Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

Oktober 2024

Phishing-Simulationen sind ein wichtiges Hilfsmittel, um Unternehmen resilienter gegen Cyberbedrohungen zu machen. Doch sie bergen Tücken im Hinblick auf den Datenschutz.

Bild: iStock.com/Baris-Ozer

Resilient – oder ein erfolgreicher Cyberangriff?

Phishing-Tests: Richtig gemacht, Daten geschützt

Trainings mit simulierten Angriffen helfen, IT-gestützte Betrugsversuche (Phishing) zu erkennen. Doch eine Phishing-Simulation erfordert sorgfältige logistische Planung und interne Kommunikation. Einige Punkte sind zu berücksichtigen, um solche Simulationen erfolgreich durchzuführen.

Eine auf den ersten Blick eher unscheinbare E-Mail landet im Posteingang einer Mitarbeiterin der Buchhaltung. Absender ist angeblich der Chef des Unternehmens, und die Betreffzeile lautet „Bitte um Rechnungsprüfung". Die E-Mail ist perfekt getarnt. Sie enthält die offizielle Signatur des Chefs und, wie im Unternehmen üblich, einen freundlichen Tonfall. Grammatik und Rechtschreibung sind selbstverständlich richtig, wie in Zeiten von künstlicher Intelligenz (KI) in der Cyberkriminalität üblich.

In der E-Mail bittet der Absender die Kollegin, einen Anhang zu öffnen und die darin enthaltenen Rechnungsdaten zu prüfen. Ohne Verdacht zu schöpfen, öffnet sie den Anhang. Was sie nicht ahnt: Dieser Anhang ist ein Trojaner. Die Schadsoftware nistet sich still und leise in das Firmennetzwerk ein und zieht sensible Daten ab.

Innerhalb von Stunden erlangen die Kriminellen Zugriff auf vertrauliche Informationen und können das Unternehmen in der Folge erheblich schädigen. Dieser Angriff hätte sich möglicherweise verhindern lassen, wenn alle Mitarbeitenden besser auf solche Phishing-Angriffe vorbereitet gewesen wären.

Zum Glück war das keine reale Situation, sondern eine, die ich gerne in Schulungen zum Thema einsetze. Mit Beispiel-E-Mail. Sie wären doch sicher nicht darauf hereingefallen?

Die Bedrohung durch Phishing

Phishing ist aktuell die größte Bedrohung im Hinblick auf Cyberangriffe. Statistiken zeigen, dass 80 % aller erfolgreichen →

Editorial

Ricarda Veidt, Chefredakteurin

Testen: Auf die Umstände kommt es an

Liebe Leserin, lieber Leser! Suchen Sie verzweifelt nach einer Funktion in Outlook, die Sie nicht mehr finden können? Dann haben Sie möglicherweise (un-)freiwillig auf die neue Version des E-Mail-Programms umgestellt. Doch die eingeschränkte Funktionalität ist nicht das einzige Manko des Microsoft-Updates: Lesen Sie auf Seite 17, welche datenschutzrechtlichen Herausforderungen sich daraus für Nutzende in Europa ergeben und warum Mitarbeiter die neue Version besser noch nicht testen sollten.

Ausdrücklich erwünscht sind Tests hingegen, wenn es darum geht, für Phishing zu sensibilisieren. Doch gut gemeint ist nicht gleich gut gemacht. Damit Phishing-Simulationen für alle Beteiligten zu einem Lernerfolg werden, gibt es einige Punkte zu beachten. Nützliche Tipps zur logistischen Planung und internen Kommunikation finden Sie im Titelbeitrag.

Nicht nur bei Phishing-E-Mails, sondern auch bei fremdsprachigen Zertifikaten lohnt sich ein zweiter Blick. Der aktuelle Daten-Schluss zeigt dies besonders anschaulich!

Herzliche Grüße
Ihre Ricarda Veidt

Cyberangriffe mit erfolgreichem Phishing beginnen. Dieses zielt darauf ab, Mitarbeitende zu täuschen und sensible Informationen zu erlangen oder schädliche Software zu installieren.

Was die Lage zusätzlich erschwert: Es häufen sich rechtliche Anforderungen, mehr Resilienz, also mehr Widerstandsfähigkeit gegen Cyberkriminalität, zu entwickeln.

Laut Berichten wie dem BSI-Lagebericht und dem ENISA Threat Landscape Report führen etwa 35 % der Unternehmen weltweit regelmäßig Phishing-Simulationen durch. Diese Unternehmen stellen danach oft fest: Eine erhebliche Anzahl von Mitarbeitenden fällt anfänglich auf diese Phishing-Versuche herein.

Datenschutz von Anfang an in Phishing-Simulationen einbinden

Bereits in der Planungsphase von Phishing-Simulationen gilt es, Datenschutzaspekte zu berücksichtigen. Es ist sinnvoll, frühzeitig Datenschutzbeauftragte (DSB) in den Prozess einzubinden. So können Unternehmen und Organisationen sicherstellen, dass sie alle datenschutzrechtlichen Anforderungen erfüllen. Dann können sie z.B. eine Schwellenwertanalyse oder, falls erforderlich, eine Datenschutz-Folgenabschätzung (DSFA) durchführen.

Hierzu gehört dann auch, die Verarbeitung personenbezogener Daten auf das notwendige Mindestmaß zu beschränken. Ebenso gilt es, bevorzugt anonymisierte oder aggregierte Daten zu verwenden. Diese Daten reichen in den meisten Fällen aus. Schulungen und Trainings lassen sich damit hervorragend gestalten.

Psychologische Tricks und soziale Anreize in Phishing-Mails

Clever agierende Cyberkriminelle nutzen häufig psychologische Tricks und soziale Anreize, um ihre Phishing-Mails erfolgreich zu machen. Menschen neigen dazu, auf bestimmte emotionale Auslöser zu reagieren, und genau das machen sich die Kriminellen zunutze.

Hilfsbereitschaft: Phishing-Mails appellieren oft an das Bedürfnis der Menschen, anderen zu helfen. Beispielsweise könnten Angreifende eine E-Mail versenden, die vorgibt, von einem Kollegen zu stammen, der dringend Unterstützung durch die angeschriebene Person bei einem Projekt benötigt.

Vertrauen: Viele Angriffe nehmen Bezug auf eine vermeintliche vorherige Kommunikation oder eine bestehende Beziehung. Ein Beispiel könnte sein: „Wie kürzlich besprochen sende ich Ihnen die angeforderten Dokumente."

Autorität: Kriminelle nutzen die natürliche Hierarchie in Unternehmen oder Behörden aus, indem sie E-Mails im Namen von Vorgesetzten senden. Mitarbeitende, die E-Mails von Autoritätspersonen erhalten, neigen dazu, diese ohne weitere Prüfung zu befolgen. Siehe unser Eingangsbeispiel.

Druck oder Angst: Einige Phishing-Mails drohen mit negativen Konsequenzen, z.B. mit Strafen oder Disziplinarmaßnahmen, wenn die betreffende Person bestimmte Anweisungen nicht befolgt.

Gier: Versprechen von Belohnungen, finanziellen oder unternehmensweiten Vorteilen können dazu führen, dass Mit-

arbeitende unbedacht auf Phishing-Mails reagieren.

Neugier: Aktuelle oder brisante Themen dienen dazu, die Neugier zu wecken. Ein Beispiel wäre eine E-Mail, die brisante Informationen oder Gerüchte ankündigt.

Eitelkeit und Schmeichelei: Manche Phishing-Mails zielen darauf ab, das Ego der Zielperson zu streicheln, indem sie ihr Anerkennung zollen oder ihr besondere Fähigkeiten zuschreiben, die sie dringend nutzen soll.

Zeitdruck/Dringlichkeit: Kriminelle setzen oft auf Dringlichkeit, um die Opfer dazu zu bringen, impulsiv zu handeln. Typische Beispiele sind Aussagen wie „Ihr Konto wird in 24 Stunden gesperrt" oder „Sonderangebot nur noch heute gültig". Diese Taktik nutzt die Angst vor verpassten Gelegenheiten oder negativen Konsequenzen, um eine schnelle Reaktion zu erzwingen.

Verknappung: Die Illusion von Knappheit soll oft den Eindruck erwecken, schnelles Handeln sei notwendig, um eine Gelegenheit nicht zu versäumen. Beispielsweise könnte eine E-Mail behaupten: „Nur noch 3 Plätze verfügbar – jetzt anmelden!" Diese Taktik bedient sich der menschlichen Angst, etwas Wertvolles zu verpassen.

Herausforderungen beim Einsatz von Phishing-Simulationen

Wenn Unternehmen solche emotionalen oder sozialen Anreize in Phishing-Simulationen nutzen, um die Reaktionen der Belegschaft zu testen, müssen sie sorgfältig vorgehen. Eine der größten Herausforderungen besteht darin, wie sie mit den Ergebnissen umgehen – v.a. wenn sie ermitteln wollen, welche Mitarbeitenden auf welche Arten von Phishing-Mails besonders anfällig reagieren.

Gezielte Schulung und Datenschutzbedenken

Es liegt nahe, die Erkenntnisse aus den Phishing-Simulationen dazu zu nutzen, Schulungsprogramme gezielt auf die individuellen Schwächen der Mitarbeitenden zuzuschneiden. Dies könnte durch die Identifikation von Mustern geschehen, bei denen bestimmte Gruppen in der Belegschaft häufiger auf bestimmte psychologische Anreize reagieren.

Um datenschutzrechtliche Herausforderungen zu vermeiden, kann ein Unternehmen einen externen Dienstleister beauftragen. Dieser führt die Simulationen durch und liefert nur aggregierte, prozentuale Ergebnisse.

Dieser Ansatz schützt die Identität der einzelnen Mitarbeitenden, während das Unternehmen dennoch gezielte Schulungen entwickeln kann. Eine solche Vorgehensweise ist in der Regel datenschutzrechtlich unbedenklich. Denn hier verarbeitet das Unternehmen keine personenbezogenen Daten, die direkt auf Einzelpersonen zurückzuführen sind.

PRAXIS-TIPP

Werten Unternehmen Phishing-Simulationen ohne Personenbezug und nur mit prozentualen Ergebnissen aus, ist abzuwägen, ob und wie sinnvoll es ist, den Betriebsrat zu informieren oder nicht. Denn falls nicht, können sie auch Betriebsratsmitglieder in die Simulationen einbeziehen. Sie sollten aber zumindest den Betriebsrat über die geplante Kampagne informieren, um Missverständnisse oder Bedenken im Vorfeld auszuräumen.

Einbindung des Betriebsrats

Die Verantwortlichen sollten prüfen, ob und inwieweit sie den Betriebsrat einbinden müssen, sobald sie die Phishing-Simulation planen und durchführen. Die Kampagne könnte so angelegt sein, dass sie eine Kontrolle von Verhalten und Leistung der Mitarbeitenden darstellt. In diesem Fall ist eine Beteiligung des Betriebsrats erforderlich, um die Rechte der Belegschaft zu wahren.

Transparente Kommunikation und Einhaltung der Datenschutzrichtlinien

Transparenz ist der Schlüssel. Die Verantwortlichen müssen die Belegschaft grundsätzlich darüber informieren, dass Phishing-Simulationen geplant sind, wie sie die Daten der Mitarbeitenden verwenden und welche Maßnahmen sie im Rahmen der Phishing-Simulationen ergreifen.

Sie sollten die Belegschaft aufklären: Die Ergebnisse der Simulationen dienen nicht dazu, die Mitarbeitenden zu bewerten oder zu sanktionieren. Der Fokus liegt vielmehr darauf, die allgemeine Sicherheitskultur zu verbessern. Die Mitarbeitenden sollten aber keine konkreten Hinweise und Daten erhalten, sonst verpufft der Effekt der Phishing-Simulation möglicherweise.

Unternehmen sollten die Verarbeitungstätigkeit analysieren und dabei eine Schwellenwertanalyse für eine DSFA durchführen. So können sie die möglichen Risiken für die Rechte und Freiheiten der Mitarbeitenden bewerten und geeignete Maßnahmen ergreifen, um diese Risiken zu minimieren.

Eine DSFA kann dann erforderlich sein, wenn Unternehmen die Tests selbst durchführen, also nicht von einem Dienstleister anonymisiert durchführen lassen, der ausschließlich prozentuale Ergebnisse übermittelt. Ebenso kann eine DSFA nötig sein, wenn Projektverantwortliche Anreizprofile erstellen wollen, um Mitarbeitende gezielt trainieren zu können.

Logistische Vorbereitung und interne Kommunikation

Um eine Phishing-Simulation durchzuführen, müssen die Verantwortlichen deren Logistik sorgfältig planen und die Simulation im Haus kommunizieren. Sie müssen das IT-Team, das die eingehenden Meldungen bearbeiten soll, im Vorfeld vertraulich informieren.

Dieses IT-Personal muss genau darüber informiert sein, wie es mit den Meldungen umgehen soll, um sie geordnet und →

effizient verarbeiten zu können. Hierbei muss durch geeignete Protokolle und Kommunikationswege sichergestellt sein, dass das Team keine Meldungen übersieht und dass alle Reaktionen koordiniert und konsistent sind.

ACHTUNG!

In bestimmten Bereichen müssen alle Beteiligten informiert sein. Sonst kann der Fall eintreten, der in der September-Ausgabe im Daten-Schluss behandelt wurde. Hier hat ein Entscheider überreagiert, weil er nicht in die Kampagne eingebunden war und eine unvorhersehbare Reaktion auslöste. Dies hätte sich mit der Vorab-Information vermeiden lassen.

Vertraulichkeit und Umgang mit Fehlern

Ein sensibler Aspekt der Phishing-Simulation ist die Reaktion auf Mitarbeitende, die eine verdächtige E-Mail nicht melden, aber die Mail anklicken. Die Reaktion auf solche Situationen muss sorgfältig geplant sein, um Fehler wie Datenschutzverletzungen oder das Risiko von Spott oder Schikane zu vermeiden. Es ist besser, eine Kultur des Lernens und der Unterstützung zu fördern, als Mitarbeitende zu bestrafen oder bloßzustellen.

Auswertungen und Berichte

Die Auswertung des Trainings und der Phishing-Simulation ist ein zentraler Bestandteil des Prozesses. Eine detaillierte Analyse der Reaktionen der Belegschaft liefert wertvolle Erkenntnisse darüber, wie gut die Schulungen gewirkt haben und welche Bereiche das Unternehmen noch verbessern muss.

Dabei sollten Projektverantwortliche u.a. Erfolgsquoten, häufige Fehler und die allgemeine Reaktionszeit erfassen und analysieren. Diese Daten sind nützlich, um die Schulungen anzupassen und künftige Phishing-Simulationen effektiver zu gestalten.

Haben die Verantwortlichen die Ergebnisse ausgewertet, müssen sie Berichte erstellen und sie an Beteiligte weiterleiten. Dazu zählen IT-Abteilung, DSB, Informationssicherheitsbeauftragte (ISB) und Unternehmensführung.

Diese Berichte sollten nicht nur die Ergebnisse der Simulation zusammenfassen. Vielmehr sollten sie auch konkrete Handlungsempfehlungen und Verbesserungsmaßnahmen enthalten. Eine verständliche Kommunikation der Ergebnisse und vorgeschlagener Maßnahmen ist Grundlage dafür, dass alle Ebenen des Unternehmens die Bedeutung der Initiativen für Resilienz und Cybersicherheit erkennen und die Initiativen unterstützen.

Schulungen kontinuierlich verbessern und anpassen

Phishing-Simulationen und Schulungen sollten kein einmaliges Ereignis sein, sondern Teil eines kontinuierlichen Prozesses. Das Unternehmen sollte die Erkenntnisse aus der Simulation nutzen, um Schulungsprogramme zu überarbeiten und an die neuesten Bedrohungen anzupassen.

Die Mitarbeitenden sind kontinuierlich auf die Gefahren aufmerksam zu machen. Das Unternehmen sollte deren Fähigkeiten zur Resilienz trainieren und fördern, also sie dabei unterstützen, Phishing-Angriffe zu erkennen und zu melden.

Ein langfristig erfolgreicher Ansatz erfordert, das Bewusstsein für Cybersicherheit in den Unternehmensabläufen zu verankern. Die Belegschaft muss Schulungen und Simulationen als integralen Bestandteil des Arbeitsalltags ansehen.

Dazu gehört auch, dass das Management eine Vorbildfunktion einnimmt und die Bedeutung von Cybersicherheit regelmäßig betont. Nur so kann es sicherstellen, dass die Mitarbeitenden wachsam bleiben und dazu beitragen, das Unternehmen vor Cyberbedrohungen zu schützen.

Zusätzliche Überlegungen und Empfehlungen

Schulung neuer Mitarbeitender: Integrieren Sie Neuzugänge so schnell wie möglich in das Phishing-Schutzprogramm. Eine intensive Schulung in den ersten Wochen der Beschäftigung kann dabei unterstützen, das notwendige Bewusstsein von Anfang an zu fördern.

Integration in die IT-Infrastruktur: Stellen Sie sicher, dass alle Systeme und Plattformen, die das Unternehmen nutzt, um Phishing-Versuche zu erkennen und zu melden, nahtlos in die bestehende IT-Infrastruktur integriert sind.

Feedback der Belegschaft: Nehmen Sie Anregungen von Mitarbeitenden entgegen und reagieren Sie darauf. Außerdem sollten Sie regelmäßig Feedback von den Mitarbeitenden einholen, wie gut und wie nützlich sie die Schulungen und Simulationen fanden. Dies trägt dazu bei, diese Programme weiter zu verbessern.

Die Resilienz stärken

Phishing-Simulationen sind ein unverzichtbares Instrument, um die Belegschaft auf die Realität moderner Cyberbedrohungen vorzubereiten. Unternehmen sollten Simulationen sorgfältig planen, Fehler sensibel handhaben und die Ergebnisse gründlich auswerten. So können sie ihre Resilienz stärken und zugleich eine Kultur der Achtsamkeit und Verantwortung im Umgang mit Daten fördern.

Der Erfolg dieser Maßnahmen hängt jedoch davon ab, dass das Unternehmen sie regelmäßig durchführt, auswertet und an neue Bedrohungen anpasst. Denn nur eine kontinuierliche Verbesserung und das Engagement auf allen Ebenen kann sicherstellen, dass „Geht nicht gibt's nicht" auch in der Cybersicherheit gilt.

Checklisten zu diesem Beitrag finden Sie unter www.datenschutz-praxis.de/datenschutzbeauftragte/checkliste-phishing-simulationen.

Eberhard Häcker ist seit vielen Jahren selbstständig und mit großer Leidenschaft sowie Kreativität externer Datenschutzbeauftragter.

Bild: iStock.com/kukhunthod

Auskunftsersuchen gemäß DSGVO stellen Unternehmen und Organisationen vor Herausforderungen. Eine davon: Nur die betroffene Person selbst darf die angefragten Informationen erhalten.

Auskunftsanspruch der DSGVO

Auskunftsersuchen: So lassen sich Fehler vermeiden

Der Auskunftsanspruch ist einer der wichtigsten Ansprüche von betroffenen Personen. Diese nutzen ihn immer häufiger – manchmal einfach nur, um zu sehen, ob Unternehmen ihre Datenschutzprozesse im Griff haben. Ein Grund mehr, sich diesem Thema zu widmen.

Rufen Sie als Datenschutzbeauftragte (DSB) den Beschäftigten bestimmte Grundsätze immer wieder ins Gedächtnis! Denn Fehler oder Versäumnisse beim Auskunftsanspruch können gravierende Folgen haben.

Auskunft nur an den richtigen Adressaten

Den schlimmsten datenschutzrechtlichen Fauxpas begehen Verantwortliche, wenn ein Auskunftsersuchen an die falsche betroffene Person gelangt. Deshalb steht an erster Stelle, die Identität der Person festzustellen, die das Ersuchen stellt.

Erwägungsgrund 64 der Datenschutz-Grundverordnung (DSGVO) beschreibt, dass Verantwortliche alle vertretbaren Mittel nutzen sollten, um die Identität einer Auskunft suchenden Person zu überprüfen. Welche das sind, lässt die DSGVO offen. Möglich ist etwa, bei der vermutlich betroffenen Person nachzufragen oder das Antwortschreiben postalisch zuzusenden und persönlich an die betroffene Person zu adressieren.

Es gilt in jedem Einzelfall abzuwägen, welche Mittel erforderlich sind, um die Identität festzustellen. Dabei ist zu beachten, um welche Daten es sich handelt, die in der Auskunft vorkommen. Sind sensible Daten betroffen (z.B. Gesundheitsdaten, siehe Art. 9 DSGVO)? Dann sollte die Identitätsprüfung strenger ausfallen und ein großes Augenmerk auf der datenschutzkonformen Übermittlung dieser Daten liegen.

Kategorien oder konkrete Empfänger?

Art. 15 Abs. 1 Buchst. c DSGVO besagt, dass „die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden", der betroffenen Person mitzuteilen sind. Dabei haben sich die Unternehmen in der Vergangenheit aus praktischen Gründen darauf berufen, dass lediglich die Kategorien von Empfängern mitzuteilen seien.

Am 12. Januar 2023 hat der Europäische Gerichtshof (EuGH) entschieden, dass jeder Betroffene das Recht hat, zu erfahren, wer die Empfänger seiner personenbezogenen Daten sind. So stehe es im Ermessen des Betroffenen, ob es ihm ausreiche, lediglich die Kategorien der Empfänger zu erfragen, oder ob er Auskunft über die konkrete Identität der Empfänger verlange. Eine Ausnahme bestehe nur dann,

- wenn es dem Verantwortlichen nicht möglich ist, die Empfänger zu identifizieren, oder
- wenn der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind.

In diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen. Das EuGH-Urteil lässt sich nachlesen unter https://ogy.de/ecor.

Fristverlängerung bekannt geben

Gemäß Art. 12 Abs. 3 DSGVO muss der Verantwortliche der betroffenen Person die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen.

Diese Frist lässt sich um weitere zwei Monate verlängern, wenn dies unter Berücksichtigung der Komplexität und →

der Anzahl der Anträge erforderlich ist. In einem solchen Fall muss der Verantwortliche den Betroffenen innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung unterrichten.

Die Gründe für die Fristverlängerung sind anzugeben. Eine Bestätigung oder eine Genehmigung durch den Betroffenen ist nicht erforderlich.

PRAXIS-TIPP

Im Zweifel sollten Verantwortliche den Weg der Fristverlängerung um zwei Monate wählen, bevor sie sich eine nicht fristgerechte Antwort zuschulden kommen lassen. Verspätete Auskünfte können einen Schadensersatzanspruch nach sich ziehen.

Das Arbeitsgericht Oldenburg hat einer betroffenen Person 10.000 Euro Schadensersatz zugesprochen, da der datenschutzrechtliche Auskunftsanspruch verletzt wurde (ArbG Oldenburg, Urteil vom 09.02.2023 – 3 Ca 150/21). In diesem Fall hatte das Unternehmen einem ehemaligen Arbeitnehmer den datenschutzrechtlichen Auskunftsanspruch zu spät erfüllt. Pro Monat der Nichterteilung der Auskunft erhielt die betroffene Person 500 Euro als Schadensersatz.

Im vorliegenden Fall kam der Verantwortliche erst im Laufe des Gerichtsverfahrens dem Auskunftsersuchen nach. Der Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO soll Präventionscharakter und eine Abschreckungsfunktion haben.

Ansprechpartner für das Auskunftsersuchen

Es ist Aufgabe der Verantwortlichen, sicherzustellen, dass Prozesse existieren, die Anfragen von Betroffenen intern in die richtigen Bahnen leiten. Nur wenn sich der Betroffene für seinen Auskunftsanspruch an eindeutig nicht mit der Sache betraute Personen wendet, muss der Verantwortliche darauf nicht antworten.

Sehr geehrte/r Herr / Frau XXX,

wir haben Ihre Auskunftsanfrage vom XX.XX.XXXX erhalten.
Selbstverständlich werden wir unserer gesetzlichen Verpflichtung nach Art. 15 Datenschutz-Grundverordnung (DSGVO) nachkommen und Ihnen die entsprechende Auskunft zukommen lassen.
Aufgrund der Komplexität Ihrer Anfrage wird dies etwas Zeit in Anspruch nehmen. Wir informieren Sie daher darüber, dass wir Ihrem Auskunftsbegehren bis spätestens XX.XX.XXXX nachkommen werden.
Falls Sie weitere Fragen hierzu oder andere Anliegen den Datenschutz bei der XYZ GmbH betreffend haben, können Sie sich jederzeit an [KONTAKTDATEN DSB oder einer sonstigen Anlaufstelle für weitere Informationen] wenden.
Informationen über die Datenverarbeitung bei der XYZ GmbH können Sie unserer Webseite unter XXXX entnehmen.

Mit freundlichen Grüßen,
XYZ GmbH

Mögliche Formulierung für eine Fristverlängerung

Bei E-Mail-Adressen dürfte es anders aussehen, gerade wenn diese im Bereich des Kundenservice angesiedelt sind. Dann kann man davon ausgehen, dass die E-Mail an die richtigen Ansprechpartner weitergeleitet wird oder ein Hinweis erfolgt, an wen sich der Betroffene wenden kann. Wichtig ist darüber hinaus, dass der Verantwortliche die Betroffenen über den entsprechenden Kanal informiert hat, wo solche Anfragen zu stellen sind. Dies ist in der Regel die Datenschutzerklärung auf der Website des Unternehmens.

BEISPIEL

Die norwegische Aufsichtsbehörde hatte einen Fall zu entscheiden, bei dem es um ein Auskunftsersuchen ging, das per E-Mail an den Geschäftsführer eines großen Unternehmens gerichtet war (nachzulesen unter https://ogy.de/f8jq). Im vorliegenden Fall stellte ein ehemaliger Mitarbeiter einen Auskunftsanspruch, den er per E-Mail an den CEO des Unternehmens mit 880 Mitarbeitenden in 14 Ländern schickte. Diese E-Mail war eine von ca. 200 eingehenden Nachrichten pro Tag für den CEO. Zu dem Betroffenen hatte dieser darüber hinaus keine direkte Beziehung.

Derartige Anträge gelten laut der norwegischen Aufsichtsbehörde nicht als wirksam, wenn der für die Verarbeitung Verantwortliche der betroffenen Person einen geeigneten Kommunikationskanal zur Verfügung stellt – in diesem Fall die E-Mail-Adresse für Datenschutzanfragen auf der Website des Unternehmens.

Fazit: Auskunftsersuchen nicht auf die leichte Schulter nehmen

Niemand sollte Anfragen von betroffenen Personen auf die leichte Schulter nehmen. Denn selbst wenn es nicht gleich ein Bußgeld hagelt, können nicht funktionierende Datenschutzprozesse ein Indiz für weitere Mängel im Datenschutz-Managementsystem sein. Daher lohnt es sich, die Beschäftigten immer wieder dafür zu sensibilisieren, wie sie mit solchen Anfragen korrekt umgehen.

Doris Kiefer ist Rechtsanwältin und leitet als Head of Data Protection das Datenschutzteam eines E-Commerce-Unternehmens für ganz Europa.

Bild: iStock.com/Choreograph

Aus datenschutzrechtlicher Sicht wichtig beim KI-Einsatz: Alle Mitarbeitenden müssen wissen, wie sie die KI nutzen dürfen – und wie eben nicht.

Künstliche Intelligenz rechtskonform nutzen

KI-Richtlinie: Grundlagen zum Einsatz von KI im Unternehmen

Künstliche Intelligenz (KI) ist Teil der Unternehmensstrategie geworden. Der AI Act (KI-Verordnung) zur Regelung des Einsatzes von KI ist in Kraft. Die ersten Umsetzungsfristen laufen im Februar 2025 ab. Nicht alle Mitarbeitenden müssen das Wissen von „KI-Beauftragten" haben, aber alle müssen wissen, was sie (nicht) dürfen. Eine KI-Richtline ist deshalb ein wichtiges Compliance-Element.

KI bietet viele Möglichkeiten beim Einsatz in Unternehmen – nicht zuletzt, um Prozesse zu optimieren sowie Arbeitsabläufe und Entscheidungen zu unterstützen. Trotz dieser Chancen und Vorteile birgt der Einsatz von KI aber Risiken, die es zu „managen" gilt.

KI-Richtlinie im Unternehmen

Eine unternehmensinterne KI-Richtlinie ist ein Baustein dieser Compliance-Pflicht. Hier bestehen Parallelen zur Organisation des Datenschutzes im Unternehmen. Datenschutzbeauftragte (DSB) können sich daher einbringen und die Unternehmensleitung dabei unterstützen, eine KI-Richtlinie zu erstellen und zu implementieren.

Aufgrund der Besonderheiten des Einsatzes von KI ist die KI-Richtlinie – anders als unternehmensinterne Datenschutzrichtlinien – nicht monothematisch, sondern muss verschiedene (rechtliche) Aspekte abdecken. Daher erfordert die Unterstützung durch den DSB den – nachfolgenden – Blick über den datenschutzrechtlichen Tellerrand.

Mitarbeitende dürfen KI nicht eigenmächtig einführen

Führen Mitarbeitende KI-Systeme eigenmächtig ein, kann dies erhebliche rechtliche und sicherheitstechnische Konsequenzen nach sich ziehen.

Die Entscheidung über die Einführung und Nutzung von KI-Systemen sollte daher zentral bei der Unternehmensleitung liegen. DSB sowie (je nach Bedarf) IT-Abteilung und Compliance-Management sind in den Bewertungs- und Entscheidungsprozess frühzeitig einzubinden. Die KI-Richtlinie soll sicherstellen und allen Mitarbeitenden (einschließlich freier Mitarbeitender!) verdeutlichen, dass sie diese Entscheidungsinstanz nicht „unterlaufen" dürfen!

Die KI-Richtlinie muss daher den Mitarbeitenden erklären, um was es geht: →

PRAXIS-TIPP

Ein Hinweis zur Erstellung einer KI-Richtlinie: Machen Sie den Mitarbeitenden deutlich, dass eine eigenmächtige Einführung zur Haftung – auch einer persönlichen – führen kann. Diesen Aspekt sollten Sie in der Richtlinie klar und prägnant, aber auch prominent formulieren, damit keine Zweifel an der (arbeits)rechtlichen Konsequenz bei Missachtung entstehen.

Exkurs: Verpflichtung von Subunternehmen

Bei den Überlegungen, wie eine KI-Richtlinie zu gestalten ist, liegt der Fokus auf den Mitarbeitenden. Dieselben Überlegungen gelten aber auch in Bezug auf Subunternehmer – insbesondere für Auftragsverarbeiter! So können Dienstleister beispielsweise auch mit KI(-Systemen) in Berührung kommen oder selbst KI(-Systeme) einsetzen wollen.
Es sollte nicht möglich sein, die unternehmensinternen Regeln in Bezug auf KI durch den Einsatz von Subunternehmen zu unterlaufen. Daher ist es wichtig, einen klaren Rahmen dafür zu schaffen, ob und in welcher Form KI-Systeme integriert sind.
Frühzeitige Vorkehrungen und Vereinbarungen mit den Subunternehmen sind wichtig, um sicherzustellen, dass die Auftragnehmer ihre Sorgfaltspflichten in Bezug auf KI einhalten.
Hier gibt es Parallelen zur datenschutzrechtlichen Einbindung von Auftragnehmern. Deshalb können DSB in diesen Konstellationen dabei unterstützen, zusätzliche Vorgaben zu erstellen und zu implementieren.

Auswirkungen des AI Acts

Der AI Act reguliert (nur) sog. KI-Systeme und definiert sie in Art. 3 Nr. 1 AI Act. Diese Definition ist jedoch recht kompliziert und damit nicht zwingend allgemein praxistauglich. Eine KI-Richtlinie muss daher einfach und verständlich erläutern, was sie als KI-Systeme erfasst. Je klarer die Beschreibung und je geringer der Ermessensspielraum, desto sicherer ist die Möglichkeit, den KI-Einsatz unternehmerisch zu steuern.

Bevor ein KI-System zum Einsatz kommt, ist es anhand der Risikokategorien des AI Acts einzuordnen (Stichwort: Risikotaxonomie des AI Acts). Danach entscheidet sich, ob das KI-System überhaupt so zum Einsatz kommen darf (siehe unten: Verbotene Praktiken) sowie welche Anforderungen durch den AI Act gelten.

Des Weiteren ist zu prüfen, ob es sich um ein KI-System mit allgemeinem Verwendungszweck (General Purpose AI) handelt. Denn für diese gelten weitere, gesonderte Anforderungen.

Darüber hinaus ist zu bewerten, ob das Unternehmen nur Betreiber – mit anderen Worten: der einfache Nutzer – des KI-Systems ist oder ob es eine der anderen Rollen des AI Act (z.B. Anbieter) einnimmt. Denn das ist der zweite wichtige Aspekt, um festzulegen, welche Anforderungen des AI Act zu beachten sind. Der AI Act weist unterschiedlichen Rollen unterschiedliche Pflichten zu.

Diese Bewertung ist entscheidend, um KI-Systeme sicher zu implementieren und zu nutzen, aber auch nicht leicht. Dies einzuordnen kann daher nicht (allein) die Aufgabe und Kompetenz der „einfachen Nutzenden" sein, die die KI-Richtlinie adressiert. Daher muss sichergestellt sein, dass die Mitarbeitenden es erkennen, wenn sie KI einsetzen und verpflichtet sind, davor die erforderliche Freigabe einzuholen (siehe oben).

KI-Kompetenz der Mitarbeitenden

Alle, die KI-Systeme im Unternehmen nutzen, müssen nach Art. 4 AI Act (KI-Kompetenz) geschult sein. Unternehmen müssen sicherstellen, dass ihre Mitarbeitenden über diese KI-Kompetenz verfügen.

Die Aufgabe, diese Schulung sicherzustellen, liegt primär bei der Unternehmensleitung. Dennoch kann die KI-Richtlinie Mitarbeitende dazu ermutigen, ihre eigenen Kenntnisse zu hinterfragen.

Deshalb ist auch wichtig, das Verbot der eigenmächtigen Einführung von KI-Systemen zu betonen. Denn viele KI-Anwendungen sind „convenient" und nutzungsfreundlich, aber nicht immer rechtskonform .

Verbotene Praktiken ausschließen

Bestimmte Praktiken der KI-Systeme sind nach Art. 5 Abs. 1 AI Act strikt verboten. Diese muss die KI-Richtlinie klar benennen und verbieten. Dieses Verbot gilt bereits ab Februar 2025.

ACHTUNG!

Auch KI-Systeme, die ursprünglich nicht für unzulässige Zwecke bestimmt waren, sind verboten, wenn jemand sie hierzu „umfunktioniert". Die KI-Richtlinie sollte ein „Umfunktionieren" daher ebenfalls ausdrücklich untersagen.

Unterschied zwischen offenen und geschlossenen Systemen

Für die Bewertung des Zulässigen ist entscheidend, ob Inhalte auf eigenen Systemen verbleiben (geschlossene Systeme) oder mit dem Einbringen in die KI die „beherrschte" eigene Unternehmensumgebung (also die geschlossenen Systeme) verlassen (siehe auch: DSK, Orientierungshilfe KI und Datenschutz vom 06.05.2024, Rn 15 ff.). Offene Systeme bieten zwar Zugang zu größeren Wissensdatenbanken und Anpassungsmöglichkeiten, erfordern jedoch, sorgfältig zu überprüfen, wer auf die Inhalte zugreifen kann.

Diese Unterscheidung wirkt sich auf die urheberrechtliche, aber v.a. auch auf die datenschutzrechtliche Bewertung aus. Die „Betriebsart" ist daher eine wesentliche Festlegung für die Nutzung von KI. Datenschutzbeauftragte sollten daher darauf hinwirken, dass dieser Unterschied dokumentiert wird und Eingang in die Bewertung des KI-Einsatzes findet.

Schutz von Betriebs- und Geschäftsgeheimnissen

Der Schutz von Betriebs- und Geschäftsgeheimnissen ist für jedes Unternehmen existenziell. Das sollte gerade beim Einsatz von KI-Systemen Beachtung finden. Denn hier besteht – vereinfacht gesagt – das Risiko, dass je nach Ausgestaltung andere „mitlesen" können.

Der AI Act hat nicht den Schutz von Geschäfts- und Betriebsgeheimnissen zum Gegenstand. Daher ist es unerlässlich, in die KI-Richtlinie Maßnahmen zum Schutz solcher Informationen zu integrieren. Darüber hinaus können auch vertragliche Geheimhaltungspflichten zugunsten von Dritten bestehen. Für diese sind erst recht die Schutzmaßnahmen zu ergreifen.

Die KI-Richtlinie sollte klar formulieren: Es ist untersagt, Informationen „einzugeben", die Betriebs- und Geschäftsgeheimnisse, urheberrechtlich geschützte Informationen oder personenbezogene Daten betreffen. Ausgenommen sind nur Fälle, in denen die entsprechende Instanz im Unternehmen (siehe oben) eine Freigabe erteilt hat.

Urheberrecht ist zu beachten

Das Urheberrecht kann bei der Nutzung von KI in unterschiedlichen Konstellationen Relevanz erlangen. Diese Konstellationen sind zu beachten, wenn Unternehmen eine KI-Richtlinie gestalten:

Die Frage der Urheberrechte an KI ist vielschichtig und betrifft sowohl die Entwickler von KI als auch Unternehmen, die diese Systeme einsetzen. KI kann als Computerprogramme oder Datenbanken urheberrechtlich geschützt sein. Ob und wann ein solcher Schutz besteht, wird in der Fachliteratur kontrovers diskutiert.

Unternehmen, die KI einsetzen möchten, müssen dennoch eines sicherstellen: Sofern die KI urheberrechtlich geschützt ist, müssen sie über die entsprechenden Urheber- und/oder Nutzungsrechte verfügen. Dies umfasst sowohl die Software selbst als auch die zugrunde liegenden Inhalte und Datenbanken. Die KI-Richtlinie sollte daher klare Vorgaben enthalten: Mitarbeitende müssen die Berechtigung für die konkrete Nutzung prüfen, bevor sie die KI nutzen.

Eine weitere Konstellation betrifft den Fall, dass Mitarbeitende urheberrechtlich geschützte Inhalte einbringen, wenn sie KI nutzen. Unternehmen müssen sicherstellen, dass sie keine urheberrechtlich geschützten Inhalte ohne Genehmigung verwenden, wenn sie eine KI trainieren oder einsetzen.

Dies gilt insbesondere für Daten, die zum Einsatz kommen, um die KI-Modelle zu verbessern. Die KI-Richtlinie sollte präzise festlegen, welche Schritte Mitarbeitende beachten müssen, um Urheberrechtsverletzungen zu verhindern.

Die dritte Konstellation ist die Frage, ob Inhalte, die mittels KI geschaffen wurden, urheberrechtlich schutzfähig sind. Obwohl die KI-Richtlinie dies nicht regeln kann, sollte sie vor diesem Problem warnen.

Nach deutschem Urheberrecht können nur natürliche Personen Werke im Sinne des Urheberrechts schaffen. Vereinfacht: Es gibt kein Urheberrecht an Inhalten, die ohne menschliches Zutun allein durch KI generiert werden.

Dies wird relevant, wenn das Unternehmen solche Inhalte gegen Entgelt Dritten überlassen will. Denn dann stellt sich die Frage: Für was zahlen Dritte eigentlich ein Entgelt, wenn keine Nutzungsrechte eingeräumt werden können, weil kein Schutz durch das Urheberrecht besteht?

Ebenso besteht dann durch das Urheberrecht kein Schutz dagegen, dass andere Dritte die Inhalte nutzen. Zwar kennt das Urheberrecht auch Leistungsschutzrechte für Werke, die keine Werke im Sinne des Urheberrechts sein müssen, jedoch ist deren Schutz eingeschränkt.

Die KI-Richtlinie sollte regeln, wie im Unternehmen dokumentiert wird, ob den jeweiligen Inhalt ein Mensch oder allein KI erstellt hat. Damit ist zukünftig die Grundlage für eine Bewertung gegeben.

Datenschutzrecht: Viele Herausforderungen

Aus datenschutzrechtlicher Sicht stellt sich eine Vielzahl an Fragen bei der Nutzung von KI. Diese muss und kann eine KI-Richtlinie nicht für jeden Anwendungsfall im Vorhinein und pauschal beantworten. Die KI-Richtlinie muss jedoch →

Exkurs: GeschGehG – kein Schutz ohne Schutzmaßnahmen

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) schützt – anders als das frühere Gesetz gegen den unlauteren Wettbewerb (UWG) – ein Geheimnis nicht allein deshalb, weil das Unternehmen es als Geheimnis einordnet. Das GeschGehG gewährt nur dann Schutz, wenn ein Unternehmen auch angemessene Schutzmaßnahmen ergriffen hat. Unternehmen müssen sicherstellen, dass sie geeignete organisatorische und technische Maßnahmen implementieren, um ihre Geheimnisse effektiv zu schützen. Die hierfür getroffenen Schutzmaßnahmen dürfen nicht durch oder im Rahmen des Einsatzes von KI unterlaufen werden.

Hinweis zum Urheberrecht: Recht auf Bearbeitung

Das Recht zur Nutzung umfasst nicht immer stets auch das Recht zur Bearbeitung – vereinfacht: das Recht zur Veränderung und Nutzung des Veränderten. Unter diesem Aspekt gilt es daher, den Einsatz im Unternehmen zu hinterfragen. Auch hier zeigt sich: Unternehmen müssen verhindern, dass Mitarbeitende KI eigenmächtig nutzen. Denn auch für eine Urheberrechtsverletzung kann das Unternehmen in die Haftung genommen werden.

Ein Fall für den DSB – Datenschutz beim Training von KI-Systemen

Eine Besonderheit ist das Training von KI. Für Mitarbeitende ist es wichtig zu verstehen, dass auch diese Datenverarbeitung den datenschutzrechtlichen Vorschriften unterliegt. Die KI-Richtlinie muss derart klar und verständlich formuliert sein, dass Mitarbeitende keine Zweifel daran haben, was zu beachten ist. Auf jeden Fall ist zu verhindern, dass personenbezogene Daten ungewollt als Trainingsdaten Verwendung finden.

für den Datenschutz gerade mit Blick auf KI sensibilisieren. Bei diesem vielschichtigen Thema können DSB unterstützen.

Die KI-Richtlinie sollte Mitarbeitende dazu anhalten, die datenschutzrechtliche Rolle einzuordnen: Ist das Unternehmen alleinverantwortlich (Art. 4 Nr. 7 Alt. 1 DSGVO), gemeinsam verantwortlich (Art. 4 Nr. 7 Alt. 2 DSGVO) oder Auftragsverarbeiter (Art. 28, 4 Nr. 8 DSGVO)? Diese Klarheit ist entscheidend, um die rechtlichen Verantwortlichkeiten im Umgang mit personenbezogenen Daten festzulegen.

ACHTUNG!

Wenn die genutzte KI personenbezogene Daten enthält, ist deren Nutzung datenschutzrechtlich zu bewerten. Dies gilt sowohl für das Training einer KI als auch für die Anwendung der (trainierten) KI.

Die KI-Richtlinie sollte deutlich klarstellen, was unter personenbezogenen Daten zu verstehen ist (zum Personenbezug siehe Eckhardt, Datenschutz PRAXIS 11/2023, S. 14). Gerade hier gibt es viele Missverständnisse, die bei einer nachträglichen Bewertung zu bösen „Aha-Effekten" führen können.

Bei jedem Einsatz von KI zu beachten sind insbesondere das Verbot mit Erlaubnisvorbehalt im Zusammenspiel mit der Zweckbindung (Art. 6 DSGVO), die Datenminimierung (Art. 5 Buchst. c DSGVO) sowie Data Protection by Design and Default (Art. 25 DSGVO). Ein klarer Fall für den DSB.

Eines gerät häufig aus dem Blick: Es ist nicht nur zu prüfen, ob die Nutzung personenbezogener Daten zulässig ist. Vielmehr besteht auch die Pflicht, die betroffene Person zu informieren, insbesondere bei einer zweckändernden Weiterverarbeitung.

Der oder die Verantwortliche muss auch hinterfragen, ob der Einsatz der künstlichen Intelligenz zu einer automatisierten Entscheidungsfindung im Sinne von Art. 22 DSGVO führt. Das erfordert eine zusätzliche Zulässigkeitsprüfung sowie Informationspflichten nach Art. 13 und Art. 14 DSGVO.

Die KI-Richtlinie sollte auch festlegen, dass zu prüfen ist, ob eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO erforderlich ist. Und sie sollte festlegen, dass eine Verarbeitung erst zulässig ist, nachdem dies geprüft wurde. Obwohl es Überschneidungen mit den Anforderungen des AI Act gibt, sind die Schutzziele nicht deckungsgleich.

Auch wenn das nun innovationshemmend klingt (und vielleicht auch ist), ist es geltendes Recht. Verstöße können zur Untersagung (Art. 58 Abs. 2 Buchst. f DSGVO) führen, ebenso zu Sanktionen (Art. 83 DSGVO) sowie Schadensersatzansprüchen (Art. 82 DSGVO).

Klarheit der KI-Richtlinie

Wichtig ist: Die KI-Richtlinie muss so formuliert sein, dass sie für alle Mitarbeitenden verständlich ist. Und sie muss es ihnen ermöglichen, die rechtlichen Rahmenbedingungen einzuhalten, ohne eine rechtliche Detailprüfung vorzunehmen.

Diese muss durch die zuständige Instanz im Unternehmen erfolgen, an die sich die Mitarbeitenden wenden können. Daher muss die KI-Richtlinie diese Instanz ebenfalls benennen. Mit der KI-Richtlinie kann daher einhergehen, eine entsprechende Instanz im Unternehmen einzurichten.

Sensibilisierung der Mitarbeitenden ist Kernaufgabe beim Einsatz von KI

Die zusammengestellten Aspekte – ohne Anspruch auf Vollständigkeit – zeigen, dass der Einsatz von KI aus rechtlicher Sicht ein Querschnittsthema ist. Die Mitarbeitenden für mögliche Risiken zu sensibilisieren, ist eine Kernaufgabe der Unternehmensleitung beim Einsatz von KI. Gerade bei den relevanten Aspekten, bei denen nicht pauschal„Schwarz-weiß"-Aussagen möglich sind, ist es wichtig, die Mitarbeitenden zu sensibilisieren, damit das Unternehmen der Compliance-Pflicht genügen kann.

Dr. Jens Eckhardt ist Rechtsanwalt und Partner bei pitc legal Eckhardt Rechtsanwälte Partnerschaft mbB in Düsseldorf.
Juri Knaub ist ebenfalls Partner und Rechtsanwalt bei pitc legal Eckhardt Rechtsanwälte Partnerschaft mbB.

Datenschutzaufsicht Sachsen

Ratgeber „Achtung Kamera!“

Bild: iStock.com/KHAFIZH

Die rechtlichen Vorgaben für die Videoüberwachung erläutert sehr detailliert ein Ratgeber aus Sachsen. Seine drei Hauptkapitel behandeln die Videoüberwachung durch Unternehmen und Privatpersonen, die Videoüberwachung im öffentlichen Bereich (insbesondere durch Kommunen) und das Sondergebiet der Videoüberwachung durch die Polizei in Sachsen.

Enge „Haushaltsausnahme“

Bei Privatpersonen ist die Videoüberwachung im Nachbarschaftskontext besonders streitträchtig (S. 41), aber auch die Dokumentation von Ordnungswidrigkeiten, etwa von Parkverstößen, mittels Video (S. 67). Dabei ist jeweils zu beachten, dass die „Haushaltsausnahme“ von Art. 2 Abs. 2 Buchst. c DSGVO nur einen engen Anwendungsbereich hat (S. 32).

Dashcams – rechtlich riskant!

Dashcams (auch „Unfallkameras“ genannt) sind bei Autofahrern sehr beliebt. Radfahrer und Motorradfahrer verwenden sie in Form von Helmkameras. Damit die Verwendung solcher Kameras keine Bußgelder nach sich zieht, empfiehlt es sich, die umfangreichen Hinweise zu diesem Thema zu beachten (S. 70–76). Ein neuer Trend scheinen Innenkameras in Autos zu sein. Werden sie heimlich betrieben, kann dies erheblichen Ärger mit sich bringen (S. 71).

Viele Hinweise zu Sonderfragen

Branchenspezifische Besonderheiten ergeben sich bei Videoaufnahmen etwa im Einzelhandel (S. 57) oder in medizinischen Einrichtungen (S. 59). Sie sind im Ratgeber der Datenschutzaufsicht Sachsen ebenso detailliert behandelt wie die Grundsätze, die bei der Videoüberwachung von Beschäftigten maßgeblich sind (S. 44–53). Der Ratgeber berücksichtigt auch sehr spezielle Themen wie die Baustellenüberwachung (S. 56) oder die Parkraumüberwachung (S. 80–82). Selbst Themen wie Wildkameras (S. 79) sind behandelt.

Quelle: Datenschutzaufsicht Sachsen, Achtung Kamera! Hinweise zur Videoüberwachung für Bürgerinnen und Bürger, Wirtschaft und Behörden, 2. Aufl., Juni 2024. Die Broschüre (Umfang: 116 Seiten) ist abrufbar unter https://ogy.de/n4c8, aber auch gedruckt erhältlich.

Datenschutzaufsicht Baden-Württemberg

Navigator „KI & Datenschutz“

Zum Thema „KI und Datenschutz“ haben sich bereits zahlreiche Datenschutzaufsichtsbehörden geäußert. Einen möglichst umfassenden Überblick dazu will die Datenschutzaufsicht Baden-Württemberg bieten. Sie hat deshalb eine „Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschutzrechts in aufsichtsbehördlichen Orientierungshilfen zu Künstlicher Intelligenz“ erstellt.

Tabelle „10 mal 10“

Eine Tabelle benennt zehn zentrale Themenstellungen, die bei KI-Anwendungen regelmäßig eine Rolle spielen. Dazu gehören etwa der Grundsatz der Datenminimierung und die Frage, welche Rechte betroffene Personen haben. Zu jedem Thema weist die Tabelle nach, was dazu in zehn Papieren von Aufsichtsbehörden zu finden ist. Die Palette der berücksichtigten Dokumente reicht von der Hambacher Erklärung der Datenschutzkonferenz (DSK) von 2009 bis zu mehreren Darstellungen aus dem Jahr 2024, etwa der „Checkliste KI“ des Bayerischen Landesamts für Datenschutzaufsicht vom Januar 2024.

Nach Auffassung der Datenschutzaufsicht Baden-Württemberg ergibt sich – trotz unterschiedlicher Schwerpunkte im Detail – ein sehr einheitliches Bild in der Auslegung. Es bleibt abzuwarten, ob dies allgemeine Zustimmung finden wird.

Quelle: Datenschutzaufsicht Baden-Württemberg, Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA), Stand: Juli 2024, abrufbar unter https://ogy.de/kzhf.

Europäischer Datenschutzausschuss

Datenschutzrahmen EU–USA

Zwei Einstiegshilfen zum Datenschutzrahmen EU–USA hat der Europäische Datenschutzausschuss (EDSA) verabschiedet. Der erste Text richtet sich an natürliche Personen, also an „Normalbürger“. Der zweite Text wendet sich dagegen an Unternehmen in der EU, die Daten an Unternehmen in den USA übermitteln.

Beide Papiere beantworten jeweils kurz vier Grundfragen. Dazu gehört für „Normalbürger“ etwa die Frage, wie sie eine Beschwerde wegen Verletzung ihrer Rechte durch US-Organisationen einreichen können. Unternehmen erhalten beispielsweise Hinweise dazu, unter welchen Voraussetzungen ihre US-Geschäftspartner sich auf eine Zertifizierung nach dem Datenschutzrahmen berufen können.

Quellen: Europäische Datenschutzausschuss (EDSA), EU-U.S. Data Privacy Framework: F.A.Q. for European Indivduals / EDSA, EU-U.S. Data Privacy Framework: F.A.Q for European Businesses; beide Papiere wurden am 16.07.2024 angenommen. Sie sind (nur auf Englisch) abrufbar unter https://ogy.de/kwu0.

Dr. Eugen Ehmann ist u.a. Spezialist für transatlantischen Datenschutz. Auch dieses Jahr moderiert er zusammen mit Daniela Will den Datenschutzkongress IDACON. Dieser findet vom 05.11. bis 07.11.2024 statt. Die Anmeldung ist noch möglich unter www.idacon.de.

Bild: iStock.com/alexsl

Vermieter und Hausverwaltungen sind gegenüber den Mietparteien verpflichtet, die Datenschutz-Grundverordnung einzuhalten. Praxisbeispiele zeigen, worauf hier besonders zu achten ist.

Datenschutz rund um Immobilien

Miete und Wohneigentum datenschutzkonform verwalten

Wer als Vermietender, Wohnungseigentümer oder Hausverwaltung im Datenschutz wann was zu tun oder zu lassen hat, ist den Handelnden oft unklar. Daher bekommen die Aufsichtsbehörden immer wieder Beschwerden. Der Artikel zeigt Praxisfälle für DSB, die in dieser Branche beraten.

Vermieter, Wohnungseigentümer, Hausverwaltungen und Immobilienmakler müssen als Verantwortliche im Arbeitsalltag die Regeln der Datenschutz-Grundverordnung (DSGVO) einhalten. Was bedeutet das genau? Die vorgestellten Fälle stammen aus dem Tätigkeitsbericht der Sächsischen Datenschutz- und Transparenzbeauftragten für 2023. Der Bericht findet sich unter dem Link https://ogy.de/qxyh.

Einsatz von Funk-Rauchwarnmeldern

Der Vermieter lässt in der Mietwohnung Funk-Rauchwarnmelder installieren. Der Mieter befürchtet eine Überwachung seines Verhaltens und meint, es liege eine automatisierte Verarbeitung personenbezogener Daten vor, sodass seine Einwilligung erforderlich sei.

Funk-Rauchwarnmelder sind in der Lage, mit jeweils anderen Funk-Rauchwarnmeldern zu kommunizieren. Das bedeutet, geht bei einem der Melder der Alarm los, aktiviert das auch die anderen Melder in der Wohneinheit.

Wer Funk-Rauchwarnmelder betreibt, verarbeitet personenbezogene Daten. Deshalb gilt die DSGVO. Die Verpflichtung zum Einbau von Rauchwarnmeldern ergibt sich aus den jeweiligen Landesbauordnungen. Damit ist die Rechtsgrundlage für die Datenverarbeitung Art. 6 Abs. 1 Buchst. c DSGVO, da eine gesetzliche Grundlage vorliegt. Eine Einwilligung des Mieters ist damit nicht erforderlich.

Allerdings sind Vermieter verpflichtet, ihre Mieterinnen und Mieter entsprechend Art. 13 DSGVO vor dem Einbau der Rauchwarnmelder zu informieren, insbesondere darüber, welche personenbezogenen Daten die Geräte konkret erfassen (Tätigkeitsbericht, S. 86).

Datenübertragung durch fernablesbare Messgeräte

Um die Heizkosten in einem Mehrfamilienhaus zu erfassen, erhalten die Heizkörper in den Wohnungen der Mieter fernablesbare Messgeräte. Über eine WLAN-Verbindung gelangen die Verbrauchswerte zusammen mit einer personenbeziehbaren Kennung an einen Dienstleister oder den Hauseigentümer.

Bei den Verbrauchswerten der Wohnung handelt es sich um personenbezogene Daten im Sinne der DSGVO. Rechtsgrundlage für die Erfassung der Werte ist Art. 6 Abs. 1 Buchst. c DSGVO. Die zugehörige gesetzliche Grundlage findet sich in der Heizkostenverordnung. Die Verbrauchsdaten sind zum Zweck der Abrechnung über die Nebenkosten zu ermitteln. Erfolgt die Abrechnung nicht über den Hauseigentümer oder Vermieter selbst, sondern über einen Dienstleister, so muss der Vermieter als Verantwortlicher mit dem Dienstleister einen Vertrag über eine Auftragsverarbeitung nach Art. 28 DSGVO schließen.

Der Verantwortliche ist verpflichtet, seine Mieterinnen und Mieter als betroffene Personen nach Art. 13 DSGVO über diese Auftragsverarbeitung zu informieren. Eine separate Informationspflicht über den Einsatz der fernablesbaren Messgeräte und ggf. installierter Datensammler sieht die Sächsische Datenschutz- und Transparenz-

beauftragte nicht, hält es aber für angemessen, die Mieter trotzdem darüber zu informieren, um Diskussionen zu vermeiden.

Daten von Eigentümern einer Wohnungseigentumsgemeinschaft

Eigentümer von Wohnungen innerhalb einer Eigentumsgemeinschaft können vor ihren Miteigentümern nicht unbekannt bleiben. Anderenfalls wären die gesetzlichen Regelungen nicht umsetzbar. Denn die Eigentümerinnen und Eigentümer haben Rechte und Pflichten gegenüber ihren Miteigentümern. Geregelt ist dies im Wohnungseigentumsgesetz (WEG).

In den meisten Fällen verwaltet eine Hausverwaltung die Eigentumsgemeinschaften. Sie kümmert sich nach den Regeln des WEG um die Finanzen der Wohnungseigentumsgemeinschaft, die Instandhaltung des Gebäudes sowie die Beschlussfassungen der Eigentümer.

Um diese Aufgaben erfüllen zu können, benötigt die Hausverwaltung die Kontaktdaten aller Eigentümer. Es gehört zu ihren gesetzlichen Aufgaben nach dem WEG, eine entsprechende Eigentümerliste zu führen, um z.B. zur Eigentümerversammlung einladen zu können. Rechtliche Grundlage hierfür ist Art. 6 Abs. 1 Buchst. c DSGVO in Verbindung mit dem WEG.

Die Hausverwaltung muss Eigentümern Einsicht in die Verwaltungsunterlagen geben (§ 18 Abs. 4 WEG), wozu auch die Eigentümerliste gehört. Die einzelnen Eigentümer müssen für verschiedene Zwecke im Rahmen des WEG ihre Miteigentümer kontaktieren können. Datenschutzrechtliche Grundlage ist wieder Art. 6 Abs. 1 Buchst. c DSGVO.

Umstritten ist jedoch, in welchem Umfang die Hausverwaltung personenbezogene Daten einzelner Eigentümer an die Miteigentümer herausgeben darf. Nach der Rechtsprechung des Landgerichts Düsseldorf (04.10.2018, Az. 25 S 22/18) sind dafür Name und ladungsfähige Anschrift, also die Adresse, ausreichend.

Für die Herausgabe weiterer Kontaktdaten wie Telefonnummern oder E-Mail-Adressen durch die Hausverwaltung ist eine Einwilligung der jeweiligen Eigentümer nach Art. 6 Abs. 1 Buchst. a DSGVO notwendig. Der Fall ist nachzulesen auf S. 90 des Tätigkeitsberichts.

Werbeansprachen durch die Hausverwaltung

Nutzt die Hausverwaltung die personenbezogenen Daten aus der Eigentümerliste für eigene Zwecke, so ist die Zulässigkeit dieser Verwendung danach zu beurteilen, ob der Zweck mit der Verwaltungstätigkeit zusammenhängt.

Die Hausverwaltung ist nach dem WEG handelndes Organ der Wohnungseigentümergemeinschaft (§§ 9b, 27 WEG). Nutzt der Verwalter die Eigentümerliste für Geburtstags- oder Festtagsgrüße an die Eigentümerinnen und Eigentümer, so steht das noch im Zusammenhang mit der Verwaltungstätigkeit und ist aus Sicht der Sächsischen Datenschutz- und Transparenzbeauftragten von Art. 5 DSGVO gedeckt. Eine Unzulässigkeit nach den Regeln des Gesetzes gegen den unlauteren Wettbewerb (UWG) kommt hier nicht in Betracht, da zwischen den Eigentümern und der Hausverwaltung eine gesetzlich vorgesehene Beziehung besteht und kein Unternehmer-Kunden-Verhältnis. Daher ist das UWG nicht anwendbar.

Will die Hausverwaltung jedoch über den Rahmen der Verwaltungstätigkeit hinaus Werbeansprachen, z.B. zum regionalen Immobilienmarkt, gegenüber den Eigentümerinnen und Eigentümern vornehmen, so ist dafür zwingend eine Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO notwendig (Tätigkeitsbericht, S. 125).

Wohnungsfotos aufnehmen

In einer vermieteten Wohnung wollen der Vermieter bzw. ein Makler Fotos anfertigen, um die Wohnung zwecks Neuvermietung oder Verkauf inserieren oder ein Exposé für den Verkauf gestalten zu können.

Im Beschwerdefall, den die Sächsische Datenschutz- und Transparenzbeauftragte zu beurteilen hatte (Tätigkeitsbericht S. 122), lag eine mündliche Einwilligung der aktuellen Mieter vor, Fotos anzufertigen. Allerdings hatten sich die Mieter vorbehalten, die Fotos vor der Veröffentlichung durch den Makler freizugeben, was dieser bestritt. Letztlich waren persönliche Einrichtungsgegenstände der Mieter auf den Fotos zu sehen, die der Makler im Internet veröffentlicht hat.

Für Fotos der Inneneinrichtung einer vermieteten Wohnung ist immer die Einwilligung der betroffenen Mieter erforderlich (Art. 6 Abs. 1 Buchst. a DSGVO). Die Einrichtung einer Wohnung und persönliche Gegenstände gehören zum persönlichen Lebensbereich der Bewohnerinnen und Bewohner und lassen bei Veröffentlichung Rückschlüsse auf diese zu. Die Einwilligung sollte sowohl das Anfertigen der Fotos als auch – soweit benötigt – das Veröffentlichen umfassen. Um Missverständnisse zu vermeiden, empfiehlt es sich in solchen Fällen, die Einwilligung schriftlich einzuholen.

Zu beachten ist, dass die betroffenen Mieter ihre Einwilligung widerrufen und verlangen können, die Fotos zu löschen. So hat sich auch der konkrete Fall gelöst: durch eine Aufforderung, die Fotos zu löschen, sowie die Bestätigung des Maklers, die Fotos gelöscht zu haben.

PRAXIS-TIPP

Die Mieter rechtzeitig zu informieren, kann den Verantwortlichen Beschwerden bei den Aufsichtsbehörden ersparen. Ein bedachter Umgang mit den Persönlichkeits- und Datenschutzrechten von Mietern und Wohnungseigentümern vonseiten der Verantwortlichen reduziert den Ärger und minimiert das Risiko von Bußgeldern.

Rechtsanwältin Andrea Gailus ist in eigener Anwaltskanzlei tätig und befasst sich neben dem Zivilrecht schwerpunktmäßig mit IT- und Datenschutzrecht.

Bild: Das Bild wurde mit einer eigenen, lokalen Dr.-DSGVO-KI generiert

Die Nutzung von KI-Services in der Cloud birgt aus Datenschutzsicht zahlreiche Probleme. Ein lokal betriebenes KI-System (Offline-KI) kann helfen, viele dieser Probleme zu vermeiden.

Cloud-Services ersetzen für besseren Datenschutz

Offline-KI: künstliche Intelligenz für Unternehmen

Eine Offline-KI läuft auf einem eigenen Server. Sie muss keine Daten mit Dritten austauschen, kann aber bei Bedarf auf das Internet zugreifen oder mit anderen IT-Systemen kommunizieren. Oft leistet eine solche KI mehr als ChatGPT. Wann lohnt sich eine Offline-KI und was bietet sie genau?

Viele Probleme, die vor wenigen Jahren kaum oder nur mit sehr hohem Aufwand zu lösen waren, sind dank künstlicher Intelligenz (KI) nun gut zu bewältigen. KI kann zahlreiche Prozesse in Unternehmen und Behörden unterstützen. Beispielhaft genannt seien:

- Suche nach Wissen
- Dokumente digitalisieren
- Sprache in Text umwandeln (Meetings, Podcasts, Videos)
- Empfehlungen für Anfragenbearbeitungen generieren
- Blog-Artikel erstellen
- Marketing-Unterlagen (Bilder, Präsentationen) generieren
- Informationen aus Texten, Bildern oder Videos extrahieren

Massive Datenverarbeitung

Kein anderes System verarbeitet potenziell mehr Daten als ein KI-System. Es beginnt bereits in der Anfangsphase eines KI-Modells, etwa eines Sprachmodells, auch Large Language Model (LLM) genannt. Diese Phase heißt „Pre-training". Der Prozess ist vergleichbar mit der Erziehung eines Kindes und der anschließenden Ausbildung als Erwachsener. Für das Training sind üblicherweise viele Milliarden Textdokumente erforderlich, um die nötige Qualität zu erzielen.

Ein fertiges Sprachmodell lässt sich dann befragen, indem man einen Prompt eingibt, also eine textliche Anfrage in natürlicher Sprache. Der Prozess, der die Antwort auf den Prompt generiert, heißt Inferenz. Dabei verarbeitet die KI sowohl die Eingabedaten als auch die Daten, die im KI-Modell vorhanden sind.

Das KI-Modell ist eine Art elektronisches Gehirn, das aus einem sehr großen künstlichen neuronalen Netz besteht. In diesem neuronalen Netz ist das „Wissen" des KI-Modells gespeichert.

Rechtliche Fragen

Bei der Nutzung von KI-Systemen und Servern in der Cloud – z.B. bei ChatGPT oder Microsoft Azure – stellt sich die Frage, was mit den Eingabedaten und den Antworten des KI-Modells beim Cloud-Anbieter passiert. Ebenso bleibt oft unklar, auf welchen Trainingsdaten Closed-Source-Modelle wie ChatGPT von OpenAI oder Gemini von Google basieren.

Bei Cloud-Diensten gibt es letztendlich keine Möglichkeit, Datensicherheit und Datenschutz sicherzustellen. Vielmehr kommt im besten Fall ein rechtlich verbindliches Dokument zustande, etwa ein Auftragsverarbeitungsvertrag o.Ä. Dies erfordert es oft, einen Juristen hinzuzuziehen, der die Vertragslage prüft. Damit ist dann bestenfalls formal bestätigt, dass die Datenproblematik gelöst ist.

Insbesondere große Cloud-Anbieter sind oft von Sicherheitslücken, Datenskandalen und Hackerangriffen bedroht. Beispiele sind etwa die Azure-Schwachstelle vom 07.06.2024 mit einem Schweregrad 10 von 10 oder die zeitweilige Sperre von ChatGPT aus Datenschutzgründen in Italien. Immerhin gibt es z.B. mit Mistral auch europäische Anbieter, bei denen der amerikanische CLOUD Act keine Rolle spielen dürfte.

Kriterien für KI-Systeme

Neben den angerissenen rechtlichen Fragen beim Einsatz von KI aus der Cloud gibt es eine Reihe weiterer Aspekte, die bei KI-Systemen zu betrachten sind:

- Qualität der Ergebnisse
- Zuverlässigkeit der Ergebnisse
- Kenntnis der Zuverlässigkeit
- Kosten
- Abhängigkeit
- Strategie

Selbst ChatGPT als hoch entwickeltes KI-System lässt bei einigen Fragestellungen eine akzeptable Qualität der Antworten vermissen. Bei guten Ergebnissen stellt sich in zahlreichen Anwendungsfällen zudem die Frage, ob nicht sehr gute Ergebnisse möglich wären, die im Endeffekt mehr Zeit und Kosten sparen würden.

Die Qualität der Ergebnisse hängt zwar eng mit der Zuverlässigkeit zusammen. Jedoch ist es ein Unterschied, ob zu einem guten oder schlechten Ergebnis bekannt ist, dass es gut oder schlecht ist, oder ob diese Kenntnis nicht existiert. Zuverlässig kann ein KI- System nur dann sein, wenn es in sehr vielen Fällen eine als korrekt anzusehende Antwort liefert. Es sagt idealerweise zu jeder Antwort dazu, ob sie diese als zuverlässig einstuft oder ob Unsicherheiten bestehen. Auch die Angabe von Quellen in jeder KI-Antwort trägt zur Glaubwürdigkeit eines KI-Systems bei.

Zur Strategie eines Unternehmens gehört auch die Automatisierung von Unternehmensprozessen mithilfe von KI. Einige Unternehmen und Behörden versuchen, die Mitarbeitenden mit einer Chatbox oder einem Copilot-Zugang zufriedenzustellen. Dieser bequeme Weg ist der schnellste, aber wahrscheinlich nicht der beste.

Alles, was mit Automatisierung zu tun hat, spielt sich in der Black Box der Cloud-Anbieter ab. Die Integration eigener IT-Prozesse und IT-Systeme gehen viele Unternehmen oft gar nicht erst an, wenn sie überhaupt möglich wäre.

Alternative zu Cloud-Diensten: Offline-KI

Die Alternative zu kostspieligen Cloud-Diensten heißt Offline-KI. Ein gutes Argument für eine solche KI, die auf eigener Hardware oder Miet-Hardware läuft, ist deren Antwortqualität. Ein paar Beispiele sollen dies illustrieren:

- Audiotranskription ist mit Offline-KI deutlich besser möglich als mit Microsoft Teams.
- Wissen zu finden, funktioniert oft viel besser mit Offline-KI als mit Universalsystemen.
- Übersetzte Bilder zu erzeugen, die Texte enthalten, ist mit Offline-KI sehr gut möglich, mit ChatGPT hingegen kaum.
- Ein Frage-Antwort-Assistent auf Basis einer Offline-KI kann viel zuverlässigere Antworten geben, als ChatGPT es jemals tun kann. Auch die Geschwindigkeit kann deutlich höher liegen.

Zusätzlich bietet eine Offline-KI die maximal mögliche Datenkontrolle. Daten gehen nirgendwo hin, außer man möchte es. Die KI kann offline arbeiten, muss es aber nicht. Bei Bedarf kann sie auf das Internet oder auf das Intranet eines Unternehmens zurückgreifen. Auch die Zugriffskontrolle auf Daten durch ein Berechtigungssystem ist möglich. Datenschutzbeauftragte (DSB) können Offline-KI daher als eine Option in ihre Beratung aufnehmen.

Eine Offline-KI läuft auf einem KI-Server, der im Eigentum des Unternehmens oder der Behörde ist. Alternativ kann man Server von einem deutschen Anbieter in einem deutschen Rechenzentrum mieten. Mit einem vorinstallierten KI-System und Betreuung sind diese Server schon ab 400 Euro im Monat erhältlich.

Der Motor der Offline-KI ist eine weltweit etablierte KI-Plattform, die auf der Programmiersprache Python basiert. Dazu kommt ein sehr leistungsfähiges Open-Source-KI-Modell. Damit ist alles Wesentliche über die Kosten gesagt. Egal, wie oft Sie oder Ihre Mandanten dieses KI-System nutzen: Die Kosten sind abgesehen von den Stromkosten üblicherweise immer gleich. Lizenzgebühren fallen nicht an.

Juristische Fragen stellen sich bei einem eigenen KI-System kaum. Der Vertrag zur Auftragsverarbeitung (AVV) entfällt bei eigener Hardware. Für einen Miet-Server bei einem deutschen Anbieter kann dessen AVV ohne Begriffe wie „Data Privacy Framework“, „CLOUD Act“ oder „EO 12333“ auskommen.

Die Entwicklung im KI-Umfeld schreitet rasend schnell voran. Offline-KI bietet die Möglichkeit, noch leistungsfähigere Sprachmodelle anstelle des bisher genutzten einzusetzen, sobald diese verfügbar sind. Der Aufwand hierfür ist oft ausgesprochen gering.

Wann lohnt sich eine Offline-KI?

Die erste Frage lautet: Wofür soll die KI zum Einsatz kommen? Je besser Ihre Mandanten oder Ihr Unternehmen mögliche Anwendungsfälle für die KI beschreiben, desto eher lassen sich die gesetzten →

Kosten für KI in der Cloud

Cloud-Dienste rechnen typischerweise nach Intensität der Nutzung ab. Die Kosten bleiben niedrig bei geringer Nutzung und können bei häufiger oder anspruchsvoller Nutzung sehr hoch ausfallen. Niemand weiß vorab genau, wie oft man ein KI-System befragen muss, bis man das gewünschte Ergebnis erzielt. Das Verbessern einer KI, der wohl interessanteste Punkt für Unternehmen, ist in der Cloud besonders kostenintensiv.
Nutzungsabhängige Entgelte, die sich zudem nicht vorhersagen lassen, sind eine Barriere, die einer strategischen Vorgehensweise zuwiderlaufen können. Ein Beispiel: Aktuell sind bereits KI-Systeme möglich, die sich selbst kritisieren und sich selbst verbessern. Diese Selbstverbesserung erfordert eine Dauerschleife. Nutzungsabhängige Entgelte und eine Dauerschleife passen für die Buchhaltung nicht gut zusammen.

Ziele erreichen. Ein solches Ziel kann es sein, Prozesse zu beschleunigen und zu optimieren

Sehr gute Anwendungsfälle für Offline-KI sind z.B., spezielles Wissen zu recherchieren oder Mitarbeitende bei der Bearbeitung von Anfragen zu unterstützen. Auch die Automatisierung von Prozessen ist ein guter Anwendungsfall.

Wissen zu finden, lässt sich durch eine KI-gestützte semantische Suche antreiben. Die semantische Suche zielt darauf ab, die Intention und den Kontext hinter den Anfragen zu verstehen, um relevantere Ergebnisse zu liefern. Dies ist sogar auf preiswerter Hardware unterhalb der oben genannten Kosten möglich. Viel Wissen liegt in unternehmenseigenen Dokumenten. Naturgemäß sollen diese Informationen nicht in den Besitz von Dritten gelangen und müssen es mit einer Offline-KI auch nicht.

Eine Offline-KI kann Mitarbeitende in den verschiedensten Bereichen dabei unterstützen, ihre Arbeit effizienter zu gestalten und bessere Ergebnisse zu produzieren.

BEISPIEL

Ein beispielhafter Prozess sieht wie folgt aus: Der Kunde eines Autoverleihers schreibt eine E-Mail, in der er einen Schaden am Mietwagen meldet. Beim Einparken könnte ein Außenspiegel in Mitleidenschaft gezogen worden sein. Ein Mitarbeiter beim Autoverleiher soll den Fall nun bearbeiten. Regelt er den Fall auf Kulanzbasis? Legt er eine Pauschale fest, und falls ja, wie hoch ist diese? Benötigt der Mitarbeiter weitere Angaben vonseiten des Kunden? Reicht er den Fall bei der Versicherung ein?

Die Offline-KI gibt dem Mitarbeitenden eine Empfehlung, wie der Fall am besten zu bearbeiten ist. Die Antwort basiert auf früheren Fällen, die dem Autoverleiher vorliegen. Das versetzt oft auch nicht so erfahrene Mitarbeitende in die Lage, die beste Bearbeitungsmöglichkeit zu wählen – ohne erfahrene Mitarbeitende zu fragen oder etwas Falsches zu entscheiden.

Analog dazu kann Offline-KI Beschäftigte im Support dabei unterstützen, Fehlermeldungen oder Feature Requests für Software-Produkte effizient zu bearbeiten. Auch Anfragen von Bestandskunden automatisch zu erkennen oder Fragen nach einem Angebot oder Beschwerden – all das lässt sich mit einer Offline-KI sehr gut umsetzen.

PRAXIS-TIPP

Unternehmen und Behörden, die weitergehende Anwendungsfälle mit KI optimieren wollen, sind gut beraten, ihr eigenes KI-System zu nutzen. Ein solches KI-System (Offline-KI) ist nicht nur der Datenschützer bester Freund, weil Daten nirgendwo hin gehen müssen. Auch der Entscheider und die Entscheiderin wird es lieben, weil die Ergebnisse optimierbar und die Kosten niedrig und fix sind. Mittlerweile ist es sogar in Deutschland möglich, eine entsprechende KI-Infrastruktur für wenig Geld zu erhalten. Wer ein KI-System hingegen lediglich für unverfängliche Daten verwendet und es als Suchmaschine oder zum Abfragen von Weltwissen nutzt, benötigt wohl kein eigenes KI-System. Hier tut es auch ein beliebiger Cloud-Anbieter, sofern die Antwortqualität der KI und die Kosten vertretbar sind. Eine Offline-KI bietet jedenfalls neben der kontrollierbaren Qualität der Ergebnisse, den geringen Kosten und der Datensicherheit strategische Vorteile für Unternehmen und Behörden. Preiserhöhungen oder andere Nutzungsbedingungen von Cloud-Anbietern sind somit vom Tisch. Der Weg ist frei für eine sich selbst verbessernde KI ohne Mehrkosten.

Checkliste: zentrale Fragen beim Einsatz von KI

- Verwendet die KI unternehmenseigene Daten?
- Verarbeitet die KI personenbezogene Daten?
- Werden Geschäftsgeheimnisse verarbeitet?
- Verarbeitet die KI vertrauliche oder andere sensible Daten?
- Wofür wird die KI genutzt?
- Wie oft wird die KI genutzt?
- Was passiert mit den Antworten und Ergebnissen der KI?
- Was lässt sich in die KI eingeben?

Dr. Klaus Meffert ist Diplom-Informatiker und seit 30 Jahren in der IT-Beratung sowie Software-Entwicklung tätig. Im Blog Dr. DSGVO schreibt Dr. Meffert regelmäßig zu aktuellen Themen des Datenschutzes und zu KI (dr-dsgvo.de).

Bild: iStock.com/Jean-Luc Ichard

Microsoft versucht mit Nachdruck, das neue Outlook am Markt zu etablieren. Von den Neuerungen dürften aber manche Datenschutzbeauftragte nicht begeistert sein.

Das neue Outlook, Teil 1

Datenschutz mit der neuen Version von Microsoft Outlook

Seit August stellt Microsoft mit Windows 11 24H2 das neue Outlook zur Verfügung, das gleich mehrere Anwendungen ersetzen soll. Dabei ergeben sich datenschutzrechtliche Fragen, auf die dieser Artikel – der erste einer Serie – im Folgenden näher eingeht.

Das von Microsoft sogenannte neue Outlook soll mehrere Anwendungen ersetzen. Dazu zählt Windows Mail in Windows 10 und 11.

Nutzer und Nutzerinnen des klassischen Microsoft Outlook können in der Übergangsphase mit einem Schieberegler, der prominent in der rechten oberen Ecke des Anwendungsfensters platziert ist, auf das neue Outlook wechseln. Gleiches gilt für Windows Mail und die Kalenderanwendung in Windows 10/11 vor der Installation von Windows 11 24H2.

Hinzu kommt: Bei Windows 11 24H2 wird das neue Outlook bereits als Alternative für Windows Mail und die Kalenderanwendung mitinstalliert.

Microsoft will das neue Outlook mit einigem Druck durchsetzen. Aus datenschutzrechtlicher Sicht ergeben sich dabei mehrere Probleme.

E-Mails und Login-Daten laufen über Microsoft-Server

Eines der größten Probleme beim Einsatz des neuen Outlook besteht darin, dass alle E-Mails und alle Anmeldedaten, die in Outlook gespeichert sind, über Microsoft-Server laufen. Damit landen sie in der Microsoft-Cloud.

Für Anwendende, die ohnehin auf Microsoft-Konten oder Microsoft 365 setzen, ist dies kein Problem. Allerdings ist nicht klar, ob sich durch die Umstellung der Software auch die genutzten Server bei Microsoft ändern. Nutzer aus Europa sollen zwar auf europäischen Servern landen, aber sicher ist das nicht.

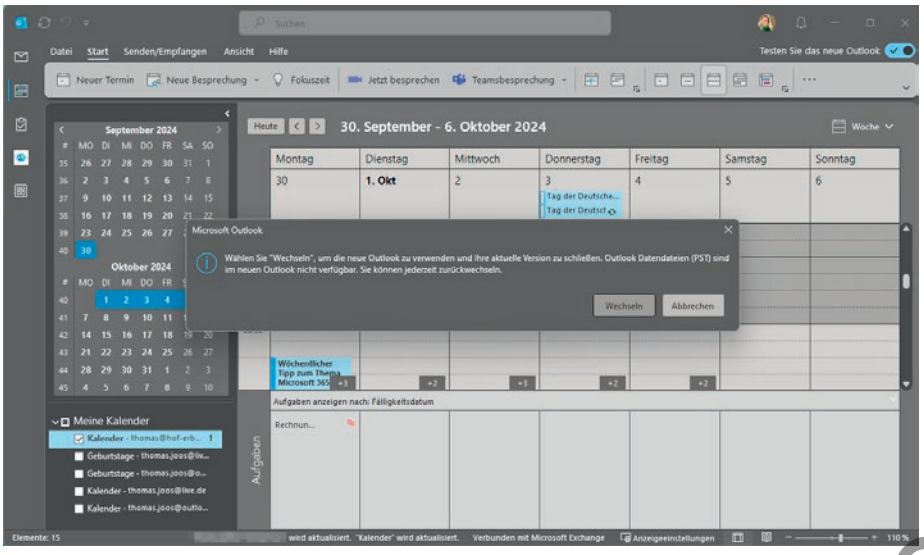
Ein größeres Problem entsteht für Nutzer und Unternehmen, die ihr Postfach nicht bei Microsoft hosten, aber trotzdem auf das neue Outlook setzen. Denn auch hier laufen die E-Mails künftig über Microsoft-Server und Microsoft speichert die Anmeldedaten. Wer das nicht will, darf das neue Outlook nicht einsetzen.

Das hat Folgen für Datenschutzbeauftragte in Unternehmen, die zwar Outlook und Windows Mail und Kalender einsetzen, deren Postfächer aber nicht bei Microsoft gehostet sind. Denn sie müssen sich nun mit dem Datenschutz für Microsoft-Server und der damit verbundenen Datenspeicherung auseinandersetzen. Dies gilt auch für Unternehmen, in denen die Mitarbeitenden ihre eigenen Geräte im Homeoffice nutzen und künftig zu Hause auf das neue Outlook setzen.

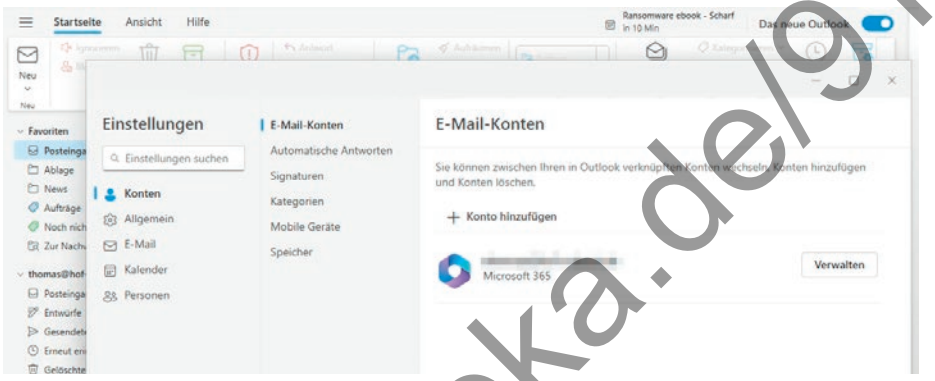
Noch kein Zwang zum Umstieg

Während Windows 10/11 die Installation des neuen Outlook erzwingt, können herkömmliche Outlook-Nutzerinnen und -Nutzer weiterhin auf ihr klassisches Outlook aus dem Office-Paket oder aus den Microsoft-365-Apps setzen. Microsoft unterstützt das bisherige Outlook weiterhin, mindestens bis 2029. Es zeichnet sich jedoch eine Umbenennung von Outlook in „Klassisches Outlook“ ab. Dies gilt für alle Versionen außer „Neues/New Outlook“.

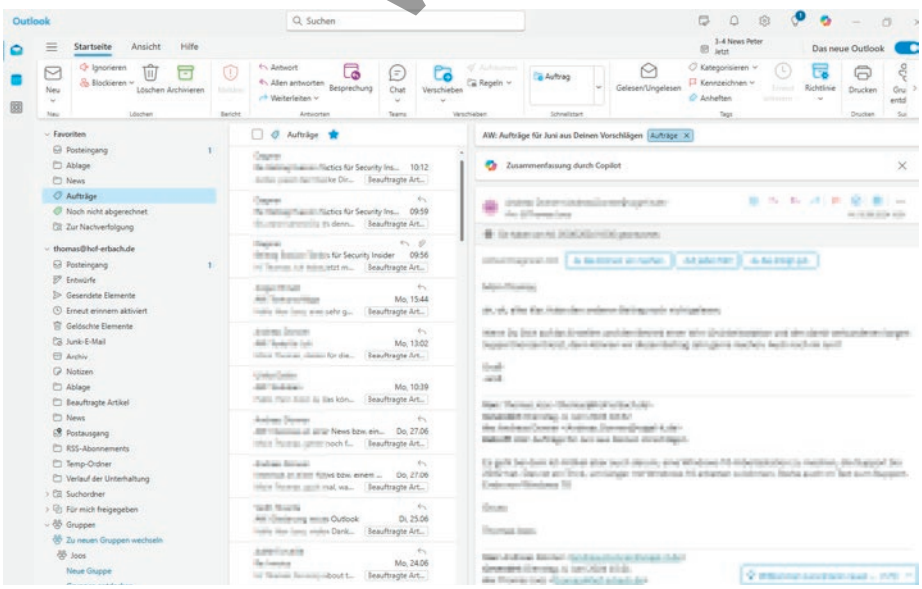
Es ist zu erwarten, dass Microsoft bei der Verteilung des neuen Outlook weiterhin sehr aggressiv vorgehen wird. Im Internet gibt finden sich Berichte, wonach die neue Version automatisch installiert wurde, obwohl die Nutzer den Schiebe- →



Das neue Outlook lässt sich über einen Schieberegler in der Outlook-App testen



Die Einstellungsmöglichkeiten im neuen Outlook sind sehr begrenzt im Vergleich zu bisherigen Outlook-Versionen



Die Bedienoberfläche des neuen Outlook bietet viele Optionen, aber weniger als das klassische Outlook

regler „Testen Sie das neue Outlook" nicht gesetzt hatten.

Angesichts der aktuell verfügbaren Funktionen gibt es kaum einen Grund, von Outlook 2021/2024 oder den Microsoft-365-Apps auf das neue Outlook zu wechseln, im Gegenteil. Aktivieren die Nutzer jedoch den genannten Schieberegler, installiert sich das neue Outlook. Es soll die vorhandenen Postfächer übernehmen. Dies funktioniert derzeit allerdings nicht fehlerfrei.

So muss bei diesen Anwendern vermutlich der Support oder die IT-Abteilung eingreifen, um alle vorhandenen Postfächer aus dem klassischen Outlook in das neue Outlook zu übernehmen. Microsoft stellt unter https://ogy.de/im1o Informationen zur technischen Umstellung zur Verfügung und unterstützt Administratoren und Anwendende bei der Einführung des neuen Outlook.

Das klassische Outlook soll bis mindestens 2029 weiterbestehen. Dies zeigt, dass Microsoft nicht sicher ist, alle notwendigen Funktionen des bisherigen Outlook im neuen Outlook implementieren zu können.

Dem neue Outlook fehlen Funktionen

Beim Einsatz des neuen Outlook kann es zu Problemen kommen, wenn einzelne Funktionen fehlen. So ist es noch nicht möglich, lokale Exchange-Postfächer anzubinden.

Das neue Outlook unterstützt derzeit nur Exchange Online. Dies soll sich in Kürze ändern. Wie die Integration erfolgt und ob sich daraus datenschutzrechtliche Probleme ergeben, ist noch nicht absehbar.

Hinzu kommen weitere fehlende Funktionen. Es würde den Rahmen dieses Beitrags sprengen, alle Funktionen und Einstellungen aufzuzählen, die im neuen Outlook fehlen. In Bezug auf Sicherheit und Datenschutz ist das Fehlen des Trust Centers hervorzuheben, in dem sich viele

Einstellungen für Sicherheit und Datenschutz konfigurieren lassen.

Setzen Unternehmen spezielle Erweiterungen, APIs oder Sicherheitsprogramme für Outlook ein, ist nicht sicher, ob diese mit dem neuen Outlook funktionieren. Auch dies sollte man im Vorfeld testen, bevor Benutzerinnen und Benutzer den Schieberegler betätigen und das neue Outlook aktivieren und damit den Zugriff auf ihr bisheriges klassisches Outlook beenden.

Ein weiteres Problem sind die fehlenden PST-Dateien. Diese lassen sich mit dem neuen Outlook nicht mehr verwenden. Außerdem kann das neue Outlook keine Daten exportieren oder importieren.

Hier müssen sich IT-Abteilungen etwas einfallen lassen, um zu verhindern, dass Anwendende in Zukunft PST-Dateien auf anderen Wegen öffnen, die datenschutzrechtlich bedenklich sind. So kann es schnell passieren, dass Anwenderinnen und Anwender Cloud-Dienste nutzen, die sensible Unternehmensdaten ins Internet verlagern, oder Zusatztools, bei denen der Datenschutz nicht gewährleistet ist. Microsoft hat bereits angekündigt, dass auch das neue Outlook irgendwann PST-Dateien unterstützen soll.

Es ist zumindest möglich, den Test aus dem neuen Outlook heraus mit dem gleichen Schieberegler zu beenden. Ob dies jedoch immer ohne Datenverlust geschieht, lässt sich nicht mit Sicherheit sagen.

ACHTUNG!

Funktionen, um automatisch Outlook-Profile zu erstellen, sowie Sicherheitseinstellungen, die über Gruppenrichtlinien oder das Microsoft Security Compliance Toolkit umgesetzt sind, verlieren mit dem neuen Outlook ihre Gültigkeit. Hier muss sich die IT-Administration neue Wege überlegen. Denn die meisten Einstellungen laufen über Registry-Einstellungen, die keine Auswirkungen auf das neue Outlook haben. Dies gilt sowohl für die Bereitstellung von Profilen als auch für die Sicherheitseinstellungen.

Warnungen vor neuem Outlook

Der frühere Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) warnte in einem Rundschreiben, ein datenschutzkonformer Einsatz des neuen Outlook sei aktuell nicht möglich. Die Nutzung des neuen Outlook von Microsoft werfe erhebliche Datenschutzfragen auf. Die Übermittlung von Zugangsdaten in die Cloud, ohne klare Transparenz und wirksame Einwilligung, stelle ein potenzielles Risiko dar.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht den Fall kritisch und warnt vor einem Kontrollverlust durch Cloudzwang. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Lutz Hasse rät dazu, auf die neue Outlook-Version zu verzichten und bei der klassischen Version zu bleiben.

Datenschutzbeauftragte müssen sich mit Outlook befassen

Das neue Outlook kommt. Unternehmen sollten sich mit dem Thema auseinandersetzen, v.a. im Hinblick auf Datenschutz, Sicherheit und notwendige Funktionen sowie das Zusammenspiel mit anderen Anwendungen.

In Windows 11 24H2 ist das neue Outlook automatisch enthalten. Man kann jedoch das klassische Outlook beibehalten. Zusätzlich sollten sich die Verantwortlichen im Unternehmen überlegen, wie sie die Umstellung auf das neue Outlook steuern. Teilweise ist auch eine Sperrung möglich.

Dieses und weitere Themen behandeln die nächsten Teile dieser Artikelserie zum neuen Outlook.

Thomas Joos ist freiberuflicher Autor und Consultant. Er hat zahlreiche Fachbücher und Texte veröffentlicht. Außerdem berät er mittlere und große Unternehmen in den Bereichen Netzwerke, Cloud, KI und Security.

IMPRESSUM

Verlag:
WEKA Media GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA Media GmbH & Co. KG
Gesellschafter der WEKA Media GmbH & Co. KG sind als Kommanditistin: WEKA Business Information GmbH & Co. KG und als Komplementärin: WEKA Media Beteiligungs-GmbH

Geschäftsführer:
Jochen Hortschansky
Kurt Skupin

Redaktion:
Ricarda Veidt, M.A. (V.i.S.d.P.)
E-Mail: ricarda.veidt@weka.de
Andreas Dumont, München
Dr. Wilhelm Greiner, Mitteilerei, Kinding

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 0 82 33.23-5 72 68
E-Mail: anton.sigllechner@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben Print + Online-Zugriff 279 € (zzgl. MwSt. und Versandkosten)
12 Ausgaben als PDF im Heftarchiv + Online-Zugriff 269 € (zzgl. MwSt.)

Druck:
Burscheid Medien GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4129

ISSN:
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

Haftung:
Die WEKA Media GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Erfüllungsort und Gerichtsstand ist Kissing.

ISO/IEC-27001-Zertifizierungen

Die cybersichere Aufzugsanlage

Zertifizierungen nach der internationalen Norm ISO/IEC 27001 werden immer wichtiger. Dabei gilt es allerdings, sich diese genau anzusehen. Denn was viele nicht beachten: Nicht die Zertifizierung an sich, sondern der Gegenstand der Zertifizierung ist dabei von entscheidender Bedeutung.

Im Konferenzraum herrscht angespannte Stille. Das Team hat gerade ein wichtiges Projekt vollendet, bei dem es einen chinesischen Dienstleister eingebunden hat.

Die Anforderungen an Informationssicherheit und Datenschutz sind dabei hoch. Die Frage, ob der Dienstleister den strengen internationalen Standards entspricht, steht im Raum.

Mit einem Lächeln präsentiert der Projektleiter das ISO/IEC-27001-Zertifikat des Dienstleisters. Er schiebt das Dokument über den Tisch. Es ist frisch ausgestellt. Die Sprache ist Mandarin. Trotzdem können alle den vertrauten ISO-Stempel sehen. Kein Zweifel. 27001-Zertifikat.

„Das spart uns viel Arbeit", freut sich der IT-Leiter. „Wenn die zertifiziert sind, ist alles in Ordnung." Sieht so aus, als kann das Projekt fortgesetzt werden.

Der Datenschutzbeauftragte, der sich erst kürzlich intensiv mit dem chinesischen Gesetz PIPL (Personal Information Protection Law) auseinandergesetzt hat, ist skeptisch. Er greift nach dem Zertifikat und mustert es genauer. Er möchte mehr zum Datenschutz wissen und öffnet sein Notebook.

Hinterfragen schadet nicht

Mittels ein paar schneller Scans mit der Kamera und einigen Klicks auf einer Übersetzungs-App lässt er das Dokument durch eine KI-gesteuerte Übersetzung laufen. Die ersten Sätze der Übersetzung erscheinen auf seinem Bildschirm. Er schaut verdutzt und erklärt: „Wir haben hier die Bestätigung, dass wir beim Partner in China sicher Aufzug fahren können."

Das Dokument war lediglich die Zertifizierung für die Sicherheit der offenbar sehr umfangreichen Aufzugsanlage des Hochhauses, in dem der Dienstleister sitzt. Manchmal ist es eben nicht genug, nur ein Zertifikat zu sehen – man muss auch prüfen, was genau zertifiziert ist.

Eberhard Häcker ist seit vielen Jahren selbstständig und mit großer Leidenschaft sowie Kreativität externer Datenschutzbeauftragter.

In der nächsten Ausgabe

KI-Basics

Müssen DSB den Unterschied kennen zwischen KI-Modell und KI-System? Ja, müssen sie, um mitreden zu können.

Der Klassiker Verarbeitungsverzeichnis

KI-VO, NIS2 & Co. – neue Anforderungen bedingen überarbeitete Beschreibungen!

Verantwortlichkeit bei KI

Wer ist für ein KI-System verantwortlich? Geht es um personenbezogene Daten, betrifft diese Frage auch den Datenschutz.