SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

Daten stehen im Fokus – in der Wirtschaft für neue Geschäftsmodelle, in der Werbung für die Personalisierung, aber auch bei den Kriminellen. Dabei sind insbesondere personenbezogene Daten begehrt, denn diese Daten betreffen uns Menschen.
In Ihrer neuen Ausgabe finden Sie aktuelle Hinweise zu den Motiven der Internetkriminalität, zum richtigen Umgang mit Fotos, die Personen zeigen, und zu den Verhaltensregeln, die Sie beachten sollten, wenn es zu einer Datenpanne kommt.
Ebenso befasst sich diese Ausgabe mit den oftmals ungeliebten Cookie-Bannern. Denn wenn Anbieter von Websites sie richtig machen und nutzen, helfen sie dabei, dass Sie die Kontrolle über Ihre Daten behalten, wenn Sie Websites besuchen. Dann haben auch Sie Ihre Daten im Fokus.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

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

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Dezember_2023

1 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 zuzustimmen, ohne zu lesen, ist deshalb nicht richtig.

Cookie-Banner werfen Fragen auf

Viele Internetnutzer und Betreibende von Webseiten sind genervt, berichtet der Digitalverband Bitkom. Betreiber von Webseiten müssen Prozesse und Formulare für ihre Webangebote einführen, um Cookies nutzen zu dürfen. Der Grund: Webseitenanbieter dürfen alle Cookies, die als nicht unbedingt erforderlich gelten, nur mit aktiver Einwilligung setzen, so will es das TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz).

Für die Internetnutzenden 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 gehen Nachfragen von Bürgerinnen und Bürgern ein, was es mit den Cookie-Bannern auf sich hat und wie sie sich verhalten sollen.

Nutzen Sie die Cookie-Banner zu Ihrem Vorteil?

Die Lösungen finden Sie am Ende des Beitrags.

Frage 1: 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.

Frage 2: 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.

Cookie-Banner müssen nicht immer sein

Nicht jeder Einsatz von Cookies ist einwilligungsbedürftig, so die deutschen Datenschutz-Aufsichtsbehörden. Der Bundesgerichtshof (BGH) hatte in einem Urteil klargestellt, dass nur für Cookies, die nicht zur Bereitstellung der Webseite oder App erforderlich sind, eine aktive Einwilligung der Webseitenbesucher erforderlich ist.

Für die Nutzerinnen und Nutzer hat dies Datenschutz-Vorteile: Jeder 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 der Cookie-Einsatz erfolgt 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 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. Diese Banner sind letztlich Teil Ihrer informationellen Selbstbestimmung. Jede und jeder soll selbst darüber entscheiden können, welche personenbezogenen Daten er oder sie von sich preisgeben möchte und wer sie verwenden darf.

Und hier die Lösungen für die Quizfragen:
Lösung Frage 1: 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 oder Nutzerin genau, ob Sie das möchten oder nicht.

Lösung Frage 2: Die Antwort 2. ist richtig. Es gibt bereits viele Cookie-Banner, aber nicht alle sind vollständig in den Informationen. Teilweise werden auch Cookies 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.

2 BILDER UND DATENSCHUTZ

Spezielle Regelungen zum Umgang mit Bildern von Personen enthält die DSGVO zwar nicht. Dennoch bietet sie Lösungen für die wesentlichen Fragen rund um dieses Thema.

Ein spektakulärer Fall: Erinnerungsfotos im Kindergarten

Kurz nachdem die Datenschutz-Grundverordnung (DSGVO) ab 25. Mai 2018 galt, machte ein Kindergarten Erinnerungsfotos mit allen Kindern, die in die Grundschule wechselten. Doch die Freude von Kindern und Eltern über die Fotos war deutlich getrübt. Denn die Gesichter der Kinder waren entweder verpixelt oder mit schwarzen Balken über den Augen versehen. Die Begründung des Kindergartens: Die DSGVO verlangt das leider so!

Diese Aussage war Unfug. Dass die Kinder fotografiert werden, war angekündigt und die Eltern waren damit ersichtlich einverstanden. Zudem wurden die Bilder nur den beteiligten Kindern und Eltern ausgehändigt. Also im Ergebnis alles kein Problem. Der Fall zeigt jedoch deutlich, wie groß die Unsicherheit beim Thema „Bilder und DSGVO“ manchmal sein kann. Dabei besteht dazu keinerlei Anlass.

Keine Spezialregelungen in der DSGVO

Wer den Text der DSGVO zur Hand nimmt, erlebt eine Überraschung: Für Abbildungen von Personen finden sich keinerlei spezielle Regelungen! Allerdings gilt natürlich: Wenn Personen auf einem Bild zu identifizieren sind, dann enthält dieses Bild personenbezogene Daten. Dies hat der Europäische Gerichtshof so formuliert: „Das von einer Kamera aufgezeichnete Bild einer Person fällt unter den Begriff der personenbezogenen Daten.“

Rein private Fotografien

Vom Prinzip her ist die DSGVO somit auf Abbildungen von Personen anwendbar. Freilich gibt es davon eine wichtige Ausnahme: Sie betrifft den Fall, dass Bilder im rein persönlichen oder rein familiären Rahmen entstehen. Wer also seine Kinder am Strand fotografiert oder seine Freundin neben dem Weihnachtsbaum, muss sich dabei nicht um Vorgaben der DSGVO kümmern. Für solche „ausschließlich persönliche[n] oder familiäre[n] Tätigkeiten“ gilt die DSGVO nicht (siehe Art. 2 Abs. 2 Buchst. d DSGVO).

Kommerzielle Verwendung von Fotografien

Anders sieht es aus, wenn privat entstandene Bilder kommerziell verwendet werden. Klassisches Beispiel: Ein Mann betreibt einen Ponyhof. Er fotografiert seine elfjährige Tochter auf einem Pony. Solange er dieses Bild im privaten Bereich belässt, findet die DSGVO keine Anwendung. Stellt er das Bild dagegen auf die Homepage des Ponyhofs, hat er den rein privaten Bereich verlassen und die DSGVO ist anwendbar.

Der Fall hat sich tatsächlich so ereignet. Die Eltern des Kindes lebten getrennt, hatten aber die gemein-same elterliche Sorge. Die Mutter hatte etwas dagegen, dass die Tochter auf der Homepage erscheint. Sie konnte einen entsprechenden Unterlassungsanspruch durchsetzen. Das lag vor allem daran, dass sie als Mit-Sorgeberechtigte übergangen worden war.

Das Bild im Zutrittsausweis

In einem Industriebetrieb wird für jeden Beschäftigten ein Zutrittsausweis mit Bild ausgestellt. Das soll sicherstellen, dass sich Unbefugte keinen Zutritt zum Gelände verschaffen

können. Das Anfertigen eines Bildes und seine Anbringung im Ausweis sind in diesem Fall erforderlich, um das Arbeitsverhältnis ordnungsgemäß durchführen zu können. Damit ist dieses Vorgehen erlaubt. Schützenswerte Interessen der Beschäftigten beeinträchtigt das nicht. Denn die Zutrittsausweise bleiben in der Hand der Beschäftigten.

Gruppenfotos von Arbeitsjubilaren

Gruppenfotos von Arbeitsjubilaren sind zur Durchführung des Beschäftigungsverhältnisses nicht erforderlich. Daher ist die Einwilligung jedes einzelnen nötig, der auf dem Foto zu sehen sein soll. Diese Einwilligung bedarf sogar der Schriftform, wenn nicht ganz besondere Umstände vorliegen (§ 26 Abs. 2 Satz 3 Bundesdatenschutzgesetz). Der deutsche Gesetzgeber hat damit für Einwilligungen im Arbeitsleben eine Schriftform eingeführt, die in der DSGVO nicht vorgesehen ist. Er durfte dies tun, weil die DSGVO solche ergänzenden Regelungen der Mitgliedstaaten erlaubt.

Einwilligungslisten

Einen großen Vorteil hat die Schriftform: Es ist klar dokumentiert, wer einverstanden ist. Dabei ist es übrigens kein Problem, wenn eine Liste verwendet wird, auf der alle unterschreiben. Oben auf der Liste muss lediglich stehen, um was es geht. Dazu gehören vor allem der Anlass („Fotos von Arbeitsjubilaren") und Angaben dazu, wo die Bilder veröffentlicht werden sollen (Beispiel: „In der Firmenzeitschrift und im Firmennetz“).

Eines zeigen alle Beispiele sehr deutlich: Wer mit gesundem Menschenverstand vorgeht, wird bei Bildern kaum in Konflikt mit der DSGVO geraten.

3 SPIELREGELN FÜR DEN UMGANG MIT DATENPANNEN

Eine Verletzung des Datenschutzes „beichten“ zu müssen, ist immer unangenehm. Jeder weiß, dass es Folgen haben kann, im schlimmsten Fall auch arbeitsrechtliche. Deshalb schweigen manche lieber. Doch Vorsicht! Das Verschweigen einer Datenpanne kann alles noch viel schlimmer machen.

Der verschwundene Laptop

Ein Laptop mit Kundendaten ist weg. Wahrscheinlich blieb er vor ein paar Tagen schlicht im Zug liegen. Das Gerät ist schon fünf Jahre alt und wurde nur noch ausnahmsweise benutzt. Also vermisst es niemand wirklich. Und die Kundendaten sind im EDV-System natürlich noch vorhanden. Da wird auch keiner misstrauisch. Also lieber mal einfach nichts sagen nach dem Motto „wird schon gut gehen“? Das ist keine gute Idee.

Meldepflicht gegenüber der Datenschutzaufsicht

Unternehmen müssen jede „Verletzung des Schutzes personenbezogener Daten“ der Datenschutzaufsicht melden. So regelt es Art. 33 DSGVO. Diese Meldepflicht ist in keiner Weise eingeschränkt. Das bedeutet: Der Verlust eines Laptops mit personenbezogenen Daten muss der Aufsicht in jedem Fall gemeldet werden. Dies gilt auch dann, wenn die Daten verschlüsselt waren. Das hat seinen Sinn. Denn wer weiß, ob die Verschlüsselung wirklich so gut ist, wie alle im Unternehmen glauben? Die Datenschutzaufsicht sieht das möglicherweise ganz anders.

Sehr knappe Meldefrist von 72 Stunden

Das Brisante dabei: Bei der Meldung an die Datenschutzaufsicht ist eine Frist von 72 Stunden

zu beachten. Wird sie grundlos überschritten, droht dem Unternehmen schon deshalb ein Bußgeld. Ausreden von der Art „Unser Mitarbeiter hat uns die Panne intern nicht verraten“ gelten dabei nicht. Die Antwort darauf wäre: „Dann bringen Sie Ihren Mitarbeitern eben bei, dass Datenpannen gleich zu melden sind.“ Wird die Frist versäumt, kann die Aufsicht gegen das Unternehmen eine Geldbuße verhängen.

Online-Formulare für die Meldung einer Schutzverletzung

Alle Aufsichtsbehörden stellen auf ihren Homepages Online-Formulare zur Verfügung, mit denen Unternehmen Schutzverletzungen melden können. Das hat sich bewährt und hilft vor allem auch dabei, die kurze Meldefrist von 72 Stunden zuverlässig einzuhalten. Solche Meldungen sind keine gesetzliche Aufgabe der betrieblichen Datenschutzbeauftragten. Nur wenn ihnen diese Aufgabe besonders zugewiesen wurde, müssen sie sich darum kümmern.

Ausnahme: Benachrichtigung der Betroffenen

Ob den betroffenen Personen, um deren Daten es geht, „etwas passieren“ kann, spielt bei der Meldepflicht gegenüber der Aufsichtsbehörde keine Rolle. Dieser Aspekt wird erst wichtig, wenn es um die Benachrichtigung der Betroffenen geht. Diese Benachrichtigung ist in der DSGVO gesondert geregelt (Art. 34 DSGVO). Demnach müssen Betroffenen nur dann benachrichtigt werden, wenn ihnen „voraussichtlich ein hohes Risiko droht“. Hier gilt also ein völlig anderer Maßstab als bei der Benachrichtigung der Aufsichtsbehörde.

Am Beispiel des verschlüsselten Laptops wird wieder deutlich, was das bedeutet: Sind die Daten auf dem Laptop nach dem Stand der Technik verschlüsselt, droht kein hohes Risiko, wenn er Unbefugten in die Hände gerät. Die Folge: Die Betroffenen müssen nicht benachrichtigt werden. Daten auf mobilen Datenträgern zu verschlüsseln, „lohnt“ sich also für Unternehmen! Es erspart ihnen im Ernstfall die Benachrichtigung der Betroffenen.

Die Spielregeln der DSGVO im Überblick

Die Spielregeln für den Umgang mit Datenpannen lassen sich so zusammenfassen:

- Jeder Mitarbeiter, dem eine Datenpanne unterläuft, muss möglichst sofort seine Vorgesetzten einschalten.
- Nur so lässt sich vermeiden, dass dem Unternehmen ein teures Bußgeldverfahren droht.
- Meldungen von Unternehmen an die Datenschutzaufsicht müssen bei Datenpannen ausnahmslos erfolgen.
- Für diese Meldungen gilt eine Frist von 72 Stunden! Sie lässt sich nur einhalten, wenn jeder Mitarbeiter Pannen sofort intern meldet. Sonntage und Feiertage verlängern sie nicht.
- Eine Meldung an die Datenschutzaufsicht hat für sich allein noch keine negativen Konsequenzen. Es kann aber natürlich vorkommen, dass die Datenschutzaufsicht nachfragt, was eigentlich genau passiert ist.
- Eine Meldung an die Datenschutzaufsicht führt nicht automatisch dazu, dass die Betroffenen über die Datenpanne benachrichtigt werden.
- Eine solche Benachrichtigung der Betroffenen ist an enge Voraussetzungen geknüpft.
- Die Benachrichtigung der Betroffenen lässt sich in der Regel vermeiden, wenn die Daten verschlüsselt sind.

4 DAS SIND DIE ZIELE DER CYBERKRIMINELLEN: IHRE DATEN!

Cyberkriminalität nimmt immer bedrohlichere Ausmaße an. Straftaten im Bereich Cyber-crime liegen in Deutschland auf einem sehr hohen Niveau, so das Bundeskriminalamt (BKA). Wer sich besser schützen will, muss die Ziele der Internetkriminellen kennen.

Das Internet wird immer häufiger zu Tatmittel und Tatort

Die Polizeiliche Kriminalstatistik (PKS) zeigt deutlich: Ein Bereich, bei dem seit Jahren kontinuierlich Anstiege zu verzeichnen sind, ist die Cyberkriminalität. Cybercrime ist eine Bedrohung für Wirtschaft und Gesellschaft, so der Digitalverband Bitkom, Partner des BKA. Unternehmen und Behörden sind gleichermaßen gefordert, mehr gegen Cyberkriminalität zu tun.

Cyberangriffe sind meistens finanziell motiviert

Während man früher davon ausging, dass viele Online-Attacken deshalb stattfinden, weil die Angreifen-den ihr Hacking-Können ausprobieren und zeigen wollen, ist man sich heute sicher, dass die Motive hinter den Attacken meistens finanzieller Natur sind: Man will Kontobestände räumen, Kryptowährungen stehlen oder führt gegen Bezahlung eine kriminelle Auftragsarbeit aus, einen Spionage-Auftrag oder einen Angriff auf den Wettbewerber des „Kunden“.

Auch wenn es letztlich meist um Geld geht, sind die Ziele der Internetkriminellen zuerst und insbesondere Daten. Denn Daten sind wertvoll und können etwa Zugang zu Bankkonten verschaffen oder bieten Einblicke in Geschäftsgeheimnisse. Erfolgreiche Cyberangriffe bedeuten deshalb auch, dass der Datenschutz leider nicht ausgereicht hat.

Datenschützer warnen vor Internetkriminalität

In Zeiten der fortschreitenden Digitalisierung und der um sich greifenden Cyberkriminalität wird damit der Schutz personenbezogener Daten noch wichtiger. Die Gefahr von Cyberangriffen wächst, warnt zum Beispiel die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Angreifenden sind zunehmend professionell organisiert und in der Lage, Sicherheitslücken schnell zu nutzen. Sie verfügen über Werkzeuge, um Schwachstellen der Systeme zu identifizieren. Auch Betrugs- und Phishing-Maschen sind deutlich professioneller geworden.

Viele Unternehmen und Internetnutzende fürchten Cyberangriffe und Cybercrime.

Furcht vor Cyberattacken allein schützt nicht

Zweifellos ist es gut, wenn man bei der Nutzung des Internets nicht sorglos ist und sich Gedanken macht, was passieren könnte. Allerdings sollte man sich deutlich machen, auf was es die Internetkriminellen abgesehen haben: auf die personenbezogenen Daten.

Datenschutz ist deshalb auch ein zentraler Schutz vor Internetkriminalität und wird mit der digitalen Transformation nicht etwa zum Hindernis. Datenschutz ist im Gegenteil zwingend erforderlich, um den Cyberkriminellen so viel Gegenwehr wie nur möglich zu bieten.

Wissen Sie, was Cyberkriminelle wollen?

Machen Sie den Test!

Internetkriminelle interessiert das Geld und nicht die Daten. Die Daten will nur die Werbewirtschaft. Stimmt das?

1. Nein, die Cyberkriminellen haben finanzielle Motive. Aber um an Geld zu kommen, missbrauchen und verkaufen sie Daten.
2. Ja, Datenschutz hat nichts mit dem Schutz vor Cyberkriminalität zu tun.

Lösung:

Die Antwort 1. ist richtig. Das Hauptziel jeder Cyberattacke sind Daten, und die meisten dieser Daten haben Personenbezug. In 62 Prozent der Unternehmen, in denen zuletzt sensible digitale Daten gestohlen wurden, handelte es sich laut Bitkom um Kommunikationsdaten (Bericht Wirtschaftsschutz 2023). Diese Daten aber enthalten in aller Regel personenbezogene Informationen.

Gegen Internetkriminelle sind wir machtlos. Das Internet ist eben gefährlich. Ist das so richtig?

1. Ja, gegen Cyberattacken kann man letztlich nichts machen.
2. Nein, wenn man die Daten schützt, kann es zwar zu Cyberangriffen kommen, aber die Angreifenden können keine Daten erbeuten.

Lösung:

Die Antwort 2. ist richtig. Es gibt zwar keinen hundertprozentigen Schutz vor Internetkriminellen, man muss davon ausgehen, dass es zu erfolgreichen Cyberangriffen kommt. Doch das Ziel der Angriffe, die Daten, lassen sich weitaus besser schützen, als dies heute noch geschieht. Sind die Daten zum Beispiel stark verschlüsselt, kann ein Internetkrimineller sie zwar stehlen, aber nichts damit anfangen.

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