Reply from Sygic a.s. Bratislava, Slovakia.

*** With data on tens of millions of users, how do you ensure how do you ensure the owners are aware of about how their data is collected and used?**
It is our obligation to inform users of Sygic apps and/or services about how we process their data pursuant to Articles 13 and 14 of the GDPR. We provide this information in our privacy policy available at https://www.sygic.com/sk/company/privacy-policy. This privacy is also available inside our applications, in app stores, at our e-shop website and generally at every data or consent collection point. When we request specific consent from end-users, we refer to this privacy policy but we may also provide further / additional information. For example, we share advertisement IDs with our partners based on a data subject consent which provides additional information, such as a list of such partners, which is subject to change. Currently, we collect such consents only on Android devices.

*** When the location data contains detailed, continuous latlong-information, how do you ensure individual users can not be identified and tracked based on their patterns of movement?**
If we look at the whole dataset, we consider data processed about our users personal data meaning that the identification of individual users is possible. However, we share anonymous/aggregated data with our business partners and we also share personal data of our users based on their consent (for example advertisement IDs). In the first scenario, we have undergone a thorough analysis of whether such information can be regarded an information about identifiable person pursuant to the recital 26 of the GDPR.

The data in question only reveals that a certain device transfers from point A to point B at certain time and speed. Each connection of points A and B is hashed with Session ID which technically cannot be reverse-tracked with any other information we store about our users. This is ensured technically by setting of our product servers. It also ensured by the non-persistent character of the Session ID so that no two sessions can be linked together via the same Session ID. We have assessed whether patters of movement could be used to track or identify a certain repeating point and subsequently an individual. We have made this assessment in light of the test prescribed in recital 26 of the GDPR:

"To determine whether a natural person is identifiable, account should be taken of ***all the means reasonably likely to be used****, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person,* ***account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*** *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

Given the circumstances in which we share such data and objective factors we came to conclusion that in this scenario such means are not reasonably likely to be used. Therefore, we do not consider this data personal. One has to understand that definition of personal data does not come down to whether identification is hypothetically or theoretically possible, but down to whether such identification is reasonably likely given the circumstances of the case. Of course our position is different when such data is combined with advertising IDs – then we regard such dataset personal data and request consent of the user before sharing.