Newsletter 03/2026

FOX Group

Aktuelles zum Geschäftsgeheimnisgesetz (GeschGehG)

Das **Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)** hat die Rechtslandschaft für Unternehmen seit seinem Inkrafttreten im Jahr 2019 grundlegend verändert. Während früher der Wille zur Geheimhaltung oft ausreichte, fordern Gerichte heute den Nachweis **angemessener Geheimhaltungsmaßnahmen**. Aktuelle Urteile aus den Jahren 2024 und 2025 schärfen dieses Profil weiter und setzen klare Grenzen für die betriebliche Praxis.

Früher schützte das Gesetz fast jede Information, die ein Arbeitgeber als "geheim" deklarierte. Heute ist ein Geschäftsgeheimnis nur dann rechtlich geschützt, wenn es einen kommerziellen Wert besitzt und der Inhaber nachweislich Schutzvorkehrungen getroffen hat. Ohne diese Maßnahmen verlieren Unternehmen ihren Anspruch auf Unterlassung oder Schadensersatz, selbst wenn ein Mitarbeiter Daten offensichtlich entwendet.
Die aktuelle Rechtsprechung zum GeschGehG zeigt: Geheimnisschutz ist kein Selbstläufer mehr. Unternehmen müssen proaktiv ein **Geheimnisschutz-Management** etablieren. Wer heute noch auf alte Standardverträge und offene Serverstrukturen setzt, riskiert im Ernstfall den Verlust seiner wertvollsten Assets – ohne Chance auf rechtliche Gegenwehr.

Thema 1

Aktuelles zum Geschäftsgeheimnis gesetz (GeschGehG)

Thema 2

Orga. Maßnahmen in der KI-Richtlinie technisch umsetzen

Thema 3

Wann soll das Passwort nun geändert werden?

Organisatorische Maßnahmen in der KI-Richtlinie technisch umsetzen

Mit der zunehmenden Verbreitung von Künstlicher Intelligenz (KI) in Unternehmen steigt auch die Verantwortung im Umgang mit sensiblen Informationen und ethischen Fragestellungen. Die Eingabemasken bieten dem Anwender dabei die Möglichkeit, Daten einzugeben, die ethischen und moralischen Grundsätzen widersprechen oder personenbezogene Daten beinhalten. Firmen versuchen, diese Eingabemöglichkeiten über organisatorische Maßnahmen, und KI-Richtlinien zu lösen.
Da eine Regelung nur so gut ist, wie die Mittel, diese zu überprüfen, sind viele organisatorische Maßnahmen im Kontext KI ein eher zahnloser Tiger. Obgleich z.B. ChatGPT Enterprise die Möglichkeit für Administratoren bietet, Protokolle von Gesprächen und Aktivitäten zu exportieren sowie regelmäßig zu kontrollieren, lassen Administratoren diese Option im Tagesgeschäft aus Mangel an Kapazitäten ungenutzt.

Web-Content-Filter, wie sie bereits für die Überwachung von unethischen oder unmoralischen Inhalten im Web eingesetzt werden, könnten das verhindern. In Bezug auf die Nutzung von Online-KI-Angeboten könnten damit nicht nur unethische oder unmoralische Inhalte, sondern auch personenbezogene Daten herausgefiltert werden. In den USA gibt es Anbieter, die in diese Richtung gehen, die aber erstens, ihre Daten in den USA verarbeiten und bzw. nur den unethischen Inhalt sperren.
Ein echter KI-Proxy prüft alles gleichzeitig: unethische Inhalte und unmoralische Eingaben sowie die Eingabe von personenbezogenen Daten werden grundsätzlich nicht weitergegeben. Anwendende erhalten einen entsprechenden Hinweis. Beinhalten Suchanfragen personenbezogene Daten, werden diese vom KI-Proxy **pseudonymisiert** und dann als **Pseudonym** an den externen KI-Dienst weitergegeben. Beim Erhalt der Antwort des externen KI-Diensts wird das Pseudonym durch die gespeicherten Klardaten ersetzt und die Anwendung erhält eine sinnvolle Antwort.

Beim Einsatz einer internen KI im Unternehmen, um z.B. Mitarbeitende im Verkauf bei der Suche nach Produktinformationen zu unterstützen, werden bei der Eingabe von personenbezogenen Daten diese vorrangig im Unternehmen gesucht, vorausgesetzt, die Eingabe ist durch Firmenrichtlinien erlaubt.

Durch dieses Vorgehen zwingen nicht nur organisatorische Maßnahmen die Mitarbeitenden zur Einhaltung von Vorgaben. In diesem Fall verhindern technische Maßnahmen Regelverstöße und minimieren das Überwachungsvolumen der Administratoren.

Wann soll das Passwort nun geändert werden?

Die Anforderungen an sichere Passwörter haben sich in den letzten Jahren erheblich verändert. Sowohl die DSGVO als auch die ISO 27001 sprechen keine konkreten Passwortlängen vor, verlangen jedoch Sicherheitsmaßnahmen, die dem *Stand der Technik* entsprechen. Genau dieser Begriff ist entscheidend: Er verpflichtet Organisationen dazu, Sicherheitsmechanismen einzusetzen, die nachweislich wirksam und zeitgemäß sind.

Während früher komplexe, schwer merkbare Passwörter im Vordergrund standen, gilt heute ein anderer Ansatz als modern. Studien und Praxisempfehlungen zeigen, dass lange Passphrasen – also mehrere Wörter in Kombination – deutlich widerstandsfähiger gegen Brute-Force-Angriffe sind als kurze, künstlich komplexe Zeichenfolgen. Eine Mindestlänge von 12 bis 14 Zeichen setzt sich als Best Practice durch, und viele Unternehmen gehen inzwischen bewusst darüber hinaus, um ein angemessenes Sicherheitsniveau sicherzustellen.

Auch beim Thema Passwortwechsel hat sich der Stand der Technik gewandelt. Die ISO 27001 fordert ein wirksames Identitäts- und Zugangsmanagement, schreibt jedoch keine regelmäßigen Passwortwechsel ohne Anlass mehr vor. Der Grund dafür ist logisch: Häufige, verpflichtende Wechsel führen nachweislich zu schwächeren Passwörtern, da Mitarbeitende zu vorhersehbaren Mustern greifen. Stattdessen gilt es als zeitgemäß, Passwörter **nur bei Verdacht auf Kompromittierung** oder **nachweisbaren Sicherheitsereignissen** zu ändern. Dieser risikobasierte Ansatz harmoniert mit der DSGVO, die verlangt, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen geschützt werden – und zwar effektiv, nachprüfbar und verhältnismäßig.

Zusammengefasst bedeutet Stand der Technik heute: längere, nutzerfreundliche Passwortphrasen, kein erzwungenes Passwortwechseln ohne Anlass und die Ergänzung durch moderne Verfahren wie Mehrfaktorauthentifizierung. Diese Kombination erfüllt nicht nur die Anforderungen von ISO 27001 und DSGVO, sondern erhöht auch die tatsächliche Sicherheit im Alltag.

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