Reply from Tamoco, London, UK.

With a total global reach of about 200 million devices and around 700 apps that use your SDK, how do you ensure the owners are aware of about how their data is collected and used?

Tamoco ensures that each user gives consent at an app level before data is collected. We put the user in control of their data and provide a robust three-tier opt-out process which is as follows.

The user can revoke location collection in the following ways:

- Turning off location services at the OS level - this can be done for specific apps or across the entire device. This will stop data being collected or sent to Tamoco immediately.
- Users can opt out with the app directly
- The user can reset their advertising ID, or they can select the setting 'do not track' - this will ensure that all data sent to Tamoco is unidentifiable and will return a string of zeroes. How our system deals will 'do not track' requests is based on the official Digital Advertising Alliance and the NAI guidelines.

Ultimately Tamoco respects any request from the OS respecting the users wish to opt-out of location sharing.

As you offer data in a feed updated virtually in real-time, does this present any specific challenges from a privacy perspective?

Our privacy, consent and opt-out processes are not affected by the time between data collection and data processing. Whether we provide data in near real-time or with a significant delay, the same process and protections are applied. These are explained further below.

With data offered in raw lat-long format how do you ensure individual users can not be identified and tracked?

In some cases, we may track a device on an individual level - but we do not provide this to a third party, without the required contractual protections in place.

These follow the core principles of GDPR Article 5(1), specifically (c) making sure any data provided is "limited to what is necessary in relation to the purposes".

In all cases where we provide sensitive data, but particularly where we supply lat-long, associated with an individual's device, we have specific contractual obligations in place that prohibit the processing of sensitive information. (We follow the definition given in the GDPR).