SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

so manches im Datenschutz ist nicht offensichtlich. Umso wichtiger ist es, sich mit den Details vertraut zu machen. So erfahren Sie in dieser Ausgabe, dass es nicht nur in Word-Dokumenten, sondern auch in den beliebten PDFs Datenschutzfallen gibt, und was Sie dagegen tun können.
Auch der bekannte Auskunftsanspruch hat unbekannte Seiten. Gilt er zum Beispiel noch nach dem Tod? Diese Ausgabe liefert Ihnen die Antwort.
Über ChatGPT und die Risiken für den Datenschutz wird viel gesprochen. Doch wussten Sie, dass Künstliche Intelligenz (KI) der Datensicherheit auch helfen kann? Erfahren Sie gleich, wie das möglich ist.
Und bei den immer beliebteren Smartphone-Apps sollten Sie eines nicht übersehen: Was geschieht mit den Nutzungsdaten? Lesen Sie, worauf Sie achten sollten.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

August_2023

1 DATENSCHUTZFALLEN BEI PDF-DOKUMENTEN

Sie müssen ein Word-Dokument weiterleiten? Sie wollen dabei Ärger mit dem Datenschutz vermeiden? Sie wandeln das Word-Dokument deshalb in ein PDF-Dokument um? An sich eine gute Idee. Gerade deshalb sollten Sie wissen, was dabei an Details zu beachten ist. Leider kosten manche wichtigen Hilfsmittel etwas.

PDF: ein guter Ansatz!

Word-Dokumente gehören zum Alltag im Büro. Oft ist es nötig, sie weiterzuleiten, etwa als Anhang einer E-Mail. Nachteil dabei: Der Empfänger kann alle möglichen Veränderungen sichtbar machen, die das Dokument erfahren hat. Dabei kann er meist auch erkennen, von wem die Veränderung stammt. Der Name oder zumindest ein Kürzel stehen dabei.

Tückisch: die Zusatzdaten bei Word

Solange das Dokument intern zwischen Kolleginnen und Kollegen ausgetauscht wird, die daran arbeiten – kein Problem! Denn dann soll ja gerade jeder wissen, wer was verändert hat. Anders sieht es aus, wenn das Dokument nach außen geht. Dann ist das nicht akzeptabel und womöglich ein Datenschutz-Problem. Für solche Fälle gilt der Tipp: Wandeln Sie Word in PDF um!

Vorteile einer Umwandlung in PDF

Dieser Ratschlag ist ebenso häufig wie richtig. Die Umwandlung hat durchaus einige Vorteile. Ein PDF-Dokument kann nur noch mit relativ aufwendigen Mitteln verändert werden. Damit ist das, was Sie verschickt haben, gewissermaßen fixiert. Außerdem ist nicht mehr festzustellen, wer wann etwas am Word-Dokument verändert hat. Die Nachweise hierfür gehen bei der Umwandlung in ein PDF-Dokument verloren, so die Idee dahinter.

Einige typische Fallen

In Wirklichkeit bleiben einige Tücken, die man kennen sollte:

- Folgende Daten übernimmt ein PDF-Dokument vom Word-Dokument: Name der Word-Datei, Angaben zum Bearbeiter (falls sein Name in der Datei steht, also auch der!) und verwendete Software. Wenn es sinnvoll ist, sollte man daher den Dateinamen und die Angaben zum Bearbeiter in den Dateieigenschaften innerhalb des Office-Programms ändern.
- Manchmal sollen Teile eines PDF-Textes geschwärzt werden. Dafür bietet Adobe Acrobat unter „Werkzeuge“ – „Schutz“ die Funktion „Inhalt schwärzen und entfernen“. Das Programm ist kosten-pflichtig, beseitigt aber den Text, der geschwärzt wird.
- Keine gute Idee ist es dagegen, den Text lediglich mit einem schwarzen Feld zu überlagern. Ein solches Feld kann der Empfänger problemlos wieder entfernen.
- Wenn Teile eines PDF-Dokuments nachträglich „weggeschnitten“ werden, sind sie in Wirklichkeit nur ausgeblendet. Der Empfänger des Dokuments kann diese Teile problemlos wiederherstellen.

Eine besonders wichtige – aber kostenpflichtige – Funktion

Am zuverlässigsten ist es, das PDF-Dokument mit der (kostenpflichtigen) Funktion „vertrauliche Dokumente veröffentlichen“ zu bearbeiten, bevor man es weitergibt. Diese Funktion erzeugt das Dokument komplett neu. Alle unerwünschten Inhalte sind danach beseitigt. Ebenso kann man mit dem Tool in PDF-Dateien mit der entsprechenden Funktion „verborgene Informationen suchen und entfernen“.

2 AUSKUNFTSANSPRUCH NACH ART. 15 DSGVO – AUCH NOCH NACH DEM TOD?

Jede Person hat Anspruch auf Auskunft über personenbezogene Daten, die sie betreffen. So regelt es Art. 15 Datenschutz-Grundverordnung (DSGVO). Aber was ist, wenn die betroffene Person verstirbt? Geht ihr Auskunftsanspruch dann auf den (oder die) Erben über?

Wenn es um Geld geht, wird es ernst

Wenn es um Geld geht, kämpfen Menschen oft erbittert um ihr Recht. Das gilt besonders bei einem Erbfall. Viele Erben versuchen, mit allen denkbaren Mitteln an Informationen über möglicherweise vorhandene Vermögenswerte zu kommen. Besonders interessieren sie sich für Bankguthaben aller Art.

Auskunftsansprüche gegen Banken sind wichtig

Wohl deshalb waren mehrere Aufsichtsbehörden für den Datenschutz in Deutschland schon mit Erben konfrontiert, die Auskunftsansprüche des verstorbenen Erblassers gegenüber Banken geltend machen wollten. Ähnliche Fälle gab es in Österreich. Dabei sollte man bedenken: Der Anspruch auf Auskunft nach Art. 15 DSGVO ist inhaltlich sehr umfassend. Zudem muss die Auskunft kostenlos erteilt werden. Diese Besonderheiten machen den datenschutzrechtlichen Auskunftsanspruch sehr attraktiv.

Oft wollen Erben von einer Bank nicht nur wissen, welches Guthaben ein Girokonto aktuell im Ergebnis ausweist, sondern auch, wie die Kontobewegungen im Lauf der letzten zehn Jahre ausgesehen haben. Letzteres ist von Interesse, wenn die Erben Schenkungen zurückfordern wollen, die der Verstorbene gemacht hat. Der Verstorbene selbst hätte derartige Auskünfte von der Bank auf der Basis von Art. 15 DSGVO verlangen können. Schließlich geht es dabei um Daten, die ihn betreffen. Die Frage ist, ob dieses Auskunftsrecht nach seinem Tod seinen Erben zusteht.

Mit dem Tod endet das Auskunftsrecht nach Art. 15 DSGVO

Alle Aufsichtsbehörden sind sich einig, dass hier jedenfalls das Auskunftsrecht nach Art. 15 DSGVO nicht weiterhilft. Es stand dem Verstorbenen zu seinen Lebzeiten zu, wird aber nicht vererbt. Vielmehr erlischt es mit seinem Tod. Dies gilt sogar dann, wenn der Verstorbene kurz vor seinem Tod gerade dabei gewesen war, einen Auskunftsanspruch nach Art. 15 DSGVO gerichtlich durchzusetzen. Das Verfahren vor Gericht wird dann beendet, ohne dass das Gericht über den Auskunftsanspruch entscheidet.

Als Begründung für diese Sichtweise beziehen sich alle Aufsichtsbehörden auf Erwägungsgrund 27 Satz 1 zur DSGVO. Er lautet kurz und knapp: „Diese Verordnung [also die DSGVO] gilt nicht für die personenbezogenen Daten Verstorbener.“ Der Hintergrund hierfür: Die DSGVO soll die Grundrechte betroffener Personen schützen. Grundrechte stehen jedoch nur lebenden Personen zu. Das gilt auch für das Grund-recht auf Datenschutz.

Abweichende nationale Regelungen gibt es nur für Teilbereiche

Da die DSGVO nichts regelt, ist der Weg für Regelungen durch die Mitgliedstaaten frei. Das bringt Satz 2 von Erwägungsgrund 27 zur DSGVO so zum Ausdruck: „Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vor-

sehen.“ Diese Möglichkeit hat der deutsche Gesetzgeber für einen wichtigen Bereich genutzt, nämlich für die Wiedergabe von Abbildungen einer Person. Dafür gilt: „Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“.

Aber was ist, wenn die abgebildete Person verstorben ist? Dann ist Folgendes zu beachten: „Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten.“ So regelt es § 22 des Kunsturheberrechtsgesetzes. Dabei sollte man sich durch den Namen des Gesetzes nicht irritieren lassen. Denn selbstverständlich geht es bei diesem § 22 nicht um das Urheberrecht, sondern um das Persönlichkeitsrecht.

Vertragliche Auskunftsansprüche reichen oft weniger weit

Im Ausgangsfall der Erben, die sich über die Kontobewegungen auf dem Girokonto eines Verstorbenen informieren wollen, hilft allenfalls noch ein vertraglicher Auskunftsanspruch weiter. Ein Girokonto wird auf der Basis eines Vertrags zwischen dem Kontoinhaber und der Bank geführt. Stirbt der Kontoinhaber, treten die Erben in alle Rechte ein, die sich aus diesem Vertrag ergeben. Dazu gehören auch vertragliche Auskunftsansprüche, sofern sich solche Ansprüche aus dem Vertrag ergeben.

Genau das ist in der Praxis oft das Problem. So könnte etwa bei einem Girokonto geregelt sein, dass vertragliche Auskunftsansprüche nur für die letzten drei Jahre bestehen – selbst wenn noch ältere Daten vorhanden sind. Das Auskunftsrecht nach Art. 15 DSGVO ist dagegen zeitlich nicht begrenzt. Dass sich Erben auf dieses Recht nicht berufen können, hat in solchen Fällen daher handfeste praktische Konsequenzen.

3 BESSERE DATENSICHERHEIT DURCH CHATGPT

Aus der Sicht von Datenschutz und Datensicherheit sehen viele ChatGPT ausgesprochen kritisch. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt andere Akzente. Es sieht in ChatGPT eine Chance zur Verbesserung der Datensicherheit – vorausgesetzt, man setzt es dafür sinnvoll ein. Denn das menschliche Denken wird durch ein solches System nicht überflüssig.

Oft stehen die Risiken im Vordergrund

Kann man mithilfe von ChatGPT täuschend echte Spam-Mails erzeugen? Ja, das ist natürlich möglich. Und funktioniert die Programmierung von Schadsoftware mit diesem System? Ja, oft sogar sehr gut. Diese Risiken sieht selbstverständlich auch das BSI. Es fasst die Situation so zusammen: Der Einsatz eines Sprachmodells wie ChatGPT „verstärkt das Bedrohungspotenzial einiger bekannter IT-Sicherheitsbedrohungen“.

Was schadet, kann aber auch Nutzen stiften

Doch auch für ChatGPT gilt das, was der heute vergessene Dichter Hölderlin vor über 200 Jahren so formuliert hat: „Wo aber Gefahr ist, wächst das Rettende auch.“ Zwar zitiert ihn das BSI nicht. In einem Arbeitspapier geht es aber ausführlich darauf ein, welche Chancen für eine Verbesserung der IT-Sicherheit ChatGPT bietet. Dabei spricht es eine große Palette von Möglichkeiten an.

Unerwünschte Inhalte lassen sich herausfiltern

Die erste Möglichkeit ist die „Detektion unerwünschter Inhalte“. Diese Formulierung wirkt zunächst sehr abstrakt. Sie spricht die Kehrseite der Produktion unerwünschter Inhalte an. Ein System, das „gut gemachte“ Spam-Mails erzeugen kann, erkennt derartige Spam-Mails in der Regel auch sehr gut. Das bietet für Opfer von Spam-Mails die Möglichkeit, sich auf Augenhöhe gegen die Täter zu wehren.

Datenverkehr lässt sich analysieren

Eine weitere Möglichkeit bildet die Unterstützung bei der Analyse von Datenverkehr. Eine solche Analyse ermöglicht es beispielsweise, ungewöhnliche Vorgänge im Netzwerkverkehr zu erkennen. Sie können auf Schadsoftware hinweisen, die im Netzwerk unterwegs ist. Auch verdächtige Einlog-Vorgänge lassen sich mithilfe gut gemachter Analysen herausfiltern.

Eine Untersuchung auf Sicherheitslücken ist möglich

Überraschend dürfte für viele sein, dass sich ein System wie ChatGPT auch dazu einsetzen lässt, vorhandene Programmcodes auf bekannte Sicherheitslücken zu untersuchen. Oft konzentriert sich die Aufmerksamkeit auf neue Sicherheitslücken, die bisher niemand im Fokus hatte. Zwar sind solche neuen Sicherheitslücken gewiss wichtig. Oft genug entstehen jedoch Schäden durch längst bekannte Sicherheitslücken, die man nur hätte berücksichtigen müssen.

Große Datenmengen sind rasch auszuwerten

Generell hilfreich kann ein System wie ChatGPT sein, wenn es um die Analyse großer Textmengen geht. Die Notwendigkeit dazu tritt im Bereich der IT-Sicherheit vor allem auf, wenn es zu Sicherheitsvorfällen gekommen ist. Dann gilt es oft, große Mengen von Texten rasch zu analysieren, um das Ausmaß des Vorfalls abschätzen zu können.

Die äußere Qualität von Texten täuscht oft

Chancen ohne Risiken gibt es generell so gut wie nie. Das gilt auch bei den eben geschilderten Möglichkeiten. Hier gilt ebenfalls: Systeme wie ChatGPT erzeugen Texte, die meist sprachlich fehlerfrei sind und zumindest auf den ersten Blick inhaltlich sehr überzeugend wirken, oft sogar auf den zweiten Blick. Deshalb ist immer darauf zu achten, welche Daten für das Training des Systems verwendet wurden. Wer mit seiner Hilfe beispielsweise nach Schadsoftware sucht, muss vorher überlegen, welche Typen von Schadsoftware das System überhaupt „kennen“ kann.

Geben und Nehmen sind zwei Seiten der Medaille

Daten bekommt bei Systemen wie ChatGPT nur der, der auch Daten gibt. Eine scheinbar harmlose Eingabe von Daten enthält oft sensible oder vertrauliche Informationen. Was mit ihnen geschieht, ist nicht nachvollziehbar. In jedem Fall fließen sie in die vorhandene Datenbasis ein. Das kann dazu führen, dass sie sich in nicht vorhersehbaren Zusammenhängen irgendwo wiederfinden. Theoretisch lässt sich dieses Risiko vermeiden, indem man eine eigene Datenbasis aufbaut und ein System wie ChatGPT nur mithilfe dieser Basis nutzt. Praktisch realisieren lässt sich das allerdings nur für wenige Unternehmen und mit erheblichen Ressourcen.

Hier gibt es vertiefte Informationen

Wer sich detailliert informieren will, sollte auf das 21-seitige Papier „Große KI-Sprachmodelle – Chancen und Risiken für Industrie und Behörden“ des BSI zurückgreifen. Es ist am 3. Mai 2023 erschienen und hier abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.html

4 SMARTPHONE-APPS: DIE SUCHE NACH DEM DATENSCHUTZ

Die Bedeutung mobiler Geräte nimmt weiter zu. Die Zahl der installierten Apps auf Smartphones und Tablets wächst und wächst. Doch wie steht es um den Datenschutz bei den mobilen Anwendungen? Die Antwort fällt nicht immer leicht, ist aber zunehmend wichtig für die Privatsphäre.

Da gibt es eine App für …

Ob Information, Kommunikation, Unterhaltung, Einkaufen oder Reisen: Smartphones sind für einen Großteil der Menschen in Deutschland ein unverzichtbarer Teil ihres Alltags geworden. Dementsprechend wächst auch das Angebot an Apps.

Mit der Hilfe von Apps erweitern Smartphones und Tablets fortlaufend ihre Funktionen, sie ersetzen die Digitalkamera, das Bücherregal, die Spielekonsole. Diese Funktionsvielfalt erscheint nützlich und macht die mobilen Endgeräte so beliebt, doch sie führt auch zu einer Konzentration von Nutzungsdaten auf jeweils nur einem Gerät.

Apps gibt es für Geld oder Daten

Wer jetzt denkt, Apps seien doch kostenlos und vielleicht auch deshalb so beliebt, hat zum Teil recht. Die Mehrzahl der mobilen Anwendungen bekommt man tatsächlich, ohne dafür zu bezahlen. Doch ob der Anbieter seine App wirklich ohne Gegenleistung bereitstellt, steht auf einem anderen Blatt.

Viele Apps finanzieren sich über Werbung. Damit die Werbung möglichst relevant und damit erfolgreicher ist, sammeln zahlreiche Apps Daten über ihre Nutzerinnen und Nutzer. Daran wäre nichts auszusetzen, wenn denn die Anwendenden darüber informiert wären und darin eingewilligt hätten.

Tatsächlich sammeln und werten die Apps die Nutzungsdaten oftmals aus, ohne eine Information und Zustimmung der Anwenderinnen und Anwender. Das ist nicht nur bei kostenlosen Apps der Fall. Auch kostenpflichtige Apps können Daten einsammeln, um für ein Zusatzgeschäft zu sorgen.

Wo ist die Datenschutzerklärung?

Ob eine App Daten sammelt, welche Daten sie sammelt und zu welchem Zweck das geschieht, aber auch wer die Daten des Nutzers oder der Nutzerin erhält, all das soll in einer Datenschutzerklärung zu finden sein, die vor der Installation der App einzusehen sein muss.

Aber auch nach der Installation der App muss es möglich sein, die Datenschutzerklärung einzusehen. Insbesondere bei einem Update der App kann sich etwas getan haben, das auf den Datenschutz Einfluss hat.

Wer aber bei Apps nach einer Datenschutzerklärung sucht, wird leider nicht immer fündig, im Gegenteil!

Datenschutz hinterfragen: im App-Store und in der App selbst

Ob eine App eine Datenschutzerklärung hat oder nicht, sollte darüber entscheiden, ob man die App überhaupt installiert und nutzt. Die App-Stores wie Google Play für Android-Apps haben in aller Regel einen Link bei der App-Beschreibung, der zur Datenschutzerklärung führt. Leider ist dieser Link nicht so leicht zu finden, zum Beispiel bei den Kontaktdaten des App-Entwicklers oder der App-Entwicklerin.

Noch schwieriger ist es, wenn man die App bereits installiert hat. Hier erscheint es eher wie eine Ausnahme, wenn eine App auch einen Bereich für die Datenschutzerklärung hat. Selbst bei bekannten Apps lässt sich nicht davon ausgehen, dass sie wirklich umfassend über den Datenschutz informieren.

Wer also nicht mit seinen Daten für eine App bezahlen will, ohne genau zu wissen, wer was zu welchem Zweck erfahren wird, sollte auf Apps ohne Datenschutzhinweise verzichten. Tatsächlich wollen viele Apps mehr erfahren, als sie wissen müssten. Das klassische Beispiel sind etwa Apps mit Taschenlampen-Funktion, die auf Standortdaten und Fotos zugreifen wollen. Da sollte einem das Licht aufgehen, dass hier eine App womöglich Nutzungsdaten sammeln will.

Es gibt aber inzwischen auch Apps, die ausdrücklich auf unnötige Datenzugriffe verzichten und so besonders datenschutzfreundlich sind. Das Projekt „Privacy Friendly Apps“ (https://secuso.aifb.kit.edu/105.php) hat kostenfreie Open-Source-Apps aus den Bereichen Fitness & Gesundheit, Tools, Spiele und Sicherheit entwickelt, etwa einen Schrittzähler oder eine App für den Wetterbericht. Die Privacy Friendly Apps fordern lediglich die Berechtigungen an, die für die Funktionalität notwendig sind. Sie enthalten keine Tracking-Mechanismen und verzichten auf Werbung. Jegliche Daten werden nur auf den Geräten der Nutzenden gespeichert.

Wissen Sie, was eine App über Sie weiß?

Machen Sie den App-Test!

Kostenpflichtige Apps sammeln keine Nutzungsdaten. Stimmt das?

1. Nein, man kann nicht davon ausgehen, dass der Anbieter einer App, die Geld kostet, keine Zusatzgeschäfte mit Daten machen will.
2. Ja, man bezahlt dann mit Geld und nicht mit seinen Daten.

Lösung:

Die Antwort 1. ist (leider) richtig. Selbst kostenpflichtige Apps können Berechtigungen für Datenzugriffe verlangen, die nicht erforderlich sind, und dann Daten über die Nutzerin oder den Nutzer sammeln, um die Daten an Dritte weiterzugeben oder die Daten selbst zu nutzen.

Apps ohne Datenschutzhinweise werten auch keine Nutzerdaten aus. Ist das so richtig?

1. Ja, dann sind bei der App keine personenbezogenen Daten im Spiel.
2. Nein, gerade wenn die Datenschutzerklärung fehlt, kann es sein, dass die App verstärkt Nutzerdaten sammelt und analysiert.

Lösung:

Die Antwort 2. ist richtig. Informiert eine App nicht über den Datenschutz, nimmt es der Anbieter offensichtlich nicht sehr genau mit dem Schutz der Privatsphäre. Eine informierte Einwilligung des Nutzers oder der Nutzerin ist nicht möglich. Stattdessen kann es sein, dass unnötige Datenzugriffe erfolgen und Nutzungsprofile erzeugt werden, ohne dass der oder die Betroffene eine Ahnung davon hat. Verzichten Sie daher auf Apps ohne Datenschutzhinweise.

Lagen Sie richtig? Apps sind praktisch und erleichtern den Alltag. Und mit den richtigen Vorsichtsmaß-nahmen lassen sich die damit verbundenen Risiken vermeiden.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de