There have been rumours about this for some time now, particularly in the US media. Specifically, there is the claim that certain IP phones made in China record conversations on behalf of the Chinese government.

External providers such as Alibaba are automatically provided with all the data and IP phones are generally not secured. Does that also apply to Europe?

To find out more, we decided to ask one of our specialists to comment on the most important allegations made. Snom's Luca Livraga is someone who knows his stuff. He is the team leader of international technical support at Snom and has worked for the company since 2014.

Snom: *Mr Livraga, some news circulating in the US have highlighted some really serious security breaches. Is it then conceivable that Snom phones are also forwarding information to public authorities or even to the German government?*

Luca Livraga: "Snom phones conform in every respect with the provisions of the European Data Protection Act. This also means that no one, not even the government of a European country, can eavesdrop on even a single phone without a prior court order or approval by various committees, for instance, in the case of anti-terrorism investigations. The only thing that is definitely recorded by Snom phones is the globally agreed data for tracing an emergency call, a legal obligation. In this case, the IP address of the phone can then be traced back to its location (address, maybe even floor) from the legitimate place."

Snom: *In the scenarios described, you can go even further and claim that the phones made in China are not protected by any security certificates and all data is automatically secured on the PC of the user. What about Snom?*

Luca Livraga: "Firstly, we have always worked with certificates, because they represent a real hurdle for any attempt at unauthorised use. Also, the accusation that all data is automatically stored on a PC, does not apply to us. Nevertheless, professionals can create a 'track' of the connection data for one or several

conversations, for instance when troubleshooting. However, only with the express approval of the other person – and the recoded data is of no use to anyone here."

Snom: *We have one last question: can Snom phones pass on the call data or even whole conversations to third-party providers such as online retailers?*

Luca Livraga: "Again, a definite no. Snom phones can be serviced remotely. Here, settings such as names, times or call groups can be adjusted and changed by the trusted dealer after prior approval and consent. But even these interventions are subject to the data protection act. As a result, the dealer is also legally obliged here to make all personal information of the user anonymous. At Snom, we even make sure all personal data is deleted beforehand on phones sent in for repairs, so as to prevent any possible misuse. We have also decided to store all data to be processed on exclusively German servers, the country which currently has the strictest rules in the field of data protection. We are really doing everything possible to ensure our IP end-devices cannot be misused."

Snom: *These are really reassuring answers. So you can assure us that all Snom phones are secure?*

Luca Livraga: "If you stick to our specifications, then certainly. But this also includes the maintenance of the end devices, such as the regular updates, the use of secure passwords and also the use of a telephone system that is subject to the same priorities. Otherwise, it's like locking the car, but leaving the hood open! But seriously, Snom has a strong feeling of commitment to its customers, and this includes very high standards in areas such as software, hardware and security."

Snom: *Thank you for the interview.*