#59 Cookies, DSGVO und Cyberkriminalität

Herzlich willkommen beim Rechtsschutz Podcast!

In dieser Folge widmen wir uns Themen wie Cookies, DSGVO und Cyberkriminalität

Dabei gehen wir unter anderem auf diese Schwerpunkte ein:

Gleich zu Beginn das Thema der Woche:

Cookies – Was muss ich als Websitebetreiber beachten?

Bei den FAQs rund um's Recht geht es um das Thema:

Datenschutzgrundverordnung – Wie kam es überhaupt dazu?

Im Rechts- Lexikon sind wir beim Buchstaben „C" wie Cyberkriminalität

Das Thema der Woche: Cookies – was muss ich als Websitebetreiber beachten?

Die Mehrheit der österreichischen Unternehmen betreibt mittlerweile eine Website. Dabei ist es für Unternehmen oft relevant zu erfahren, wie der Besucher so tickt. Und vor allem wie der eigene Service oder das Produkt ankommt.

Dafür gibt es verschiedene automatisierte Analysedienste. So können zum Beispiel der Standort, die Verweildauer oder das Geschlecht identifiziert werden. Der Besucher klickt dafür nur auf den „Cookie-Banner" und schon geht es mit der Analyse los! Aber ist das überhaupt erlaubt? Gibt es da möglicherweise Stolpersteine für Unternehmen?

Wir haben uns die Fragen eines Kunden genauer angeschaut und beantworten diese hier in unserem Rechtsschutz-Podcast für Sie:

Frage 1: Ich habe gestern von einem Kunden ein Abmahnschreiben erhalten. Ich nutze das Produkt Google Analytics und angeblich ist dieses Rechtswidrig, weil gegen die DSGVO verstoßen wird. Es droht eine Meldung bei der Datenschutzbehörde. Was soll ich davon halten?

Tatsächlich gibt es solche Abmahnschreiben und sie sind auch ernst zu nehmen. Ursprünglich ging die Initiative von dem Österreicher Max Schrems und seiner Datenschutzorganisation – dem Verein NOYB – aus. Er hat beim Europäischen Gerichtshof einige Datenschutzklagen gegen diverse Großkonzerne, wie Facebook, eingebracht.

Das Ergebnisse: der Europäische Gerichtshof meint, dass bei Google Analytics nicht sichergestellt ist, dass der europäische Datenschutz tatsächlich eingehalten wird. Es handelt sich dabei nämlich um ein US-Unternehmen, welches auch Daten nach Amerika transferiert.

Mittlerweile liegt eine erste Musterentscheidung der österreichischen Datenschutzbehörde dazu vor. Es wird wohl langfristig darauf hinauslaufen, dass es einen Gleichklang aller europäischer Datenschutzbehörden in diesem Zusammenhang geben wird. Derzeit besteht auch kein rechtsgültiges Datentransfer-Übereinkommen zwischen der EU und der USA, welches das Tracking erlauben würde.

Frage 2: Was ist der Hintergrund für diese Diskussion?
Es muss hier langfristig eine EU-konforme Websitegestaltung erfolgen. Google Analytics wird von über 80 % der Website-Betreiber in Europa verwendet. Teilweise auch ohne deren Wissen. Eine Möglichkeit ist es, sich weiterzubilden und in andere Softwareangebote zu investieren.

In vielen Fällen wird einem Unternehmen in solch einem Abmahnschreiben nur eine kurze Frist zur Umstellung gewährt. In 60 Tagen muss die Umstellung erfolgen, sonst erfolgt eine Datenschutz-Beschwerde.

Nach den allgemeinen Bestimmungen der DSGVO ist die Verarbeitung von personenbezogenen Daten zwar nicht notwendigerweise von einer Einwilligung abhängig, sondern kann auch mit einem sogenannten „berechtigtem Interesse" verarbeitet werden.

Nach den Bestimmungen des österreichischen Telekommunikationsgesetzes ist allerdings bei Cookies immer eine Einwilligung erforderlich. Nur wenn es sich um technisch notwendige Cookies handelt ist nach dem Telekommunikationsgesetz keine Einwilligung erforderlich. Das sind Cookies, die für die Erbringung der auf der jeweiligen Webseite angebotenen Dienste unbedingt erforderlich sind. Da Tracking-Cookies für die Funktion einer Webseite aber nicht erforderlich sind, ist grundsätzlich eine Einwilligung notwendig. Fraglich ist, welche Art der Einwilligung rechtskonform ist.

Es reicht jedenfalls nicht das bloße Pop-up aller Cookies mit dem Hinweis, dass der Nutzer mit sämtlicher Nutzung einverstanden ist. Also auch dem Datentransfer nach Amerika. Es muss dem Nutzer klar und deutlich ersichtlich sein, welcher Datenverwendung er genau zustimmt. Auch die bloße standardisierte Website Datenschutz-Erklärung im Impressum reicht für eine Zustimmung zur Datenanalyse zum Beispiel mit Google Analytics nicht aus! Eventuell kann aber die Zustimmung im „Cookie-Banner" mit der Datenschutz-Erklärung und näheren Erläuterung zur Verwendung der Daten verlinkt werden.

Hierfür ist es notwendig, in die eigene IT zu investieren und eine Art Cookie-Checker auf der Website zu installieren. Tipp: Es sollte ein Tool sein, das keinen Amerika-Bezug hat. Die Frage ist dann auch, braucht man als Unternehmen diese vielen Infos über den Website-Besucher überhaupt? Die Kosten-Nutzen Frage spielt hier eine große Rolle.

Frage 3: Ich weiß gar nicht, was auf meiner Website alles getrackt wird?
Sinnvoll ist es, die Cookies und die Zustimmung dazu genau zu analysieren und selbst einmal durchzuprüfen. Wann erfährt der Kunde überhaupt, was mit seinen Daten passiert? Kann dies einfacher und weniger kompliziert erfolgen? Bei solchen Entscheidungen sind idealerweise auch die Webdesigner einzubinden.

Frage 4: Ich habe von Abmahnungen wegen der Verwendung von Google Schriften auf Websites gehört? Um was genau geht es hier?
Wenn die Schriftarten direkt über die Server von Google eingebettet worden sind, werden bei Website-Aufrufen die jeweiligen IP-Adressen direkt an Google übermittelt. Wenn darauf nicht in den Datenschutzbestimmungen der Website hingewiesen wird und keine konkrete Einwilligung eingeholt wurde, verstößt das gegen das geltende Datenschutzrecht. Im anwaltlichen Schreiben gefordert werden Unterlassung und Schadensersatz. Zusätzlich droht eine Anzeige bei der Datenschutzbehörde. Wenn Sie so ein Schreiben erhalten oder vorbeugen möchten, kontaktieren Sie am besten uns. Sie erhalten hierzu entsprechende Informationen unserer rund 60 Juristinnen und Juristen.

In diesem Zusammenhang ist der „D.A.S. Website-Check" auf jeden Fall empfehlenswert. Hier zeigt ihnen ein erster Prüfbericht auf Ampelbasis – grün, gelb, rot - rasch und übersichtlich auf, ob und wo auf den ersten Blick Schwachstellen vorhanden sind und Sie tätig werden sollten. Von datenschutzrechtlich relevanten Google Fonts über AGB und Cookies bis hin zum Impressum. Also, lassen Sie sich ein paar Sorgen abnehmen.

RECHTS FAQ: Wie kam es zur DSGVO?

Die DSGVO ist seit dem 25. Mai 2018 in Kraft und sorgte von Anfang an für Verwirrungen:

Was genau regelt die neue Datenschutzgrundverordnung?

Welche Rechte haben Nutzer?

Und was bedeutet die DSGVO für Unternehmen?

Aber beginnen wir chronologisch. Wie ist denn überhaupt die DSGVO entstanden.

Das Safe-Harbor-Abkommen
Die Idee einer europäischen Datenschutzgrundverordnung ist nicht neu. Schon im Jahr 2012 hat der damalige EU-Kommissionspräsident Barroso angekündigt, dass er einen „Single Market for Data" schaffen wolle. Die Idee war, einen einheitlichen Rahmen für den Datenschutz in der EU zu bilden. Ziel war es die Bewegung von Daten innerhalb der EU zu erleichtern. Es dauerte noch einige Jahre, bis die Verordnung tatsächlich in Kraft trat. Der Grund dafür war das sogenannte Safe-Harbor-Abkommen, ein Abkommen zwischen der EU und den USA. Dieses Abkommen ermöglichte es US-Unternehmen Daten von europäischen Nutzern in die USA zu übertragen, ohne dass diese Unternehmen den europäischen Datenschutzbestimmungen unterliegen mussten.

Im Jahr 2015 kam es zu den ersten Bewegungen: Der Europäische Gerichtshof entschied, dass das Safe-Harbor-Abkommen nicht mehr gültig ist. Der Grund: Die USA können europäischen Nutzern keinen ausreichenden Schutz ihrer Daten garantieren. Diese Entscheidung war das Startsignal für die EU. Wenn sich die USA nicht an die europäischen Datenschutzbestimmungen halten, dann müssen wir unseren eigenen Datenschutz stärken – das war die Idee.

Die DSGVO seit 2016
Genau wegen dieser Idee wurde im Jahr 2016 die Datenschutzgrundverordnung (DSGVO) verabschiedet. Sie ist am 25. Mai 2018 in Kraft getreten. Die DSGVO hat zum Ziel, den Datenschutz in der EU zu stärken und die Bewegung von personenbezogenen Daten innerhalb der EU zu erleichtern. Sie regelt, wie Unternehmen mit personenbezogenen Daten umgehen müssen und gibt Nutzern mehr Kontrolle über ihre eigenen Daten.

Aber die Einführung der DSGVO war nicht kritiklos: Unternehmen beklagten sich über die hohen Kosten, die mit der Umsetzung der Verordnung verbunden sind. Und auch viele Nutzer waren verwirrt darüber, welche Rechte ihnen die DSGVO tatsächlich einräumt.

In den letzten Jahren gab es immer wieder neue Entwicklungen rund um die Datenschutzgrundverordnung. Und auch in den kommenden Jahren wird es weitere Anpassungen geben. Eines ist auf jeden Fall klar: Datenschutz ist ein immer wichtigeres Thema.

Natürlich finden Sie auch im Bereich Rechtschutz dafür Hilfestellungen. Wie der Daten-Rechtsschutz, der bei der „D.A.S. Rechtsschutzversicherung" für die Abwehr ungerechtfertigter Ansprüche gemäß DSGVO genutzt werden kann. Oder der Internet-Rechtsschutz. Diese Produktlösung gibt rechtliche Hilfe im Urheberbereich, bei Domainstreitigkeiten sowie Unterlassungsansprüchen zum Schutz Ihrer Persönlichkeit im Internet, beispielsweise dem sogenannten „Recht am eigenen Bild".

Im Rechts- Lexikon sind wir beim Buchstaben „C" wie Cyberkriminalität

Die weltweite Vernetzung durch Internet, Smartphones und Co hat das Leben für die Menschen in vielen Bereichen leichter gemacht. Aber trotz der vielen Vorteile haben sich in der Vergangenheit auch neue Herausforderungen gezeigt. Also wo Licht ist, da gibt es auch Schatten.

Sowohl im Privatbereich als auch für Unternehmen ist das Internet sicherlich nicht mehr wegzudenken. Elektronische Datenverarbeitung, finanzielle Transaktionen und Betriebsinterna werden immer öfter im Netz oder einer Cloud abgewickelt. Das bringt auch kriminelle Energie hervor und ruft diesbezüglich Subjekte auf den Plan. 2021 verzeichneten die zuständigen Behörden zirka 46.200 diesbezügliche Vergehen, wovon 17.000 geklärt werden konnten. Rund 22.500 Fälle sind dem Internetbetrug zu zu ordnen, und nahmen im selben Zeitraum um knapp 20 Prozent zu, wobei hier der Bestellbetrug am

häufigsten ist. Eine massive Zunahme, nämlich ein Plus von 70 Prozent, mussten im Bereich der Cyberkriminalität festgestellt werden. Das sind Hacking, Datenbeschädigungen oder –fälschungen und Datenverarbeitungsmissbrauch. Und das sind die offiziell gemeldeten Vorfälle. Die Dunkelziffer ist wohl deutlich höher.

Mit Phishing, Viren und gut organisierten Angriffen kommen Nutzer und Unternehmen zu Schaden. Betriebsgeheimnisse oder Kundendaten werden gestohlen und verkauft, Bankdaten geknackt und Systeme lahmgelegt. Das führt zu erheblichen wirtschaftlichen Schäden und kann für betroffene Betriebe auch existenzbedrohend sein. Mit einem weltweiten Jahresumsatz von fast 1,5 Billionen Euro hat die Internetkriminalität der bisherigen Nummer 1, dem Drogenhandel, den Rang abgenommen.

Alle Unternehmen können von Cyberkriminalität betroffen sein. Wir haben Ihnen hier zur Veranschaulichung sechs spektakuläre Fälle von Datendiebstahl herausgesucht:

Einer der ersten großen Datendiebstähle fand im Jahr 2002 statt. Ein ehemaliger Mitarbeiter der Firma AOL gelangte an die Daten von 92 Millionen AOL-Kunden und veröffentlichte sie im Internet. Das Leak umfasste neben Namen und E-Mail-Adressen auch Telefonnummern, Postadressen und Kreditkartennummern.

Ein weiterer spektakulärer Fall ereignete sich 2007 bei der US-amerikanischen Firma TJX. Durch einen Hack gelangten Diebe an die Kreditkartendaten von mehr als 45 Millionen Kunden. Die Firma gab den Datendiebstahl erst mehrere Monate später bekannt, was zu einem hohen Schaden für das Unternehmen führte.

Im Jahr 2014 wurden bei der US-amerikanischen Firma Sony Pictures rund 100 Terabyte an Daten gestohlen und unter anderem E-Mails, Dokumente sowie Videoclips veröffentlicht. Der Angriff galt vermutlich dem Film „The Interview“. Hier geht es um den Mordanschlag auf den nordkoreanischen Staatschef Kim Jong-un. Der Film sollte ursprünglich am 25. Dezember 2014 in den Kinos veröffentlicht werden, dies verzögerte sich jedoch aufgrund des Angriffs.

Noch ein großer Datendiebstahl ereignete sich im Jahr 2015 bei der US-Behörde Office of Personnel Management (OPM). Durch einen Hack gelangten Diebe an die sensiblen Daten von mehr als 21 Millionen Menschen. Viele hochrangige Regierungsbeamte waren hier involviert.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) war 2015 Ziel eines Angriffs. Dabei wurden rund 18 Gigabyte an Daten gestohlen, unter anderem E-Mails und Dokumente mit vertraulichen Informationen. Zum Glück konnte der Angriff relativ schnell entdeckt werden und die gestohlenen Daten wurden nicht veröffentlicht.

Spektakulär war auch der Datendiebstahl bei der US-amerikanischen Firma Yahoo im Jahr 2016. Durch einen Hack gelangten Diebe an die Daten von mehr als 500 Millionen Yahoo-Kunden. Das Leak umfasste neben Namen und E-Mail-Adressen außerdem Telefonnummern, Postadressen und Kreditkartennummern.

Und auch in Österreich kam es immer wieder zu Datendiebstählen. Erst im Mai dieses Jahres wurde die Kärntner Landesverwaltung Opfer eines Hacker-Angriffs, bei dem zahlreiche sensible Daten gestohlen und im Internet veröffentlicht wurden.

Cyberkriminalität und Datendiebstahl ist ein ernstes Problem, das immer häufiger vorkommt. Durch die steigende Digitalisierung werden mehr und mehr Daten gespeichert und sind damit leider auch anfälliger für Angriffe von außen. Daher wichtig: Schützen Sie sich und Ihre Daten so gut wie möglich!

Auch mit entsprechenden Rechtsschutz Produktlösungen können Sie sich als Unternehmerin und Unternehmer rechtlich absichern. Beispielsweise mit dem Cyber-Rechtsschutz. Mit Präventionsmaßnahmen, wie dem schon erwähnten Cybercheck, und auch rechtlicher Hilfe im Falle des Falles. Nämlich Schadensersatz- und Strafrechtsschutz-Maßnahmen, Beratungs-Rechtschutz sowie Versicherungsstreitigkeiten, wenn Sie im kausalen Zusammenhang stehen.

Und damit kommen wir auch schon zum Ende dieser Folge. Abonnieren Sie den Podcast, damit Sie keine Folge verpassen!

Übrigens: Wir meinen, Texte sollen möglichst leicht lesbar und verständlich sein. Daher beziehen sich sämtliche verwendeten Bezeichnungen auf alle Menschen gleichsam.

Danke für‘s Zuhören und bis zum nächsten Mal beim Rechtsschutz Podcast.