MOBILE DATENTRÄGER

RICHTLINIE

Version 1.0 • 08/2023

Richtlinie Mobile Datenträger

Warum diese Richtlinie?

Mobile Datenträger sind hinsichtlich des Datenschutzes und der Datensicherheit besonders gefährdet und unterliegen einer besonderen Sorgfaltspflicht. Diese Richtlinie trägt dazu bei, die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen auf mobilen Datenträgern sicherzustellen.

Geltungsbereich

Diese Richtlinie regelt den Umgang mobiler Datenträger und gilt für alle Mitarbeiter und in allen Standorten unseres Unternehmens bei der Verwendung dieser Geräte. Alle Beschäftigten sind verpflichtet, die in dieser Richtlinie festgelegten Pflichten und Vorgaben einzuhalten.

Definition

Mobile Datenträger werden wie folgt definiert: Es sind leicht zu transportierende Geräte, die der Speicherung von Daten dienen. Hierzu gehören unter anderem externe Festplatten, Speicherkarten, USB-Sticks oder optische Speichermedien.

Grundsätze der Nutzung von mobilen Datenträgern

Mobile Datenträger können aufgrund ihrer Mobilität schnell verloren gehen oder gestohlen werden. Dadurch können unbefugte Dritte in Besitz von Daten unseres Unternehmens, unserer Kunden oder Geschäftspartner kommen. Es sind folgende Vorsichtsmaßnahmen zu berücksichtigen:

RICHTLINIE

Einschränkung der Nutzung

Nur Beschäftigte, die aufgrund ihrer Tätigkeit bei unserem Unternehmen zwingend auf die Nutzung von mobilen Datenträgern angewiesen sind, dürfen diese Geräte benutzen.

Ausschließlichkeit

Es dürfen ausschließlich die von unserem Unternehmen bereitgestellten mobilen Datenträger verwendet werden. Die Verwendung eigener Datenträger ist den Mitarbeitenden verboten.

Beschäftigte dürfen ein mobiles Speichergerät keinesfalls Dritten überlassen. Dieses Verbot schließt Familienangehörige mit ein.

Mitarbeitende dürfen keinesfalls eigenständig Software auf den überlassenen Datenträgern installieren.

Verschlüsselung

Alle Daten auf den mobilen Datenträgern sind grundsätzlich verschlüsselt zu speichern. Die Verschlüsselung ist bei personenbezogenen oder firmeninternen Daten zwingend notwendig, sollte aber aus Sicherheit generell erfolgen.

Die Verschlüsselung muss mit einem von der IT freigegebenen Tool erfolgen. Der Schlüssel muss bei der IT-Abteilung hinterlegt werden. Eine Entschlüsselung der Daten muss für unser Unternehmen jederzeit möglich sein.

Eine unverschlüsselte Speicherung von Daten ist nicht erlaubt. In Ausnahmefällen kann sie vom Vorgesetzten genehmigt werden. Die Genehmigung hat in Schriftform (z. B. per Mail) zu erfolgen.

Private Daten

Es ist verboten, private Daten gemeinsam mit Daten unseres Unternehmens auf einem mobilen Datenträger zu speichern.

Speicherdauer

Mobile Speicher sind ausschließlich für die temporäre Speicherung von Daten zugelassen. Sollen Daten von mobilen Datenträgern langfristig gespeichert werden, sind sie, sofern sie bislang nicht vorhanden sind, unverzüglich auf die hierfür vorgesehenen Server unseres Unternehmens zu übertragen.

Virenschutz

Mitarbeitende unseres Unternehmens haben darauf zu achten, dass die mobilen Datenträger, die sie nutzen, regelmäßig mit einem aktuellen Anti-Viren-Programm auf Malware geprüft werden. Dies gilt insbesondere, bevor Daten auf unsere Server übertragen werden sollen.

Besonderer Schutz

Die Beschäftigten muss jederzeit gewährleisten, dass Unbefugte nicht in den Besitz der Daten gelangen können. Daher ist eine besonders sorgfältige und sichere Verwahrung des mobilen Datenträgers notwendig, um diesen vor Diebstahl und Verlust zu schützen.

Grundsätzlich gilt:
Lassen Sie das Gerät
NIE unbeaufsichtigt.

RICHTLINIE

Mobile Datenträger von Dritten

Es ist verboten, mobile Datenträger von Dritten, speziell Datenträger, die gefunden werden, an unsere IT-Systeme anzuschließen! Oft werden solche Datenträger bewusst platziert, um unsre Systeme zu infiltrieren und Malware einzuschleusen.

Gefundene Datenträger sind der IT-Abteilung bzw. dem Administrator auszuhändigen.

Schließen Sie NIE einen mobilen Datenträger, den Sie gefunden haben, an Ihren Computer an.

Sie könnten das gesamte Firmennetzwerk infizieren!

Diebstahl und Verlust

Der Diebstahl oder Verlust eines mobilen Daten-Speichers muss UMGEHEND der IT-Abteilung oder dem Vorgesetzten gemeldet werden! **Auch am Wochenende oder im Urlaub.**

In vielen Fällen besteht eine gesetzliche Informationspflicht gegenüber Aufsichtsbehörden und Betroffenen. Eine verspätete Meldung kann Bußgelder in erheblicher Höhe nach sich ziehen.

Sonstiges

Der Mitarbeiter kann sich bei Fragen der Umsetzung an die IT-Abteilung wenden.

RICHTLINIE

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

RICHTLINIE