Newsletter Datenschutz

konzept 17
Datensicherheit trifft Vertraulichkeit

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,
wenn es derzeit ein Thema der Digitalisierung gibt, das Unternehmen, Privathaushalte und den Datenschutz gleichermaßen beschäftigt, dann ist es die Künstliche Intelligenz (KI). Aus diesem Grund steht KI im Mittelpunkt dieser neuen Ausgabe.
Der erste Beitrag erklärt, warum es für den verantwortungsvollen Einsatz von KI entscheidend ist, geeignete Kenntnisse und Fertigkeiten zu erwerben – also eine fundierte KI-Kompetenz aufzubauen. Der zweite Artikel zeigt eindrucksvoll, welche Möglichkeiten KI bietet, etwa bei der Erzeugung von Stimmen. Dabei werden auch rechtliche Grenzen und potenzielle Gefahren deutlich.
Beitrag 3 macht klar, dass die Risiken für den Datenschutz beim Einsatz von KI keineswegs nur theoretischer Natur sind. Datenschutzaufsichtsbehörden haben bereits Datenpannen und Verstöße gegen Datenschutzvorgaben festgestellt, wenn Unternehmen KI einsetzen. Lesen Sie dazu spannende Praxisfälle.
Den Abschluss dieser Schwerpunkt-Ausgabe bilden ein Beitrag und ein Wissenstest zu den neuen Phishing-Gefahren durch KI. Erfahren Sie, wie sich das scheinbar vertraute Phishing verändert hat – und wie KI es noch gefährlicher macht.

Ihr Frank Berns, Datenschutzbeauftragter

Impressum
Redaktion: Frank Berns,
Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

KI-Kompetenz – warum ist sie nötig?

Immer mehr Unternehmen fordern ihre Beschäftigten dazu auf, an einem allgemeinen KI-Training teilzunehmen. Oft wird es als Selbstlern-Kurs online angeboten. Die Teilnahme ist in der Regel verbindlich. Was ist der Hintergrund dafür?

KI findet sich inzwischen an jedem Arbeitsplatz

Fragt man Beschäftigte, ob sie an ihrem Arbeitsplatz bereits KI einsetzen, verneinen das nach wie vor recht viele. In aller Regel täuschen sie sich. Denn wer beispielsweise eine gängige Suchmaschine benutzt, bekommt bei den meisten Anfragen an erster Stelle eine KI-erzeugte Antwort. Ein Hinweis darauf steht im Normalfall sogar „kleingedruckt" darunter. Manche Fachleute bezeichnen so etwas als „Schatten-KI". Dieser Vergleich passt recht gut. Denn wenn ein Mensch sich bei passendem Licht bewegt, ist sein Schatten einfach da. Er begleitet ihn, ob er sich darum kümmert oder nicht. Und er lässt sich auch nicht „abschalten".

Das ist bei einer KI-Anwendung zwar anders. Zumindest Suchmaschinen bieten die Möglichkeit, KI-erzeugte Antworten auszublenden. Aber wer tut dies schon? Schließlich sind die Antworten oft erfreulich gut. Außerdem gibt es immer mehr unternehmenseigene Anwendungen, die nur auf der Basis von KI funktionieren. Bei ihnen etwas abschalten zu wollen, wäre schlicht widersinnig. Spätestens mit ihnen ist KI an jedem Arbeitsplatz präsent.

Die EU verlangt KI-Kompetenz von Beschäftigten

Das „KI-Gesetz" der EU enthält einen Artikel 4 mit der Überschrift „KI-Kompetenz". Er besteht nur aus wenigen Zeilen, hat es aber in sich. Sein erster Satz fordert, dass die Betreiber von KI-Systemen Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal über ein ausreichendes Maß an KI-Kompetenz verfügt. Ein Unternehmen, das in irgendeiner Weise KI einsetzt, muss sich an diese Vorgabe halten. Schon wegen der allgegenwärtigen „Schatten-KI" muss ein Unternehmen vorsorglich davon ausgehen, dass alle Beschäftigten KI einsetzen. Abgesehen davon wird dies ohnehin bald an jeden Arbeitsplatz der Fall sein. Denn KI-Projekte laufen mehr oder weniger umfangreich überall.

KI-Kompetenz kann vieles bedeuten

Was „KI-Kompetenz" heißt, gibt das KI-Gesetz nur sehr allgemein vor. Im Kern geht es dabei darum, die Chancen von KI zu nutzen, ohne dabei die Risiken auszublenden. Dabei hilft in jedem Fall ein allgemeiner Überblick darüber, was man von KI erwarten kann, wo mit unsinnigen Antworten zu rechnen ist und wie man mit klugen Anfragen

die Qualität der Antworten möglichst hochhalten kann. Für die meisten Beschäftigten reicht das völlig aus. Das gilt vor allem, wenn sie KI gelegentlich als Instrument einsetzen. Das KI-Gesetz überlässt jedem Unternehmen die Festlegung, welche Beschäftigten welche Kenntnisse brauchen. Generelle Vorgaben für alle gibt es nicht. Es ist auch kein System offiziell zertifizierter Schulungen vorgesehen. Eine Online-Schulung, die alle Beschäftigten absolvieren müssen, ist vor diesem Hintergrund ein guter Einstieg in das Thema.

Erzeugung von Stimmen mit KI

KI ermöglicht es, menschliche Stimmen für unterschiedliche Zwecke zu erzeugen. Manchmal geht es einfach um privaten Spaß, manchmal aber auch um kommerzielle Anwendungen. Manche verfolgen sogar kriminelle Absichten. All dies ist Anlass genug, sich einmal die rechtlichen Vorgaben und Grenzen anzusehen.

KI-erzeugte Stimmen bieten ungeahnte Möglichkeiten

Sie möchten einer Freundin zum Geburtstag eine Sprachnachricht schicken – gesprochen von ihrem Lieblingsschauspieler? Sie brauchen für einen Werbespot eine markante Stimme? All das ist heute leicht möglich! Doch leider funktioniert auch Folgendes: Ein Krimineller hinterlässt auf Ihrem Anrufbeantworter eine Nachricht, scheinbar gesprochen von jemandem aus der Personalabteilung, dessen Stimme Sie kennen. Die Nachricht bittet Sie um Rückruf unter einer Handynummer – angeblich ganz dringend. Ihr Personaldatensatz sei beschädigt worden. Sie sollen bitte rasch eine Reihe persönlicher Daten durchgeben, von der Steuernummer bis zur Kontonummer. Ach ja: „Falls ich nicht gleich rangehen kann, bitte auf den AB meines Handys sprechen." Auch das ist Teil der Nachricht.

Seien Sie bei ungewöhnlichen Anrufen kritisch

Natürlich wäre es im obigen Beispiel ganz einfach, eine Mail über das Firmennetz an den Personaler zu schreiben, dessen Stimme Sie gehört haben. Oder Sie könnten ihn unter seiner bekannten Telefonnummer im Firmennetz anrufen. So ließe sich schnell klären, ob wirklich er angerufen hat – oder doch jemand anderes. Nur: Bisher rechnet kaum jemand damit, dass ein Anruf gefälscht sein könnte. Deshalb haben solche Betrugsmaschen derzeit noch beste Erfolgsaussichten. An die Stimme eines ahnungslosen Personalers zu kommen, ist in der Praxis kein Problem. Solche Menschen telefonieren ständig – das gehört fast immer zu ihrem Job. Bei jedem beliebigen Telefonat lässt sich die Stimme aufnehmen und anschließend weiterverarbeiten.

Kommerzielle Nutzung erfordert rechtliche Vereinbarungen

Jede leistungsfähige KI kommt mit einem Auftrag wie „Erzeuge mir den nachfolgenden Text mit einer Stimme, die so ähnlich klingt wie die Stimme von …" problemlos klar. Das scheint auf den ersten Blick eine gute Möglichkeit zu sein, um sich die Kosten für einen professionellen Sprecher zu sparen. Doch genauso wie es ein Recht am eigenen Bild gibt, existiert auch ein Recht an der eigenen Stimme. Niemand muss dulden, dass seine Stimme kommerziell verwendet wird,

ohne vorher um Erlaubnis gefragt zu werden. Oft wäre eine solche Erlaubnis sogar zu bekommen – allerdings nur gegen Bezahlung. Denn es gibt viele Menschen mit markanter Stimme, die sich gern buchen lassen. Manche von ihnen leben sogar davon. Das könnten sie nicht mehr, wenn ihre Stimme mithilfe von KI hinter ihrem Rücken kostenlos nachgeahmt werden dürfte.

Markante Stimmen sind sogar nach dem Tod geschützt

Manche glauben, dass man die Stimmen verstorbener Personen frei verwenden könnte. Das scheint viele Möglichkeiten zu bieten – denn längst verstorbene Schauspieler mit markanten Stimmen gibt es genug. Ein Beispiel, das zumindest viele Ältere kennen, wäre etwa „Loriot". Doch Vorsicht: So einfach ist es rechtlich nicht. Das Recht an der eigenen Stimme ist Teil des allgemeinen Persönlichkeitsrechts. Es schließt auch nach dem Tod des „Stimminhabers" die unerlaubte Nutzung der Stimme für kommerzielle Zwecke aus.

Stimmen sind oft personenbezogen – aber nicht immer

Auf den ersten Blick scheinen menschliche Stimmen ein Musterbeispiel für personenbezogene Daten zu sein. Das kann zutreffen, muss aber nicht. Entscheidend ist, ob eine Stimme einem bestimmten Menschen zugeordnet werden kann.

Wenn es sich um eine „Allerwelts-Stimme“ handelt, werden die meisten Hörer diese Stimme niemandem zuordnen können. Dann fehlt der Personenbezug. Anders sieht es beispielsweise bei der Stimme eines bekannten Schauspielers aus. Manche Stimmen sind so bekannt, dass nahezu alle sie einer bestimmten Person zuordnen können. Dann liegt der Personenbezug auf der Hand. Die Unterscheidung ist wichtig dafür, ob die DSGVO zu beachten ist oder nicht. Im Zweifel sollte man davon ausgehen, dass sie gilt – das vermeidet spätere rechtliche Schwierigkeiten.

Harmlose private Scherze sind in Ordnung

Manche befürchten jetzt vielleicht, hier sei wieder einmal alles verboten. Doch so schlimm ist es nicht. Einen privaten Geburtstagsgruß mit der Stimme eines bekannten Politikers oder Schauspielers aufzunehmen, ist durchaus in Ordnung. Die Sache muss dann aber wirklich im privaten Bereich bleiben. Deshalb gehört ein solcher Gruß weder in soziale Netzwerke noch auf eine Homepage.

Was Sie aus Datenpannen mit KI lernen sollten

Künstliche Intelligenz (KI) ist nicht nur in aller Munde – sie ist bereits in vielen Unternehmen im Einsatz und verarbeitet auch personenbezogene Daten. Aufsichtsbehörden haben bereits mögliche Datenschutzverletzungen aufgedeckt. Diese Datenpannen zeigen, worauf Sie bei KI besonders achten sollten.

KI zwischen Chancen und Risiken

„KI-Modelle revolutionieren zahlreiche Branchen und stellen uns zugleich vor große Herausforderungen in Sachen Transparenz, Sicherheit und Datenschutz“, sagte Prof. Dr. Louisa Specht-Riemenschneider, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Wie Umfragen des Digitalverbands Bitkom zeigen, sehen das viele Unternehmen genauso.

8 von 10 Unternehmen halten KI für die wichtigste Zukunftstechnologie, so Bitkom. Doch 48 Prozent beklagen die hohen Anforderungen an den Datenschutz, 39 Prozent haben Angst, dass Daten in falsche Hände geraten. Die Bedenken sind leider nicht unbegründet, denn es kommt bereits zu Datenschutz-Pannen bei der Nutzung von KI.

Aufsichtsbehörden berichten von Datenschutzproblemen bei KI

Wie bei jeder Verarbeitung personenbezogener Daten muss es auch bei Nutzung von KI eine rechtliche Grundlage geben, damit die Daten genutzt werden dürfen. Unternehmen können also nicht einfach ihren Datenbestand mithilfe einer KI-Lösung auswerten, um daraus neue Erkenntnisse zu gewinnen – auch wenn dies aus Unternehmenssicht verlockend erscheinen mag. Zudem muss der Einsatz von KI den betroffenen Personen mitgeteilt werden, die Nutzung muss also transparent sein.
Ein Beispiel aus der Praxis: Bei einer Immobilienvermittlungsplattform stellte eine Datenschutzaufsicht im Rahmen einer Beschwerde fest, dass der Betreiber die Kommunikation mit Kundinnen und Kunden für das Training eines KI-Systems zur effizienteren Bearbeitung von Kundenanfragen nutzte – ohne die Betroffenen darüber zu informieren. Es fehlten also die Information, die Aufklärung und die Transparenz.

In einem weiteren Fall prüfte die Datenschutzaufsicht eine kommerzielle Fotoplattform, die bereits ins Internet hochgeladene Fotos – zumindest teilweise personenbezogen – Unternehmen gegen Bezahlung unter anderem für das Training von KI-Modellen anbot. Dieses Vorgehen war nur teilweise in der Datenschutzerklärung der Plattform abgebildet. Es mangelte also erneut an Transparenz und an einer rechtlichen Grundlage, denn die Bilder waren ursprünglich nicht zur Weitergabe und zum KI-Training bei Drittunternehmen bestimmt.

Vorsicht bei KI als Entscheidungsunterstützung

Der Datenschutz verlangt zudem, dass Personen nicht durch automatisierte Entscheidungen erheblich beeinträchtigt und benachteiligt werden. Ein Beispiel ist die automatische Prüfung durch eine KI, ob eine Person einen Kredit erhält oder nicht. Auch hier kommt es in der Praxis zu Datenschutzverletzungen.
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte gegen ein Unternehmen aus der Finanzwirtschaft ein Bußgeld in Höhe von 492.000 Euro wegen Verstößen gegen die Rechte betroffener Kunden bei automatisierten Einzelentscheidungen.
Trotz guter Bonität wurden die Kreditkartenanträge mehrerer Kunden durch automatisierte Entscheidungen abgelehnt. Diese Entscheidungen wurden auf Basis von Algorithmen und ohne menschliches Eingreifen getroffen.

Als die betroffenen Kunden eine Begründung verlangten, erfüllte das Unternehmen seine gesetzlich vorgegebenen Informations- und Auskunftspflichten nicht ausreichend.

KI-Nutzung ohne Personenbezug?

Ein Weg, Datenschutzprobleme beim KI-Einsatz zu vermeiden, ist der Verzicht auf personenbezogene Daten – etwa durch Anonymisierung. Doch diese muss auch technisch wirksam sein, sonst bleibt der Personenbezug bestehen. Auch hier gab es bereits Pannen.

Bei einem Unternehmen, das ein KI-basiertes Forderungsmanagement anbietet, prüfte eine Datenschutzaufsicht, ob die geplante Anonymisierung der Schuldnerdaten für das Training der KI-Modelle tatsächlich zu anonymen Daten führt. Die KI-Systeme sollen eine personalisierte Ansprache zur erfolgreicheren Eintreibung von Forderungen ermöglichen. Aber nur, wenn sich die scheinbar anonymen Daten nicht mehr eindeutig einer Person zuordnen lassen, entfällt der Personenbezug – und damit auch die datenschutzrechtlichen Vorgaben.

Fazit: Datenschutz bleibt Pflicht – auch bei KI

Es zeigt sich: Für die Nutzung von KI müssen alle Datenschutzvorgaben beachtet werden, die auch sonst bei der Datenverarbeitung gelten. Leider wird die neue Technologie noch häufig eingesetzt, ohne den Datenschutz vollständig zu berücksichtigen. Es fehlen rechtliche Grundlagen, Informationen für die betroffenen Personen oder wirksame Verfahren zur Anonymisierung.
KI ist also auch im Datenschutz keine Zukunftsmusik mehr – es gibt bereits reale Pannen bei der Umsetzung. Helfen Sie mit, dies zu vermeiden!

Die neue Qualität der Phishing-Attacken

Phishing-Mails erscheinen als „alte Bekannte" unter den Online-Bedrohungen: E-Mails, mit denen versucht wird, Passwörter zu stehlen. Doch in Zeiten von Künstlicher Intelligenz (KI) verwandeln sich Phishing-Attacken und werden noch gefährlicher. Das sollten Sie wissen!

Phishing: Seit Langem bekannt, aber sehr gefährlich

Kaum eine Studie zur Online-Sicherheit nennt Phishing nicht als eines der größten Risiken aus dem Cyberraum: So besagt etwa der aktuelle Bericht zur Bedrohungslandschaft 2025 („ENISA Threat Landscape") der EU-Agentur für Cybersicherheit ENISA: 60 Prozent aller beobachteten Attacken waren Phishing. Damit ist Phishing der häufigste Angriffsweg.

Tatsächlich spricht man im Datenschutz und in der IT-Sicherheit schon so lange über Phishing, dass man meinen könnte, dieses Risiko sei gut bekannt und sollte eigentlich abnehmen. Doch das Gegenteil ist der Fall: Phishing-Attacken haben eine neue, noch gefährlichere Qualität angenommen.

Phishing entwickelt sich weiter

Phishing bleibt eine der größten digitalen Bedrohungen, doch die Angriffsmethoden haben sich weiterentwickelt. Das berichtet zum Beispiel der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern. KI-generierte E-Mails, perfekt imitierte Sprache in Sprachnachrichten oder täuschend echte Deepfakes in Online-Meetings machen es selbst erfahrenen Personen schwer, Betrugsversuche zu erkennen. Diese Angriffe nutzen nicht nur technische Schwächen, sondern zielen direkt darauf ab, menschliches Verhalten kriminell zu beeinflussen.

Gerade durch KI sind die Inhalte der Phishing-Nachricht täuschend echt und passen perfekt zu den Opfern. Was früher ein großer Aufwand für Internetkriminelle gewesen wäre, gelingt dank KI nun automatisch und mit wenig Aufwand. Dabei kommen die KI-generierten Inhalte über alle Kommunikationswege zu den Opfern – inzwischen auch in Video-Meetings.

Phishing-Schutz auf allen Ebenen

Weil sich Phishing-Attacken immer schwerer erkennen lassen, raten die Datenschutzaufsichtsbehörden zu einem umfassenden Schutz, der auch technische Komponenten beinhaltet. So empfiehlt zum Beispiel der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern:

- Vorsicht bei unerwarteten Nachrichten, insbesondere wenn zur Eingabe persönlicher Daten aufgefordert wird.
- Links überprüfen, indem man mit der Maus darüber fährt. So wird die tatsächliche URL (Web-Adresse) angezeigt, die dann entsprechend verifiziert werden kann. Alternativ helfen Link-Checker oder URL-Checker.
- Bank-Links nur über verifizierte Favoriten oder Lesezeichen im Browser aufrufen.
- Zwei-Faktor-Authentifizierung (2FA) ist ein wichtiger Schutz für Konten und Daten. Sie sollte, wann immer möglich, eingerichtet werden. Neben dem Passwort ist ein zweiter unabhängiger Identitätsnachweis erforderlich – etwa ein Code aus einer App, eine Push-Benachrichtigung oder ein biometrischer Scan (z.B. Fingerabdruck).

Wissen Sie, welche neue Gefahren bei Phishing-Angriffen bestehen?

Frage: Phishing ist eine Cyberattacke über E-Mail. Stimmt das?

1. Nein, Phishing kann auf vielen Wegen erfolgen, nicht nur über E-Mail.
2. Ja, Phishing-Mails sind seit Langem bekannt.

Lösung Frage 1: Die Antwort 1. ist richtig. Phishing-Mails sind zwar besonders bekannt und häufig, aber Phishing kann auch per SMS, Chat-Nachricht in sozialen Netzwerken, Fax oder Brief erfolgen. Nicht zuletzt ist auch Phishing per Telefon möglich. Dank kriminell genutzter KI lassen sich bekannte Stimmen täuschend echt imitieren, um Vertrauen zu erwecken und geheime Informationen zu entlocken.

Frage: Durch Künstliche Intelligenz (KI) wird nur der Inhalt der Phishing-Mails „besser", mehr ändert sich nicht. Stimmt das?

1. Ja, mit KI lassen sich sehr gute Texte erzeugen, die zum Empfänger und damit zum Opfer passen.
2. Nein, KI kann noch mehr: Phishing-Attacken lassen sich damit komplett automatisieren – sie erfolgen gezielt und dennoch massenhaft.

Lösung Frage 2: Die Antwort 2 ist hier richtig. Durch KI verändert sich Phishing deutlich: Früher waren Phishing-Versuche oft an fehlerhaftem Deutsch oder unpassendem Bezug zu erkennen. Heute sind die E-Mails sehr genau auf die Opfer zugeschnitten. KI ermöglicht schnelle Hintergrundrecherchen und automatisierte Angriffe. Das Ergebnis sind keine simplen Massen-Mails, sondern zielgenaue Attacken auf viele Personen gleichzeitig.