Wie schützt man Datenträger gemäß Datenschutz-Grundverordnung?

Smartphones, Tablets, SD-Karten, USB-Sticks, externe Laufwerke und Laptops enthalten Datenspeicher in Form von Flash-Bausteinen oder magnetischen Festplatten. Werden auf diesen mobilen Speichermedien oder auch auf CDs und DVDs **personenbezogene Daten** gespeichert, so müssen diese gemäß Art. 5 Abs. 1 lit. f Datenschutz-Grundverordnung (DS-GVO) durch geeignete technische und organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust abgesichert werden. Gemäß Art. 32 Abs. 1 lit. a DS-GVO kann dies gegebenenfalls unter anderem durch **Verschlüsselung** gewährleistet werden. Auch eine **sichere Verwahrung** an einem unzugänglichen bzw. besonders geschützten Ort wäre als organisatorische Maßnahme denkbar. Um eine effektive Verschlüsselung zu gewährleisten, sind auf verschiedenen mobilen Speichermedien unterschiedliche technische Maßnahmen anwendbar.

Für Smartphones und Tablets mit dem Betriebssystem Android steht ab der Version 5 (Lollipop) eine Geräteverschlüsselung zur Verfügung (zu finden unter Sicherheitseinstellungen). Hierbei wird vom Betriebssystem der gesamte Datenspeicher des Gerätes verschlüsselt. Der Speicher kann dann ohne den Sperrcode, der gleichzeitig als Gerätesperre und Bildschirmsperre dient, nicht von Unbefugten ausgelesen werden, falls das Gerät verloren geht.

Bei Smartphones und Tablets mit dem Betriebssystem iOS der Firma Apple existiert die Geräteverschlüsselung ab der Version 7. Damit die Verschlüsselung zum Tragen kommt, muss ebenfalls eine sogenannte Code-Sperre eingerichtet werden. Dadurch wird wie bei Android bei jedem Einschaltvorgang des Gerätes ein Passwort abgefragt.

Im Übrigen ermöglicht die bloße SIM-Sperre keinen Schutz vor unbefugten Zugriff auf den Speicher und die Daten, sondern verhindert nur, dass die SIM-Karte für Telefonate genutzt werden kann.

Auch bei Laptops ist eine komplette Geräteverschlüsselung möglich. Im Betriebssystem Windows (bei Version 7 nur in der Ausführung Ultimate oder Enterprise, bei Version 8 und 10 in der Ausführung Professional und Enterprise) kann die Festplatte mit Hilfe des integrierten *Bitlockers* verschlüsselt werden. Steht keine integrierte Verschlüsselungsmethode zur Verfügung, kann das freie und quelloffene *VeraCrypt* eine Verschlüsselung ermöglichen. Bei VeraCrypt ist neben der Verschlüsselung der gesamten Betriebssystem-Festplatte auch die Verschlüsselung eines Datei-Containers möglich. Hierbei wird ein zuvor definierter Speicherbereich verschlüsselt, in welchem dann die zu schützenden Daten abgelegt werden können.

Bei externen Festplatten und USB-Sticks können ebenfalls Bitlocker oder VeraCrypt angewendet werden, indem jeweils das gesamte Medium verschlüsselt oder ein verschlüsselter Container darauf angelegt wird.

Hilfsweise können zu transportierende Dateien auch vorab (z. B. bei CDs und DVDs) in ZIP-Archiven verschlüsselt werden. Dabei muss über ein Archivierungsprogramm, wie z. B. WinZIP, 7-Zip, WinRAR o. ä., ein Passwort für das zu erstellende Archiv vergeben werden, wonach dieses automatisch verschlüsselt erstellt wird. Auch Büro-Software-Produkte wie Microsoft Office, Libre Office oder Adobe Acrobat unterstützen die passwortgeschützte Speicherung einzelner Dokumente.

Bei allen Verschlüsselungsverfahren, die ein Passwort bzw. einen Sperrcode benötigen, gilt: Je länger und komplexer das Passwort, desto sicherer die Verschlüsselung!

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstr. 9, 39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
www.datenschutz.sachsen-anhalt.de

SACHSEN-ANHALT
Landesbeauftragter für den Datenschutz