Daten löschen bevor Laptops verkauft werden – auch das ist Datenschutz!

Die Zeit online berichtete am 6. Juli 2019 über einen Datenschutzvorfall. Die Bundeswehr verkaufte einen Laptop, und auf diesen befanden sich noch Daten. Was sind die möglichen Folgen?

Der Sachverhalt

Nach der Pressemeldung, die in der Zeit online am 6. Juli 2019 veröffentlicht wurde, verkaufte die deutsche Bundeswehr einen Laptop, auf dem sich noch vertrauliche Daten befanden.

Die Daten betrafen eine als «**Verschlusssache - Nur für den Dienstgebrauch**» eingestufte **Bedienungsanleitung für einen Raketenwerfer**.

Ein bayerischer Oberförster kaufte den Laptop im Jahr 2018 über Ebay, und hat bei der Bundeswehr seinen „Fund“ im März 2019 gemeldet.

ABO SHOP AKADEMIE JOBS MEHR ▾ E-PAPER AUDIO APPS ARCHIV ANMELDEN

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen Digital Campus ▾ Arbeit Entdecken Sport ZEITmagazin Podcasts mehr ▾ Z+

Verteidigung

Bundeswehr verkauft Laptop mit vertraulichen Daten

6. Juli 2019, 13:56 Uhr / Quelle: dpa

Berlin (dpa) - Die Bundeswehr soll einen gebrauchten Laptop verkauft haben, auf dem noch vertrauliche Informationen waren. Dabei handele es sich um die als «Verschlusssache - Nur für den Dienstgebrauch» eingestufte Bedienungsanleitung für einen Raketenwerfer. Das berichtet die «Süddeutsche Zeitung». Anscheinend sei die Festplatte vor dem Verkauf nicht gelöscht worden. Laut Verteidigungsministerium könnten aus der Beschreibung des Raketenwerfers «keine kritischen Erkenntnisse abgeleitet werden». Ein oberbayerischer Förster hatte den Laptop 2018 bei Ebay gekauft seinen Fund im März gemeldet.

Hinweis

Diese Meldung ist Teil des automatisierten Nachrichten-Feeds der Deutschen Presse-Agentur (dpa). Die dpa ist eine Nachrichtenagentur, die Medien mit selbst recherchierten und formulierten Meldungen zu aktuellen Ereignissen beliefert.

Verhinderung des Zugriffs durch unbefugte Personen

Wenn ein Verantwortlicher **Geräte, auf denen personenbezogene Daten gespeichert sind, außer Haus gibt**, zB zur Reparatur oder dauerhaft (Verkauf), dann hat er dafür zu sorgen, dass diese Daten **nicht in die Hände von unbefugten Personen kommen**.

Art 5 Abs 1 lit f DSGVO normiert das **Prinzip der Integrität und Vertraulichkeit** und schreibt vor, dass personenbezogene Daten „*in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem*

Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Folgen des Vertraulichkeitsverlustes

Ein **Verstoß gegen das Prinzip der Vertraulichkeit**, dh eine Offenlegung der personenbezogenen Daten an unbefugte Personen, und zwar dadurch, dass der Verantwortliche keine angemessenen **technischen und organisatorischen Maßnahmen iSd Art 32 DSGVO** trifft, bewirkt nicht nur

- eine **Verpflichtung, den Datenschutzvorfall zu melden** (der Behörde / den betroffenen Personen), sondern fällt auch unter
- die **Strafsanktion** des Art 83 Abs 5 lit a DSGVO (bis zu 4 % des Umsatzes bzw. EUR 20 Mio) bzw. kann auch
- **Schadenersatzverpflichtungen** gem. Art 82 DSGVO auslösen.

Data Breach durch unberechtigten Zugriff – Meldepflicht

Hat eine Person Zugriff auf personenbezogene Daten, die dazu nicht berechtigt ist, liegt ein **Datenschutzvorfall (Data Breach)** vor, der uU der Aufsichtsbehörde (Datenschutzbehörde) gem. Art 33 DSGVO (sofern ein Risiko für die betroffenen Personen nicht ausgeschlossen ist) und/oder auch den betroffenen Personen gem. Art 34 DSGVO (bei hohem Risiko für die betroffenen Personen).

Weitergabe von Geräten mit Daten

Werden Geräte aus dem Gebrauch der Organisation **ausgeschieden**, dh entweder verschrottet oder uU verkauft oder auf anderem Weg **weitergegeben** (zB an Dienstnehmer), dann ist darauf zu achten, dass **sämtliche personenbezogenen Daten** (aus Sicht des Datenschutzes) und

auch **sonstige betriebliche Daten** (aus Sicht des Geheimnisschutzes) in einer Art und Weise **gelöscht bzw. vernichtet** werden, die eine Wiederherstellung unmöglich macht.

Vorgaben für IT-Sicherheit / Datenschutz bei Reparatur oder Wartung von Geräten mit personenbezogenen Daten

In Pkt. 8.3.2. (**Betriebsmittelverwaltung**) des Österreichischen Informationssicherheitshandbuches (abrufbar unter www.sicherheitshandbuch.gv.at) wird vorgeschlagen, dass **Datenträger mechanisch zerstört** werden, wenn **Geräte außer Betrieb genommen**, oder im Rahmen einer Reparatur getauscht werden:

> ***Außerbetriebnahme, Reparaturtausch:***
>
> ***Datenträger**, die schutzwürdige Daten enthalten und außer Betrieb genommen oder im Zuge einer Reparatur ausgetauscht werden sollen, sind **mechanisch zu zerstören** (vgl. dazu auch ÖNORM S 2109 Akten- und Datenvernichtung sowie 14.6 Wartung).*

Dies sollte in einer **Anweisung** oder **Richtlinie für die Verwaltung von Betriebsmitteln** auch schriftlich in der eigenen Organisation dokumentiert werden, und den beteiligten Personen nachweislich zur Kenntnis gebracht werden.

Werden Geräte zur **Reparatur** oder **Wartung außer Haus** gegeben, dann ist darauf zu achten, dass **nur befugte Personen** diese tatsächlich erhalten, und **Zugriff auf die Daten** haben, sofern dieser Zugriff notwendig ist.

Es kann sich bei dieser Tätigkeit um eine **Auftragsverarbeitung** handeln (zB wenn eine Datenbank wiederhergestellt werden soll), oder auch um einen **(einfachen) Reparaturauftrag**, wenn zB das Display eines Mobiltelefons getauscht werden soll, wobei dann darauf zu achten ist, dass eine **Vertraulichkeitsvereinbarung** abgeschlossen wird.