SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

die Digitale Transformation betrifft nicht nur die IT, die Arbeit vieler Beschäftigter transformiert sich, mit Auswirkungen auf den Datenschutz.
In Ihrer neuen Ausgabe finden Sie deshalb wichtige Hinweise zum Datenschutz bei dem praktischen Einsatz von Anwendungen, die KI (Künstliche Intelligenz) nutzen. Dies betrifft in Zukunft mehr und mehr die tägliche Arbeit in vielen Unternehmensbereichen.
Aber auch die Art der genutzten Geräte und die Arbeitsorte wandeln sich. So werden Smartwatches inzwischen vermehrt auch beruflich genutzt. Zudem hat das Homeoffice in zahlreichen Tätigkeitsbereichen einen festen Platz erobert, zusätzlich zum Büro in der Unternehmenszentrale. Deshalb werden sowohl die intelligenten Uhren als auch der Arbeitsplatz daheim in dieser Ausgabe näher behandelt.
Doch es gibt auch noch Arbeitsmittel, die schon seit vielen Jahren eine Rolle spielen, wie die Visitenkarten. Erfahren Sie auch hierzu, worauf es im Datenschutz ankommt.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

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

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

April_2024

1 DATENSCHUTZPFLICHTEN BEIM EINSATZ VON KI-ANWENDUNGEN

Künstliche Intelligenz (KI) ist mehr als ChatGPT. Aber erst dieses Werkzeug hat vielen deutlich gemacht, was KI bereits alles kann. Dabei muss einem immer bewusst sein: Die Vorgaben des Datenschutzes gelten auch beim Einsatz von KI. Sie sind immer zu beachten, wenn personenbezogene Daten im Spiel sind.

ChatGPT macht die Möglichkeiten der KI bewusst

ChatGPT ist in Deutschland seit Ende 2022 öffentlich verfügbar. Die Nutzung der Basisversion ist kostenlos. Bedienen lässt sich das System ohne besondere Einweisung. Schnell erzielt man beeindruckende Ergebnisse. Diese Vorteile haben dazu geführt, dass die Nutzerzahlen schnell explodiert sind. Und doch ist ChatGPT nur eines von vielen KI-Systemen. Ein bekanntes weiteres Beispiel bildet das Übersetzungsprogramm DeepL.

Kreativität und Vorsicht ergänzen sich gut

Viele probieren vor allem ChatGPT „einfach mal so“ am Arbeitsplatz aus. Das kann die Kreativität fördern und neue Ansätze aufzeigen. KI-Leitlinien des Unternehmens sind dabei immer zu beachten. Sie enthalten oft Vorgaben dafür, wie der Einsatz von KI-Systemen zu dokumentieren ist. Im Übrigen sind alle selbst für das verantwortlich, was sie am Arbeitsplatz tun. Dazu gehört es auch, sich um den Datenschutz zu kümmern.

Der Personenbezug der Daten ist entscheidend

Generell kommt der Datenschutz immer dann ins Spiel, wenn Daten personenbezogen sind. Wie brisant personenbezogene Daten sind, spielt dabei keine Rolle. Privatanschriften von Kunden unterfallen selbstverständlich dem Datenschutz, die interne Telefonliste eines Unternehmens aber auch. Schon einzelne personenbezogene Daten in einem größeren Dokument machen das gesamte Dokument personenbezogen.

Auch KI-Systeme gehören in das „Verzeichnis der Verarbeitungstätigkeiten“

Wer personenbezogene Daten in ein KI-System eingibt, verarbeitet diese Daten. Eine solche Verarbeitung muss in das „Verzeichnis der Verarbeitungstätigkeiten“ aufgenommen werden, das jedes Unternehmen führt. Dieses Verzeichnis ist in Art. 30 DSGVO vorgeschrieben. Ausnahmen für KI-Systeme sucht man im Gesetz vergebens.

Rechte betroffener Personen gelten auch bei KI-Systemen

Personen, deren Daten verarbeitet werden, haben bekanntlich ein sehr weitgehendes Auskunftsrecht. Dazu gehört auch die Auskunft darüber, für welchen Zweck ihre Daten verarbeitet werden. Gewiss ist die Versuchung groß, ChatGPT „mal einfach so“ mit Daten von Kundinnen und Kunden zu testen. Dann erstreckt sich der Auskunftsanspruch aber auch darauf, welche Daten dafür verwendet worden sind.

Im Zweifel lieber mal die obere Ebene fragen

Wer ChatGPT und ähnliche Systeme einfach mal ausprobieren möchte, sollte dafür öffentlich zugängliche Texte benutzen. Sie finden sich beispielsweise auf der Homepage des eigenen Unternehmens. Ein erster Versuch könnte zum Beispiel darin bestehen, bei ChatGPT die Zusammenfassung eines längeren Textes zu bestellen. Wer mit internen Daten des Unternehmens experimentieren will, sollte dies dagegen unbedingt vorher absprechen.

2 VISITENKARTEN UND DATENSCHUTZ

Auch beim Umgang mit Visitenkarten soll der Datenschutz eine Rolle spielen? Diese Vorstellung scheint für viele weit hergeholt. Und dennoch sollte man sich darüber einige Gedanken machen. Vor allem wenn es um den Austausch von Visitenkarten auf Fachmessen geht. Denn im geschäftlichen Kontext ist manches zu beachten.

Die Visitenkarte ist lebendiger denn je

Totgesagte leben länger, sagt ein Sprichwort. Es trifft auch auf Visitenkarten zu. Man benutzt sie bei weitem nicht mehr so oft wie früher. Aber gerade bei einer ersten Kontaktaufnahme im beruflichen Bereich sind Visitenkarten einfach nützlich. Das gilt vor allem auf Fachmessen. „Nach Corona“ sind die Besucherzahlen dort wieder beachtlich. Und die Anbahnung neuer Kontakte ist natürlich stets sehr erwünscht.

Manchmal ist der Austausch von Visitenkarten reine Privatsache

Die DSGVO will den Datenschutz umfassend regeln. An einer Stelle hält sie sich jedoch zurück. Nämlich dann, wenn natürliche Personen Daten ausschließlich für persönliche oder familiäre Angelegenheiten verarbeiten. Im Klartext: Wenn zwei Menschen miteinander Visitenkarten austauschen, um rein privat miteinander Kontakt zu haben, ist das kein Thema für die DSGVO. Der Begriff „privat“ erfasst dabei alle möglichen Dinge, von einem gemeinsamen Hobby bis zu einer persönlichen Beziehung. Geschäftliche Absichten dürfen dabei weder direkt noch indirekt eine Rolle spielen.

Der Austausch führt zu einer Erhebung von Daten

Eine Visitenkarte enthält üblicherweise außer dem Namen noch eine oder mehrere Anschriften und eine oder mehrere Telefonnummern. Hinzu kommt fast immer eine persönliche E-Mail-Adresse. Dass solche Kontaktdaten personenbezogen sind, liegt auf der Hand. Wer von einem anderen eine Visitenkarte entgegennimmt, erhebt diese Daten. Er hat sie zur Verfügung, um künftig etwas damit zu machen.

Der Zweck der Datenerhebung ergibt sich aus der Situation

Maßgeblich ist, wofür jemand seine Visitenkarte übergibt. Das ergibt sich aus der Situation. Manchmal ist Anlass, dass ein Vertrag geschlossen wird. Dann geht es um den Austausch der Daten genau für diesen Zweck. Hierzu ein Beispiel: Jemand kauft auf einer Messe eine neue Haustür. Es muss noch genau ausgemessen werden, wie groß die Tür sein muss. Geliefert wird sie dann einige Zeit später. Dann darf der Händler die Daten von der Visitenkarte seines Kunden etwa dazu verwenden, um die nötigen Termine auszumachen.

Dieser Zweck ist maßgeblich

So gut wie nie werden die Beteiligten bei einer solchen Situation über den Zweck des Datenaustausches sprechen. Er liegt für sie auf der Hand, denn allen Beteiligten ist klar, worum es geht. Niemand kommt auf die Idee, diesen Zweck schriftlich festzuhalten oder dergleichen. Das ist auch nicht erforderlich. Zugleich liegt darin aber der Quell für Missverständnisse. Das Risiko für solche Missverständnisse trägt derjenige, der die Daten verwendet.

Werbung ist ein anderer Zweck

Angenommen, im Beispiel von eben überlegt es sich der Käufer der Haustür noch einmal. Er ruft zwei Tage nach dem Besuch der Messe an und macht den Kauf rückgängig. Dann darf der Händler die Daten aus der Visitenkarte nicht einfach dazu verwenden, um später eine andere Haustür anzubieten. Denn mit der Durchführung des ursprünglich geschlossenen Vertrages hat das dann nichts mehr zu tun. Es geht vielmehr um reine Werbung. Und darin liegt ein völlig anderer Zweck.

Sammelboxen für Visitenkarten sind möglich, aber…

E-Mail-Adressen sind unentbehrlich, um Werbenewsletter zu versenden. Die Herausforderung für Unternehmen liegt darin, an entsprechende E-Mail-Adressen zu kommen. Eine Möglichkeit besteht darin, auf Fachmessen und dergleichen Visitenkarten mit E-Mail-Adressen „einzusammeln“. Manche Unternehmen stellen dafür einfach eine Box auf. Auf dieser Box stehen solche oder ähnliche Texte: „Interesse an unserem Newsletter? Bitte werfen Sie hier Ihre Visitenkarte ein.“ Damit allein ist das Unternehmen aber datenschutzrechtlich nicht auf der sicheren Seite.

Eine Einwilligung muss nachweisbar sein

Werbung mittels elektronischer Post ist nur zulässig, wenn der Betroffene eindeutig eingewilligt hat. So legt es das Gesetz gegen unlauteren Wettbewerb (UWG) fest. Dafür hat sich das Verfahren des „Double-Opt-In“ etabliert. Es ist auch hier zu beachten. Das geht rechtssicher so: Mit einer ersten Mail fragt das Unternehmen an, ob es die Daten aus der Visitenkarte für Newsletter verwenden darf und bittet dafür um Bestätigung. Ist diese Bestätigung erfolgt, erhält der Interessent eine zweite Mail mit einem Bestätigungslink. Erst wenn er auch ihn anklickt, ist die Einwilligung sicher nachgewiesen.

3 SMARTWATCHES: DAS DATENRISIKO AM HANDGELENK

Smartwatches, die intelligenten Armbanduhren, liegen im Trend und werden auch beruflich genutzt. Um ihre Datensicherheit ist es jedoch nicht gut bestellt.

Technik-Fans aufgepasst!

Die sogenannten Wearables wie Smartwatches und Fitness-Tracker begleiten immer mehr Menschen durch ihren privaten und beruflichen Alltag. Doch leider wird bei aller Begeisterung vergessen, was diese am Körper getragenen Geräte für unsere Privatsphäre bedeuten können.

Geräte, die wir als Nutzerin oder Nutzer am Körper tragen, sind ständig bei uns. Sie müssen den Nutzenden nicht verfolgen, sondern sind mit der Person direkt und eng verbunden. Diese Nähe sollte Anlass genug sein, um über die Funktionen der Smartwatches und anderer Wearables genauer nachzudenken. So sind Smartwatches nicht einfach nur Armbanduhren, die anstelle eines Zifferblatts ein hübsches buntes Display haben, das neben der Uhrzeit auch Fotos des Nutzers oder der Nutzerin anzeigen kann. Smartwatches sind mobile Computer, die sich am Handgelenk tragen lassen, und haben inzwischen häufig bereits die gleiche Leistungsfähigkeit wie Smartphones.

Smartwatches können mehr, als die Uhrzeit zu verraten

Viele Technik-Begeisterte, die sich für eine Smartwatch interessieren, wünschen sich etwa das Anzeigen der Daten von Fitness-Apps wie der zurückgelegten Strecke beim Joggen. Andere würden mit ihrer Smartwatch gerne Gesundheitsdaten wie Puls oder Blutdruck messen und bei Bedarf automatisch Verwandte oder den Arzt informieren. Zudem möchten viele die Smartwatch als Navigationsgerät einsetzen und zum Anzeigen eingegangener SMS oder E-Mails nutzen, ohne dafür immer auf das Smartphone schauen zu müssen.

Offensichtlich gelangen so vertrauliche Daten wie private und berufliche E-Mails und SMS und sogar hochsensible Gesundheitsdaten auf die intelligenten Armbanduhren. Trotzdem haben vergleichsweise wenige Nutzerinnen und Nutzer Angst vor Datenmissbrauch, zum Beispiel die Sorge, dass Hacker die Smartwatch angreifen könnten. Doch es stellt sich die Frage, wie datenschutzfreundlich und sicher Smartwatches und andere Wearables wirklich sind.

Prüfungen der Aufsichtsbehörden sind alarmierend

Mehrere Aufsichtsbehörden für den Datenschutz haben sich bereits dieser Frage angenommen und verschiedene Wearables sowie die zugehörigen Fitness-Anwendungen überprüft – mit ernüchterndem Ergebnis.

Bereits die Datenschutzerklärungen erfüllen meistens nicht die gesetzlichen Anforderungen. Sie sind in der Regel viele Seiten lang, nur schwer verständlich und enthalten lediglich pauschale Hinweise zu essenziellen Datenschutzfragen, so die Aufsichtsbehörden. Beunruhigend sind auch die Aussagen zur Datenweitergabe: Die Nutzenden erfahren oftmals weder, an wen genau die Daten weitergegeben werden, noch können sie widersprechen. Generell sind die Daten aber auch für Werbezwecke und zur Profilbildung äußerst interessant.

Viele der tragbaren Fitness-Geräte bieten keine Möglichkeit, Daten selbstständig vollständig zu löschen. Weder im Gerät selbst noch im Nutzerkonto gibt es eine Löschfunktion. Mitunter werden die Fitness-Daten der Nutzenden nicht nur von der Smartwatch auf das Smartphone übertragen, sondern direkt an den Anbieter oder an Partnerunternehmen des Anbieters. In der Regel ist dies mit Risiken verbunden, derer sich die Nutzenden bewusst sein sollten, so die Datenschützer.

Sicherheitsfunktionen sind bei Smartwatches noch eine Seltenheit

Im Vergleich zu Smartphones sind Smartwatches auch kaum mit Sicherheitsfunktionen ausgestattet, obwohl viele Modelle vergleichbare Betriebssysteme und die Möglichkeit haben, Apps zu installieren. Einen Schutz vor Schadsoftware, eine Verschlüsselung der gespeicherten Daten, eine Verschlüsselung der Datenübertragung und einen Zugangsschutz zumindest über eine Passwortabfrage findet man nur bei einigen Modellen.

Neben der Privatnutzung der Smartwatches nimmt auch der berufliche Einsatz zu. Es gibt inzwischen bereits ausgesprochene Business-Smartwatches. Firmen-Mails landen dann ebenso auf der Smartwatch wie digitale Dokumente. Denn der Speicherplatz ist dank internem Speicher der Smartwatch, Erweiterung über Speicherkarten und verknüpfte Cloud-Speicherdienste durchaus üppig. Trotzdem haben selbst die Business-Smartwatches kaum angemessene Sicherheitsfunktionen zu bieten. Einige bringen zwar einen Passwortschutz mit, aber erst wenige Anbieter haben die Möglichkeit geschaffen, dass Sicherheits-Apps auch für Smartwatches entwickelt und später installiert werden.

Vorsicht ist angebracht

Misstrauen Sie also der so beliebten Smartwatch. Machen Sie diese nicht einfach zu Ihrem persönlichen Begleiter und Assistenten, der immer dabei ist und alle Termine und E-Mails kennt. Sonst könnten die vertraulichen Daten schneller die Armbanduhr verlassen, als Sie denken, und Sie hätten womöglich ein echtes Datenrisiko am Handgelenk.

Nutzen Sie die vielfältigen Funktionen deshalb nur mit Vorsicht. Achten Sie darauf, dass die Verbindungen zwischen Smartwatch und anderen Geräten keinesfalls ständig aktiv sind. So unterbinden Sie auch eine mögliche Übermittlung der aktuellen Standortdaten und eine dauerhafte Ortung durch Dritte.

4 DATENSCHUTZ IM HOMEOFFICE:
BETRIEBLICHE DATEN ALS UNTERMIETER

Beschäftigte im Homeoffice sind in Fragen des Datenschutzes zwar nicht auf sich allein gestellt, aber ihr notwendiger Anteil an Schutzmaßnahmen ist höher, als viele glauben. Es geht um mehr als die Sicherheit für Notebook und Smartphone.

Selbst sind die Frau und der Mann

In vielen Unternehmen ist deutlich geworden, dass das Homeoffice nicht mehr komplett verschwinden wird. Im Gegenteil: Viele Firmen sehen das Homeoffice als gleichberechtigten Arbeitsplatz neben dem Büro im Firmengebäude. Man spricht dann von hybriden Arbeitsplätzen.

Doch wirklich gleichberechtigt sind Homeoffice und Büroschreibtisch in der Firma nicht. Denn der Firmenarbeitsplatz kann von den zentralen Maßnahmen der IT-Sicherheit profitieren. Im Homeoffice sind die Beschäftigten selbst gefragt, für die Sicherheit der personenbezogenen Daten stärker aktiv zu werden.

Schützen Sie die Daten im Homeoffice?

Die Lösungen finden Sie am Ende des Beitrags.

Frage 1: Werden betriebliche Geräte im Homeoffice genutzt, ist kein weiterer Datenschutz durch die Beschäftigten notwendig. Stimmt das?

1. Nein, die betrieblichen Daten sind im Homeoffice vielen Risiken ausgesetzt. Reiner Endgeräteschutz reicht nicht.
2. Ja, denn die betrieblichen Daten werden auf den Notebooks und Smartphones, die das Unternehmen gestellt hat, genauso geschützt wie in der Firmenzentrale.

Frage 2: Schwachstellen bei privaten Geräten sind keine Gefahr für die betrieblichen Daten im Homeoffice. Stimmt das?

1. Ja, denn die betrieblichen Daten bleiben ja auf den Geräten des Unternehmens.
2. Nein, mögliche Angriffe auf unsichere Privatgeräte könnten auf die betrieblichen Geräte und Daten übergehen.

Betriebliche Notebooks und Smartphones reichen nicht

Viele Unternehmen verzichten darauf, ausschließlich betriebseigene IT in den Homeoffices zuzulassen, oftmals aus Kostengründen. Die Mehrzahl der Unternehmen setzt darauf, dass die Beschäftigten auch private Geräte betrieblich einsetzen.

Ist dies der Fall, müssen die Beschäftigten die eigenen Geräte wie Notebook und Smartphone genauso stark absichern, wie dies der Arbeitgeber mit den betrieblichen Geräten tut. Insbesondere müssen private und betriebliche Daten und Anwendungen strikt getrennt werden: Der Zugriff privater Apps und unbefugter Dritter, wozu auch die eigene Familie der Beschäftigten zählt, auf betriebliche personenbezogene Daten muss ausgeschlossen werden.

Doch selbst die Bereitstellung von Smartphones und Notebooks durch den Arbeitgeber reicht nicht für den Datenschutz im Homeoffice, es ist mehr an Selbstdatenschutz durch die Beschäftigten gefragt.

Homeoffice muss sichere Umgebung werden

Tatsächlich nutzen selbst betriebliche Smartphones und Notebooks im Homeoffice auch Geräte, die eben doch private Geräte sind. Dies können die Drucker im Homeoffice sein, das Headset, die Webcam, die Maus, der Bildschirm und insbesondere der Internet-Router, mit dem die Verbindung ins Internet, aber meist

auch die Verknüpfung mit dem Firmennetzwerk aufgebaut wird.

Internet-Router sind beliebte Angriffsziele für Hacker, denn sie werden häufig vernachlässigt. Die Sicherheitseinstellungen werden nicht kontrolliert, die Firmware des Routers nicht regelmäßig aktualisiert. Das WLAN-Passwort „kennen“ auch die Smart-Home-Anwendungen, die häufig so reich an Schwachstellen sind, dass ein Angreifer dort das Passwort auslesen kann, um dann den Datenverkehr im Homeoffice zu überwachen.

Nicht nur an die IT denken

Doch nicht nur die komplette private IT, die die Beschäftigten im Homeoffice nutzen, ist Gegenstand des Selbstdatenschutzes, da die IT-Sicherheitsabteilung des Arbeitgebers hier nicht aktiv wird. Auch die Dokumente auf dem heimischen Schreibtisch, die Ausdrucke im privaten Müll und die Telefonate auf dem Balkon oder der Terrasse können zu Datenschutz-Problemen führen.

Wer im Homeoffice arbeitet, muss an den Home-Datenschutz denken. Das umfasst etwa auch das Absperren der heimischen Bürotür, wenn andernfalls unbefugte Zugriffe auf Daten und Dokumente möglich werden könnten.

Und hier die Lösungen für die Quizfragen:

Lösung Frage 1: Die Antwort 1. ist richtig. Die betrieblich gestellten Endgeräte nutzen die restliche IT-Ausstattung, die im Homeoffice vorhanden ist, zum Beispiel den Drucker, die Webcam und den Internetrouter. Haben diese privaten Geräte Schwachstellen, die Angreifer ausnutzen können, ist der Datenverkehr im Homeoffice und aus dem Homeoffice unsicher. Zudem können fehlerhaft entsorgte Ausdrucke oder Telefonate in Anwesenheit Dritter ebenfalls betriebliche Daten in Gefahr bringen. Nur die betrieblichen Endgeräte allein können nicht für die erforderliche Datensicherheit sorgen.

Lösung Frage 2: Die Antwort 2. ist richtig. Datensicherheit im Homeoffice ist nur möglich, wenn alle Risiken in der IT-Ausstattung berücksichtigt werden. Wenn also betriebliche und private IT-Geräte verwendet werden, reicht eine sichere betriebliche IT nicht aus, auch die Privatgeräte brauchen den richtigen Schutz. Gerade wenn private Geräte aus dem Consumer-Bereich ohne spezielle Sicherheitsfunktionen verwendet werden, kann dies zu gefährlichen Sicherheitslücken im Homeoffice führen.

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