Reliable even in a crisis: highest level of protection for sensitive personal data

UNSER HEER

The Austrian federal army, as a strategic reserve of the Republic of Austria, is deployed for "the provision of assistance during natural disasters" (Military Law 2001) as well as for its core military missions.

During the weeks-long coronavirus lockdown, there was a lot of talk about hygiene rules, social distancing, protective equipment and the obligation to wear a mask in public places. Behind the scenes, however, the authorities and the crisis team had additional issues to resolve. The federal army has undertaken many types of activities in the fight against the virus. For example, soldiers from the Tyrol military command provided support to the government to check cars and people at border crossings. In doing so, the soldiers collected health-related data from people entering the country; taking temperatures to check for fever was their most important task. This personal health data had to be transmitted to a central server, so the requirement was for a traceable and – especially– secure way to share the health-related data of people arriving in Austria between all the authorities and institutions involved.

Data protection requirements within cross-organisational civil and military collaboration during the COVID-19 deployment

At the start of the army's deployment, this data was shared by hand, email, Dropbox or WhatsApp as there was no alternative available to the participating organisations. As well as being slow and complicated, this method is not secure and does not comply with European data protection laws. So the requirement was for a traceable and – especially– secure way to share the health-related data of people arriving in Austria between all the authorities and institutions involved.

In order to avoid this time-consuming and risky approach for the rest of the deployment duration, the Tyrol military command looked for an IT solution that would improve collaboration between the "blue light" organisations, including emergency services (e.g. the Red Cross), customs, police and firefighters; critical infrastructure companies; and the ÖBH (Österreichisches Bundesheer, Austrian Federal Army).

Challenges of different technical and human requirements

As the organisations involved all had different IT technologies and areas of focus, they decided that interlinking the various IT systems would not help them achieve their goal and was not the right solution for cost reasons.

The requirement was for a way of sharing information that was fast, secure and especially user-friendly for the permanent and temporary soldiers as well as the civil staff and voluntary workers from the blue light organisations. Securing data meant that the information would be consistently protected at every stage and that it could not be sent to third parties or opened from "outside', i.e. decrypted.

In addition, the IT system had to be quick to learn and be aligned as far as possible with familiar functions from IT apps in order to minimise the duration and cost of training.

"Thanks to the solution's ease of use, for me as an administrator as well as for the users, it is fast and straightforward to set up and use – and that's particularly important in crisis situations. The solution is exceptionally well-suited to civil/military use due to its maximum data security and complete traceability."

Administrator of the Tyrol Military Command