Newsletter 09/2025

FOX Group

Schon ein Berechtigungskonzept erstellt?

Ein funktionierendes Berechtigungskonzept soll regeln, wer auf Daten zugreifen darf. Wer es nach dem Need-to-know-Prinzip vornimmt, sorgt dafür, dass Mitarbeitenden- und Kundendaten nicht von Unberechtigten eingesehen werden können. Insbesondere bei sensiblen Daten ist der Schutz der Daten gesetzlich gefordert.

Fachleute diskutieren, ob das Fehlen eines Berechtigungskonzepts bereits eine Datenschutzverletzung bedeute und somit meldepflichtig sei, weil es sich zumindest um eine mögliche Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit handele.

Ohne einen Standpunkt einzunehmen, kann Folgendes gesagt werden: Fehlt ein intaktes Berechtigungskonzept, ist dies ein Verstoß gegen Art. 5 Abs. 1 (f) sowie Art. 32 DSGVO und erhöht das Risiko eines möglichen Bußgeldrisikos für das Unternehmen.

Mehr dazu: DSGVO Art. 5 Abs. 1. f, Art. 6 Abs. 1 und Art. 32 DSGVO

Wieder das Passwort vergessen?

In der Vergangenheit wurden Mitarbeitende dazu angehalten an einem vorgegebenen Datum oder Zeitpunkt das aufwändig und reiflich überlegte, mit Daten aus dem Umfeld oder Privatleben erdachte Zugangspasswort zum Firmenendgerät zu ändern. Empfehlungen über Kombinationsformen und Passwortlängen sowie Verbote, das schon verwendete Passwort zu nutzen, führten zu abstrusen Passwortkreationen. Am Ende schrieben Mitarbeitende ihre Passwörter auf Haftzettel an die Monitore oder klebten diese unter die Tastatur, um nicht erneut bei der EDV-Abteilung unangenehm als Passwortverweigerung aufzufallen.

Findige Mitarbeitende probieren sich aus und machen sich auf die Suche nach Schlupflöchern, um den Zeitaufwand beim Passwort zu verkürzen. Unternehmen begegnen diesem Phänomen mit der Zurverfügungstellung von Passwort-Managern inklusive Passwortgeneratoren und folgen Empfehlungen Passwörter aktiv alle sechs bis zwölf Monate zu tauschen, was bereits eine Erleichterung bedeutet. Aber ein regelmäßiges Wechseln von Passwörtern führt erfahrungsgemäß dazu, dass zunehmend schwächere Passwörter verwendet werden.

Schaut man in die Norm für Informationssicherheit bzw. befragt man die Experten vom BSI-Grundschutz, so wird darauf hingewiesen, zusätzlich zu den starken Passwörtern eine Zwei-Faktor-Authentisierung zu aktivieren oder ganz auf Passkeys umzusteigen, eine einmalig und mit wenigen Klicks in den Sicherheitseinstellungen der Webseite oder App Möglichkeit sich zu authentifizieren, also weg von Passwörtern.

Einige Endgeräte ermöglichen die Authentifizierung per Fingerabdruck oder per Gesichtsscan. Aus Sicht des Datenschutzes wird jedoch dringend davon abgeraten. Die Aufsichtsbehörde für Datenschutz in Baden-Württemberg hat hierfür eine umfangreiche Auflistung von Empfehlungen zusammengetragen.

Kurz zusammengefasst: Nutzung von sehr starken Passwörtern, diese nur dann ändern, wenn es Anzeichen dafür gibt, dass diese in fremde Hände gelangt sind.

Empfehlungen: https://www.baden-wuerttemberg.datenschutz.de/hinweise-zum-umgang-mit-passwoertern/

Ab dem 12. September gilt der EU-Data Act

Der Data Act ist eine EU-Verordnung (2023/2854), die am 12. September 2025 in Kraft getreten ist und einen fairen Zugang und Nutzung von Daten in der Europäischen Union regelt. Sein Hauptziel ist es, die Verfügbarkeit von Daten aus vernetzten Produkten und Diensten zu erhöhen, die Datennutzung für Innovationen zu fördern und den Wechsel zwischen Cloud-Diensten zu erleichtern. Der Data Act ergänzt die DSGVO, senkt aber nicht das Datenschutzniveau insbesondere bei personenbezogenen Daten. Zusätzlich stärkt er die Rechte von Nutzern an Daten, die von ihren Geräten gesammelt werden, fördert Innovationen und erleichtert den Wechsel zwischen Cloud-Anbietern, indem er die Abhängigkeit von großen Datenanbietern aufbricht.

Im Klartext heißt es: durch den Data Act sollen:

- Nutzer einen leichten und kostenfreien Zugang zu Daten erhalten, die sie selbst erzeugen, etwa von vernetzten Geräten wie Autos oder Smart-Home-Geräten.
- bessere Bedingungen für den Datenaustausch geschaffen werden, indem sie verhindert, dass einzelne Akteure eine zu starke Kontrolle über die Daten erlangen.
- Durch die erhöhte Verfügbarkeit und den verbesserten Zugang zu Daten soll datengestützte Innovation gefördert werden.
- Es soll Unternehmen einfacher gemacht werden, zwischen verschiedenen Cloud- oder Edge-Diensten zu wechseln.
- Unternehmen müssen Nutzern den Zugang zu ihren Daten ermöglichen und dürfen die Weitergabe von Daten durch Nutzer an Dritte nicht vertraglich verhindern.

Für Unternehmen gilt ab sofort: Nutzer müssen umfassend über die von den Produkten und Diensten generierten Daten informiert werden. Hierzu zählt auch die Art und Weisen, welche Datenmenge und wie oft Daten gesammelt werden.

https://www.bmv.de/SharedDocs/DE/Anlage/DG/Digitales/eu-data-act-deutsche-fassung-22-12-23.pdf

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer