PF3A

Privacy First Accurate Audio Analytics

Technical Guidelines

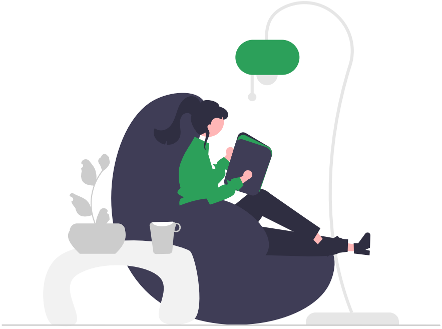
Version 1.0 draft 03

October 2024

PF3A.com

This document is a hybrid PDF file which embeds an editable ODF version.

Table of Contents



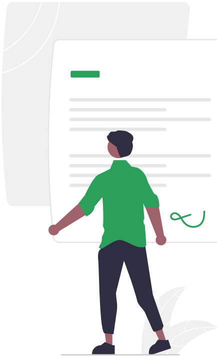
Legal Disclaimer

The PF3A (Privacy First Accurate Audio Analytics) technical guidelines are provided as a general resource and are not legal advice.

If you have any legal questions or concerns about implementing these guidelines, please consult your own legal counsel before proceeding.

The specific way these guidelines are applied may have legal implications, especially concerning privacy regulations like GDPR, depending on the country where they are implemented.

This document is provided "as is," without any warranty of any kind, express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, or non-infringement.



Contributing

The more voices, the better the outcome!

In the spirit of Podcasting 2.0, everyone is invited to bring their unique contributions to help shape PF3A (Privacy First Accurate Audio Analytics).

Just as podcasting thrives through diverse voices and open collaboration, PF3A is built on the belief that a broad range of ideas and perspectives makes the community stronger.

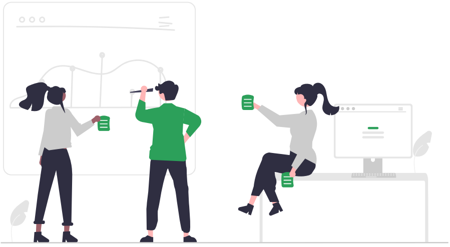
Whether you’re a developer, content creator, announcer, someone working in advertising, part of a radio network, working for a company that provides services for podcasters, part of a team that offers audience analytics to podcasting and/or radio networks, or a representative of a Data Protection Authority—or simply passionate about privacy and analytics—your input is invaluable.

Together, we can create guidelines that truly reflect the needs and values of the entire radio/podcasting community.

You can contact us at hello@pf3a.com to get involved or ask any questions.

Contributors

- Benjamin Bellamy, Ad Aures



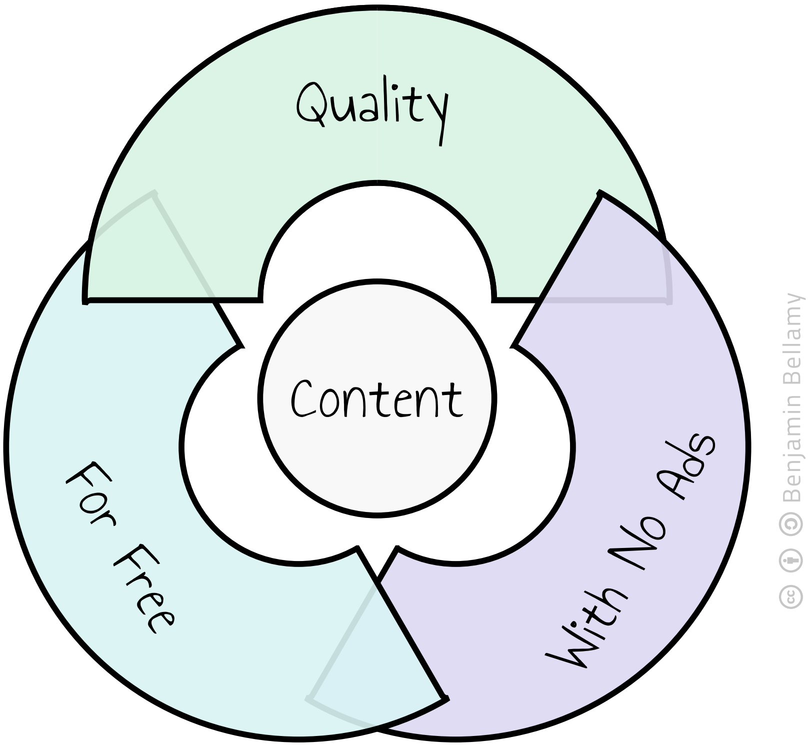
About Podcasting

When the internet surged in popularity during the 1990s, it carried a hopeful promise: quality content, freely accessible, and without ads.

But reality soon proved that sustaining quality content requires a trade-off.

In a fair and sustainable ecosystem, you can only have two out of three options:

- quality content for free (with ads),
- quality content without ads (not for free),
- or free content without ads (but not quality).



Make a choice: You can only have two.

Many digital platforms have built closed ecosystems, or "silos," to enable easy ad-based or subscription-based monetization within controlled environments.

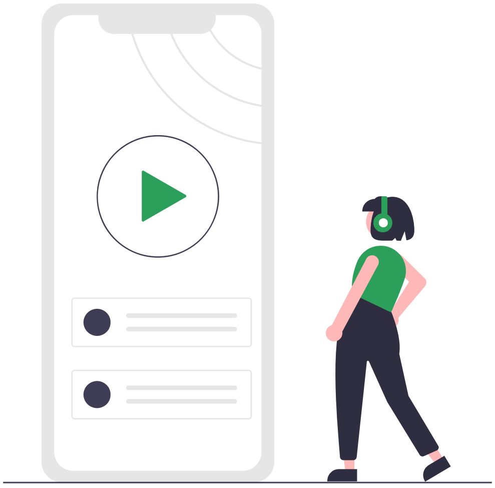
However, podcasting has charted a unique course.

Built on decentralized technology from before the Web 2.0 era, podcasting has resisted centralization, allowing podcasters to choose where they host content (e.g., Blubrry, Buzzsprout, Castopod…) and listeners to choose their preferred listening platforms (e.g., Apple Podcasts, Spotify, Podcast Addict, AntennaPod, Anytime Podcast Player).

This openness supports a wide diversity of voices and creativity, free from the content constraints of algorithm-driven silos.

Yet, this heterogeneous and richly varied ecosystem comes at a cost: implementing standardized features, such as audience analytics and monetization, across so many different platforms and providers is complex.

The ultimate goal of this document is to ease these difficulties by proposing a privacy-first, accurate analytics system that any platform can implement, fostering a vibrant and sustainable podcasting ecosystem for creators, listeners, and advertisers alike.



About GDPR

The General Data Protection Regulation (GDPR) was the original motivation for creating these guidelines, as it sets strict rules on handling personal data for European citizens.

Understanding GDPR's principles and requirements provides essential context for this document and ensures that our approach to audio analytics aligns with these legal obligations.

Additionally, other regulations worldwide, such as the California Consumer Privacy Act (CCPA) in the United States and Lei Geral de Proteção de Dados (LGPD) in Brazil, similarly emphasize data privacy and user rights.

Together, these regulations guide our commitment to protecting user data across diverse legal environments.

GDPR essentials

The **General Data Protection Regulation** (GDPR) was enacted on 14 April 2016 and applied on 25 May 2018, replacing the 1995 Data Protection Directive.

GDPR applies specifically to all personal data and requires compliance from:

- all **European companies**,
- any service dealing with **European citizens**,
- and any service handling users **in Europe**.

It enforces services to provide users with the **Right to Access**, enabling them to access, correct, or delete their data.

Non-compliance can result in penalties up to €20 million or 4% of an organization's annual global turnover.

Lawful Purposes

When processing personal data under GDPR, as a service provider, **you must carefully choose the lawful purpose(s)** that genuinely apply to the service you provide.

This choice isn't about convenience; it's about matching your **data practices** to one of GDPR's six lawful purposes in a way that aligns with the actual nature of the service and the user's expectations.

Under GDPR, users have the right to refuse data processing based on legitimate interest or user consent.

Article 5 states that personal data must be processed **lawfully**, **fairly**, and **transparently**.

Article 6 outlines six lawful purposes for processing:

- Three common ones:
  - **Contractual obligations** with the user where data is essential to provide the service (**no user confirmation needed**)

    Example: When a user signs up for a paid service, storing their payment information is necessary to fulfill the contract, allowing the service to process transactions and provide access.
  - **Legitimate interests** of the platform (**opt-out**)

    Example: A platform may track user activity to improve its recommendation algorithms. Users should have the option to opt out.
  - **User consent** (explicit user agreement, **opt-in**)

    Example: A newsletter service asks users for explicit consent to receive promotional emails. Only those who opt in will be added to the mailing list.
- And three less common ones:
  - **Legal obligations** (no user confirmation needed)

    Example: A financial institution may be required to store customer data for a set period to comply with anti-money laundering laws.

  - **Vital interests** (no user confirmation needed)

    Example: In a medical emergency, a hospital may process personal data to provide urgent treatment to an unconscious patient, protecting their life and health.

  - **Public interest** (no user confirmation needed)

    Example: A government agency may collect citizen data to conduct a national census, aiming to support public planning and resource allocation.

Under GDPR, the **purpose limitation principle** restricts how data can be used based on its original collection purpose. If your web server logs data like IP addresses and user agents to meet legal obligations, such as maintaining security or complying with regulatory requirements, that data cannot later be repurposed for other objectives—like marketing analytics—without explicit user consent.

Using data beyond its initial lawful purpose would constitute a **diversion of purpose** and violate GDPR, as each new purpose requires an appropriate lawful basis and, in cases like marketing, typically necessitates user consent.

> 💡 If no personal data is involved, **GDPR does not apply**.

Personally Identifiable Information (PII)

Under GDPR, **personal data** is any information that **can be linked to an identifiable person**, directly or indirectly.

Although GDPR doesn't offer a fixed list of what constitutes personal data, context determines whether specific information can be associated with an individual.

For example, a user's language is generally **not** personally identifiable information (PII) since it's shared by many people, making identification impossible on that basis alone.

> 💡 A **user's IP address**, when used to listen to a podcast, qualifies as **PII**.

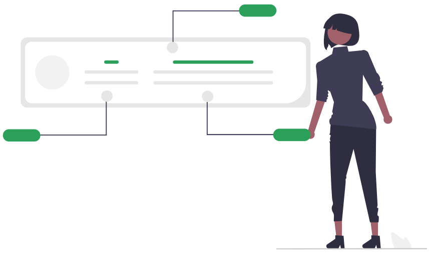
Pairing it with additional information, like the User Agent (software used), further increases identifiability.

Even a **hashed** combination of IP address and User Agent (using algorithms like SHA1 or MD5) **is still treated as PII** because it remains traceable back to the individual.

The IP address of a proxy server used by thousands of people within a company can be considered PII, as the proxy administrator may still trace specific user actions within that shared network.

The IP address of a **server** is generally **not considered personal data**, as it is tied to the server itself rather than to any individual.

A notable CJEU decision, Breyer (CJEU - C-582/14), clarified that even a dynamic IP address can be classified as personal data if an entity (such as a German state agency) has the means to identify a person through supplementary information, further underscoring how the context around data determines its classification under GDPR.



About Audio Analytics

Audience analytics for audio content have been a staple of the media landscape for decades, initially relying on listener polls and surveys to gauge engagement. With the advent of the internet, audience measurement has become automated, allowing data to be collected more efficiently, affordably, and accurately.

Audience measurement serves two primary purposes:

- Supporting **monetization** through advertisements
- Improving **content quality** by identifying what listeners actually engage with.

This document focuses on podcasting but is also relevant to online radio and other forms of audio delivered via the internet—whether by download, progressive download, or streaming.

Multiple specifications exist for audio audience measurement, with the **IAB Tech Lab**'s “Podcast Measurement Technical Guidelines” (often called “IABv2”) being one of the most widely recognized.

The initial version was released in September 2016, with the latest, version 2.2, published in May 2024, publicly available for free at: IAB Tech Lab Podcast Measurement Guidelines.

While anyone can implement these guidelines, IABv2.2 now requires that organizations seeking compliance undergo a formal certification process to be listed on the IAB Tech Lab website, tying official compliance to certification.

As a freely available public resource, the IAB guidelines are widely adopted across the podcasting ecosystem. Naturally, they were created with advertising in mind—after all, the IAB stands for “Interactive Advertising Bureau”.

When IABv2 was initially published in 2017, GDPR (enforced in 2018) had yet to be fully integrated into industry standards, and it was impossible for IABv2 to anticipate its requirements entirely.

In practice, IABv2 does not fully align with GDPR standards; although it doesn’t blatantly violate GDPR, it does fall short of compliance.

The IABv2 guidelines aim to standardize counting methods and provide advertisers with confidence that their ads have been heard by real listeners.

This framework is built around five key steps: Apply filtering logic, Apply file threshold logic, Identify and aggregate uniques, Generate metrics, Audit the process (feedback loop)

These steps help ensure:

- The exclusion of non-user downloads, such as those from bots, crawlers, or testing environments
- Deduplication by filtering out repeated downloads within a 24-hour window
- Exclusion of downloads that represent less than one minute of listening (as ads are generally within the first minute)

However, IABv2 relies on identifying users by combining "**User IP**" and "**User Agent**" which qualifies as personally identifiable information.

> 💡 GDPR’s lawful purpose for storing such information, even for 24 hours, requires either user consent or legitimate interest with an option to opt-out—currently, the podcast ecosystem lacks a standardized method for collecting this consent.

About PF3A

The goals of this new specification are twofold:

- To ensure compliance with GDPR and protect personally identifiable information
- To offer a technical solution for achieving more accurate analytics while adhering to GDPR

The approach is simple:

- Avoid using personally identifiable information wherever possible, which removes the need for user consent.
- If personally identifiable information is necessary, obtain explicit user consent.

PF3A offers **two complementary approaches** to audio analytics, each designed to meet different needs and implementation requirements:

- **PF3A/S** is a **server-side** solution that integrates with existing infrastructures to provide comprehensive data on audience interactions.

  It is relatively easy to deploy, as it can be implemented on web or prefix servers without requiring changes to listening applications.

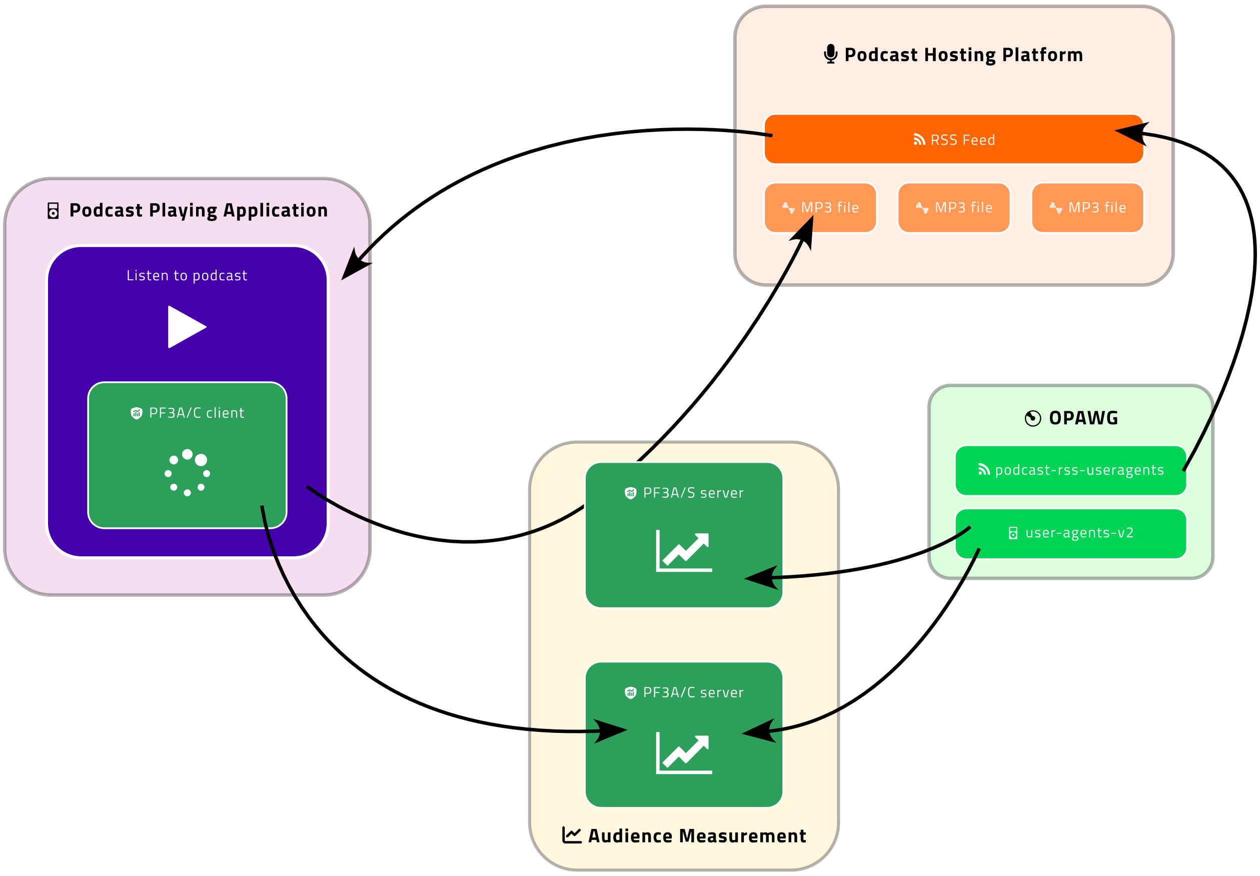
  PF3A/S is ideal for capturing broad engagement metrics across a large user base, making it compatible with current analytics setups.

- **PF3A/C** is a **client-side** approach focused on accuracy, particularly for capturing Listening Through Rate (LTR).

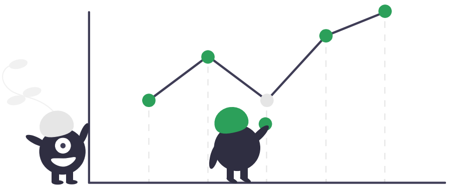
  This solution requires integration within listening applications, which allows for more precise insights into listener behavior.

By sending periodic beacons from the user's device, PF3A/C provides detailed data on how much of the content is listened to, which is especially useful for content refinement and effective monetization.

Together, PF3A/S and PF3A/C can be used independently or in tandem to deliver a powerful, privacy-focused analytics solution that balances compatibility and accuracy.



A PF3A simplified schematic



Server Side Analytics: PF3A/S

PF3A/S provides **server-side analytics** similar to IABv2, but with a strong emphasis on privacy. PF3A/S can be implemented either directly on a web server that serves audio files or through a prefix server, such as OP3.

In the case of a prefix server, it receives an HTTP request, processes it, and then redirects the listener to the actual audio file server with a 30x HTTPS redirection.

> 💡 Importantly, PF3A/S never stores the user's IP address or User Agent, focusing solely on working with anonymous metrics.

PF3A/S is designed to prioritize user privacy and does not include mechanisms that require storing personally identifiable information (PII).

Unlike other analytics standards, PF3A/S does not implement deduplication processes or a 1-minute minimum filter, both of which traditionally rely on identifying individual users.

This approach ensures that PF3A/S analytics remain privacy-friendly by focusing on aggregated data without tracking or identifying specific users.

PF3A/S Workflow

Participant: Podcast Hosting Server or Podcast Prefix Server

1. **Filter** Out Non-User IP Addresses

   Remove IPs associated with bots, crawlers, and non-human traffic. This can be done using resources like ipcat to filter out known non-user IP ranges.

2. **Ignore** Incomplete Requests

   Disregard requests that are clearly incomplete, such as those with a minimal byte range request (`Range: 0-1`), which typically indicate non-user activity or partial probing.

3. **Identify** Application, Browser, Device, and PF3A/C Capability

Use OPAWG/user-agents-v2 to convert the user agent string into specific details about the application (app or browser), device type, and whether PF3A/C capabilities are supported by the listening application.

4. **Identify** the RSS Podcast Platform. Use OPAWG/podcast-rss-useragents to identify the RSS podcast platform if the hosting platform utilizes it and has appended `?_from=[rss-ua-slug]` to enclosure URLs. This information provides a clearer understanding of the platform generating requests.

5. **Geolocation** of IP Address

   Convert the IP address to a specific country or region to understand where the download request originates.

6. Track Downloaded **Amount**

   For each download request:

   - If the file is fully downloaded, count it as 1 complete download.

   - If only a portion is downloaded, store the download ratio as:

   ```
   (downloaded byte range size / total file size)
   ```

     to reflect partial engagement.

7. **Store** Key Data Points

   Log each event with the following attributes:

   - Date and Time of request

   - Podcast GUID and Episode GUID for unique identification

   - Country/Region based on IP geolocation

   - Application/Browser type

   - Device Type

   - PF3A/C-enabled status (indicating whether the app is capable of PF3A/C tracking)

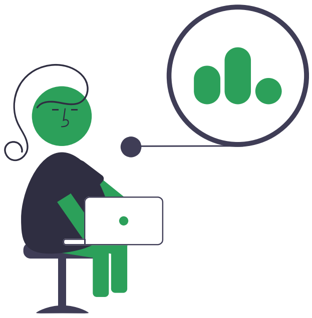
   - Amount Downloaded (either 1 for full download or the calculated partial ratio)

Note on PF3A/C-Enabled Status

This feature will be added to the User-Agents-v2 repository.

PF3A/C-enabled applications will indicate this capability in their user agent strings, allowing detection here.

The purpose of tracking PF3A/C-enabled status is to gauge the proportion of downloads from applications that are likely to play the audio files, enhancing analytics on actual listener engagement.



Client Side Analytics: PF3A/C

PF3A/C provides **client-side analytics**, comparable to analytics systems used by platforms like Spotify or Apple but designed to be **interoperable**, similar to NPR's now-defunct RAD project.

PF3A/C works by sending a beacon signal from the listener's application to one or more analytics servers every minute, offering precise measurement of the Listening Through Rate (LTR).

Additionally, PF3A/C can be extended to collect user data if the listening application gathers **user consent**. With consent, this data is then sent securely to the analytics server, ensuring that user privacy remains a priority while enabling more detailed insights if authorized by the listener.

The Listening Through Rate (LTR) is a valuable metric that serves both key purposes of audio analytics: enhancing content quality and supporting monetization. For content creators, LTR reveals how much of an episode listeners actually engage with, helping them understand which segments capture attention and where listeners may drop off.

This insight allows for more targeted content improvements. For advertisers and sponsors, LTR provides confidence that their messages are reaching engaged audiences, as higher LTR indicates listeners are staying tuned throughout the episode.

> 💡 LTR does not require any personally identifiable information (PII); it only relies on data about how the content is consumed, not information about the user.

PF3A/C architecture

The architecture and workflow for **PF3A/C** involve three main components, each playing a critical role in providing accurate, privacy-compliant audience analytics:

1. **PF3A/C-Compatible Podcast Playing Application**

   > **Participant**: Podcast Playing Application

   - A compatible listening app integrates PF3A/C functionality to track listening behavior and sends a beacon every time a full minute of the podcast has been played.

     This beacon is sent only when the listener has completed 100% of a minute, ensuring precise Listening Through Rate (LTR) data.

   - The timing of the beacons is set as follows: the first minute starts at 0:00 and ends at 0:59, the second minute from 1:00 to 1:59, and so on.

     Partial minutes (e.g., when only part of a minute is played) are not recorded or sent.

   - For each completed minute, the app sends a REST message to the collection server with the following data:

     - **Date and Time** of the completed minute
     - **Podcast GUID** for identifying the podcast
     - **Episode GUID** for identifying the specific episode
     - **Country/Region** of the listener (if available)
     - **Application Name** for the player used
     - **Device Type** (e.g., mobile, tablet, desktop)
     - **Minute Number** indicating which specific minute of the episode was completed.

- REST message example:

  ```
  {
    "date_time": "2023-10-25T14:23:00Z",
    "podcast_guid": "fb205f6b-5962-508f-9e0a-771468a4c1ec",
    "episode_guid": "cb5f914e-c0a6-4cd8-bd77-aefb34a0b854",
    "country": "France",
    region": "Occitanie",
    "application_name": "Anytime Podcast Player",
    "device_type": "Mobile",
    "minute_number": 36
  }
  ```

2. **PF3A/C Data Collection Server**

> **Participant**: Podcast Hosting Server or Podcast Prefix Server

- A designated server endpoint receives and stores the data sent by compatible PF3A/C applications.

  This server is responsible for:

  - Receiving the REST message from the app for each completed minute.

  - Storing the data in a structured format to allow analysis of listening patterns and minute-by-minute audience engagement.

- REST Server answers:

  - **200** Success: Indicates that the beacon message was successfully received and processed. This confirms that the listening data (such as the completed minute) has been stored without issues.

  - **404** Podcast/Episode Unknown: Sent if the podcast and/or episode GUID provided does not match any podcast in the server's database. This response informs the application that the specified podcast and/or episode is not recognized.

  - **403** Forbidden: Indicates that the application does not have the required permissions to access the endpoint. This might occur if the app or the user is not authorized to submit data to this server.

  - **429** Too Many Requests: Returned when the application has exceeded the request rate limit, signaling it should slow down and retry after a specified time.

3. **Podcasting 2.0 `<podcast:pf3a>` Tag**

> **Participant**: Podcast Hosting Server

- The `<podcast:pf3a>` tag in the podcast's RSS feed communicates to PF3A/C-enabled apps where to send beacon data.

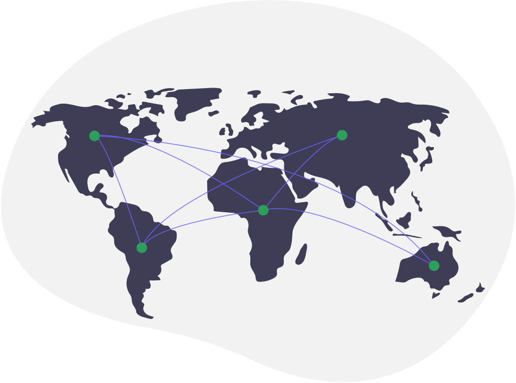
  This tag specifies the server endpoint URL(s) for data collection.

  Multiple URLs can be included, allowing data to be sent to multiple collection servers if needed.

- Example of the `<podcast:pf3a>` tag:

```
<podcast:pf3a url="https://server.tld/pf3a" />
```

This architecture enables the **PF3A/C** system to collect detailed, minute-by-minute listening data, enhancing analytics accuracy without compromising user privacy.



Glossary

Audience Analytics: Data analysis focused on understanding listener behaviors and engagement with podcast content.

Bot: Automated software that performs tasks, like indexing content, often used by search engines and web analytics.

CCPA (California Consumer Privacy Act): California law granting residents rights over personal data held by businesses.

CJEU (Court of Justice of the European Union): The highest court in the EU for interpreting EU law, ensuring its uniform application across member states, and ruling on issues related to EU regulations, including GDPR compliance and data protection cases.

Closed Silo: A restricted environment where content is locked within a single platform, limiting external access and sharing.

File Download: A method of saving audio files directly from a server to a listener's device.

FLOSS (Free/Libre and Open Source Software): Software that is free to use, modify, and distribute, supporting transparency and collaboration.

GDPR (General Data Protection Regulation): A comprehensive EU regulation governing data protection and privacy.

Hash function: A cryptographic function that converts data, such as an IP address or User Agent, into a fixed-size string of characters. While commonly used for data integrity and anonymization, hashing does not eliminate the personal nature of data—hashed personally identifiable information (PII) is still considered PII because it remains uniquely linked to an individual. For example, hashing "John Doe" using the MD5 algorithm produces the output `4c2a904bafba06591225113ad17b5cec`, which is still identifiable if someone knows the hash function and input. Mathematically, a hash function is an injective (one-way) function, meaning each input maps to a unique output but is difficult to reverse, although a given hash can only be reliably recreated with the same original input.

IAB (Interactive Advertising Bureau): An organization that develops industry standards for digital advertising and media.

IAB TechLab: A subgroup of IAB that creates technical standards, including for podcast analytics and measurement.

IP Address: A unique identifier assigned to each device connected to the internet, often used for location-based analytics.

LGDP (Lei Geral de Proteção de Dados Pessoais): Brazil's data protection law that ensures privacy rights for individuals.

LTR (Listening Through Rate): A metric measuring how much of an episode listeners typically complete.

OPAWG (Open Podcast Analytics Working Group): An organization focused on developing transparent and open analytics standards for podcasts.

OP3 (Open Podcast Prefix Project): An open-source / open-data initiative that enables standardized tracking of podcast downloads and engagement by adding a tracking prefix to podcast URLs, supporting transparent and consistent audience measurement across platforms.

Open Ecosystem: A system where content is freely distributed across various platforms and accessible to everyone, fostering interoperability.

PF3A/S: A server-side solution for podcast analytics that provides comprehensive download data without storing personally identifiable information (PII), compatible with existing web and prefix servers.

PF3A/C: A client-side solution for podcast analytics that tracks minute-by-minute listening behavior via beacons from compatible apps, offering precise listening metrics while respecting user privacy.

PII (Personally Identifiable Information): Any data that can directly or indirectly identify an individual, such as an IP address, email address, or a combination of information like IP address and User Agent.

Podcast Hosting Software: Services or platforms that store and distribute podcast audio files and metadata.

Podcast Index: A comprehensive database of podcast episodes and shows that helps make content discoverable.

Podcast Hosting Platform: A service that stores and distributes podcast audio files and metadata, enabling podcasters to publish episodes and syndicate them via RSS feeds (such as Blubrry, Buzzsprout, Captivate, Castopod...).

Podcast Listening Application: An app where users can browse, subscribe to, and listen to podcasts (such as Apple Podcasts, Spotify, Pocket Casts, Podcast Addict, AntennaPod...).

Podcast Prefix Solution: A tracking technology that adds a URL prefix to podcast episode links, allowing for standardized measurement of download and engagement data without altering the content itself.

Podcast (common definition): A digital audio series that users can subscribe to, download and listen to on demand.

Podcast (real definition): A media enclosure, typically audio or video, embedded within an RSS feed, allowing users to subscribe and automatically receive new episodes in any compatible podcast player.

Podcasting 2.0: A movement aimed at improving podcasting through open standards and community-driven innovation. Podcasting 2.0 solutions, applications and services can be found on NewPodcastApps.com.

Podcasting: The process of creating and distributing podcasts to an audience through audio content.

Podcast-rss-useragents (by OPAWG): A comprehensive list of user agents specifically used by apps and services to query RSS feeds for podcasts, which enables more accurate tagging of audio files and improves podcast consumption statistics. This list allows for better identification of podcast apps by supplementing audio user agents (e.g., by appending ?_from=[rss-ua-slug] to audio requests), especially useful when default user agents (e.g., AppleCoreMedia) cannot be modified.

Progressive Download: A technique where an audio file is downloaded gradually, allowing playback as data is received.

Proxy Server: An intermediary server that routes requests from multiple users to external resources, masking individual IP addresses but still allowing certain administrators to trace specific user actions within the shared network.

RAD (Remote Audio Data by NPR): A now-defunct podcast analytics technology developed by NPR that allows podcasters to track listener behavior, such as playbacks and skips, by embedding tags in audio files, helping content creators gain insights into audience engagement.

REST (Representational State Transfer): An architectural style for designing networked applications that allows different systems to communicate via HTTP requests, typically using standard operations like GET, POST, PUT, and DELETE. In PF3A/C, REST is used for sending analytics data from podcast playing applications to collection servers in a structured, standardized format (e.g., JSON).

RSS (Really Simple Syndication): A web feed format that allows automatic distribution of updates, essential for podcast delivery.

Streaming: Real-time audio delivery where content plays continuously without needing to fully download first.

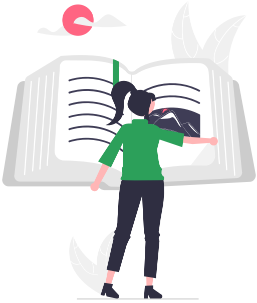
Unique Download: A download instance that is counted once per user or device, avoiding duplication in analytics.

Unique User: An individual listener identified in analytics, often using IP or device data.

User Agent: Information about the device and application used to access content, like a web browser or podcast app.

User-Agents-v2 (by OPAWG): A comprehensive, open-source collection of widely compatible regular expression patterns developed by the Open Podcast Analytics Working Group to identify and analyze podcast player user agents.

Web Crawler: A bot specifically designed to scan and index content across the internet.



Licenses

This document is published by Benjamin Bellamy @ Ad Aures under the Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license:

- You are free to share it (copy and redistribute the material in any medium or format) and adapt it (remix, transform, and build upon the material) for any purpose, even commercially.
- You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

The PF3A logo “🛡” is released by Benjamin Bellamy @ Ad Aures under the Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.
It may be downloaded from the Podcast Font: https://podcastfont.com/#pf3a

This document was written with LibreOffice which is licensed under the Mozilla Public License v2.0.: https://www.libreoffice.org/download/license/

Schematic made with Inkscape, which is licensed inder the GNU General Public License

All drawings are from unDraw by Katerina Limpitsouni and are distributed under a free license.

The “Podcast Font”, “Inter”, “Titilium Web” and “Annie Use Your Telescope” fonts used in this document are licensed under the SIL Open Font License.

“Roboto Mono” font is licensed under the Apache License, Version 2.0 license.

> 🎙 “GO PODCASTING!”