Kurz notiert

Nach dem **Verbraucherstreitbeilegungsgesetz** ist ein Onlineunternehmer verpflichtet, auf seiner Website darauf hinzuweisen, „inwieweit er bereit ist oder verpflichtet ist, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen". Wenn sich ein Unternehmen zu einem solchen Verfahren bereit erklärt, dazu aber nicht verpflichtet ist, treffen es keine weiteren Informationspflichten, entschied jüngst der Bundesgerichtshof (Az.: VIII ZR 263/18).

Internetdienste sollen künftig **Passwörter zu Nutzerkonten** an Ermittlungsbehörden herausgeben müssen. Das sieht ein Gesetzesentwurf gegen Rechtsextremismus und Hassrede der Bundesregierung vor, der auf teils heftige Kritik stößt. Nach Auffassung der Bundesregierung existiert eine solche Pflicht bereits im Rahmen der Pflicht zur Herausgabe von Bestandsdaten.

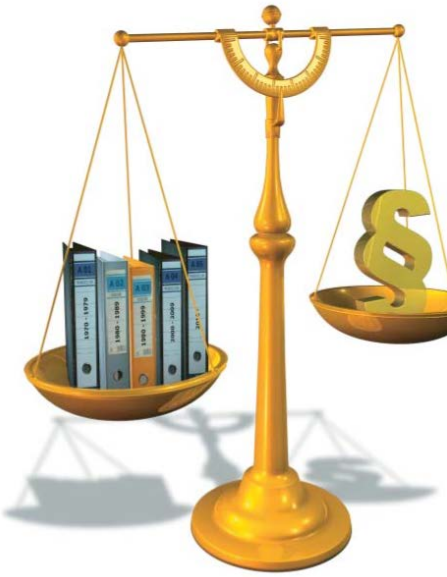
Das **Netzwerkdurchsetzungsgesetz** soll nach Plänen der Bundesregierung verschärft werden. Neben der Pflicht zur Entfernung rechtsverletzender Inhalte sollen Betreiber sozialer Netzwerke solche Inhalte künftig auch proaktiv an das Bundeskriminalamt melden.

Das Landesarbeitsgericht München hat das Vorliegen eines **Arbeitsverhältnisses eines Crowdworkers** mit dem Betreiber der Crowdworking-Internetplattform verneint. Begründet wird dies damit, dass der Crowdworker keine Verpflichtung zum Übernehmen von Aufträgen hat.

Nach einem Urteil des österreichischen Verfassungsgerichts ist die geplante Einführung eines **„Bundestrojaners"** sowie einer automatischen Kennzeichenerfassung verfassungswidrig. Gegen die verdeckte Überwachung verschlüsselter Nachrichten spricht danach unter anderem die Privatsphäre der unbeteiligten Kontakte des Überwachten sowie die Unverletzlichkeit des Hausrechts.

Alle Meldungen: Tobias Haar

GoBD erlauben Abfotografieren



Seit Jahresanfang gilt eine Neufassung der GoBD. Diese „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" gelten für alle Unternehmen, die steuerlich relevante Daten mithilfe von IT verarbeiten. Unter bestimmten Voraussetzungen fallen auch E-Mails darunter. Dabei gilt wie bislang auch für Buchungsbelege eine Aufbewahrungsfrist von mindestens zehn Jahren und für Handels- und Geschäftsbriefe von mindestens sechs Jahren. Die GoBD 2020 ersetzen die Vorgängerversion von 2014. Beispielsweise ist nun neben dem Scannen auch das Abfotografieren von Belegen mittels Smartphone gestattet.

Weitere Regelungen umfassen das Speichern relevanter Daten auf Servern im Ausland. Eine wesentliche Erleichterung ist, dass künftig sechs Jahre nach Umstellung auf neue Buchhaltungssysteme Altsysteme nicht mehr zum Zwecke der Steuerprüfung weiterbetrieben werden müssen. Die neuen Regelungen sind in der kommenden *iX* 3/2020 im Detail nachzulesen. (ur@ix.de)

Gesetz reguliert Kryptohandel in Deutschland

Zum Jahresanfang ist das „Gesetz zur Umsetzung der Änderungsrichtlinie zur vierten EU-Geldwäscherichtlinie" in Kraft getreten. Es reguliert künftig digitale Vermögenswerte in Deutschland. Unternehmen, die Dienstleistungen in diesem Bereich erbringen, benötigen dann eine Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht. Digitale Anlageprodukte werden künftig als „Kryptowerte" bezeichnet und umfassen unter anderem auch Bitcoins und Co. sowie digitale Wertpapiere, sogenannte Security Token. Erlaubnispflichtig ist „die Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern und zu übertragen, für andere", also für Dritte. Für in diesem Bereich bereits tätige Unternehmen gibt es eine Übergangsfrist. Sie müssen der BaFin allerdings bis 31. März 2020 ihre Tätigkeit schriftlich anzeigen und bis 30. November 2020 einen vollständigen Erlaubnisantrag nachreichen. Das Gesetz stößt auf Kritik und wird mitunter als „deutscher Sonderweg" bezeichnet. So können sich Anbieter aus anderen EU-Staaten nicht auf die Niederlassungsfreiheit und die Regelungen des Binnenmarkts nach den EU-Verträgen berufen. Zudem sind die Erlaubnisanträge aufwendig und mit erheblichen Kosten verbunden. Befürworter unterstreichen, dass für Anbieter und Kunden in Deutschland nun eine höhere Sicherheit beim Handel mit Kryptowerten besteht, was den Finanzmarktplatz Deutschland aufwerten wird. Unterdessen arbeitet die BaFin an den Details der Erlaubnisvoraussetzung und den Genehmigungsverfahren. (ur@ix.de)

DSGVO-Bußgeld gegen TK-Unternehmen

Ende 2019 hatte die Berliner Datenschutzbehörde gegen das Immobilienunternehmen Deutsche Wohnen ein Bußgeld in zweistelliger Millionenhöhe wegen eines Verstoßes gegen die Datenschutz-Grundverordnung verhängt. Kurz vor Weihnachten hat nun auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, ein Bußgeld in Höhe von über 9,5 Millionen Euro gegen das TK-Unternehmen 1&1 Telecom GmbH verhängt. Der Vorwurf lautet auf unzureichende technische und organisatorische Maßnahmen zum Schutz von Kundendaten. Konkret wurde dem Unternehmen zum Verhängnis, dass offenbar Name und Geburtsdatum ausreichten, um über die Telefon-Hotline weitere personenbezogene Kundendaten zu erfragen. 1&1 hat sich im Rahmen des Verfahrens „einsichtig und äußerst kooperativ" gezeigt, wie es in einer Pressemitteilung heißt. Daher sei das Bußgeld auch „im unteren Bereich des möglichen Bußgeldrahmens" festgesetzt worden, so der Bundesdatenschutzbeauftragte.

Auch Kleinstunternehmen stehen mehr und mehr im Fokus des Bundesdatenschutzbeauftragten. Weil ein anderes TK-Unternehmen der „gesetzlichen Auflage nach Artikel 37 DSGVO zur Benennung des betrieblichen Datenschutzbeauftragten trotz mehrmaliger Aufforderung nicht nachgekommen ist", wurde es mit einem Bußgeld in Höhe von 10000 Euro belegt. (ur@ix.de)

DSGVO: Schranken der Identifizierung bei Löschanfragen

Die Datenschutz-Grundverordnung (DSGVO) gibt in Artikel 17 Betroffenen ein umfassendes Recht auf Löschung der bei einem Unternehmen gespeicherten personenbezogenen Daten, wenn dem nicht ein schutzwürdiges Interesse an der Speicherung durch das Unternehmen entgegensteht. Die DSGVO regelt im Detail, wann dies der Fall ist. Nicht ausdrücklich geregelt ist die Frage, inwieweit ein Unternehmen überprüfen darf oder sogar muss, ob es sich bei einem Antragsteller tatsächlich um den Betroffenen handelt. Die Datenschutzbehörde Österreichs hat jüngst Stellung zur Frage nach der Identifikation bezogen.

Wenn ein Unternehmen beim Erheben der personenbezogenen Daten keine Absicht hatte, den Betroffenen zu identifizieren, und ihm – wie im konkreten Fall – das Einrichten eines Nutzerprofils unter Pseudonym ermöglicht, scheidet bei einem Löschungsbegehren ein Anspruch auf Identifikation aus. Die darf dann nur insoweit erfolgen, „als sie notwendig ist, um die Berechtigung zur Ausübung des Löschungsrechts zu überprüfen". In der Begründung heißt es weiter: „Ein pseudonymer Nutzer kann sich etwa durch Kenntnis der Log-in-Daten (User-ID, Passwort), durch Angaben zum gespeicherten Dateninhalt des Profils oder durch die nachgewiesene Verfügungsgewalt über die Mailbox, deren E-Mail-Adresse anlässlich der Registrierung angegeben worden ist, identifizieren. Neue Daten (wie Vorname, Familienname, Wohnadresse, eine Ausweiskopie oder das grafische Bild einer eigenhändigen Unterschrift) müssen aus diesem Anlass nicht erhoben werden". (ur@ix.de)

Kurz notiert

Das **Passgesetz** soll dahingehend ergänzt werden, dass Passfotos für Ausweisdokumente am Ort der Antragstellung erstellt werden müssen. Das sieht ein Gesetzesentwurf der Bundesregierung vor, der durch Morphing veränderte Passbilder verhindern soll.

Google drohen in der Türkei erhebliche Bußgelder wegen der Voreinstellung der **Google-Suchmaschine** auf Android-Handys. Aus diesem Grund werden derzeit keine Lizenzen für Geräte mehr erteilt, die für den türkischen Markt produziert werden. Auf Beschwerde eines russischen Suchmaschinenbetreibers war Google 2019 zu einer Millionenstrafe verurteilt worden.

Indien und Kalifornien verschärfen Datenschutz

Kalifornien ist als Bundesstaat der Vereinigten Staaten von Amerika wie alle anderen Bundesstaaten zuständig für die Verabschiedung von Datenschutzgesetzen. Diese gelten dann für die Verarbeitung von Daten durch Unternehmen mit Geschäftstätigkeiten in Kalifornien. Dazu ist kein Unternehmenssitz erforderlich, sondern es genügt, wenn ein deutsches Unternehmen beispielsweise personenbezogene Daten von in Kalifornien ansässigen Personen erhebt und verarbeitet. Zum 1. Januar trat nun der California Consumer Privacy Act (CCPA) in Kraft. Er greift für Unternehmen, die einen Bruttoumsatz von mehr als 25 Millionen US-Dollar erwirtschaften, mehr als 50 % ihres Umsatzes mit dem Verkauf personenbezogener Daten erzielen oder Daten von mehr als 50 000 Verbrauchern, Haushalten oder Geräten verkaufen oder anderweitig kommerziell mit dritten Personen teilen. Für die Daten von Jobbewerbern, Mitarbeitern, Organen et cetera gilt für die Einhaltung der CCPA-Vorgaben eine Übergangsfrist bis Anfang 2021. Zudem ist der CCPA nachrangig zu etwaigen Spezialgesetzen.

Der CCPA verlangt unter anderem eine an die neue Regulierung angepasste Privacy Policy, also eine Datenschutzerklärung. Bei Internetauftritten wird eine Anpassung an die neue Gesetzeslage empfohlen. Ähnlich der Datenschutz-Grundverordnung steht vom CCPA geschützten Personen ein Recht auf Auskunft, Sperrung und Löschung ihrer Daten zu. Dazu müssen entsprechende Prozesse etabliert sein. Die Vorgaben nach der DSGVO und dem CCPA ähneln einander zwar, können aber dennoch im Detail unterschiedlich sein. Zum Schutz personenbezogener Daten sind „angemessene Sicherheitsmaßnahmen" zu ergreifen.

Auch in Indien gibt es Überlegungen, das Datenschutzrecht zu modernisieren. Sollte der vorliegende Gesetzesentwurf verabschiedet werden, kommt es zu erheblichen Änderungen. So soll die Zentralregierung berechtigt sein, das Einhalten des Datenschutzrechts durch Behörden „im Interesse der Souveränität und Integrität Indiens, der Sicherheit des Staates, der freundschaftlichen Beziehungen zu ausländischen Staaten, der öffentlichen Ordnung" und aus weiteren Gründen auszusetzen. Details des Gesetzes befinden sich derzeit in der Abstimmung. Wahrscheinlich ist jedoch, dass insbesondere auf die Betreiber sozialer Netzwerke verschärfte Vorgaben zukommen, die allerdings auch zum Schutz vor Fake News und zur besseren Verfolgbarkeit von Straftaten geeignet sein sollen. (ur@ix.de)

Aktive Cyberwehr gefordert

Auf dem „Tag der Sicherheit" des Bundesinnenministeriums und des Bundesverbands der deutschen Industrie Anfang Dezember wurde erneut die Abwehr von Angriffen auf Datennetze diskutiert. Eine seit einiger Zeit kontrovers diskutierte Frage betrifft das vom Bundesinnenministerium geforderte Recht auf „aktive Cyberwehr". Dessen Leiter der Abteilung „Cyber- und Informationssicherheit" Andreas Könen fordert eine Grundgesetzänderung, damit gegen Botnetze und DoS-Angriffe eine Teilnahme an internationalen Aktionen zur Gefahrenabwehr möglich ist. Hierzu zählt er Netzsperren oder auch die Sperrung bestimmter Angriffskanäle. Der Konzernsicherheitskoordinator der Deutschen Telekom, Axel Petri, forderte die Möglichkeit, „digital die Grenzen hochziehen zu können", und hierfür einen Zusammenschluss von Ländern, „die Ethik und Werte teilen". Negativ bewertet er Pläne des Gesetzgebers zur Einführung verpflichtender Backdoors oder zur Ausnutzung weiterer Schwachstellen. (ur@ix.de)