



Setzen Sie Künstliche Intelligenz (KI) ein?

Planen Sie in Ihrem Unternehmen Künstliche Intelligenz einzusetzen und sind sich unsicher, welche Anforderungen laut KI-Verordnung beim Einsatz zu erfüllen sind. Wie die KI-Verordnung und die DSGVO zusammenspielen. Gibt es Fragen, die Sie lieber direkt geklärt sehen möchten?

Die complimant AG plant am 5. März 2025 eine kostenlose Informationsveranstaltung zum Thema Künstliche Intelligenz (KI). Wir geben Ihnen in diesem Termin einen grundlegenden Einblick in das Thema Künstliche Intelligenz und einen Überblick über den Anforderungsrahmen der Verordnung 2024/1689, kurz KI-Verordnung. Im Anschluss können Sie uns Ihre Fragen stellen.

hier nun der Link zur Veranstaltung: <https://eveeno.com/ki-verordnung>

Ihr Franz Obermayer (Vorstand)

Thema 1

**Setzen Sie
Künstliche
Intelligenz (KI)
ein?**

Seite 1

Thema 2

**Sind Spionage-
Apps erlaubt?**

Seite 2

Thema 3

**End-zu-End
Verschlüsselung
im E-Mail
Versand**

Seite 3



Sind Spionage-Apps erlaubt?

In modernen Krimis werden Smartphones regelmäßig zur Erstellung von Bewegungsprofile genutzt. Eine solche Möglichkeit ist für Eltern gewiss verführerisch. In diversen Ländern sind Parental-Control-Apps bereits seit Jahren in Gebrauch und Anbieter lassen sich dies gut bezahlen.

Die Installation von Spionage-Apps ist bei den eigenen Kindern kritisch diskutiert, so ist die unautorisierte Installation auf fremden Endgeräten per Strafgesetzbuch (StGB) geahndet. Beginnend mit §202c StGB, dem Vorbereiten des Ausspähens und Abfangens von Daten bis zu § 202a StGB, dem Ausspähens von Daten, können derartige Aktivitäten mit Freiheitsstrafen belegt werden.

Spätestens mit der Einschulung besitzt die überwiegende Mehrheit der Kinder heute ein Smartphone, um sich mit Gleichaltrigen auszutauschen. Wenn Eltern in die Endgeräte Ihrer Kinder Einsicht haben, lesen sie auch, was andere Kinder schreiben. Werden diese Informationen weitergetragen, kann es für Eltern unangenehm werden, wenn sie plötzlich mehr wissen als üblich. Man gerät gegebenenfalls schnell in Erklärungsnot.

Wie jedes Schwert, so ist auch die Nutzung einer solchen App zweischneidig. Zum einen können Menschenrechte anderer verletzt werden, zum anderen sollte jedem klar sein, dass der Hersteller oder App-Anbieter auf die Daten zugreifen kann. Dieser könnte ein Interesse daran haben, die Daten für eigene Zwecke zu vermarkten. Es ist auch zu erwähnen, dass Anbieter sich diese Dienste gut bezahlen lassen. Erfahrungen zeigen, dass die erhaltenen Ergebnisse dieser Überwachungs-Apps nicht zufriedenstellend sind, die Kündigungsmöglichkeiten durch den außereuropäischen Sitz des Herstellers erschwert werden.

Wie ist aber die datenschutzrechtliche Bewertung?

Die Datenschutzgrundverordnung DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten bei der Nutzung durch *private* Unternehmen und öffentliche Stellen. Bei Privatpersonen hingegen ist man im Bereich der Persönlichkeitsrechte geschützt durch das Bürgerliches Gesetzbuch (BGB).



End-zu-End Verschlüsselung im E-Mail Versand

Bei der E-Mail-Verschlüsselung gibt es zwei verschiedene Arten der Übermittlung: die Punkt-zu-Punkt -auch als Transportverschlüsselung bekannt- und die Ende-zu-Ende-Verschlüsselung.

Bei der Transportverschlüsselung findet zwischen dem E-Mail-Programm und dem E-Mail-Server eine Verbindung statt, die durch das "Transport Layer Security" (TLS) Protokoll verschlüsselt wird. Die allermeisten E-Mail-Anbietern unterstützen diese Transportverschlüsselung.

Eine verschickte E-Mail mit Transportverschlüsselung wandert zwischen Knotenpunkte und Servern bis zum Empfänger. Auf dem Weg von einem Knotenpunkt zum anderen ist die E-Mail jedoch nicht mehr verschlüsselt und liegt somit im Klartext vor. An diesen Knotenpunkten könnten Angreifer unerkannt Nachricht abfangen, kopieren oder sogar manipulieren.

Bei einer Ende-zu-Ende-Verschlüsselung wird die E-Mail selbst verschlüsselt. Nur beim Senden und Empfangen ist die E-Mail im Klartext lesbar, wenn der dafür notwendige Schlüssel vorliegt. Selbst E-Mail-Anbieter können die Nachricht nicht lesen und auch während des Transports haben Angreifer keine Chance die E-Mail zu lesen oder zu manipulieren. Nur so lässt sich gewährleisten, dass Nachrichten unverändert übermittelt werden, gemäß den drei Anforderungen der Informationssicherheit und Datenschutz (Vertraulichkeit, Authentizität, Integrität).

Bei der Ende-zu-Ende-Verschlüsselung sind zusätzliche Plugins in den E-Mail-Programmen zu aktivieren, um diese Technologie nutzen zu können.

Vor kurzem hat das Oberlandesgericht (OLG) Schleswig-Holstein (18.12.2024, Az. 12 U 9/24) entschieden: Unternehmen müssen ein angemessenes Sicherheitsniveau gewährleisten, wenn sie Rechnungen und andere sensible Daten per E-Mail versenden. Die Transportverschlüsselung reiche nach Ansicht des Gerichts nicht aus.

Kommt ein Unternehmen dieser Verpflichtung nicht nach, können Kunden Schadensersatzansprüche geltend machen. Ein Schutz, der in den technischen und organisatorischen Maßnahmen (TOM, Art. 32 DSGVO) umzusetzen ist.

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