECTS

Include private assets & integrate inbound agent & vendor castings

CASTING LIBRARY

In-house projects
Inbound vendor projects
Multi vendor project management
Archives

CONTENT OWNERS

CASTING LIBRARY

Inbound vendor projects
Multi vendor project management
In-house projects
Archives

DELIVERY & VALIDATION

- No physical file sharing
- Feedback & resharing
- Project compliance verification

VOICE DATA PRIVACY COMPLIANCE

- ✓ AUTOMATED VOICE ASSET COMPLIANCE
- ✓ TRACKED SUPPLY CHAIN TIERS COMPLIANCE
- ✓ PROJECT COMPLIANCE VISIBILITY

WHAT THEY ARE SAYING:

BANDAI NAMCO

"We require full GDPR compliance from our suppliers and receive all of our voice castings via Mediartis. It's efficient and guarantees full compliance with GDPR."
Franck Genty - European Localization Supervisor, Bandai Namco

Keywords STUDIOS

"We chose Mediartis and their tools to help our recording studios become the most secure and efficient in terms of personal data protection and GDPR compliance."
Alessandra Vincenzi - Head of Audio Localization, Keywords Studios

convergent

"Mediartis' technology protects the entire ecosystem, from service providers to final clients with real-time compliance controls, even for multi-partner projects, and makes partner compliance easy to confirm."
Chris Johnson - CEO & Founder, Convergent Risks

The dog

"We chose Mediartis first and foremost for its privacy solution, but also for the simple and efficient tools for sharing secure castings with our clients. It has optimised our in-house casting workflows enormously."
Candice Smadja - Co-founder, The Dog

Mediartis for Publishers:
Voice GDPR Compliance Controls

API + cloud

Mediartis provides publishers **voice privacy compliance visibility of castings delivered by their service providers**. Our technology automates the initial and ongoing privacy compliance of vendor resources and tracks data from import through delivery, **no matter how many service provider tiers** contribute to projects.

Partner compliance visibility

Project privacy compliance is tracked and visible to your organization – no matter how many service providers contribute to a project.

Team collaboration

Reshare with project stakeholders, whose validation and feedback are visible only to you. Send invitations in 7 languages.

Project library

Manage all projects shared with you in one workspace. Archive completed projects for future reference.

Receive partner projects on streaming

Projects are user centric and shared projects are only visible to the receiver. Data is accessed on streaming, no physical sharing of personal data which would impose compliant processing of the data by the receiver.

Real-time review & validation

Your feedback, validation and modification requests are visible in real-time only to the person who shared the project with you.

Internal project management

Integrate shared partner resources into one master project. Verify homogeneity of roles across languages.

Project confidentiality

Different user permissions let you control project visibility and accessibility: create, read, update, delete.

Project security

Data is hosted on AWS in France and encrypted: import, at rest and network circulation.

Mediartis provides your service providers with these tools:

Automated initial & ongoing solicitation, recording, and renewal of actor explicit consent independent of work contracts | Renewal of explicit consent for modifications and when new voice media is added | Communication of purpose of processing and processing duration | Privacy reporting for compliance audits & vendor privacy assessments | Secure & isolated actor access to their data | Alerts when organisational actions are required | Automatic deletion of non-compliant data | Project compliance protections | Actor modification & deletion routing & recording | Real-time compliance status for every resource | Compliance verification of tier 2, 3, 4, etc. vendor resources

Mediartis for Service Providers: Automated Voice Privacy Compliance

API + cloud

Mediartis provides a simple and painless “**voice privacy compliance in a box**” solution for dubbing and voiceover service providers.

Our technology automates the initial and ongoing privacy compliance of voice casting resources and offers privacy-secure workflows that **protect the entire supply chain**.

We help your organisation respect legal personal data processing obligations, to verify your partners are respecting theirs, and to promote your data privacy compliance and preparedness.

Automated workflows

Mediartis solicits, records and renews explicit talent opt-in consent of use of their personal data, 100% independent of work contracts (legal requirement), routes modification & deletion requests, and deletes non-compliant data.

Partner Compliance Visibility

Resource compliance tracked from platform import through to end client project delivery, no matter how many service providers/agents contribute to a project.

Project Compliance

Safeguards ensure only compliant resources are added to projects. Compliance is tracked and visible – no matter how many service providers/agents contribute to a project.

Privacy Management Tools

Compliance dashboard provides a real-time overview of database privacy status. Weekly email organization task alerts.

Talent Access to Data

24/7 secure talent access to their personal data on streaming, media included (voice media watermarked for added security) to help you respect talent access rights and keep your resources updated.

Reporting

Annual compliance reporting. Vendor privacy assessment reporting available on demand.

User Controls

Different user permissions help you secure data & respect privacy obligations of “need to access”: create, read, update, delete.

Security

Data hosted on AWS France, encrypted at import, at rest and circulating on network. All media shared via controlled streamed access – no physical sharing of personal data.

GDPR COMPLIANCE BY MEDIARTIS

Mediartis for Service Providers: Tools for Your Resources + Projects

API + cloud

Add your own resources

Add streamed access to your own media in projects. Import from your Mediartis database or drag & drop from your computer.

Integrate partner resources

Reception vendor & agent castings on Mediartis. Verify their privacy compliance and add streamed access to their resources into your projects.

Deliver projects on streaming

Share branded and interactive projects in 7 languages. Shared versions confirm project data compliance even when multiple vendors have contributed.

Personalize projects

Personalize actor names and media titles for shared versions. Add comments to propositions. Only your logo is visible in the shared version, no matter how many vendors contribute to the project.

Stay updated

Visualize real-time project validations, reviews & modification requests. Keep track of who reviewed and when.

Assign external permissions

Attribute project validation & resharing permissions.

Collaborate with your team

Invite team members to work on projects. Control access and permissions: create, read, update, delete.

Quick management

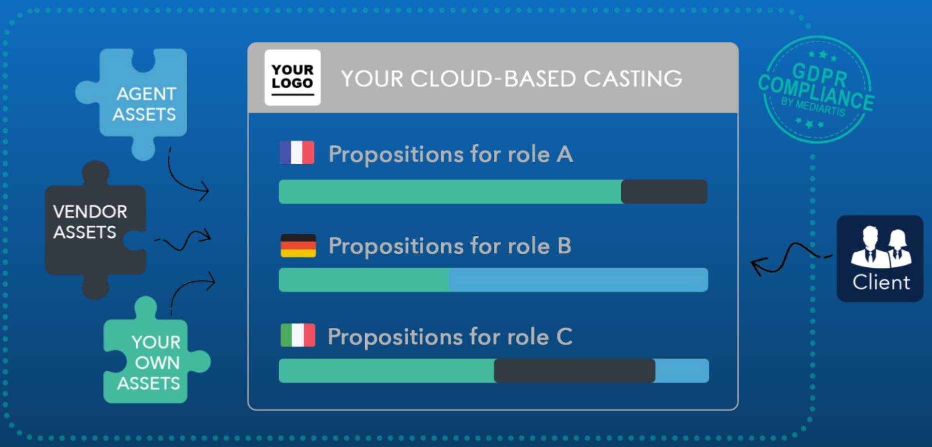
Pre-format roles through Excel import. Filter projects by validation status, creator, creation date, roles & reviews.

Secure your resources

Shared projects do not include physical files, only streamed access to your and your vendors' resources. Non-downloadable or transferable.

Multipartner Projects

- Receive castings that include resources from multiple vendors.
- Verify project privacy compliance.
- Seamlessly integrate streamed access to select resources into your project.
- Share one master casting with resources from multiple sources.
- Project compliance is visible to your end client.
- Only your logo is visible.



mediartis

CONTACT US

Do you have questions, need information or recommendations for privacy service providers? We can help.

Nicole Quilfen
Strategy & Partnerships at Mediartis

T: +33 (0)7 68 59 28 16 (CET)
E: nicole@mediartis.com
W: www.mediartis.com

The information contained in this document is for informational purposes only and does not replace legal advice. We strongly recommend that you consult with a DPO or legal consul for your specific situation and legal obligations.