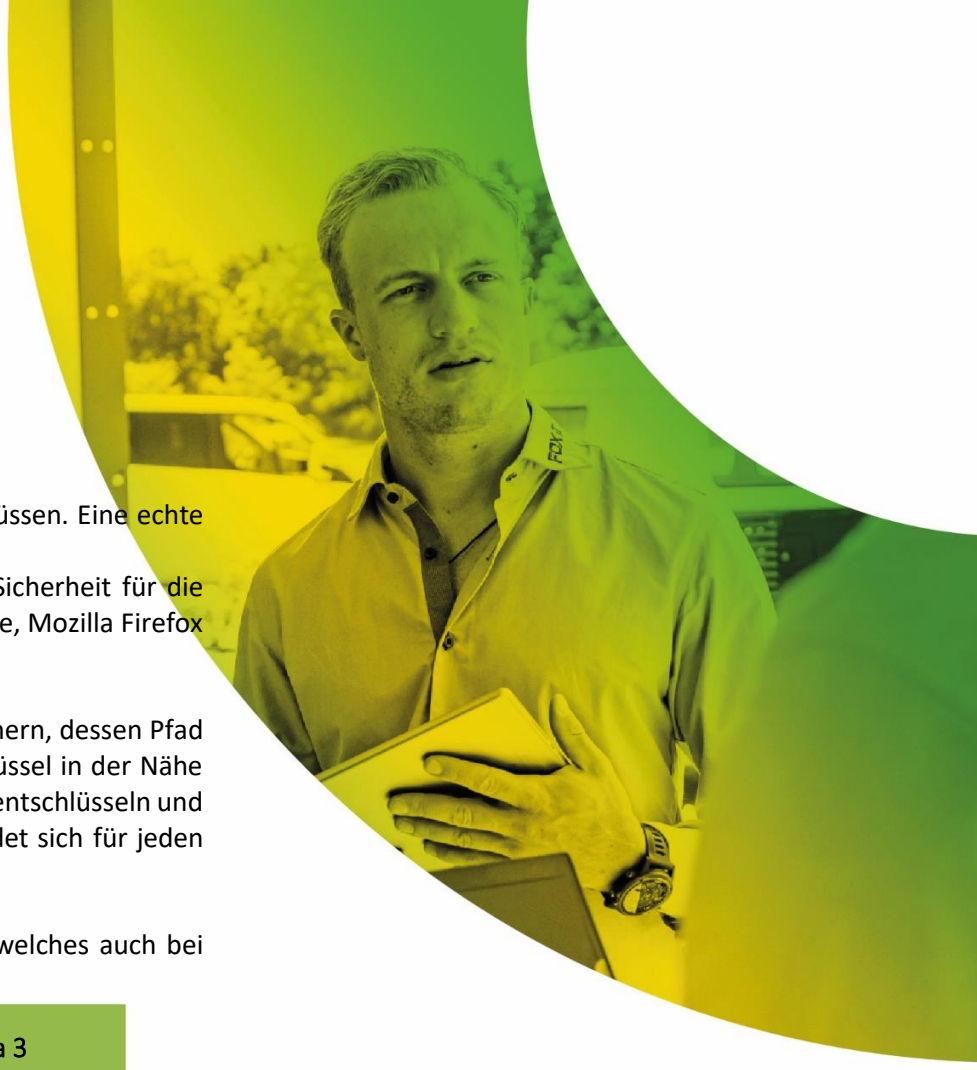
Newsletter 12/2024

FOX Group

Passwörter im Browser als Gefahr



Im Browser gespeicherte Passwörter sind bequem, da sie nicht jedes Mal neu eingegeben werden müssen. Eine echte Zeitersparnis. Aber wie sicher ist es?
Das Hauptproblem beim Speichern von Passwörtern in Browsern besteht darin, dass Benutzer die Sicherheit für die Benutzerfreundlichkeit opfern. Dies gilt insbesondere für die drei beliebtesten Browser: Google Chrome, Mozilla Firefox und Microsoft Edge, die alle Benutzerpasswörter auf höchst unsichere Weise speichern.

Der Grund dafür ist, dass alle Browser ihre Passwörter an einem sehr vorhersehbaren Ordner abspeichern, dessen Pfad nicht geheim ist. Und obwohl die Passwörter selbst verschlüsselt sind, wird der Verschlüsselungsschlüssel in der Nähe gespeichert und ist ebenfalls leicht zugänglich. Mit diesem Schlüssel kann ein Angreifer z.B. Passwörter entschlüsseln und stehlen. Eine absurde Situation: Die Tür scheint sicher verschlossen zu sein, aber der Schlüssel befindet sich für jeden versierten Nutzer unter der Fußmatte.

Daher bleibt unsere Empfehlung die Einführung eines Passwort-Management Tool (Passwort-Safe), welches auch bei gesonderten Zugriffsberechtigungen funktioniert.

KI-Manager und Datenschutzbeauftragter, ein Interessenkonflikt?

KI-Manager und Datenschutzbeauftragter. Beide Funktionen in einer Person? Geht das?
Am 01.08.2024 trat die Verordnung 2024/1689 in Kraft, unter dem Begriff „KI-Verordnung/KI-Gesetz“ oder „AI-Act“ (KI-VO). Diese EU-Verordnung sieht weitreichende Regelungen in Bezug auf Künstliche Intelligenz (KI) vor. Im Mittelpunkt – entsprechend der DSGVO - steht auch hier der Mensch.
Das Gesetz kategorisiert KI-Systeme in vier Risikoklassen: (1) Unannehmbares, (2) hohes, (3) potenziell hohes und (4) begrenztes bzw. geringeres Risiko ein. Zusätzlich verpflichtet sie die unterschiedlichen KI-Akteure (Anbieter, Importeuren, Händlern und Betreibern) Maßnahmen zu ergreifen, um die Risiken für natürliche Personen, den vier Risikoklassen entsprechend, zu minimieren. Durch diese Abhängigkeiten wird die Umsetzung der Anforderungen aus der KI-VO schnell zum komplexen Sachverhalt innerhalb des Unternehmens. Der Ruf nach einem Spezialisten ist geboren.

Instinktiv stellt sich die Frage, ob der Datenschutzbeauftragte (DSB) zusätzlich die Funktion des KI-Beauftragten übernehmen kann, ist dieser aufgrund seiner Vorkenntnisse (Art.37, Abs. 5 DSGVO) bereits mit dem Risiko für die Rechte und Freiheiten einer natürlichen Person betraut. Art. 38, Abs.6 DSGVO besagt, dass der Verantwortliche (bzw. der Auftragsverarbeiter) sicherstellen muss, dass es bei der Ausübung weiterer Tätigkeiten durch den Datenschutzbeauftragten zu keinem Interessenkonflikt kommt. Art. 38, Abs.3 DSGVO führt aus, dass der DSB bei der Erfüllung seiner Tätigkeit weisungsfrei zu sein hat.

Zentrale Frage wäre demnach, ob der Datenschutzbeauftragte in seiner zusätzlichen Funktion als KI-Beauftragte ebenso beratend und überwachend tätig ist. Ist der KI-Beauftragte in einer Stabsstelle angesiedelt und bei der Implementierung der KI operativ nicht eingebunden, kann davon ausgegangen werden, dass kein Interessenkonflikt vorliegt. Der KI-Beauftragte und der Datenschutzbeauftragte sind lediglich in Ihrer Funktion einzubinden.
Für größere Unternehmen empfiehlt es sich, die Positionen auf zwei Individuen zu verteilen, um der Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen mehr Gewicht zu verleihen. Frau Barbara Thiel (ehemalige Landesbeauftragte für den Datenschutz des Landes Niedersachsen) vertrat im diesjährigen IT-Juristentag die Auffassung, dass die Funktion des KI-Beauftragten und des Datenschutzbeauftragten durch unterschiedliche Personen wahrgenommen werden sollte, da der KI-Beauftragte tiefer in den operativen Tätigkeiten eingebunden sei.
Abschließend bleibt festzustellen, dass sich aufgrund der Aktualität der KI-VO noch keine herrschende Meinung gebildet hat und der Einzelfall zu betrachten ist. Es ist aber darauf zu achten, dass ein Interessenkonflikt bei der Tätigkeit des Datenschutzbeauftragten zu empfindlichen Sanktionen führen kann. (Siehe Urteil vom *20.09.2022*)

Urteil: https://www.datenschutz-berlin.de/pressemitteilung/525000-euro-bussgeld-gegen-die-tochtergesellschaft-eines-berliner-e-commerce-konzerns/

Adressatenorientierte Kommunikation

Der geneigte Leser unseres Newsletters stellt sich bei dem Titel zwangsläufig die Frage, ob mit dem Autor alle Renntiere in der vorweihnachtlichen Aufregung durchgegangen sind. Die Begrifflichkeit der adressatenorientierten Kommunikation ist keine Legaldefinition, es ist vielmehr der Wunsch jedes Managementsystems, die einzelnen Akteure unter Berücksichtigung ihres Aufgabengebietes und des Wissensstandes jedes einzelnen über die dem Managementsystem innewohnenden Anforderungen zu schulen.
Dabei ist es im ersten Schritt unerheblich, ob es sich um das Informationssicherheitsmanagementsystem der ISO 27000 Familie oder die Datenschutzgrundverordnung (DSGVO) handelt. Der Unterschied der beiden Managementsysteme besteht darin, dass die DSGVO eine rechtliche Anforderung darstellt, im Gegensatz zur ISO 27000 Familie. Art.32, Abs. 4 DSGVO beschreibt die Anforderungen zur Schulung von Mitarbeitern nicht direkt. Die DSGVO sieht vielmehr vor, dass der Verantwortliche und dessen Auftragsverarbeiter Schritte unternehmen, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Dadurch kann sich der Verantwortliche bzw. der Auftragsverarbeiter voll auf den Personenkreis konzentrieren, welcher wirklich mit personenbezogenen Daten in Berührung kommt. Was die DSGVO dabei nicht zum Ausdruck bringt, ist, dass datenschutzrechtliche Schulungen stufenweise ablaufen sollten.
Zum einen sind da Personen, die neu ins Unternehmen kommen und mit der Verarbeitung von personenbezogenen Daten betraut sind, auf die damit verbundenen Risiken hinzuweisen. Zum anderen sind Mitarbeiter zu betrachten, die spezielle datenschutzrechtliche Schulungen besuchen sollte, dazu zählen beispielsweise auch IT-Administratoren.

Alle diese Schulungen haben selbstredend in regelmäßigen Abständen zu erfolgen, wobei der Begriff „regelmäßig“ nicht bedeutet, dass eine Schulung alle 10 Jahre zielführend ist. Je nach Art und Umfang der zu verarbeiteten personenbezogenen Daten, sowie dem vorhandenen Risiko für die Rechte und Freiheiten einer natürlichen Person, sind Schulungen häufiger durchzuführen.

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 § 55 Abs. 2 RStV Franz Obermayer