



Europäische Alternative gesucht?

Wir Menschen sind „Gewohnheitstiere“. Was für den Alltag zutrifft, lässt sich bei der Wahl funktionierender Computersoftware ebenfalls erkennen.

Microsoft fand Anfang der 90er Jahre Einzug in die deutschen Büros und ersetzte die Schreibmaschine. Wenig später suchten die Deutschen ihre Antworten in der Google-Suchmaschine. WhatsApp gehört in 109 Ländern der Welt zu den beliebtesten Messengern, nicht nur in Deutschland, der Schweiz und Österreich. Der Gruppenzwang bindet uns Europäer an die US-Softwareprodukte.

Europäische Unternehmen erkannten schnell ihre Abhängigkeit und den Kontrollverlust über ihre Daten, der damit einhergeht. Seit geraumer Zeit lassen sich die meisten Softwareprodukte durch europäische Computerprogramme ersetzen. Fragen Sie uns!

Thema 1

**Europäische
Alternative
gesucht?**

Seite 1

Thema 2

**Schon vom
Beschäftigten-
datenschutz
gehört?**

Seite 2

Thema 3

**SMS als Zwei-
Faktor-
Authentisierung
ausgedient?**

Seite 3





Schon vom Beschäftigtendatenschutz gehört?

Nach § 26 Absatz 1 Satz 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Kollektivvereinbarungen, wie Betriebsvereinbarungen oder Tarifverträge, zum Teil durchgesetzt von Interessenvertretungen, können ebenfalls als Grundlage angewandt werden, solange sie die Vorgaben der DSGVO nicht untergraben bzw. aufweichen. Bekanntlich verweisen Unternehmen auf den §26 BDSG als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten von Beschäftigten.

Auch dürfen Betriebe personenbezogene Daten zur Aufdeckung von Straftaten verarbeiten, um durch die Tat nicht selbst straffällig zu werden. Hier bedarf es tatsächlicher Anhaltspunkte, die über den Verdachtsfall hinaus dokumentiert werden müssen. Eine präventive Überwachung widerspricht hingegen dem Grundsatz der unantastbaren Menschenwürde. Überwachungsskandale Anfang der 2000er Jahre, wie bei LIDL (Einsatz von Privatdetektiven), der Deutschen Bahn, die Videoüberwachung bei IKEA und Burger King sowie die Abnahme von Blutproben von Bewerbern bei mehreren großen deutschen Unternehmen wie Daimler, NDR, Beiersdorf und Merck deuteten auf einen dringenden Handlungsbedarf im Beschäftigtendatenschutz hin.

Auch wenn die meisten Unternehmen die Einwilligung als adäquate Rechtsgrundlage sehen, um personenbezogene Daten zu verarbeiten, so ist die rechtliche Wirksamkeit im Beschäftigungsverhältnis kaum umsetzbar. Nur in Ausnahmefällen können Beschäftigte in die Verarbeitung ihrer personenbezogenen Daten im Beschäftigungsverhältnis einwilligen. Rechtswirksam ist diese Einwilligung nur, wenn sie tatsächlich freiwillig erteilt wird.

Das zwischen Arbeitsstelle und Beschäftigten bestehende untergeordnete Verhältnis mag Zweifel aufkommen lassen, ob Beschäftigte in ihrem Angewiesen-Sein auf ein regelmäßiges Einkommen tatsächlich Ihre Einwilligung freiwillig abgeben. Zu groß die Angst, einen Nachteil zu erlangen, sowohl unter den Beschäftigten als auch gegenüber Vorgesetzten. Zu oft entfällt die Freiwilligkeit durch Einflussnahme oder Gruppenzwang.

§ 26 BDSG erkennt eine Einwilligung als wirksam ausnahmsweise dann an, wenn durch die Verarbeitung entweder ein rechtlicher oder wirtschaftlicher Vorteil enthält oder wenn Beide nachweislich gleichgelagerte Interessen verfolgen, überwiegend im Rahmen von Zusatzleistungen für den Arbeitnehmenden außerhalb des Arbeitsverhältnisses. Auch sind die Anforderungen der DSGVO an die Einwilligung zu berücksichtigen, um rechtswirksam zu werden.

In der Praxis werden Einwilligungen für die Nutzung von Fotos auf Social-Media-Plattformen eingeholt, deren Vorteil für die Mitarbeitenden fraglich ist.



SMS als Zwei-Faktor-Authentisierung ausgedient?

Um Daten und Geräte effektiver abzusichern, ist die Zwei-Faktor-Authentisierung ein Muss. Der Log-in erfolgt dann mit einem Passwort und einem weiteren Faktor. Als Begriff kennt man den Begriff Multi-Faktor-Authentifizierung (abgekürzt: MFA), insbesondere auch weil ein dritter Faktor mittlerweile keine Seltenheit ist.

Der weitere Faktor erfolgt nach Eingabe des ersten Passworts mithilfe eines PIN-Generators, einer Smartphone-Applikation, eines Hardware-Dongle (z.B. YubiKey), ein kleines USB-Gerät (Security Key NFC), einer E-Mail oder eines SMS-TANs auf das mobile Endgerät (Tablet oder Smartphone).

Letztere Variante gilt immer noch als sehr beliebter Faktor für Zugang zu Online-Portale. In der Vergangenheit geriet die Verwendung eines SMS-TANs immer mehr in Verruf. Aufgrund der stetig steigenden Anzahl von Cyber-Angriffen sieht das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Bedrohungslage nach wie vor angespannt bis kritisch. Die Nutzung raffinierter und komplexer Passwörter reicht für die Absicherung von Konten mittlerweile nicht mehr aus. Deshalb hat das BSI die Zwei-Faktor-Authentisierung unter die Lupe genommen. Das Ergebnis war für die Variante SMS niederschmetternd.

Die amerikanische Sicherheitsbehörde Cybersecurity and Infrastructure Security Agency (CISA) gab Ende 2024 einen Leitfaden heraus, in dem es um die sichere Nutzung von Mobilgeräten geht. In diesem Leitfaden wird explizit vor der Verwendung einer Multi-Faktor-Authentifizierung (MFA) per SMS gewarnt, denn diese lassen sich leicht ausspähen. Hacker, die möglicherweise in Verbindung zur chinesischen Regierung stehen, erhielten Zugriff auf Telefon- und SMS-Dienste von Telekommunikationsnetzwerken.

Es empfiehlt sich daher, den zweiten Faktor, als Absicherung, z.B. mit einer Authentifizierungs-App einzuholen.

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