comdatis
it-consulting

Infobrief Datenschutz

#einfachmittelständischpragmatisch - immer bestens informiert!

Ausgabe 12/2020

Liebe Leserin, lieber Leser,

in Zeiten der Corona-Pandemie hat sich ein großer Teil des Arbeits- und Privatlebens ins Internet verlagert. Statt täglich ins Büro zu fahren, arbeiten viele im Homeoffice. Videosprechstunden ersetzen teilweise Arztbesuche. All das bleibt nicht ohne Folgen für den Datenschutz. Deshalb finden Sie dazu passende Beiträge in Ihrer aktuellen Ausgabe.

Auch die Nutzung von Office-Programmen findet vermehrt über das Internet statt. Office 365 wird besonders häufig genutzt, ist aber kein leichter Fall für den Datenschutz. Und wer häufiger im Internet unterwegs ist, kennt die vielen Cookie-Banner. Hier gibt es ebenfalls einiges zu beachten. Ihre neue Ausgabe hält wichtige Informationen und Hinweise dazu bereit, damit die verstärkte Nutzung des Internets nicht zu erhöhten Datenrisiken bei Ihnen führt.

Das Team der comdatis wünscht Ihnen und Ihren Familien schöne Feiertage, ein erholsames Fest und einen guten Start ins neue Jahr 2021!

Viele Grüße

Ihr Team der comdatis it-consulting GmbH & Co.KG

#comdatis #einfachmittelständischpragmatisch #datenschutz #dsgvo #bdsg #digitalisierung #verfahrensdokumentation #gobd #gdpdu #gobs #informationssicherheit #itaudit

#einfachmittelständischpragmatisch - immer bestens informiert: Auf unserer Homepage www.comdatis.de finden Sie stets aktuelle Informationen zu den Themen Datenschutz, Informationssicherheit, Digitalisierung, Verfahrensdokumentation, GoBD und IT-Prüfung.

Terminvereinbarung? Das geht bei uns jetzt auch online: Einfach Homepage www.comdatis.de aufrufen, etwas nach unten scrollen und "Terminvereinbarung" auswählen, Thema und Ansprechpartner wählen und absenden. Und schon ist ein Termin für ein Onlinemeeting mit Microsoft Teams vereinbart.

Homeoffice – was sollte ich beachten?

Homeoffice von heute auf morgen wegen Corona ist eine Herausforderung. Vieles ist zu

comdatis
it-consulting

organisieren. Der Datenschutz sollte dabei mit im Blick sein. Jede und jeder kann leicht einige einfache Dinge beachten. Das bewirkt oft erstaunlich viel.

Einsatz privater Geräte nur nach Absprache

Homeoffice geht nicht ohne EDV. Wer dafür ein dienstliches Gerät zur Verfügung hat, darf nur dieses Gerät verwenden. Der Einsatz privater Geräte verlangt eine Absprache mit dem Arbeitgeber, zumindest mit dem unmittelbaren Vorgesetzten. Das muss nicht unbedingt schriftlich geschehen. Aber zumindest ein kurzer Mail-Austausch ist sinnvoll. Private Geräte können zusätzliche Risiken für den Datenschutz mit sich bringen, die am gewohnten Arbeitsplatz nicht bestehen würden.

Besonders wichtig: Updates und Virenschutz

Gerade bei privaten Geräten sind die Standardregeln der Datensicherheit zu beachten. Dazu gehören vor allem regelmäßige Updates! Am regulären Arbeitsplatz sorgt dafür oft die EDV-Abteilung, ohne dass man etwas davon merkt. Bei privaten Geräten muss sich jede und jeder selbst darum kümmern. Dasselbe gilt für den Virenschutz.

Bildschirmschoner zum Schutz der Daten

Ein Bildschirmschoner sollte Standard sein. Stellen Sie ihn so ein, dass er nach einigen Minuten ohne Aktivität „anspringt“. Das sorgt dafür, dass Familienangehörige und Besucher möglichst keine Daten sehen können. Besonders wichtig ist das, wenn Sie keinen besonderen Raum für das Homeoffice haben. Manchmal hilft es auch weiter, den Bildschirm etwas zu drehen, damit nicht jeder, der den Raum betritt, gleich alles sieht.

Tücken beim privaten Telefon

Weil der Empfang am Festnetz-Telefon oft besser ist, nutzen erstaunlich viele im Homeoffice nicht das Diensthandy, sondern den privaten Telefonanschluss. Dabei gerät oft in Vergessenheit, dass es in jedem Telefon Anruflisten gibt. Teils lässt sich diese Funktion schlicht ausschalten. Dann ist das Problem gelöst. Wenn das nicht geht oder nicht gewünscht ist, ist ein regelmäßiges Löschen der Listen nötig. Zumindest einmal in der Woche sollte man dies fest einplanen.

Papierunterlagen sicher aufbewahren!

Ganz ohne Papier geht es meistens auch im Homeoffice nicht. Wer Unterlagen aus dem regulären Büro mit nach Hause nimmt, ist für sie verantwortlich. Ein eigenes Zimmer für das Homeoffice bleibt für viele ein Traum. Aber mit der Aufbewahrung in einem abgeschlossenen Schrank/Rollschrank ist auch schon viel gewonnen.

Altpapier datenschutzkonform beseitigen!

Wo Papier benutzt wird, fällt auch Abfallpapier an. Vielleicht haben Sie ohnehin privat einen kleinen Aktenvernichter im Haus. Egal, ob er nun den Vorgaben für Bürogeräte voll entspricht – es ist besser als nichts. Keinesfalls dürfen Sie Abfallpapier mit personenbezogenen Daten „einfach so“ in die heimische Papiertonne stecken.

Corona als Auslöser von Kreativität?

Vielleicht bietet das Homeoffice aber auch einen guten Anlass dazu, von Abläufen mit Papier auf elektronische Abläufe umzustellen. Das geht erstaunlich oft. Corona kann auch kreativ machen!

comdatis
it-consulting

Videosprechstunden – ein Datenschutzrisiko?

Lange gab es sie höchstens als Nische für einige Privatpatienten: Videosprechstunden im Internet. Jetzt bieten plötzlich relativ viele Ärzte solche Sprechstunden an. Woran liegt das? Bleibt dabei vielleicht der Datenschutz auf der Strecke?

In Deutschland bisher ein reines Nischenangebot

Da und dort gab es Videosprechstunden im Internet auch schon bisher. Zielgruppe waren durchweg jüngere Privatpatienten. Anbieter waren meist Ärzte mit einer Praxis im europäischen Ausland, etwa in Großbritannien. In Deutschland waren weite Teile der Ärzteschaft skeptisch. Hier galt die eiserne Regel: Die Behandlung eines Patienten setzt voraus, dass der Arzt ihn persönlich vor sich hat. Ausnahmen waren selten.

Im Ausland teilweise stärker üblich

Im Ausland handhabte man das zum Teil schon bisher anders. Selbstverständlich geht auch dort nicht alles über das Internet. Aber vieles eben doch. Das allein wäre aber noch kein Grund für eine Änderung in Deutschland gewesen. Denn eine ernsthafte Konkurrenz für die hiesige Ärzteschaft waren diese Videosprechstunden aus dem Ausland nicht.

Corona als Mit-Auslöser

Eine Triebfeder für Veränderungen war Corona. Zumindest für eine Corona-Verdachtsdiagnose ist es oft nicht nötig, den Patienten zu sehen. Der Arzt schickt ihn zum Abstrich und sieht danach weiter. Das kann auch über Video geschehen. Ähnliche Beispiele gibt es in den meisten medizinischen Fachrichtungen.

Abrechnung jetzt auch bei Kassenpatienten möglich

Hinzu kommt, dass sich ein „Praxisbesuch per Video“ inzwischen bei den Krankenkassen abrechnen lässt. Der Spitzenverband der Gesetzlichen Krankenversicherung und die Kassenärztliche Bundesvereinigung haben vor Kurzem eine „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde“ abgeschlossen. Sie legt fest, was ein Arzt beachten muss, damit eine Abrechnung möglich ist.

Hohe Vorgaben für den Datenschutz

Zu den Anforderungen, die ein Arzt erfüllen muss, gehören genaue Vorgaben für den Datenschutz. Die Vereinbarung legt technische Spezifikationen fest, die einzuhalten sind, beispielsweise eine angemessene Verschlüsselung. Ohne sie könnte es zu einer Verletzung der ärztlichen Schweigepflicht kommen. Das können Ärzte nicht riskieren. Solche Verletzungen können eine Straftat darstellen und haben auch standesrechtliche Folgen.

Nur zertifizierte Systeme zulässig

Eine Videosprechstunde über Zoom oder ähnliche im Internet allgemein angebotene Systeme, die im Büroalltag häufig sind, ist ausgeschlossen. Zum Einsatz kommen dürfen nur Systeme von Anbietern, die eine besondere Zertifizierung durchlaufen haben. Sie sind in einer Liste bei der Kassenärztlichen

Bundesvereinigung eingetragen.

Keine Registrierung für Patientinnen und Patienten

Wichtig für alle Patientinnen und Patienten: Sie müssen sich vor der Benutzung eines solchen Systems nirgendwo registrieren lassen! Für den Arzt ist das anders. Er muss eine Registrierung beim Systemanbieter durchlaufen. Das verhindert, dass sich zwielichtige Gestalten als Ärzte ausgeben.

Videosprechstunde nur nach Terminvereinbarung

Patientinnen und Patienten, die einen Video-Termin haben wollen, müssen ihn vorher mit der Praxis vereinbaren. Dies kann etwa telefonisch geschehen oder über ein Tool zur Terminreservierung im Internet. Der Zugang zur Sprechstunde erfolgt mit einem Zugangscode, den der Arzt rechtzeitig vor dem Termin übermittelt. Es liegt in der eigenen Verantwortung des Patienten, mit diesem Zugangscode sorgfältig umzugehen. Das gilt insbesondere dann, wenn die Sprechstunde bei einem Arzt vereinbart wird, der den Patienten noch nicht persönlich kennt.

Kaum Schwachstellen für die Vertraulichkeit in der Arztpraxis

Denkbare Schwachstellen für die Vertraulichkeit liegen in der Umgebung beim Arzt oder beim Patienten, die auf dem Bildschirm nicht sichtbar ist. Beim Arzt kann man davon ausgehen, dass nicht noch andere Personen in der Praxis heimlich mithören oder mitsehen. Das wäre eine schwere Verletzung der ärztlichen Schweigepflicht.

Schwachstellen in der Wohnung des Patienten

In der heimischen Umgebung des Patienten kann es schlechter aussehen. Wer sich für eine Videosprechstunde nicht allein in einen Raum zurückziehen kann, sollte möglicherweise die Finger davon lassen. Und eine andere Person heimlich mithören zu lassen, mag zwar keine Straftat sein. Fair gegenüber dem Arzt ist es aber sicher nicht.

Ein Angebot, kein Zwang!

Beachtet man die geschilderten Sicherheitsmaßnahmen, steht nichts dagegen, eine Videosprechstunde einmal auszuprobieren. Es ist ein zusätzliches Angebot, für Kassen- wie für Privatpatienten, nicht mehr und nicht weniger.

Office 365: Was sagt der Datenschutz?

Wer einen Cloud-Dienst nutzen will, muss sich über die Folgen für den Datenschutz klar sein. Im Fall von Office 365 ist das nicht einfach und damit umso wichtiger. Die Aufsichtsbehörden für den Datenschutz haben weitere Untersuchungen angekündigt.

Rechtsunsicherheit bei Office aus der Cloud

Immer mehr Unternehmen aus Deutschland setzen Cloud-Dienste ein. Drei von vier Unternehmen nutzten im Jahr 2019 Rechenleistungen aus der Cloud, im Vorjahr waren es 73 Prozent und im Jahr 2017 erst 66 Prozent, so der Cloud-Monitor 2020 des Digitalverbands Bitkom.

Gegen die Verwendung von Cloud-Services spricht, dass es zu unerlaubten Datenzugriffen in der Cloud kommen könnte. Außerdem besteht eine gewisse Rechtsunsicherheit, von der 60 Prozent der Unternehmen berichten, die sich bisher gegen Cloud-Lösungen entschieden haben.

Diese Unsicherheit hinsichtlich der Rechtslage erstreckt sich auch auf so beliebte Dienste wie Office-Lösungen aus der Cloud. Hier ist insbesondere Microsoft Office 365 zu nennen. Selbst Aufsichtsbehörden für den Datenschutz machen deutlich, dass es zum Datenschutz bei Office 365 Unklarheiten gibt. So lautete das Fazit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen im Juli 2019: Microsoft Office 365 an Schulen einzusetzen, ist datenschutzrechtlich unzulässig, soweit Schulen personenbezogene Daten in der europäischen Cloud speichern.

In einer zweiten Stellungnahme im August 2019 erklärte die Aufsichtsbehörde dann: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat sich nach den Gesprächen mit Microsoft dazu entschlossen, den Einsatz von Office 365 in hessischen Schulen unter bestimmten Voraussetzungen und dem Vorbehalt weiterer Prüfungen vorläufig zu dulden.

Auch im Jahr 2020 sind die Fragen zum Datenschutz bei Office 365 nicht eindeutig geklärt. Die Aufsichtsbehörden in den Bundesländern haben dazu noch keine vollständig einheitliche Linie gefunden. Doch was bedeutet das für Unternehmen und für Nutzer?

Erhebliche Verbesserungen bei Office 365 notwendig

Natürlich sollte es Unternehmen und Nutzer aufhorchen lassen, wenn sich die Aufsichtsbehörden für den Datenschutz so ausführlich und detailliert mit den Datenschutzfragen eines bestimmten Cloud-Dienstes befassen. Einerseits ist dies der hohen Verbreitung von Office 365 geschuldet, die die Relevanz der Datenschutzfragen erhöht. Andererseits gibt es nach Ansicht aller Aufsichtsbehörden für den Datenschutz in Deutschland ein „erhebliches datenschutzrechtliches Verbesserungspotenzial“ bei Office 365.

Die Nutzungsbedingungen von Microsoft machen demnach nicht ausreichend klar, welche nutzerbezogenen Daten Microsoft wie verarbeitet. Die Aufzeichnung und Nutzung der von Microsoft erhobenen Telemetriedaten weist Unklarheiten auf. Es ist für die Datenschützer unklar, ob Microsoft Nutzerdaten ausreichend schützt und wie lange es diese Daten speichert. Die Weitergabe von Nutzerdaten an Unterauftragnehmer ist nicht ausreichend geregelt.

Die Aufsichtsbehörden haben deshalb beschlossen, eine Arbeitsgruppe einzurichten, die Gespräche mit Microsoft aufnehmen soll, um zeitnah datenschutzgerechte Nachbesserungen zu erreichen. Unternehmen und Nutzer tun also gut daran, die Nutzungsbedingungen und die Datenschutzerklärung zu Office 365 im Auge zu behalten. Die Aufsichtsbehörden für den Datenschutz fordern hier viele Anpassungen und Klarstellungen, damit der Datenschutz-Grundverordnung (DSGVO) der EU Genüge getan wird.

Mit der Cloud kann sich vieles ändern

Office 365 ist ein wichtiges und gutes Beispiel, warum der Wechsel hin zu einem Cloud-Dienst nicht leichtfertig geschehen sollte, sondern Prüfungen vorab und auch während der Nutzungsphase nach sich ziehen muss. Denn der Datenschutz lässt sich nicht einfach als gewährleistet annehmen.

Die früher lokal installierten Office-Programme und eine Office-Lösung aus der Cloud mögen ähnliche oder die gleichen Funktionen haben. Für den Datenschutz jedoch und für die Nutzerdaten bedeutet es einen großen Unterschied, ob eine Anwendung lokal oder über eine Cloud genutzt wird.

Die DSGVO verlangt, dass Unternehmen nur solche Cloud-Anbieter beauftragen, die ausreichende Garantien bieten, dass sie den Datenschutz nach DSGVO einhalten. Dies zu überprüfen, muss vor der Entscheidung für einen Cloud-Dienst geschehen. Und da sich Cloud-Dienste schnell in Funktionen und Nutzungsbedingungen verändern können, muss eine solche Prüfung auch während der Nutzung stattfinden.

Der Weg in die Cloud scheint einfach und bequem zu sein. Ein Webbrowser kann schon ausreichen. Doch die Folgen für den Datenschutz zu prüfen, ist komplex und nicht zu vernachlässigen. Das sollten Unternehmen beim Für und Wider von Cloud Computing stärker bedenken als bisher.

Es tut sich etwas

Aktuelle Pressemeldungen aus November 2020 deuten darauf hin, dass sich die Aufsichtsbehörden und Microsoft annähern. Nachfolgend ein Verweis auf die aktuellen Pressemeldungen:

Nachfolgende Pressemeldung von Microsoft mit der Ankündigung weiterer Maßnahmen vom 20.11.2020:
https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/

Microsoft steht außerdem bereits in Kontakt mit Datenschutzaufsichtsbehörden in Deutschland, wie aus einer Pressemeldung zu entnehmen ist: #DSGVOwirkt: Microsoft passt sich europäischem Datenschutz an | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

---

Mit Cookie-Bannern richtig umgehen

Kaum ein Internetnutzer kennt sie nicht, die sogenannten Cookie-Banner. Was jedoch weniger bekannt ist: wie wichtig diese scheinbar lästigen Banner für den Datenschutz im Internet sind. Einfach zustimmen, ohne zu lesen, ist deshalb nicht richtig.

Cookie-Banner werfen Fragen auf

Viele Internetnutzer und Betreiber von Webseiten sind genervt, berichtet der Digitalverband Bitkom. Betreiber von Webseiten müssen Prozesse und Formulare für ihre Webangebote einführen, um Cookies auch künftig nutzen zu dürfen. Der Grund: Webseitenanbieter dürfen alle Cookies, die als nicht unbedingt erforderlich gelten, nur mit aktiver Einwilligung setzen.

Für die Internetnutzer bedeutet das: Auf Webseiten erscheinen immer mehr Cookie-Banner, die Nutzerinnen und Nutzer können dort die Einwilligung zu Cookie-Einsätzen geben oder verweigern. Bei den Aufsichtsbehörden für den Datenschutz sind verstärkt Nachfragen von Bürgerinnen und Bürgern eingegangen, was es mit den Cookie-Bannern auf sich hat und wie sie sich verhalten sollen.

Cookie-Banner müssen nicht immer sein

Der Landesdatenschutzbeauftragte Rheinland-Pfalz, Professor Dieter Kugelmann, erklärte dazu: „Der Bundesgerichtshof (BGH) hat in einem Urteil klargestellt, dass für Cookies, die nicht zur Bereitstellung der Webseite oder App erforderlich sind, in jedem Fall eine aktive Einwilligung der Webseitenbesucher erforderlich ist.“

Für den Nutzer hat dies Datenschutz-Vorteile: Jede Nutzerin und jeder Nutzer kann nun erfahren, welche Informationen zur Nutzung der Anbieter erheben möchte. Jede und jeder kann in diese Datensammlung einwilligen oder sie ablehnen. Damit können Internetnutzer selbst entscheiden, welche Daten

Webseitenbetreiber über sie verarbeiten.

Für technisch notwendige Cookies müssen die Anbieter die Nutzer nicht um ihre ausdrückliche Erlaubnis fragen. Das können Cookies sein, die dafür sorgen, dass bei einem Online-Shop der Warenkorb dem Nutzer zugeordnet bleibt, während er weiter einkauft oder später den Einkauf fortsetzt. Andere Cookies dürfen nur eingesetzt werden, wenn eine sogenannte „informierte Einwilligung“ des Nutzers vorliegt. Ist dem nicht so und es erfolgt der Cookie-Einsatz ohne wirksame Einwilligung, ist die Datenverarbeitung rechtswidrig. Dann können die Datenschutz-Aufsichtsbehörden sie untersagen und mit Geldbußen ahnden.

Cookie-Banner ernst nehmen

Stören Sie sich als Internetnutzer also nicht an den Cookie-Bannern, sondern sehen Sie die Transparenz und die Wahlfreiheit positiv. Allerdings gibt es auch Cookie-Banner, die mehr versprechen, als sie halten. So dürfen die Webseitenbetreiber Cookies erst setzen, wenn der Nutzer seine Einwilligung erteilt hat, weder vorher noch ohne Einwilligung. Tatsächlich aber gibt es noch viele Cookie-Banner, die um Erlaubnis fragen, aber die Entscheidung nicht abwarten oder respektieren.

Die Datenschützer führen entsprechende Überprüfungen bei Webseiten durch, um die Privatsphäre der Internetnutzer zu schützen. Gehen Sie deshalb als Internetnutzer bewusst mit den Cookie-Bannern um. „Ein paar Klicks mehr, aber auch viel mehr Selbstbestimmung. Die informationelle Selbstbestimmung ist ein wichtiges Recht: Jede und jeder soll selbst darüber entscheiden können, welche personenbezogenen Daten er von sich preisgeben möchte und wer sie verwenden darf“, so der Hinweis von Prof. Kugelmann, den man sich als Internetnutzer zu Herzen nehmen sollte.

Nutzen Sie die Cookie-Banner zu Ihrem Vorteil? Machen Sie den Test!

Frage: Cookie-Banner sind ein Hindernis beim Online-Shopping. Stimmt das?

1. Nein, denn wenn Cookies für die Warenkorb-Funktion nötig sind, braucht es keine Cookie-Banner.
2. Ja, wer nicht zustimmt, kann nicht mehr im Online-Shop einkaufen.

Lösung: Die Antwort 1. ist richtig. Cookies, die funktional benötigt werden, wie beim Warenkorb in einem Online-Shop, bedürfen nicht der Einwilligung. Wohl aber solche, die ein Online-Shop einsetzen möchte, um ein Nutzerprofil zum Surfverhalten des Kunden oder der Kundin anzulegen. Überlegen Sie hier als Nutzer genau, ob Sie das möchten oder nicht.

Frage: Cookie-Banner verhindern jedes Online-Tracking. Stimmt das?

1. Ja, wo die Banner auftauchen, gibt es kein Nachverfolgen der Nutzeraktivitäten.
2. Nein, teilweise fehlen die Cookie-Banner für Tracking-Cookies, teilweise funktionieren die Banner auch nicht richtig.

Lösung: Die Antwort 2. ist richtig. Es gibt bereits viele Cookie-Banner, aber nicht alle sind vollständig in den Informationen. Teilweise werden auch Cookies bereits gesetzt, bevor man einwilligt oder obwohl man widerspricht. Das macht Cookie-Banner aber nicht überflüssig, sondern es zeigt, wie wichtig richtig umgesetzte Cookie-Banner sind und wie wichtig der bewusste Umgang mit ihnen ist. Einfach immer zuzustimmen, sollte auch im Internet nicht zur täglichen Praxis gehören, der Datenschutz im Internet ist entscheidend. Nutzen Sie Ihre Wahlfreiheit und informieren Sie sich über die geplante Datenverarbeitung. Es geht um die eigene Privatsphäre, die unter heimlichem Online-Tracking leiden kann.

comdatis
it-consulting

Impressum

Redaktion: Markus Olbring

Anschrift:

comdatis it-consulting GmbH & Co.KG

Deventer Weg 8, 48683 Ahaus-Alstätte

Telefon: 02567/82900-00

E-Mail: info@comdatis.de

Datenschutzinformationen: https://www.comdatis.de/agb.html

Rechtliche Informationen: https://www.comdatis.de/impressum.html