Newsletter 06/2026

FOX Group

Vertrauensverlust und Imageschaden durch KI- E-Mails

Die Nutzung von künstlicher Intelligenz beim Verfassen von E-Mails führt in der Geschäftswelt bereits zu einer spontanen Abneigung gegenüber der versendenden Person. Prominente Unternehmer sortieren Nachrichten, die in einem unnatürlichen, übertrieben journalistischen Stil verfasst sind, ungelesen aus. Solche automatisierten Anschreiben wecken bei den Empfängern das unangenehme Gefühl, nicht ernst genommen oder gar belogen zu werden, was die Chance auf eine erfolgreiche Kommunikation drastisch senkt.

Diese kritische Haltung deckt sich mit aktuellen wissenschaftlichen Erkenntnissen. Untersuchungen der Ohio State University belegen, dass Empfänger KI-generierter Nachrichten, diese als unaufrichtig wahrnehmen. Zudem zeigt eine Befragung von über tausend Angestellten in den USA das Ausmaß des Imageschadens für die Absender. Etwa die Hälfte der Befragten stuft Personen, die solche Technologien für ihre persönliche Kommunikation nutzen, als weniger kompetent und unzuverlässig ein.
Die vermeintliche Effizienz im Posteingang zerstört somit das essenzielle Fundament der geschäftlichen Kommunikation: das zwischenmenschliche Vertrauen.

Thema 1

Vertrauensverlust und Imageschaden durch KI- E-Mails

Thema 2

Haftung

nach §42 BDSG

Thema 3

Cybersicherheit für Mess-, Steuer- und Regeleinrichtungen (MSR)

Haftung nach §42 BDSG

Die DSGVO definiert in Art. 4 Nr. 7 DSGVO den Verantwortlichen als „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle …“. Die Haftung und das Recht auf Schadenersatz sind in Art. 82 DSGVO aufgeführt. Das Verhängen von Geldbußen durch die Aufsichtsbehörden wird in Art. 83 DSGVO benannt. Man könnte meinen, dass damit alles gesagt bzw. geregelt ist, leider nein. Die Bundesrepublik Deutschland geht hier noch einen Schritt weiter und hat im Bundesdatenschutzgesetz den §42 BDSG eingeführt. In diesem Paragrafen wird die „wissentliche Bereitstellung von nicht allgemein zugänglichen personenbezogenen Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein“ kodifiziert.

Neben dem Begriff des „Verantwortlichen“ gibt es im deutschen Recht noch die sogenannte Garantenstellung (Garant). Diese ist in §13 StGB beschrieben. In der IT-Sicherheit wird damit die rechtliche Pflicht von IT-Verantwortlichen, aktiv für den Schutz von Daten und Systemen einzustehen, definiert. Wer diese Position innehat, haftet bei Schäden durch vorsätzliches oder fahrlässiges „Nichtstun“ (Unterlassen) straf- und zivilrechtlich wie ein aktiver Täter.
Nun kommt es in der Praxis, in Bezug auf die unterschiedlichen Begrifflichkeiten ab und an zu Missverständnissen und der Garant wird Verantwortlicher.

Die Gesamtverantwortung für die Einhaltung datenschutzrechtlicher und informationssicherheitsbezogener Vorgaben trägt die Geschäftsleitung. Sie muss technische und organisatorische Maßnahmen schaffen, Risiken bewerten, Zuständigkeiten definieren und wirksame Kontrollmechanismen etablieren. Unterlässt die Unternehmensleitung dies, kann ihr Organisationsverschulden vorgeworfen werden. Besonders kritisch wird dies, wenn Sicherheitsmängel bekannt waren, hierfür jedoch keine angemessenen Maßnahmen entgegengesetzt wurden (Compliance).

Der Garant hingegen hat Schäden oder Rechtsverletzungen zu verhindern, da sonst arbeitsrechtliche, aber auch strafrechtliche Konsequenzen drohen.
Die Garantenstellung ersetzt jedoch nicht die Verantwortung der Geschäftsleitung. Sie lässt sich auch nicht auf den Garanten übertragen. Weder per Einwilligung noch per Vertrag bzw. Betriebsvereinbarung. Es entsteht eine abgestufte Verantwortungsstruktur: Die Unternehmensleitung muss wirksame Rahmenbedingungen schaffen, während Fachverantwortliche innerhalb ihres Aufgabenbereichs Gefahren abwehren und Verstöße verhindern müssen.

§ 42 BDSG regelt strafrechtliche Konsequenzen für Unternehmen sowie für verantwortliche Personen bei Datenschutzverstößen und nicht für das datenschutzrechtliche Vergehen von Mitarbeitenden.

Quelle: §42 BDSG

Cybersicherheit für Mess-, Steuer- und Regeleinrichtungen (MSR)

Das Bundesministerium für Arbeit und Soziales (BMAS) hat mit Datum vom 17. November 2025 die Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ geändert.

Die TRBS 1115 Teil 1 betrifft branchenübergreifend alle Arbeitgeber und Anlagenbetreiber, die digitale oder vernetzte Arbeitsmittel sowie überwachungsbedürftige Anlagen nutzen, deren technische Schutzmaßnahmen (MSR-Einrichtungen) durch Cyberbedrohungen manipuliert werden können. Insbesondere Energieversorger, die eine Vielzahl von technischen Systemen betreiben, die rechtlich als überwachungsbedürftige Anlagen eingestuft sind, fallen somit unter den direkten Anwendungsbereich der TRBS 1115 Teil 1.

So wurden im Text wichtige Begriffe nachgeschärft. Beispielsweise kam zusätzlich zur Formulierung „sicherheitsrelevant“ an entscheidenden Stellen vermehrt das Wort „cybersicherheitsrelevant“ zum Einsatz. Zusätzlich müssen Prüfer nun präzise und nachvollziehbar dokumentieren, wie die Wirksamkeit der Cybersicherheitsmaßnahmen im laufenden Betrieb dauerhaft gewährleistet bleibt.

Das Regelwerk beschreibt verschärfte Anforderungen an die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen von sicherheitsrelevanten MSR-Einrichtungen. Da langjährige Erfahrungen zur Cybersicherheit bei vielen Arbeitgebern noch nicht vorliegen können, werden diese Anforderungen durch die Erläuterungen und Beispiele in dem neuen Anhang 2 konkretisiert und der Arbeitgeber bei der Umsetzung unterstützt werden. Besonders Anhang 2 hilft mit konkreten Beispielen und Erläuterungen zu den erforderlichen Cybersicherheitsmaßnahmen, um Betreibern die Umsetzung der Gefährdungsbeurteilung zu erleichtern.

Quelle: https://www.baua.de/DE/Angebote/Regelwerk/TRBS/pdf/TRBS-1115-Teil-1-Aenderungen.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