# Newsletter Datenschutz

konzept17
Datensicherheit trifft Vertraulichkeit

## Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

viele Datenpannen entstehen, weil Nutzer Risiken noch nicht ausreichend kennen oder unterschätzen. Online-Betrug verbinden viele in erster Linie mit Phishing-Mails oder gefälschten Shops. Der erste Beitrag zeigt, dass Cyberbetrug auch ganz anders aussehen kann – etwa durch geschickte Täuschungsversuche am Telefon.

Der zweite Artikel lenkt den Blick auf unterschätzte Gefahren bei Fotos. Bilddateien enthalten oft mehr Informationen als man auf den ersten Blick vermutet. Metadaten können vertrauliche Details preisgeben. Der Beitrag erklärt, wie Sie solche Risiken erkennen und vermeiden.

Auch der Einsatz von Künstlicher Intelligenz (KI) birgt Fallstricke. Zusatzinformationen aus dem Internet, die User zur Verbesserung der KI-Antworten eingeben, können manipulative oder schädliche Anweisungen enthalten. Mehr dazu im dritten Beitrag.
Im letzten Beitrag geht es um Online-Tracking. Viele glauben, Tracking finde nur beim Besuch von Webseiten statt. Doch schon das Öffnen eines Newsletters kann offenlegen, für welche Inhalte sich Empfänger interessieren.
Ich wünsche Ihnen eine interessante Lektüre!

*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

## Cyberbetrug hat viele Gesichter

**Beim Stichwort Cyberbetrug denken viele Internetnutzende an gefälschte Online-Shops oder Phishing-Mails. Doch Internetkriminelle nutzen alle Kommunikationskanäle, um ihre Opfer zu schädigen und an vertrauliche Daten zu gelangen. Selbst klassische Briefe und Telefonanrufe sind betroffen.**

### Betrugsmails haben nicht nur Passwörter als Ziel

Phishing-Mails gehören mit einem Anteil von 60 Prozent zu den häufigsten Angriffsformen der Cyberkriminellen, berichtet die EU-Agentur für Cybersicherheit (ENISA) in ihrem aktuellen Lagebericht „Threat Landscape 2025“. Dies sollte jedoch nicht so verstanden werden, dass Betrugsnachrichten, die per E-Mail eintreffen, immer Passwörter erbeuten sollen.

Polizeibehörden wie das Landeskriminalamt (LKA) Niedersachsen warnen vor der Betrugsmasche „Sextortion“. Darunter versteht man einen Erpressungsversuch mit angeblich sexuellem Material, das per E-Mail verschickt wird. Meist behaupten die Täter, Nacktaufnahmen oder intime Videos von einem Opfer zu besitzen, und fordern daraufhin Geld, damit diese nicht veröffentlicht werden. Weil solche Mails massenhaft verschickt werden, können sie an beliebige E-Mail-Empfänger gehen – darunter auch Firmenpostfächer.

### Auch per Briefpost versuchen es Internetkriminelle

Es muss jedoch keine E-Mail sein, mit der Online-Betrüger angreifen wollen. Selbst der klassische Brief oder eine Nachricht über das Faxgerät kann für Cyberbetrug genutzt werden. Möglich wird dies zum Beispiel über QR-Codes oder durch die Angabe einer Internetadresse im Schreiben. Die Webadresse oder der QR-Code kann dann auf eine gefälschte Internetseite oder direkt zur Schadsoftware führen, mit der eine Online-Erpressung (Ransomware) gestartet wird.

Dabei sind klassische Briefe und Faxnachrichten sogar besonders gut geeignet, um Cyberbetrug zu versuchen, denn als Empfänger rechnet man bei diesen altbekannten Kommunikationsformen kaum mit digitalen Gefahren. Die Kriminellen hingegen sehen die Chance, auch auf diesem Weg ihre Opfer auf gefährliche Online-Seiten zu locken oder zu erpressen.

### Selbst am Telefon lauern Online-Betrüger

Die EU-Agentur für Cybersicherheit hat in einer Anti-Phishing-Kampagne deutlich gemacht, dass Phishing und andere Formen des Cyberbetrugs über jeden Kanal erfolgen können – ob E-Mail, Brief mit QR-Code, SMS, Videokonferenz oder Telefon. Dabei wollen Cyberkriminelle ihre Opfer am Telefon dazu verleiten, beispielsweise Einmal-Passwörter für das Online-Banking weiterzugeben. Die Täter

nutzen zunehmend digitale Methoden, um besonders glaubhaft zu wirken.
Dank Künstlicher Intelligenz (KI) lassen sich am Telefon menschliche Stimmen imitieren, sodass scheinbar eine Kollegin, ein Familienmitglied oder ein dem Opfer bekannter Bankmitarbeiter anruft und vertrauliche Informationen erfragt oder zu riskanten Handlungen auffordert – etwa zum Erwerb digitaler Gutscheine, deren Codes dann an die Täter übermittelt werden sollen.

Diese vielfältigen Formen des Cyberbetrugs sind Bedrohungen für Privatpersonen wie auch für Beschäftigte, denn die Betrugsmaschen lassen sich leicht an berufliche oder private Situationen anpassen.

### Wichtig: Skeptisch sein auf allen Kanälen

Auch wenn Sie besonders oft von Phishing-Mails hören und lesen, sollten Sie nicht nur bei E-Mails Vorsicht walten lassen, wenn man Sie um vertrauliche Informationen bittet oder Sie mit angeblichen Nacktbildern erpressen möchte.

Internetkriminelle übertragen ihre Methoden auch auf klassische Kommunikationswege. Deshalb müssen Sie Ihre Skepsis auf alle Kanäle anwenden. Das LKA Niedersachsen empfiehlt entsprechend:

- **Ruhe bewahren** und bei Erpressungsversuchen **nicht zahlen** – in der Regel liegen den Tätern keinerlei kompromittierende Aufnahmen vor.
- **Nicht antworten** – eine Antwort bestätigt nur, dass Sie erreichbar sind; dies kann weitere Kontaktversuche fördern.
- **Nachricht im Original aufbewahren** , damit sie als Beweismittel dienen kann.
- **Anzeige erstatten** bei der Polizei.
- **Verdachtsfälle im Arbeitsumfeld melden** – auch wenn der Betrugsversuch per Briefpost oder Telefon stattgefunden hat.

## Tückische Personensuche mit Fotos

**Auf dem eigenen Handy ist es eine schöne Sache: Bequem und mit hoher Treffsicherheit kann man alle Bilder eines lieben Menschen aus dem Berg von vielleicht 25.000 gespeicherten Fotos herausfiltern. Doch Vorsicht! In anderen Zusammenhängen kann eine Bildersuche schnell gefährlich werden.**

### „Google Lens" zeigt das Prinzip

Sie haben eine Pflanze vor sich und wissen nicht, was das für eine ist? Kein Problem! Sie fotografieren das Gewächs und laden das Bild in Google Lens hoch. Meist bekommen Sie sehr treffgenau ähnliche Bilder mit passenden botanischen Beschreibungen, und schnell ist das Rätsel gelöst. Nun probieren Sie dasselbe einmal mit dem Bild einer Person. Und siehe da: Sehr weit kommen Sie nicht. Anders als Sie vielleicht vermuten, liefert Google Lens nicht etwa zahlreiche weitere Bilder dieser Person, sondern teilt Ihnen kühl mit: „Personensuche ist eingeschränkt".

Das hat nicht etwa technische Gründe. Was mit dem Bild einer Pflanze funktioniert, würde vom technischen Prinzip her auch mit dem Bild einer Person funktionieren. Doch Google möchte nicht,

dass Sie Google Lens als eine Art Personensuchmaschine nutzen können. Allein mit dem Bild einer Person sollen Sie keine weiteren Bilder dieser Person finden können. Das dient dem Datenschutz und dem Schutz des Persönlichkeitsrechts. Diese Blockade funktioniert nicht hundertprozentig, aber doch sehr zuverlässig.

### Andere Software macht mehr möglich

Selbstverständlich kann man im Internet „Gesichtersuchmaschinen" finden und gegen Bezahlung auch nutzen. Ob dies legal ist, steht auf einem anderen Blatt. Deshalb bekommen Sie hier auch keine entsprechenden Tipps. Vor allem in den USA nutzen Strafverfolgungsbehörden entsprechende Software, gemäß dortigem Recht auf legaler Basis. Viel diskutiert wird in diesem Zusammenhang die Software „Clearview AI". Die Seite des Unternehmens ist leicht zu finden. Sie bietet Demo-Videos, die zeigen, was die Software leisten kann. Sie sollten sich bewusst sein, dass es derartige Software gibt und dass sie unter Umständen sogar völlig legal im Einsatz sein kann.

### „Gesichter gruppieren" in der eigenen Fotosammlung ist ok

Um etwas völlig anderes geht es, wenn Sie in Ihrer eigenen privaten Fotosammlung Bilder einer bestimmten Person zusammenstellen, etwa in einem eigenen Bilderalbum.

Hier kommen im Hintergrund zwar ähnliche Techniken zum Einsatz wie in den bisher beschriebenen Fällen. Das beeinträchtigt aber nicht die Persönlichkeitsrechte der Personen, von denen Sie Bilder besitzen. Auch die DSGVO sieht darin kein Problem. Im Gegenteil: Solche rein persönlichen oder familiären Aktivitäten will sie gar nicht regeln. Das ergibt sich aus Art. 2 Abs.2 Buchstabe d. Er sieht eine Ausnahme von ihrem Anwendungsbereich vor, für die man oft den etwas seltsamen Begriff „Haushaltsausnahme" findet.

### Viele Fotos enthalten zusätzliche „Metadaten"

Das griechische Wort „meta" bedeutet in etwa „in Verbindung mit". Damit ist klar, was mit „Metadaten" bei Fotos gemeint ist. Es geht um Daten, die zusammen mit dem Foto gespeichert werden und die Zusatzinformationen zum eigentlichen Bildinhalt liefern. Häufig halten sie den Zeitpunkt der Aufnahme fest und die Kameraeinstellungen. Aber auch der Ort der Aufnahme – und zwar in Form von GPS-Koordinaten – kann Teil der Metadaten sein.

Diese Daten sind vor allem für den gedacht, der fotografiert. Wer nach einem Familienfest oder einem Urlaub den Berg an Bildern sortieren will, greift oft gern auf den Aufnahmezeitpunkt oder den Aufnahmeort zurück. Doch Vorsicht: Metadaten können so etwas wie ein Eigenleben entwickeln! Das gilt vor allem, wenn Fotos in soziale Netzwerke oder auf einer Homepage eingestellt werden.

### Befassen Sie sich einmal mit diesen Metadaten!

Daten, die vorhanden sind, lassen sich in allen möglichen Zusammenhängen nutzen – und zwar durch alle, die auf diese Daten zugreifen können.

Das hört sich etwas abstrakt an, ist aber der entscheidende Punkt. Gar zu schnell lassen sich etwa aus GPS-Koordinaten Aufenthaltsorte rekonstruieren. Das kann harmlos sein, muss es aber nicht. Welche Möglichkeiten KI-Software künftig dabei eröffnet, lässt sich noch gar nicht abschätzen.

Bevor Sie Fotos von Personen in soziale Netzwerke einstellen, sollten Sie sich deshalb einmal mit den „Exif-Tags" dieser Bilder befassen. Damit sind die Datenfelder gemeint, die auf der Basis des Datenformats „Exif" Metadaten zu einem Foto enthalten. Auch Menschen, die üble Zwecke verfolgen, können diese Daten auslesen. Sind solche Daten gar nicht vorhanden, weil von Ihnen gelöscht, können Sie das sicher ausschließen.

## Vorsicht bei Prompt-Eingaben!

**Künstliche Intelligenz (KI) in unterschiedlichen Formen ist inzwischen überall im Einsatz. Teils überzeugen die Antworten der KI, teils nicht so ganz. Manche Tipps für bessere Antworten können auch gefährlich werden. Daher gilt: Erst denken, dann eingeben!**

### Die Qualität der Daten ist entscheidend

Auch die Antwort der besten KI kann nur so gut sein wie die Daten, die ihr zur Verfügung stehen. Das mussten schon viele schmerzlich erfahren. Denn manchmal läuft es so: Die Antwort der KI war in schönem Deutsch formuliert, ihr Inhalt schien schlüssig und gut umzusetzen. Vorgetragen in einer Runde mit Leuten vom Fach löste sie aber nur Kopfschütteln aus. Dumm gelaufen!

### Zusätzliche Daten aus dem Unternehmen können eine Idee sein


Diese unschöne Situation hätte sich vielleicht vermeiden lassen. Die KI hätte schlicht zusätzliches Futter in Form von guten Daten gebraucht. Deshalb findet sich häufig der Tipp, doch einfach zusätzlich gutes Datenmaterial in die KI einzugeben – mit einem Prompt wie „Berücksichtige diese Informationen!". Möglicherweise wären geeignete Daten sogar im Unternehmen selbst verfügbar gewesen. Dann liegt der Gedanke nahe, sie künftig in solchen Situationen in die KI einzugeben, als Teil der Prompt-Anweisungen.

Das ist an sich in Ordnung. Doch Vorsicht: Beachten Sie die Vorgaben, die dafür im Unternehmen bestehen! Manchmal gibt es Datenbestände, für die das Unternehmen die Nutzung für die KI bewusst ausgeschlossen hat. Solche Vorgaben würden Sie umgehen, wenn Sie derartige Datenbestände dann doch dafür nutzen.

### Daten aus dem Internet können zweifelhaft sein

Bei der Übernahme von Daten aus dem Internet ist in erster Linie die fachliche Qualität wichtig. Maßstab sollte dabei sein: Könnte Sie die Frage, woher Sie diese Daten genommen haben, in Verlegenheit bringen? Stets sollten Sie festhalten, welche Daten Sie benutzt haben. Diese Hinweise wirken vielleicht banal. Die praktische Erfahrung zeigt allerdings, dass ihre Beachtung oft Probleme vermeidet.

### Daten aus dem Internet können gefährlich sein

KI-Software verhält sich zum Teil anders als sonstige Software. Eine besondere Tücke liegt darin, dass über die Prompt-Eingabe sowohl Arbeitsanweisungen für die KI möglich sind als auch die Eingabe von Daten, die verarbeitet werden sollen. Beides getrennt voneinander zu halten, ist bei einer KI-Software allenfalls teilweise möglich. Daraus entstehen Gefahrenquellen.

Sie lassen sich am Beispiel von Textdokumenten recht anschaulich schildern. Beispielsweise ist ein in weißer Schrift auf weißem Grund geschriebener Text für das menschliche Auge nicht sichtbar. Er ist aber vorhanden. Dasselbe gilt für Text in der Schriftgröße null. Das menschliche Auge kann ihn nicht wahrnehmen – er ist aber vorhanden. Das bietet Manipulationsmöglichkeiten. So können Sie etwa einen Text eingeben, der äußerlich unverdächtig erscheint. Für Ihr Auge unsichtbar enthält er jedoch Anweisungen an die KI, wie sie vorgehen soll. Was das alles anrichten kann, lässt sich ohne große Fantasie erahnen.

### Chatbots und KI-Agenten können das Problem verschärfen

Prompts wie „Suche im Internet Quellen zu folgender Frage …“ kann ein dafür konzipierter KI-Agent sehr gut ausführen. Er kann dies bei entsprechenden Vorgaben auch selbstständig tun – also ohne gesonderte menschliche Anweisung für den jeweiligen Einzelfall. Damit fehlt allerdings auch die menschliche Kontrolle. Nur zu leicht ist es dann möglich, dass er auf Quellen stößt, die manipulative Vorgaben enthalten.

Solche Gefahren sind Realität, aber noch nicht lange bewusst. Sogar das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sie erst im Jahr 2023 aufgegriffen. Unter dem Stichwort „Indirect Prompt Injections“ sind auf seiner Webseite dazu vertiefte Informationen zu finden. Der Begriff „Prompt Injection“ lässt sich sinngemäß mit „Einbringen unerwünschter Vorgaben als Prompt“ übersetzen. Der Mensch, der die KI-Software benutzt, trägt dazu nichts direkt bei. Deshalb geschieht es „indirekt“, also quasi hinter seinem Rücken.

### Gefahren ernst nehmen, aber nicht überzeichnen!

Natürlich fällt es leicht, Horrorszenarien zu entwickeln, was alles passieren kann. Am Ende tritt dann leider oft eine allgemeine Angst vor Daten aus externen Quellen auf. Das führt nicht weiter. Ohne solche Daten geht es nämlich vielfach nicht. Besser ist es daher, den Grundsatz zu beherzigen: „Erst denken, dann eingeben!“ Und einem KI-Agenten kann man durchaus vorgeben, welche zuverlässigen Internetquellen er vorrangig heranziehen soll.

## Heimliche Überwachung per Newsletter

**Online-Tracking als systematische Verfolgung, Erfassung und Analyse des Nutzerverhaltens von Personen droht nicht nur, wenn Sie eine Website besuchen. Auch bei Newslettern könnte versucht werden, Ihre Interessen an den Inhalten heimlich auszuspähen. Davor warnen nun Datenschutzaufsichtsbehörden.**

### Tracking innerhalb und außerhalb des Webbrowsers

Viele Internetnutzerinnen und -nutzer haben schon davon gehört, dass beim Besuch von Internetseiten die Gefahr besteht, Online-Aktivitäten nachverfolgt werden. Tatsächlich kann jedoch an vielen Stellen ein Nachverfolgen versucht werden, um auf Basis eines Trackings ein konkretes Interessenprofil der jeweiligen Person zu erzeugen.

Wie zum Beispiel die Datenschutzbehörde von Baden-Württemberg erklärt, kann es auch Tracking-Versuche geben bei Smartphone- und Tablet-Apps, PC-Software oder Geräten aus dem Bereich des Internets der Dinge (Internet of Things, IoT) wie vernetzten Küchengeräten, Lampen, Steuergeräten für Heizungen, Alarmsystemen, Smart-TVs oder vernetzten Fahrzeugen.

Nicht vergessen werden sollte der E-Mail-Empfang, denn Tracking gibt es auch bei Werbe-Mails und Newslettern. Tatsächlich berichten die deutschen Datenschutzaufsichtsbehörden, dass bei ihnen viele Beschwerden gegen Unternehmen eingehen, die heimlich über Newsletter tracken wollen.

### Unsichtbare Bildchen können „Verräter“ sein

Nun könnte man denken, dass erst über das Öffnen eines Links, der im Newsletter genannt wird, getrackt werden kann. Doch das Nachverfolgen kann bereits damit beginnen, dass Sie eine E-Mail – wie zum Beispiel einen Newsletter – öffnen. Möglich wird dies, weil E-Mails nicht nur Texte, sondern auch Bilder enthalten können.

Für das heimliche Tracking werden unsichtbare Bilder genutzt, die meist nur 1 × 1 Pixel groß sind. Dennoch sind es Bilddateien, die aufgerufen werden können, wenn der Newsletter geöffnet wird. Das winzige Bildchen wird dabei aus dem Internet geladen und erzeugt so einen Datenstrom,

der sich nachvollziehen lässt.

Nach Datenschutzrecht ist ein solches Tracking-Pixel jedoch nicht ohne Weiteres zulässig. Wie die Aufsichtsbehörden erklären, ist nach geltendem Recht eine Einwilligung der empfangenden Person notwendig, die jedoch in der Praxis oftmals nicht eingeholt wird.

Auch wenn man den Newsletter abonniert hat, ist zuerst die Einwilligung notwendig, denn das Zähl- oder Tracking-Pixel ist technisch nicht erforderlich, damit der Anbieter den gewünschten Dienst erbringen kann.

Der Nutzende möchte die Inhalte lesen, nicht aber getrackt werden.

### Tracking-Schutz im E-Mail-Programm

Leider sind nicht alle E-Mail-Programme automatisch datenschutzfreundlich. Es kann sein, dass Sie selbst Einstellungen vornehmen müssen, um das Nachladen des Zählpixels oder das Tracking über unsichtbare Bilder zu verhindern. Dazu müssen Sie insbesondere die reine Textversion für die E-Mail-Anzeige wählen und die automatische Anzeige von Bildern ausschalten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mehrere E-Mail-Programme untersucht und gibt entsprechende Hinweise (Untersuchung „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus E-Mail-Programme“, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/E-Mail-Programme.pdf).

## Wissen Sie, wie Mail-Empfänger getrackt werden können?

***Frage: Als Empfänger eines Newsletters werde ich nur getrackt, wenn ich einen Link anklicke – stimmt das?***

1. Nein, auch innerhalb der E-Mail kann zum Beispiel ein Zählpixel sein, mit dem getrackt werden kann.
2. Ja, das Tracken findet immer nur im Webbrowser statt, also nach Anklicken eines Links

Lösung: Antwort 1 ist richtig. Auch ohne Anklicken eines Links können Nutzungsdaten erhoben werden, wenn zum Beispiel in den Newsletter ein unsichtbares Zählpixel eingebaut ist. Wird die E-Mail geöffnet, könnte ein Pixel abgerufen werden – damit findet eine heimliche Datenübertragung statt, die nachvollzogen werden könnte, wenn es keine Gegenmaßnahmen gibt.

***Frage: Das E-Mail-Programm verhindert automatisch das Tracking in Newslettern – ist das richtig?***

1. Nein, man kann nicht einfach davon ausgehen, dass E-Mail-Programm zum Beispiel das Nachladen eines unsichtbaren Pixels verhindert.
2. Ja, denn alle Mail-Programme haben neben Pishing- und Spam-Schutz auch einen integrierten Tracking-Schutz.

Lösung: Antwort 1 ist wieder richtig. Ein Tracking-Schutz bei E-Mail-Programmen ist keine Selbstverständlichkeit. Es ist also gut möglich, dass man als E-Mail-Empfänger spezielle Einstellungen vornehmen muss, um das Nachladen eines Tracking-Pixels bei Newslettern zu verhindern.