Data Management: FAQs

In this Section

At Pico, we take fans and customers' data very seriously.
This is why we take the highest industry standards on making sure we capture the data in a way that will allow you to comply with the regulations when using the data, but also to make sure that data is stored properly - with no risks.

Below you'd find the most frequently asked questions and answers to topics we find important on our data usage and protection policies.

Data security is one of our core responsibilities as we process and manage data for big organizations.
We have a strict policy when it comes to how and who manages the data, these are its highlights:

- Data is encrypted in transit with HTTPS/TLS protocols.
- The database is encrypted on rest.
- Identifiable information is always stored encrypted.
- Our logs will never include identifiable data nor usernames or passwords.
- We back up our data at least once a day.
- Only authorized personnel are able to access the database.

For more information, please contact our CIO on gdpr@picogp.com

Pico captures data that is shared during conversations and activations on the digital channels we operate in and depends on the data points you ask fans to share.
This data could include unique channel id (i.e. User's Facebook Id), full name, gender, timezone, email address, phone number, zip code, merchandise preferences, favorite players, attendance habits, ticket preferences and more.

We don't store personal data like Social Security numbers, medical records, financial records, payments records, etc.

The team is the sole owner of the data. Pico acts as a processor only.

Data is stored on our dedicated servers provided by Amazon Web Services (AWS).
The data centers are located in Europe, both in Ireland and Germany.
All of our data centers are fully encrypted, and all of the communication is encrypted as well.

During users' first interaction with us on any channel, they are asked to provide consent to the team's and Pico's Terms of Use and Privacy Policy.
These documents contain a clear, simple to understand language, that explains how the data is captured, stored and used.

Whenever a user shares contact details (i.e. email address) we ask for explicit consent to use it for future marketing communication.
Every step in the consent process is being stored with an exact timestamp that allows us to track and build an exact timeline for when users provided their consent, whether they read the terms of use and when they provided a double-opt-in consent.

In our backend, the data is stored in encrypted servers.
The access to the data is available only to authorized personnel and backups are made at least once a day.

There are multiple ways:

- The data could be used from the Pico Platform's CRM section for segmenting, filtering, sending push messages, etc.
- The data could be exported to a spreadsheet and imported to your internal platforms.
- We can connect directly to your CRM or Data Warehouse and feed your internal platforms with data automatically.

It is important to understand that data is valuable but it's much more vital to understand that end results are the key here - to make the data easily actionable.

Looking at the end results, the data in Pico is structured in an easy-to-use way. A simple filter applied to the fans database, according to the required target group, is all that's needed, to push an offer or send a message to, through one of the open communication channels with them.
i.e. If the team wants to push a ticket offer to fans, they would like to create a specific target group which includes fans who are not season ticket holders, who did attend games during the season and did show interest in last-minute tickets

In order to allow this filtering process, our data is structured with personal information columns (name, gender, location, email, age, etc.) and insights columns. The insights columns are basically a yes/no indicator to whether the fan is part of this group indicator.

i.e. If a fan asked to buy tickets on FB messenger, and then, while participating in an activation on Twitter clicked an offer to buy the merchandise we will have a column named "*asked_about_tickets*" with the value TRUE and A column named "intersted_in_merchandise" with the value TRUE.

Under the hood, when we are building the target groups, we will send the ticket offer push message only to fans who have the value TRUE in "asked_about_tickets".

Depending on the team's wish:
We could connect to their internal dataset directly through an API and feed it with information, or we could export data dumps to be imported periodically (every activation, week or month).
This integration is planned with the data team to make sure column names match and that no duplications of data exist.

We have ongoing relationships with Fanatics and TicketMaster. This means that we are redirecting fans from an activation or conversation to buy merchandise/tickets and we receive event notifications from these platforms for every fan-performed action. This could include actions like items they were looking at, items purchased, quantity and prices paid. Since each fan has a unique identity in our platform, and we know they were redirected from a Pico activation to these platforms, we can connect these actions to a unique fan’s profile.

FYI, currently, Fanatics and TicketMaster feeds us with data for every team. But, if the team wants to track purchases of sponsored activations (let’s say pizza purchase at Papa Johns) - if the sponsored website allows us to add a tracking pixel - we would have the same mechanism there.