

Informationstechnik und Recht

Expertinnen und Experten befassten sich beim 14. österreichischen IT-Rechtstag mit Rechtsproblemen, die sich in der Praxis durch den Einsatz der Informationstechnologie ergeben.

Der österreichische IT-Rechtstag, veranstaltet von *Infolaw, Forschungsverein für Informations- und Immaterialgüterrecht*, fand wegen der Corona-Krise vom 4. bis 19. November 2020 in Form von sechs virtuell abgehaltenen Veranstaltungen statt. Registrierte Teilnehmer hatten Gelegenheit, sich schriftlich über die Chat-Funktion oder, gesteuert durch den Moderator, über Mikrofon und Kamera einzubringen. Die Vortragenden unterlegten ihre Ausführungen mit Präsentationen. Die Übertragung der Referate, eines davon aus Kalifornien, erfolgte weitgehend problemlos. Bei der Panel-Diskussion wurden die Diskutierenden jeweils einzeln zugeschaltet.

Die Schwerpunkte der Veranstaltung lagen auf Rechtsproblemen bei der Softwarenutzung; bei Problemen, die sich bei Bewertungen auf Plattformen ergeben und, als dritter und meistbesuchter Themenkreis, auf Entwicklungen im Datenschutzrecht. Prof. Dr. Martin Selmayr, Leiter der Vertretung der Europäischen Kommission in Österreich, stellte die digitale Agenda der EU-Kommission vor. Nach der European Data Strategy soll sektorübergreifend ein Rechtsrahmen für gemeinsamen Datenzugang und -nutzung geschaffen werden, etwa für Industriedaten. Die gemeinsame Nutzung von Daten zwischen Unternehmen untereinander und Behörden soll gefördert und Hindernisse abgebaut werden. Datensätze im öffentlichen Bereich, etwa über den Georaum, Umwelt,



Schwerpunkte des IT-Rechtstags: Rechtsprobleme bei Softwarenutzung, Whistleblowing, Datenschutzrecht, Cookies.

Meteorologie, Gesellschaft, Mobilität, sollen frei zur Verfügung stehen.

Whistleblowing. Bereits in Kraft ist die EU-Richtlinie 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblower-RL; WBRL), die bis 17. Dezember 2021 in innerstaatliches Recht umzusetzen ist. Mag. Roland Marko, *Wolf Theiss Rechtsanwälte* (wolftheiss.com), der über die Richtlinie berichtete, wies darauf hin, dass die Aufklärung bedeutender Wirtschaftsstrafsachen zunächst durch entsprechende Hinweise ihren Anfang genommen hat. Die Richtlinie schaffe einen geregelten Rahmen für ein solches Hinweissystem, das bisher, wie etwa nach dem Bankwesen- oder Börsegesetz, auf einzelne Branchen oder Behörden beschränkt ist. Die Richtlinie umfasst Meldungen zu Verstößen in Bereichen wie öffentliches Auftragswesen, Finanzdienstleistungen, Produkt- und Verkehrssicherheit, Umweltschutz, Verbraucherschutz, öffentliche Gesundheit, Datenschutz und Si-

cherheit von Netz- und Informationssystemen, sofern die Regelungen auf im Anhang angeführte Rechtsakte der EU beruhen (Art. 2).

Hinweisgeber kann jeder sein, der im privaten oder öffentlichen Sektor tätig ist und im beruflichen Kontext Informationen über Verstöße erlangt hat. Um den Schutz nach der Richtlinie beanspruchen zu können, muss der Hinweisgeber hinreichenden Grund zu der Annahme haben, dass die Informationen über Verstöße der Wahrheit entsprechen, der Verstoß in den Anwendungsbereich der WBRL fällt und der vorgesehene Meldeweg eingehalten wurde (Art. 6).

Alle juristischen Personen des öffentlichen Sektors sowie ausgewählte juristische Personen aus den Bereichen Finanzen, Verkehrssicherheit und Umweltschutz werden ein Hinweissystem verpflichtend einzuführen haben, weiters private Arbeitgeber, die mehr als 50 Arbeitnehmer beschäftigen. Arbeitnehmern muss ein interner Meldekanal zur Verfügung gestellt werden, der auch Dritten zur Verfügung

stehen kann. Der Meldekanal (etwa ein Briefkasten, Telefon-Anschluss, eine Mail-Adresse, digitales System, Ombudsmann) muss sicher sein und die Identität des Hinweisgebers schützen. Die Entgegennahme der Meldungen hat, intern oder extern, durch eine unparteiische Person zu erfolgen.

Innerhalb von sieben Tagen ist dem Hinweisgeber der Erhalt der Meldung zu bestätigen. Innerhalb von drei Monaten hat eine Rückmeldung über die ergriffenen Maßnahmen zu erfolgen. Erfolgt innerhalb von drei bzw. allenfalls sechs Monaten keine derartige Rückmeldung, darf der Hinweisgeber die Information offenlegen, ohne den Schutz zu verlieren (Art. 15).

Die Vertraulichkeit des Hinweisgebers ist durch Art. 16 WBRL geschützt. Der Beschuldigte hat datenschutzrechtlich ein Recht auf Auskunft, Berichtigung und Löschung, wobei offen bleibt, inwieweit er zu informieren ist. Bei der Verarbeitung personenbezogener Daten, sowohl über den Hinweisgeber, Beschuldigte und involvierte Dritte, wird, selbst wenn die Daten strafbare Handlungen betreffen, von einem überwiegenden berechtigten Interesse des Verantwortlichen (Art. 6 Abs. 1 lit f DSGVO) auszugehen sein.

Was die innerstaatliche Umsetzung der RL betrifft, zeigte Roland Marko mögliche Gestaltungsspielräume auf, etwa in Form einer Erweiterung der geschützten Meldetatbestände, oder auch im Hinblick auf „wirksame, angemessene und abschre-

ckende“ Maßnahmen zur Verhinderung von Repressalien gegen Hinweisgeber (Art. 19) bzw. zu Sanktionen einschließlich Schadenersatz für Hinweisgeber, die wesentlich falsche Informationen gemeldet oder offengelegt haben (Art. 23 Abs 2).

Bewertungen auf Plattformen. Auf virtuellen Plattformen abgegebene Bewertungen von Hotels, Restaurants, Dienstleistungen, bieten Orientierungshilfen, müssen aber auch Lauterkeits- und wettbewerbsrechtlichen Bestimmungen genügen und können, insbesondere, wenn es um Einzelpersonen (Ärzte, Lehrer) geht, in Persönlichkeitsrechte eingreifen und die Tatbestände der Ehrenbeleidigung sowie der Kreditschädigung erfüllen. Es erhebt sich auch die Frage der Verantwortlichkeit des Plattformbetreibers. Wie bedeutsam das Thema ist, zeigt, dass es von zwei Vortragenden (Univ.-Ass. Dr. Stefan Holzweber, Universität Wien, und Mag. Alexandra Ciarnau, *DORDA Rechtsanwältin*) aufgegriffen wurde und Gegenstand der Panel-Diskussion war.

Wird für Bewertungen bezahlt, sei es auch nur durch die Möglichkeit der Beteiligung an Gewinnspielen, muss dies erkenntlich gemacht werden. Negative Bewertungen dürfen nicht verspätet freigeschaltet werden. Bewertungen müssen verifiziert werden können, wobei die Funktionsweise der Verifikation offengelegt werden muss.

Als praxistaugliche Rechtsgrundlage für die Verarbeitung der Daten bezeichnete Alexandra Ciarnau Art. 6 Abs. 1 lit f der DSGVO, wonach die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein muss, sofern nicht die Interessen oder



Bewertungsplattformen: Bewertungen von Hotels, Restaurants und Dienstleistungen müssen den Lauterkeits- und wettbewerbsrechtlichen Bestimmungen genügen.

Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Bei Beurteilung der Erforderlichkeit wird es darauf ankommen, welche Daten verarbeitet werden, ob es weniger invasive Mittel gibt, etwa die Verarbeitung von anonymisierten Daten, und es wird der Datenminimierungsgrundsatz zu beachten sein.

Bei der Interessenabwägung fallen nach einer in Entwicklung begriffenen Rechtsprechung zugunsten des Verantwortlichen das allgemeine Interesse und die Bedeutung der Datenverarbeitung ins Gewicht sowie das Recht auf freie Meinungsäußerung und Information, das den Empfang und die Weitergabe von Nachrichten oder Ideen schützt. Dem stehen auf Seiten des Betroffenen das Grundrecht auf Datenschutz und Geheimhaltung gegenüber. Laut Ciarnau bestehe die Gefahr einer Stigmatisierung, Ausgrenzung, Prangerwirkung mit Folgen bis hin zur Existenzvernichtung. Zugunsten des Betroffenen ist weiters zu berücksichtigen, inwieweit in mehrere Grundrechte eingegriffen wird, in das Recht auf Namensnennung nach § 43 ABGB oder in die Privatsphäre nach § 1328a ABGB. Zu berücksichtigen sind die Erwartungen des Betroffenen (ErwGr

47 DSGVO), etwa, in welcher Beziehung er zum Verantwortlichen steht, in welcher Position er sich befindet, woher die Daten stammen. Nachzuprüfen ist, ob die Informationspflichten nach Art. 13 ff DSGVO erfüllt und technische und organisatorische Sicherheitsmaßnahmen getroffen wurden, wie Schutz vor Missbrauch, Sicherstellung der Datenaktualität und zur Gewährleistung des Datenschutzniveaus. Die Interessenabwägung wird zu dokumentieren sein.

Bei Ehrenbeleidigung und Kreditschädigung kommt es darauf an, ob Tatsachen behauptet oder Werturteile abgegeben wurden. Bloße Sternbewertungen ohne aussagekräftigen Begleittext wurden nach deutscher Judikatur als Äußerung der Unzufriedenheit mit dem Leistungsangebot gewertet. Der Provider ist zu Nachprüfungen verpflichtet, wenn vom Bewerteten eingewendet wird, dass die negativ bewertete (zahnärztliche) Behandlung nicht stattgefunden habe (BGH 1.3.2016, VI ZR 34/15; „Jameda II“).

Die Panel-Diskussion drehte sich um die Frage, ob und welche Bereiche einer öffentlichen Bewertung entzogen sein sollten. Während marktgerechte Tätigkeiten einem öffentlichen Diskurs

offen stehen müssten, sei Zurückhaltung angezeigt, wenn es um Einzelpersonen (Lehrer, Ärzte, Richter) gehe. Bei Postings herrsche „der wilde Westen der Meinungsfreiheit“. Nicht jeder, der postet, ist Medienmitarbeiter im Sinn des § 9 DSGVO und genießt das dort statuierte Medienprivileg. Videos einer allenfalls überschießenden polizeilichen Amtshandlung ins Netz zu stellen, könne durch ein bestehendes öffentliches Interesse gerechtfertigt sein, nicht jedoch, den Namen des beteiligten Polizisten zu veröffentlichen.

Datenschutzrecht. Dr. Andreas Zavadil, Datenschutzbehörde, berichtete zur Spruchpraxis dieser Behörde. Aus den von Amts wegen eingeleiteten *Prüfverfahren* hob er von den zuletzt ergangenen, rechtskräftigen Entscheidungen jene vom 3.2.2020 hervor, mit der die Verarbeitung von Lehrerdaten („Lernsieg“) als grundsätzlich zulässig erklärt wurde. Durch Einstellung beendet – weil den datenschutzrechtlichen Anforderungen entsprochen wurde – wurde am 3.11.2020 das Prüfverfahren betreffend die Stopp-Corona-App. Beide Entscheidungen finden sich im *dsb-Newsletter 3/2020*. Mit Bescheid vom 16.12.2019, D213.864/0003-DSB/2019 war die datenschutzrechtliche Unzulässigkeit eines Handvenenscans für den Eintritt in ein öffentliches Bad festgestellt worden.

Was *Beschwerdeverfahren* betrifft, wurde mit Bescheid vom 2.12.2019, DSB-D124.352/0003-DSB/20129 festgestellt, dass eine Polizeibeamtin in ihrem Recht auf Geheimhaltung ihrer personenbezogenen Daten verletzt worden war, weil Fotos von einer Amtshandlung, an der sie beteiligt und identifizierbar abgebildet war, unter

Beifügung ihres Nachnamens auf Facebook gepostet (und anschließend geteilt) wurden. Die Veröffentlichung der Fotos von der Amtshandlung wurde dem Grundrecht der Freiheit der Meinungsäußerung entsprechend erachtet.

Als vom Medienprivileg des § 9 DSGVO gedeckt und damit nicht in die Zuständigkeit der DSB fallend, wurde mit Bescheid vom 21.4.2020, DSB-D124.2228, 2020-0.239.741 eine Beschwerde zurückgewiesen, in der die Löschung einer als verächtlich machend empfundenen, in einer Online-Tageszeitung erfolgten Veröffentlichung eines aufgezeichneten Telefonats begehrt wurde.

Von den rechtskräftig abgeschlossenen Verwaltungsstrafverfahren ist das Straferkenntnis vom 11.7.2019, DSB-D550.185/002-DSB/2019 bemerkenswert, mit dem ein Fußballtrainer mit 10.000 Euro Geldstrafe belegt wurde, der Spielerinnen heimlich in der Umkleidekabine und am Weg zum Duschaum mit dem Mobiltelefon gefilmt hatte. Das Verfahren nach § 63 DSG (Datenverarbeitung in Gewinn- oder Schädigungsabsicht) war von der Staatsanwaltschaft eingestellt worden.

Schadenersatz. Art. 82 DSGVO sichert jeder Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftraggeber zu. Künftig wird mit einer verstärkten Berücksichtigung des immateriellen Schadens zu rechnen sein, führte Dr. Bernhard Burtscher (Wirtschaftsuniversität Wien) aus, und begründete dies mit dem Vorrang des Unionsrechts

gegenüber dem nationalen (*effet utile*). Die bisherige Tendenz in der österreichischen Rechtsprechung, bei der Bemessung immaterieller Schäden (Schmerzensgeld) „erhebliche Eingriffe“ und „grobes Verschulden“ zu verlangen, werde im internationalen Vergleich niedrighschwelliger anzusetzen sein. Wirksamer Schutz von Persönlichkeitsrechten funktioniere nicht ohne Berücksichtigung des erlittenen ideellen Schadens.

Cookies. Die DSGVO hat, wie Mag. Nino Tlapak, *DORDA Rechtsanwälte*, darlegte, durch die Informationspflichten nach den Art. 13 und 14 die klare Verpflichtung mit sich gebracht, dass der Nutzer der durch Cookies vorgenommenen Datenerhebung vorab zustimmen muss. Wurde ursprünglich ein bloßer Hinweis im Impressum als ausreichend erachtet, ging die Entwicklung zu Informationsbannern („Weiternutzung gilt als Zustimmung“); weiter zu aufpoppenden Bannern auf der Startseite, bei denen sich die Auswahl des Nutzers auf ein „OK“ beschränkte; bis nunmehr hin zu Cookie-Bannern mit aktiver, informierter Einwilligung („Akzeptieren“, „Ablehnen“, „Alle Akzeptieren“, „Einstellungen“ und „Nur notwendige Cookies“). Nach der Rechtsprechung des EuGH (C-673/17) sind voraktivierte Checkboxen keine aktive Einwilligung. Die Einbettung von Cookies erfordert eine aktive Handlung. Die Praktik, jemanden als zustimmend anzusehen, „wenn Sie diese Website weiter nützen“, ist unzulässig. Die ePrivacy-VO, die nähere Regelungen unter anderem zu Cookies erwarten lässt, befindet sich nach wie vor im Entwurfsstadium.

Kurt Hickisch
it-rechtstag.at; infolaw.at