Rechtsanwaltskammer München

MEHR DATEN BRAUCHEN MEHR SCHUTZ: THOMAS KRANIG IM INTERVIEW

Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht spricht im Interview über die Entwicklung des Datenschutzrechts, Cloud-Computing für Anwälte und worauf es beim Schutz unserer enormen Datenmengen wirklich ankommt.

Thomas Kranig

Herr Kranig, das Thema Datenschutz hat sich mittlerweile zu einem weiten Feld mit hoher Komplexität entwickelt. Was sind aktuell die größten Herausforderungen in Sachen Datenschutzaufsicht?

Je mehr die Digitalisierung zunimmt, desto mehr werden wir gefordert. Also mit anderen Worten: was nicht bei drei auf den Bäumen ist, wird digitalisiert.

Es gibt eine Handvoll Unternehmen, die über eine unvorstellbar große Menge von Daten verfügen, aber auch Maschinen, die miteinander kommunizieren, Daten austauschen und nicht zuletzt haben und produzieren wir alle mit unseren stationären und mobilen Endgeräten eine enorme Mengen an Daten. Fast alle diese Daten sind personenbezogen und führen damit zur Anwendung des Datenschutzrechts. In rechtlicher Hinsicht befinden wir uns im letzten Drittel der Umsetzungsphase zum neuen Recht, der EU-Datenschutz-Grundverordnung. Die größte Herausforderung für uns als Datenschutzaufsicht ist, dass wir einerseits das geltende Recht nicht aus den Augen verlieren dürfen, andererseits aber viele Unternehmen von uns wissen wollen, wie das neue Recht zu verstehen ist bzw. wie wir es zu vollziehen gedenken – und in vielen Bereichen wissen wir es selbst noch nicht.

Seit 2011 sind Sie Präsident des Bayerischen Landesamtes für Datenschutzaufsicht. Welche Aufgaben sind damit verbunden und was genau ist der Unterschied zwischen Ihrer Behörde und dem Bayerischen Landesbeauftragten für den Datenschutz?

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ist die in Bayern zuständige Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich. Wir kontrollieren bei Banken, Versicherungen, Handelsgeschäften, privaten Krankenhäusern, Vereinen, Verbänden und auch bei Privatpersonen, die Daten nicht nur im privaten persönlichen Bereich nutzen, sondern sie zum Beispiel ins Internet stellen, ob die Vorschriften des Datenschutzes eingehalten werden. Nach dem statistischen Jahrbuch für Bayern sind wir für etwa 700.000 Stellen die zuständige Datenschutzaufsichtsbehörde. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) ist für die Kontrolle der öffentlichen Stellen in Bayern, der Ministerien, Landratsämter, Gemeinden oder öffentlichen Krankenhäuser zuständig. Für den Bereich der Rechtsanwaltschaft bedeutet dies zum Beispiel, dass wir für die Kontrolle der Einhaltung des Datenschutzes bei Rechtsanwälten zuständig sind und der BayLfD dies bei der Rechtsanwaltskammer als Körperschaft des öffentlichen Rechts macht.

Nehmen wir mal an, Ihre Behörde entdeckt einen Datenschutzverstoß. Welche Maßnahmen können bzw. dürfen Sie in diesem Fall ergreifen?

Leider entdecken wir ziemlich viele Datenschutzverstöße. Mehr als die Hälfte der 1400 Beschwerden, die wir pro Jahr bekommen, stellen sich nach unserer Überprüfung als Datenschutzverstoß heraus. Wir haben dann die Möglichkeit, die verantwortlichen Stellen, die mit personenbezogenen Daten Dritter umgehen, durch Anordnungen oder Bußgeldbescheide zu zwingen, das Recht einzuhalten. Wir können es aber auch, was wir derzeit noch in den meisten Fällen machen, bei einer Belehrung oder Verwarnung belassen. Anders ist die Situation derzeit noch im öffentlichen Bereich. Der Bayerische Landesbeauftragte für den Datenschutz kann nach dem derzeit geltenden Recht nur Beanstandungen, aber keine hoheitlichen Zwangsmaßnahmen aussprechen.

Was hat Sie motiviert, sich dem Thema Datenschutz anzunehmen?

Ich habe in meinem beruflichen Leben schon ziemlich viele unterschiedliche Stationen hinter mir. Die ersten vier Jahre habe ich Grundstücke um München herum und in Richtung Niederbayern gekauft, damit Autobahnen gebaut werden können. Dann durfte ich mich drei Jahre um die öffentliche Sicherheit und anschließend vier Jahre um das Baurecht im Landkreis Aschaffenburg kümmern. Der Freistaat Bayern hat mir danach im Rahmen einer Beurlaubung die Chance gegeben, einige Jahre im Medienbereich in der Privatwirtschaft tätig zu sein. Nach zwei Jahren Planfeststellung bei der Regierung von Mittelfranken bin ich dann mit einer 13-jährigen Tätigkeit im Verwaltungsgericht Ansbach etwas zur Ruhe gekommen. Als mir dann aber die Leitung und der Aufbau einer neuen Behörde angeboten wurde, die aufgrund eines Urteils des Europäischen Gerichtshofs, wonach die Datenschutzaufsicht auch im nicht-öffentlichen Bereich völlig unabhängig sein muss, geschaffen werden musste, habe ich zugesagt und das schöne Richteramt aufgegeben. Was Datenschutz tatsächlich bedeutet und wie sich dieses Rechtsgebiet, das in fast alle anderen Rechtsgebiete hineinreicht, im täglichen Vollzug anfühlt, war mir damals auch nicht ansatzweise bewusst.

Auch Rechtsanwälte kommen tagtäglich und in verschiedenen Konstellationen mit dem Datenschutz in Kontakt, sei es bei der Zusammenarbeit mit Mandanten oder auch im Umgang mit

Mitarbeitern aus der eigenen Kanzlei. Wo sehen Sie hier die größten Risikofaktoren? Und kann man wirklich alle Gefahren ausschließen?

Rechtsanwälte sind ja nicht nur durch das Datenschutzrecht, sondern auch durch ihre Berufsordnung und insbesondere das Strafgesetzbuch zur Geheimhaltung personenbezogener Daten verpflichtet. Die Einhaltung des Datenschutzes im Sinne des Umgangs mit personenbezogenen Daten ist deshalb ein elementarer Bestandteil der Ausübung des Rechtsanwaltsberufs. Beschwerden haben wir in diesem Bereich fast nie. Bei der Frage der Datensicherheit sieht es etwas anders aus. Themen, die sich darauf beziehen, wie sicher die Kommunikation mit den Mandanten erfolgt, wie sicher die Speicherung der Daten ist, wer auf welche Daten in der Kanzlei zugreifen darf, wann Daten gelöscht werden oder auch die Frage, wie Papier oder sonstige Datenträger entsorgt werden, tauchen häufiger bei uns auf. Alle Gefahren kann man sicherlich nicht ausschließen, was aber nicht dazu verleiten sollte, sich deswegen um die Fragen der Datensicherheit gar nicht zu kümmern.

Sprechen wir in diesem Zusammenhang mal über das Thema Cloud-Computing. Die Möglichkeit, Daten im virtuellen Raum zu speichern und mit anderen mobilen Endgeräten zu synchronisieren, erleichtert natürlich auch die Arbeit von Anwälten. Doch welche Fallstricke lauern in der „Wolke“ und wie kann man seine Informationen am besten schützen?

Bei einem Cloud-Anbieter liegen enorme Datenmengen von sehr vielen Kunden. Dies kann Begehrlichkeiten von Seiten des Anbieters (Stichwort: Zweckänderung der Daten), von staatlichen Stellen (z.B. Geheimdienste) und Cyberkriminellen wecken. Eine effektive Überprüfung der technischen und organisatorischen Maßnahmen zur Eindämmung der Risiken kann zumindest bei Anbietern außerhalb Europas nur begrenzt stattfinden, da der Zugang zu den Räumlichkeiten sowie der Software kaum möglich ist. Es bleibt abzuwarten, welchen Stellenwert die genehmigten Zertifizierungen unter der DS-GVO ab Mai 2018 einnehmen werden. Auch darf nicht vergessen werden, dass bei der Auslagerung von Geschäftsprozessen an einen Cloud-Anbieter eine hohe Abhängigkeit bezüglich der Verfügbarkeit entsteht. Rechtsstreitigkeiten, ein defektes Tiefseekabel oder schlicht die Insolvenz des Cloud-Anbieters können

zu erheblichen Problemen für den Geschäftsbetrieb und damit auch der Sicherstellung der Verfügbarkeit der Systeme und Betroffenenrechte führen.

Womit müssen Anwälte seitens des Bayerischen Landesamtes für Datenschutzaufsicht rechnen, wenn sie den Anforderungen der Datenschutz-Grundverordnung nicht gerecht werden?

Grundsätzlich sind Anwälte im Sinne des Datenschutzrechts „verantwortliche Stellen“, so wie andere auch, und müssen bei festgestellten Verstößen mit Anordnungen oder Bußgeldern rechnen. Ich sagte „grundsätzlich“, weil bei Anwälten doch einiges anders ist, als bei anderen Stellen. Wir respektieren das Anwaltsgeheimnis jedenfalls insoweit, dass wir in keinem Fall in Mandantenakten hineinschauen. Dies bedeutet auch, dass wir in den meisten Beschwerdefällen, die Anwälte betreffen, nicht tätig werden. Diese Beschwerdefälle betreffen nämlich ganz überwiegend die Geltendmachung von datenschutzrechtlichen Auskunftsansprüchen beim gegnerischen Rechtsanwalt. Das heißt, ein Kläger oder Beklagter möchte – mit unserer Hilfe – vom Rechtsanwalt der Gegenpartei im Wege eines datenschutzrechtlichen Auskunftsanspruchs wissen, über welche Daten der Rechtsanwalt der Gegenpartei verfügt und woher er sie hat. Ein derartiger Anspruch ergibt sich für uns aus dem Datenschutzrecht nicht, sodass wir insoweit auch nicht tätig werden.

Dass im Übrigen die Bundesrechtsanwaltskammer die Auffassung vertritt, dass staatliche Datenschutzbehörden für Rechtsanwaltskanzleien überhaupt nicht zuständig sind, sehen wir und auch, die mit den entsprechenden Streitfällen befassten Gerichte, so nicht. Wie sich die Situation ab Mai 2018, wenn die Datenschutz-Grundverordnung und auch das neue Bundesdatenschutzgesetz wirksam werden, gestalten wird, bleibt abzuwarten.

Sie sagten eingangs, dass Sie auch Beschwerden und teils komplizierte Fallgestaltungen bearbeiten. Wie können wir uns diese Beschwerden vorstellen? Aus welchen Bereichen oder Branchen kommen und was beinhalten sie?

Wir haben pro Jahr etwa 1.400 Beschwerden. Die meisten Beschwerden stammen aus dem Bereich der Videoüberwachung. Nicht alle Kameras, die es bei Aldi, Lidl, Norma & Co. für unter 100 EUR gibt, werden dafür eingesetzt, zulässigerweise das eigene Grundstück zu überwachen sondern auch – datenschutzrechtlich unzulässig – festzuhalten, was die Nachbarschaft so treibt. Beschwerden im Zusammenhang mit der Nutzung des Internets oder auch aus dem Bereich der Werbung (Werbung trotz Werbewiderspruch oder per Mail ohne Vorliegen der dafür erforderlichen Einwilligung) folgen auf den nächsten Plätzen. Alle Beschwerden beinhalten den mehr oder weniger deutlich artikulierten Vorwurf, dass die verantwortliche Stelle mit den personenbezogenen Daten der Beschwerdeführer unzulässig umgeht. Abgesehen von ganz wenigen Fällen, bei denen wir uns sofort zu einer Beurteilung der Fallgestaltungen und Beantwortung der Beschwerde in der Lage sehen, holen wir grundsätzlich eine Stellungnahme ein und bewerten dann den Umgang mit den personenbezogenen Daten der Beschwerdeführer. Das Spannende und auch Herausfordernde daran ist, dass Datenschutz ein Querschnittsrechtsgebiet ist und deshalb Beschwerden aus allen Lebensbereichen zu uns kommen, die uns zwingen, auch in den entlegensten Rechtsgebieten zu suchen, ob es dort vielleicht eine Rechtsgrundlage für den Umgang mit personenbezogenen Daten geben könnte. Eine Situation, mit der auch Rechtsanwälte, die sich nicht auf ein sehr enges Rechtsgebiet spezialisiert haben, täglich umgehen müssen.

Ein Fall, der Sie in Ihrer bisherigen Amtszeit besonders bewegt hat. Gibt es da einen?

Ja, den gab es. Wir hatten einem selbst ernannten Hilfssheriff, der durch Übersenden von zahlreichen Anzeigen und Videomaterial der Polizei seine Hilfe aufgedrängt hat, verboten, mit seiner Dash-Cam, alles was ihm vor die Linse kam, aufzunehmen und diese Daten dann ohne Einwilligung der Betroffenen an Dritte weiterzugeben. Seine dagegen beim Verwaltungsgericht erhobene Klage hatte zwar aus formalen Gründen Erfolg, die materiell-rechtlichen Aussagen des Gerichts in dem Urteil, die unsere Auffassung voll und ganz unterstützt haben, waren und sind aber nach wie vor wegweisend für die verwaltungsgerichtliche Rechtsprechung zu diesem Themenkomplex.

1977 trat die erste Fassung des Bundesdatenschutzgesetzes in Kraft. Was hat sich seitdem getan? Welche entscheidenden Meilensteine gab es in der Entwicklung des Datenschutzrechts?

1977 war eine Zeit, in der die elektronische Datenverarbeitung im Wesentlichen durch Großrechner in Rechenzentren großer Unternehmen erfolgt ist. PCs, Handys oder Tablets wie wir sie heute kennen, gab es nicht, die Gründung von Google erfolgte erst 22 Jahre, die von Facebook erst 37 Jahre später. Digitalisierung steckte in den Kinderschuhen. Bezogen auf den Datenschutz bedeutete dies, dass man insbesondere sicherstellen musste, dass niemand in die Rechenzentren rein kommt, aber sonst schon fast nichts. Wenn wir heute einerseits auf das exponentiell gestiegene Datenvolumen und andererseits auf die Verfügbarkeit und Verknüpfbarkeit dieser Daten für fast alle von uns an fast jedem Ort der Welt schauen, kann man sich vorstellen, welche Veränderungen innerhalb kurzer Zeit eingetreten sind und welche Anforderungen an den datenschutzkonformen Umgang mit diesen personenbezogenen Daten und insbesondere an die Datensicherheit zu stellen sind.

Kann man hier sogar von einem Rollenwandel sprechen?

Ich denke, man kann ganz sicher von einem Rollenwandel sprechen. Zu Beginn der elektronischen Datenverarbeitung gab es wenige Stellen, die eine überschaubare Anzahl von Daten von uns verarbeitet haben. Man kann sich das vielleicht dadurch bewusst machen, wenn man die (wenigen) Daten betrachtet, die im Rahmen der Volkszählung im Jahr 1983 von den Bundesbürgern erhoben werden sollten und die damals zu massenhaften Demonstrationen geführt haben. Heute ist es so, dass wir alle mit unseren Smartphones, Tablets und auch PCs Daten in einem größeren Umfang und mit leistungsfähigeren Geräten verarbeiten, als dies in ganzen Rechenzentren der früheren Jahre möglich war. Bezogen auf den Rollenwechsel bedeutet dies aber auch, dass wir alle nunmehr nicht nur betroffene Personen sind, mit deren personenbezogenen Daten umgegangen wird, sondern gleichermaßen auch verantwortliche Stellen, die mit personenbezogenen Daten der anderen umgehen. Wir machen das nicht immer zulässig, wenn wir Bilder von Dritten ohne deren Einwilligung auf Facebook posten oder wenn wir beim Nutzen von WhatsApp permanent alle Kommunikationsdaten von unserem Endgerät an WhatsApp bzw. Facebook übermitteln, ohne diejenigen um ihr Einverständnis gefragt zu haben, deren

Daten wir in unseren Kontakten gespeichert haben. Datenschutz ist nicht mehr nur etwas, was die anderen machen müssen, sondern wir alle.

Die nächste Änderung im deutschen Recht steht bereits vor der Tür: Ab 2018 wird die neue EU Datenschutz Grundverordnung wirksam. Welche Bedeutung hat das für unser Rechtssystem? Und wie wirkt sich das neue Gesetz auf Ihre Arbeit aus?

Selbst wenn tragende Grundsätze des Datenschutzrechts, wie das „Verbot mit Erlaubnisvorbehalt“, das heißt, dass man mit personenbezogenen Daten nicht umgehen darf, es sei denn, man hat eine Einwilligung oder es gibt eine Rechtsgrundlage dafür, nach wie vor gelten, betrachte ich das kommende Datenschutzrecht als einen gewaltigen Einschnitt und eine Paradigmenwechsel. Wir haben dann, weil Rechtsgrundlage eine Verordnung und keine Richtlinien mehr ist, einen unmittelbar geltenden und in der ganzen EU einheitlichen Rechtsrahmen, der von uns auch so vollzogen werden muss, dass der Vollzug auch in anderen Mitgliedstaaten als akzeptabel angesehen werden kann. Lassen Sie mich das am Beispiel der Videoüberwachung erläutern, was ich meine: Wir haben zur datenschutzrechtlichen Beurteilung der Videoüberwachung in Zukunft nur mehr die gesetzliche Vorgabe, dass die Interessen des Verantwortlichen (Kamerabetreibers) mit den Rechten und Freiheiten der betroffenen Personen abgewogen werden müssen. Wenn Sie sich vor Augen halten, dass Sie in London, was dort scheinbar niemanden stört, fast keinen Schritt in der Öffentlichkeit machen können ohne gefilmt zu werden und sich dagegen die Diskussionen in Deutschland oder auch in Österreich um die Videoüberwachung im öffentlichen Bereich anschauen, wird es eine gewaltige Herausforderung werden, hier einheitliche Maßstäbe zu finden. Im Übrigen sehe ich in dem neuen Recht auch einen Paradigmenwechsel dahingehend, dass jeder, der mit personenbezogenen Daten umgeht, der Datenschutzaufsicht jederzeit nachweisen können muss, auf welcher Rechtsgrundlage er das macht und dass er auch die technischen Sicherheitsmaßnahmen einhält. Da fast jeder Verstoß gegen die Datenschutz-Grundverordnung auch einen Bußgeldtatbestand darstellt und der Bußgeldrahmen auf bis zu 20 Millionen oder 4 % des Weltjahresumsatzes eines Unternehmens festgelegt wurde, wird und muss sich im Datenschutz einiges bewegen.

Wie handhaben Sie Cloud-Computing, Onlinebestellungen & Co. privat?

Ich fahre nicht mit der Pferdekutsche, während andere mit dem Auto unterwegs sind. Ich nutze das Internet intensiv, um mich zu informieren, aber auch gelegentlich etwas zu bestellen. Dabei achte ich darauf, dass die Verbindung verschlüsselt ist und mein Vertragspartner möglichst in Deutschland, jedenfalls aber in der EU sitzt. Beim Herunterladen von Apps prüfe ich, ob die Berechtigungen, die die App für ihre Dienste einholt, erforderlich scheinen. Ich nutze E-Mail und auch einen Cloud-Service eines deutschen Anbieters. Dafür muss ich zwar den Gegenwert von etwa einer Tafel Schokolade pro Jahr bezahlen, bin dafür aber sicher, dass mit meinen Daten nichts gemacht wird, außer gut auf sie aufzupassen.

Das heißt Datensparsamkeit – ja oder nein?

Datensparsamkeit bedeutet für mich, dass ich insbesondere im Internet nur die Daten von mir preisgebe, die ich preisgeben will oder preisgeben muss, um bestimmte Gegenleistungen zu bekommen. Datensparsamkeit bedeutet auf der anderen Seite, dass Unternehmen nur die Daten erheben und verarbeiten dürfen, die sie für die Erfüllung eines legitimen Zwecks benötigen. Die Nutzung des Internets bedeutet nicht automatisch, dass man sich nicht datensparsam verhält.

Das Datenschutzgrundrecht gewährleistet, so hat es uns das Bundesverfassungsgericht ins Stammbuch geschrieben, die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einen sehr großen Beitrag zum Datenschutz können wir selbst leisten, wenn wir noch viel öfter unser Hirn einschalten, bevor wir Informationen über uns in die Welt hinaus posten. Alle Daten, die wir nicht preisgeben, können auch nicht missbraucht werden. Deshalb: einen besseren Datenschutz als Datensparsamkeit gibt es nicht.

Bildquellen: stevanovicigor/iStock/Bayerisches Landesamt für Datenschutzaufsicht