Newsletter Datenschutz

konzept 17

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

vor Gefahren kann man sich nur richtig schützen, wenn man die Risiken kennt und erkennt. Das gilt auch im Datenschutz. Die moderne Technik und das komplexe Recht machen es aber im Datenschutz nicht einfach. Das zeigt zum Beispiel der erste Beitrag zu dem neuen KI-Dienst DeepSeek. Hier herrschen zum einen die Risiken, wie sie bei allen KI-Apps vorhanden sein können. Doch bei DeepSeek kommen weitere Gefahren hinzu, die Sie kennen sollten.

Wie Sie selbst für mehr Klarheit und Übersicht sorgen können, erklärt Ihnen der zweite Beitrag, der Ihnen wichtige Tipps für ein „digitales Aufräumen" gibt. Mehr Transparenz bietet auch der dritte Beitrag, wenn es um die Weiterleitung von dienstlichen Mails nach Hause geht.

Die neue Ausgabe schließt diesmal mit Hinweisen dazu, wie Sie auf mögliche Anfragen reagieren, die das Löschen von Daten verlangen. Hier stellt sich die Frage, was wann gelöscht werden muss und wer denn überhaupt eine Löschung verlangen kann.

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

Warum KI-Apps wie DeepSeek besonders riskant sein können

4 von 10 Deutschen haben generative KI (Künstliche Intelligenz) wie ChatGPT, Google Gemini oder Microsoft Copilot zumindest einmal ausprobiert. Mit DeepSeek scheint sich ein weiterer KI-Dienst einzureihen. Doch vor DeepSeek wird besonders gewarnt.

Generative KI wird oftmals im Kundenkontakt und im Marketing genutzt

ChatGPT und andere Formen von generativer KI werden nicht nur auf privaten Smartphones genutzt. Auch Unternehmen versprechen sich Vorteile von KI: Am häufigsten wird generative KI derzeit im Kundenkontakt (89 Prozent) verwendet, so eine Umfrage des Digitalverbands Bitkom. Dahinter folgt mit deutlichem Abstand der Einsatz im Marketing und in der Kommunikation (40 Prozent der befragten Unternehmen).
Offensichtlich spielen im Kundenkontakt, im Marketing und in der Kommunikation auch personenbezogene Daten eine große Rolle, der Datenschutz wird also in aller Regel berührt, wenn generative KI zum Einsatz kommt.
Deshalb warnen Datenschützerinnen und Datenschützer auch davor, einfach ungeprüft vertrauliche, zu schützende Daten in eine KI einzugeben.

Mit DeepSeek ist nun eine weitere, generative KI im Angebot. DeepSeek verblüfft und verunsichert die Technologie-Welt. Das neue KI-Modell eines chinesischen Unternehmens soll deutlich effizienter und günstiger entwickelt worden sein als die Konkurrenz aus den USA. Der neue KI-Dienst funktioniert ähnlich wie sein Konkurrent ChatGPT, ruft aber sogar noch stärkere Bedenken hervorruft als die anderen KI-Dienste.

Datenschutz- und Sicherheitsexperten warnen vor leichtfertiger KI-Nutzung

KI-Sicherheitsforscher von Robust Intelligence und der University of Pennsylvania (siehe https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reasoning-models) zeigten, dass DeepSeek einfacher durch Attacken zu manipulieren sein kann als vergleichbare KI-Dienste. Wiz Research deckte offengelegte DeepSeek-Datenbanken auf, die vertrauliche Informationen, einschließlich Chatverlauf, preisgeben können (siehe https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak).
Offensichtlich ist es um die Datensicherheit bei diesem KI-Dienst gegenwärtig nicht gut bestellt. Datenschutzaufsichtsbehörden nennen weitere Gründe, warum man bei der Nutzung von DeepSeek Vorsicht walten lassen sollte:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und andere Aufsichtsbehörden machten explizit auf die Risiken aufmerksam, die mit der Verwendung des KI-Tools DeepSeek verbunden sein können. Obwohl dieses Modell der generativen KI im Internet frei zugänglich ist, hat es der Hersteller nicht für den europäischen Markt konzipiert, erklären die Datenschützer. Nach gegenwärtigem Kenntnisstand sei davon auszugehen, dass insbesondere die Anforderungen der europäischen KI-Verordnung und der Datenschutz-Grundverordnung nicht eingehalten werden.

„Auch chinesische Unternehmen müssen rechtskonform mit den Daten europäischer Bürgerinnen und Bürger umgehen, wenn sie ihre Apps in Europa anbieten“, sagte Denis Lehmkemper, Landesbeauftragter für den Datenschutz Niedersachsen. „Wir müssen aber davon ausgehen, dass es bei DeepSeek noch erheblichen Nachholbedarf beim Datenschutz gibt.“

Mögliche Weiterleitung an Geheimdienste

Insbesondere lässt sich der Datenschutzerklärung zu DeepSeek entnehmen, dass jegliche Eingaben und gegebenenfalls hochgeladene Dokumente uneingeschränkt aufgezeichnet, übertragen, gespeichert oder analysiert werden, so die Warnung der Datenschützer. DeepSeek weist außerdem darauf hin, dass das Unternehmen nach chinesischem Recht verpflichtet werden kann, dem chinesischen Geheimdienst und den Sicherheitsbehörden Daten zu übermitteln. Da das Unternehmen und damit die für die Verarbeitung der personenbezogenen Daten verantwortliche Stelle nicht auf dem Gebiet der EU ansässig ist und keinen gesetzlichen Vertreter in der EU ernannt hat, geht zum Beispiel die Datenschutzaufsicht in Niedersachsen davon aus, dass die Zusammenarbeit des Unternehmens mit den Datenschutzbehörden in der EU unsicher ist. Datenschutzverletzungen und ein Missbrauch von Daten werden faktisch also nur sehr schwer zu unterbinden und zu ahnden sein.

Tipps der Datenschutzaufsichtsbehörden zu KI-Apps wie DeepSeek

Bevor also eine generative KI wie DeepSeek privat oder beruflich zum Einsatz kommt, sollten insbesondere diese Punkte beachtet werden:

Achten Sie bei der Auswahl einer KI-Anwendung auf Transparenz des Anbieters und eine entsprechende Dokumentation, aus der nachvollziehbar hervorgeht, dass Garantien für die Einhaltung der DSGVO gegeben werden und diese eingehalten werden.

Stellen Sie vor der Installation des KI-Dienstes sicher, dass keine (personenbezogenen) Daten abfließen können. Zum Beispiel durch eine separate, gesicherte IT-Umgebung oder andere geeignete Maßnahmen.

Wenn Sie eine Online-Schnittstelle verwenden, sollten Sie niemals personenbezogene oder vertrauliche Daten eingeben, es sei denn, es sind wirksame Maßnahmen bekannt, die einen Missbrauch verhindern können. Wenn keine Maßnahmen bekannt sind, ist davon auszugehen, dass keine vorhanden sind.

Digitales Aufräumen – eine sinnvolle Sache!

Einfach mal Datenmüll wegschaffen! Die Idee stammt von der Datenschutzaufsicht Baden-Württemberg. Das trägt zum Datenschutz bei. Es hilft aber auch, Cyberattacken abzuwehren. Denn wer den Überblick über die gespeicherten Daten verliert, wird besonders schnell zum Opfer.

Datenhaufen entstehen ständig

Das gute alte Papierbüro hatte zumindest einen Vorteil: Es war sofort zu erkennen, wer die Leidenschaft pflegte, hemmungslos Daten aufzuhäufen. Denn irgendwann war schlicht jeder freie Platz im Büro mit Ordnern und Heftmappen belegt. Elektronische Datenhaufen wachsen dagegen im Verborgenen. Dafür sind sie oft umso größer. Denn nach dem Motto „Besser haben als brauchen“ fördern viele den Wildwuchs von Daten, anstatt auch einmal zu entrümpeln.

Fehlender Überblick kann fatal enden

In so manchem Mail-Account liegen schon im Posteingang ständig Hunderte von Mails. Darunter finden sich oft zahlreiche Newsletter, die irgendwann einmal abonniert wurden. Oder Werbemails, die eigentlich niemand braucht.

Und dann ist es gar zu schnell passiert: Irgendwann kommt eine Mail, die wie eine Werbemail aussieht, aber in Wirklichkeit gar keine ist. Schnell ist sie nebenbei, etwa während eines langweiligen Telefonats, geöffnet. Dann noch versehentlich den Link in der Mail angeklickt und schon freut sich ein Cyberkrimineller darüber, dass ihm jemand die elektronische Tür freiwillig geöffnet hat.

Abbestellen schafft Luft

Aus dem Verteiler von Werbemails kann man sich löschen lassen, aus den Verteilern für Newsletter genauso. Gehen Sie das einfach an, auch wenn es zunächst fast aussichtslos erscheint! Sehr schnell werden Sie feststellen, dass sich der Posteingang im Mail-Account fühlbar leert. Das Wichtige tritt stärker hervor. Ungewöhnliches und Verdächtiges nehmen Sie leichter wahr. Jede Abbestellung erfordert zwar einige Klicks. Zugleich reduziert sie aber dauerhaft den Posteingang und zahlt sich so dauerhaft aus.

Manche Datenträger sind eigentlich bloß Müll

In vielen Unternehmen ist ihr Einsatz völlig verboten. In manchen Büros haben sie aber nach wie vor eine wichtige Funktion. Gemeint sind USB-Sticks und SD-Karten, die dem Transport von Daten dienen, etwa zu einem Kunden. Optimal wäre es natürlich, auf solche mobilen Datenträger völlig zu verzichten. Sie erweisen sich immer wieder als gefährliches Einfallstor für Schadsoftware. Sie erweisen sich immer wieder als gefährliches Einfallstor für Schadsoftware. Wenn es ohne sie nicht geht, sollten aber zumindest defekte Datenträger zügig entsorgt werden. Dasselbe gilt für Datenträger, die einfach nur herumliegen, ohne jemals zum Einsatz zu kommen.

Überflüssige Accounts können gefährlich sein

Schon die Buchhaltung-Azubis lernen es: Ein Bankkonto, das niemand benutzt, gerät aus dem Blick. Das schafft beste Möglichkeiten für Kriminelle, um das Konto für was auch immer zu missbrauchen. Ähnlich sieht es mit überflüssigen Mailaccounts und überflüssigen Kunden-Accounts bei Online-Shops aus. Bestellungen durch böswillige Außenstehende können umfassenden Ärger nach sich ziehen. Das gilt sogar dann, wenn es gelingt, die Zahlungspflicht abzuwehren.

Müllvermeidung geht auch elektronisch

Am besten ist es, wenn Müll erst gar nicht entsteht. Das gilt auch für Datenmüll. Setzen auch Sie bei einer Mail manchmal zur Sicherheit lieber

ein paar Kolleginnen und Kollegen mehr in cc als wirklich notwendig? Das kostet unnötig Arbeitszeit bei allen Empfängerinnen und Empfängern. Und es trägt dazu bei, die Mail-Accounts zu verstopfen. Vielleicht wäre das einmal ein Thema für das nächste Gespräch bei einer Tasse Tee oder Kaffee. Es wird Sie möglicherweise überraschen, auf welche Kopien die Empfängerinnen und Empfänger sehr gern verzichten würden.

Auskunftsansprüche können viel Aufwand auslösen

Manche denken sich: Wem schadet es schon, wenn auf meiner Festplatte einiges an Datenmüll liegt? Niemand sieht ihn, niemand erleidet einen Schaden. Das erweist sich spätestens dann als Trugschluss, wenn eine betroffene Person Auskunft über ihre Daten verlangt.

Ein solcher Auskunftsanspruch erfasst nämlich alle Daten dieser Person, die vorhanden sind. Ob diese Daten längst hätten gelöscht werden können, spielt keine Rolle. Solange sie vorhanden sind, ist über sie Auskunft zu erteilen.

Manchmal gibt es noch Papier-Ordner

In mehr als einem Büro gibt es Schränke mit Papier-Ordnern, angelegt vielleicht noch von einer Vorgängerin, die längst den Ruhestand genießt. Wenn Sie ohnehin am Aufräumen sind, finden vielleicht auch noch solche „Erbstücke“ den Weg zum Akten-Schredder. Sinn ergibt das in jedem Fall.

Weiterleitung von dienstlichen Mails nach Hause?

Manchmal geschieht es in bester Absicht: Jemand leitet Mails von seinem E-Mail-Account im Unternehmen an den privaten E-Mail-Account weiter. Daraus kann großer Ärger entstehen, egal aus welchen Gründen es geschieht. Lassen Sie es daher lieber bleiben.

Gut gemeint ist nicht immer gut gemacht

Der dienstliche Laptop hat ausgerechnet heute den Geist aufgegeben. Morgen müssen Sie aber einen wichtigen Kunden besuchen. Und da muss zumindest einiges von dem verfügbar sein, was Sie dort gespeichert hatten. Deshalb schicken Sie sich vom Büro-PC das Wichtigste per Mail auf Ihr privates iPad. Dahinter steckt eindeutig keine böse Absicht. Trotzdem ist eine solche Aktion keine gute Idee.

Sprechen Sie Ihr Vorgehen immer ab

Wenn jemand wie eben beschrieben

vorgeht, verlassen die Daten den „Datenbereich“ des Unternehmens und landen in seinem privaten „Datenbereich“. Auch ohne große Datenschutz-Fantasie ist klar: Das zieht schon deshalb Probleme nach sich, weil das Unternehmen nicht mehr die Hand auf den Daten hat. Wenn Sie meinen, so etwas tun zu müssen, ist also eine Absprache im Unternehmen nötig. Dies gilt besonders dann, wenn es um personenbezogene Daten geht. Aber auch andere Daten, etwa vertrauliche Kalkulationsdaten des Unternehmens, können genauso schutzwürdig sein – wenn auch auf der Basis anderer gesetzlicher Regelungen.

Private Zwecke müssen außen vor bleiben

Die Gerichte hatten mehrfach mit Fällen zu tun, in denen sich Beschäftigte Daten auf ihren privaten E-Mail-Account schickten, um sich persönlich abzusichern. Auf solche Ideen können Menschen kommen, wenn es Spannungen am Arbeitsplatz gibt. berechtigten neuen Vorwürfen. Dann fürchten sie manchmal, später irgendwann mit Vorwürfen konfrontiert zu werden. Und um sich dann wehren zu können, möchten sie „Verteidigungsmaterial“ in den Händen haben. Das ist jedoch ein Irrweg. Denn gerade ein solches Vorgehen führt später zu berechtigten neuen Vorwürfen.

Die Verantwortung wird verlagert

Wer dienstliche Daten in seinem privaten Bereich übermittelt, wird dadurch hinsichtlich dieser Daten zum Verantwortlichen im Sinn der DSGVO. Mögliche Ansprüche betroffener Personen richten sich dann gegen ihn, nicht gegen das Unternehmen, aus dessen Bereich die Daten ursprünglich stammen. Dies gilt für Auskunftsansprüche genauso wie für Schadensersatzansprüche. Dias liegt daran, dass ein Unternehmen keinerlei Zugriff auf die privaten Accounts seiner Beschäftigten hat. Dann trägt es für personenbezogene Daten in diesen Accounts jedoch auch keine Verantwortung.

Es fehlt an einer Befugnis für die Übermittlung

Jede Übermittlung von Daten braucht eine Rechtsgrundlage. Dies gilt auch, wenn jemand Daten von seinem E-Mail-Account im Unternehmen an seinen privaten E-Mail-Account übermittelt. In Betracht käme hier allenfalls, dass dies geschieht, um berechtigte Interessen zu verfolgen. So könnte man beim Ausfall des dienstlichen Laptops überlegen, ob es dem Kunden vielleicht ganz recht wäre, wenn die Daten beim Kundenbesuch trotzdem zur Verfügung stehen. Solche Überlegungen führen jedoch in die Irre.

Betroffene Personen müssten informiert werden

Wer sich darauf berufen will, eigene berechtigte Interessen zu verfolgen, muss die betroffene Person darüber informieren. Denn nur so hat die betroffene Person die Möglichkeit, auch ihre eigenen Interessen geltend zu machen. Und die können ganz anders aussehen als die Interessen dessen, der die Daten übermitteln will. ganz vernünftig“ hält, genügt nicht, um eine Datenübermittlung zu rechtfertigen.

Negative Konsequenzen sind denkbar

Wen alle bisherigen Überlegungen nicht überzeugen, der sollte zumindest an die Spielregeln des Arbeitsrechts denken. Es verletzt die Pflichten aus dem Arbeitsvertrag, wenn jemand Daten aus dem Bereich des Unternehmens ohne Absprache und Zustimmung des Unternehmens in seinen privaten Bereich übermittelt. Wenn es dabei um personenbezogene Daten, gilt dies ganz besonders. Denn sie genießen einen erhöhten gesetzlichen Schutz.

Das gilt alles auch für „höhere Ebenen“

Manche denken vielleicht, dass solche strengen Maßstäbe nur die „Kleinen“ in einem Unternehmen betreffen. Doch weit gefehlt! Das Oberlandesgericht München hat im letzten Jahr entschieden, dass sich selbst Vorstandsmitglieder an die geschilderten Spielregeln halten müssen. Weil dies ein Vorstandsmitglied nicht getan hatte, griff der Aufsichtsrat durch und berief dieses Vorstandsmitglied ab. Nach Auffassung des Gerichts völlig zu Recht!

Wenn Kunden die Löschung ihrer Daten verlangen

Datenschutzaufsichtsbehörden führen gegenwärtig eine EU-weite Prüfung zur Umsetzung des Rechts auf Löschung durch. Aus gutem Grund: Das Recht auf Löschung ist ein zentraler Pfeiler des Datenschutzes, da es Personen die Möglichkeit gibt, die weitere Verarbeitung ihrer Daten tatsächlich zu beenden. Doch wie setzt man Anfragen zur Löschung von Daten richtig um?

Die Aufsichtsbehörden erreichen häufig Beschwerden

Das Recht auf Löschung ist eines der häufigsten ausgeübten Betroffenenrechte der Datenschutz-Grundverordnung (DSGVO) und eines, zu dem bei den Datenschutzaufsichtsbehörden viele Beschwerden eingehen. Nun wollen die Aufsichtsbehörden in einer

EU-weiten Prüfaktion feststellen, wie die Umsetzung dieses Rechts in der Praxis aussieht.

Die Frage, ob das Recht Betroffener, die Löschung der eigenen Daten zu verlangen, richtig umgesetzt wird, sollten sich aber nicht nur Unternehmen stellen, die tatsächlich von ihrer zuständigen Aufsichtsbehörde kontrolliert werden. Jedes Unternehmen muss sicherstellen, dass es keine Fehler beim Umgang mit Lösch-Anfragen gibt.

Der Wert der Daten und des Datenschutzes

Das Recht auf Löschung, auch Recht auf Vergessenwerden genannt, verpflichtet die für die Datenverarbeitung verantwortlichen Stellen, personenbezogenen Daten zu löschen, wenn eine weitere Verarbeitung zur Erfüllung des Verarbeitungszwecks nicht mehr erforderlich ist, so will es das Datenschutzrecht.

Das Recht auf Löschen erscheint in Zeiten von Künstlicher Intelligenz (KI) wichtiger denn je. „Mir ist in einer Lebenswirklichkeit, in der immer mehr Datennutzung gefordert wird, sehr wichtig, dass wir durch diese Aktion das Recht auf Vergessenwerden stärken“, erklärte die Landesdatenschutzbeauftragte von NRW Bettina Gayk die Prüfaktion.

„Denn falsche oder nicht mehr erforderliche Daten dürfen nicht zum Nachteil der Betroffenen fortwährend perpetuiert werden“, so Landesdatenschutzbeauftragte Gayk.

Die wenigsten personenbezogenen Daten benötigt man für immer, so auch der Bayerische Landesbeauftragte für den Datenschutz. Wie aber entscheidet man, ob eine Löschung, die zum Beispiel eine Kundin verlangt, durchgeführt werden muss?

Viele Gründe sprechen für eine Löschung, aber nicht ungeprüft

Wenn es zu einer Anfrage zur Löschung von Daten zum Beispiel seitens einer Kundin kommt, sollte die Person, die die Anfrage entgegennimmt, selbst oder mithilfe der oder des Vorgesetzten prüfen, ob denn der Zweck, für den die Daten gespeichert wurden, bereits erfüllt ist. Wurde zum Beispiel schon die Rechnung erstellt und sind die Fristen zur Aufbewahrung abgelaufen? Dann steht in aller Regel die Löschung an.

Ebenso sind die Daten zu löschen, wenn es keine Rechtsgrundlage zur Verarbeitung gab oder die zu den Daten gehörende Einwilligung zur Verarbeitung widerrufen wird.

Wichtig ist aber zu prüfen, ob der Antrag zur Löschung auch wirklich von der betroffenen Person (zum Beispiel der Kundin) kommt, denn nur sie ist berechtigt, die Löschung zu verlangen.

Es muss also nicht auf jeden Wunsch hin die Löschung von Daten erfolgen, aber jede Anfrage zur Löschung von Daten muss überprüft werden, ob sie berechtigt ist.

Wie dies konkret ausgestaltet ist, wollen die Datenschutzaufsichtsbehörden in ihrer Prüfaktion bei mehreren Unternehmen untersuchen. Wenn man als Beschäftigte oder Beschäftigter nicht genau weiß, wie dies im eigenen Unternehmen umgesetzt ist, sollte man nachfragen, also nicht einfach löschen, aber auch nicht die Anfrage zur Löschung unbeachtet lassen.

Wissen Sie, wie Sie auf Lösch-Anfragen richtig reagieren?

Frage 1: Wenn eine Kundin per E-Mail verlangt, dass ihre Daten in der Datenbank gelöscht werden, muss dies sofort umgesetzt werden. Stimmt das?

1. Nein, zuerst einmal muss sichergestellt sein, dass es sich wirklich um die betreffende Kundin handelt.
2. Ja, immerhin sind es die Daten der Kundin, sie kann dies verlangen.

Lösung Frage 1: Die Antwort 1 ist richtig. Nur die betroffene Person (also zum Beispiel die Kundin selbst) kann die Löschung ihrer Daten beantragen. Bei einer herkömmlichen E-Mail kann man nicht einfach davon ausgehen, dass die als Absender genannte Person auch wirklich die Person ist, die die Löschung beantragen kann. E-Mail-Absender zum Beispiel können auch gefälscht werden.

Frage 2: Solange die Daten für das Unternehmen nützlich sind, muss keine Löschung erfolgen, auch wenn es die betroffene Kundin will. Stimmt das?

1. Ja, denn Daten stellen einen hohen wirtschaftlichen Wert dar, gerade in Zeiten der Künstlichen Intelligenz (KI).
2. Nein, wenn die Daten ihren Zweck erfüllt haben und keine Aufbewahrungsfrist mehr zu beachten ist, steht die Löschung an.

Lösung Frage 2: Die Antwort 2 ist hier richtig. Auch wenn Daten als das „neue Öl“ gelten, können Unternehmen nicht einfach davon ausgehen, dass der wirtschaftliche Wert eine dauerhafte Speicherung der Daten erlaubt. Das Recht auf Löschung oder Vergessenwerden setzt der Speicherung von Daten ein Ende, wenn ein Löschungsgrund eintritt. Welche Gründe dies sind, regelt die Datenschutz-Grundverordnung in Artikel 17.