Positioning on the use of Windows 10 and the importance of encrypted communication

100th Data Protection Conference

When using the Enterprise Edition of Windows 10, companies and authorities can prevent the transmission of personal telemetry data if they use the "Security" telemetry level. This was determined by the conference of the independent data protection supervisory authorities of the federal and state governments (DSK) in a decision at their 100th meeting on November 25th and 26th.

The Enterprise Edition of Windows 10 was tested in various scenarios in the IT laboratory of the State Commissioner for Data Protection (LfD) Lower Saxony. It turned out that under certain conditions (application of the "Windows Restricted Traffic Limited Functionality Baseline", telemetry level "Security") no telemetry data was transmitted to Microsoft. “With these findings, we have taken an important step so that those responsible can use Windows 10 in compliance with data protection,” says Barbara Thiel, the Lower Saxony State Commissioner for Data Protection. "I am therefore very satisfied that the data protection conference was able to agree on a common line here."

However, this study only represents a snapshot because Windows 10 is constantly being developed, according to the DSK's decision. In addition, questions about data transmission are still unanswered, which is why those responsible cannot finally be relieved of their obligation to check and provide evidence of the data protection-compliant use of Windows 10. You would have to ensure with contractual, technical or organizational measures that it can be proven that no transmission of telemetry data to Microsoft takes place. This is especially true when using the Pro and Home editions, where the telemetry level cannot currently be set to Security. According to the data protection conference, Windows 10 should offer the option of deactivating telemetry data processing through configuration in all editions offered. In order to achieve this, the data protection authorities will continue to seek talks with Microsoft.

Encryption is an essential prerequisite for digitization

The data protection conference also very clearly rejected the demands of the EU Council to allow security authorities and secret services to access the content of encrypted communication. The resolution "For the protection of confidential communication through secure end-to-end encryption - stop proposals of the Council of the European Union" emphasized that secure and trustworthy encryption is an essential prerequisite for resilient digitization in business and administration.

"If the proposals of the Council of the European Union were to be implemented, secure end-to-end encryption would be

undermined and necessary trust destroyed," according to the resolution of the data protection conference. The desired goal, namely to improve the investigative possibilities of security authorities, is not achieved in a sustainable and effective way. At the same time, the use of effective end-to-end encryption would be made virtually impossible for less technically savvy citizens.

"Such back doors contradict the basic idea of data protection through technology design," says Lower Saxony's state data protection officer Thiel. "In addition, our security authorities already have very far-reaching powers, such as source telecommunications surveillance, which are hardly ever used."

More information

Decision of the DSK: telemetry functions and data protection when using Windows 10 Enterprise

Laboratory report of the LfD Lower Saxony: Windows 10 telemetry test with user interaction

Resolution of the DSK: For the protection of confidential communication through secure end-to-end encryption - stop proposals of the Council of the European Union

Press release on the 100th DSK