Editorial – Grußwort des Forschungsprojektleiters von «BayWiDI» Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

diesen Sommer gab es nicht nur im Bereich der COVID-19-Gesetzgebung Neuigkeiten. Auch in Sachen IT-Sicherheit gibt es neue Entwicklungen: Im Raum Halle/Leipzig wird es eine dedizierte Agentur für Innovation in der Cybersicherheit geben, deren Hauptaufgabe darin bestehen wird, neue digitale Entwicklungen auf ihre Konsequenzen für die Verteidigung und innere Sicherheit zu prüfen. Derzeit befindet sich die Agentur in der Gründungsphase; bis Ende 2020 sollen bereits erste Ideenwettbewerbe stattfinden und gezielt Forschungsaufträge vergeben werden. Laut Verteidigungsministerin Kramp-Karrenbauer entsteht hier ein „Meilenstein zum Schutz unserer IT-Systeme".[1] Die Diskussion um ein selbständiges Digitalministerium, die bereits seit längerer Zeit geführt wird, nahm ebenfalls wieder Fahrt auf, nachdem in einer Umfrage unter der Bevölkerung mehr als die Hälfte der Befragten ein eigenes übergeordnetes Ressort für digitalpolitische Themen auf Bundesebene befürworteten.[2]

Derweil stellte auch die Agentur der Europäischen Union für Cybersicherheit (ENISA) ihre neue IT-Sicherheitsstrategie vor, die die Cybersicherheit als wesentlichen Aspekt der EU-Politik herausstellt. Besonderes Augenmerk legt die Agentur dabei auf die Kooperation der verschiedenen Akteure auf mitgliedsstaatlicher und europäischer Ebene, durch die ein „Ökosystem" aus mitgliedsstaatlichen Behörden, EU-Institutionen, Forschungszentren und Universitäten entstehen soll, das darüber hinaus auch Wirtschaft und Bürgerinnen und Bürger einbinden soll.[3]

Man darf gespannt sein, wie sich die verschiedenen Ansätze in der kommenden Zeit weiterentwickeln. Eines ist jedenfalls sicher: Der Bedarf für spezialisierte Einrichtungen zu den eng verwobenen Themen Digitalisierung und IT-Sicherheit ist nicht nur vorhanden, er wächst mit der zunehmenden digitalen Durchdringung (fast) sämtlicher Lebensbereiche.

In dieser Ausgabe des BayWiDI-Magazins erwartet Sie zunächst ein Beitrag von Felix Sobala zu den Auswirkungen des Schrems II-Urteils des EuGH, in welchem das Privacy Shield für ungültig erklärt wurde. Anschließend wird Priska Katharina Büttel die Probleme rund um die Corona-Kontaktlisten näher beleuchten und sich dabei auch der Frage nach einer rechtskonformen Nutzung der erhobenen Daten durch Ermittlungsbehörden annehmen. Schließlich ist Peter Fischer mit einem praktischen Leitfaden vertreten, wie die Kontaktlisten rechts- und datenschutzkonform geführt werden können.

Ich wünsche Ihnen eine unterhaltsame Lektüre.

Ihr Prof. Dr. Dirk Heckmann

Leiter des Forschungsprojekts «BayWiDI»

1 *Leithäuser*, „Meilenstein zum Schutz unserer IT-Systeme", FAZ.net, 11.08.2020, letzter Abruf am 07.09.2020.

2 Vgl. die Pressemitteilung des eco-Verbands vom 12.08.2020, letzter Abruf am 07.09.2020.

3 Vgl. die Pressmitteilung der ENISA vom 17.07.2020, letzter Abruf am 07.09.2020.

Inhalt

- Eins, zwei, hoffentlich nicht drei – Schrems ist noch nicht vorbei / 2
- Die Daten aus Corona-Kontaktlisten sind nicht vogelfrei / 6
- Datenschutz- und rechtskonformer Umgang mit Corona-Kontaktlisten / 9
- Leiter des Forschungsprojekts und AutorInnen / 11
- Impressum / 12

Eins, zwei, hoffentlich nicht drei – Schrems ist noch nicht vorbei

Reaktionen und Konsequenzen nach dem „Schrems II-Urteil“

I. Vor dem Urteil ist nach dem Urteil

Mit einiger Spannung wurde das zweite Urteil „in Sachen Schrems“, das sogenannte „Schrems II-Urteil“ des EuGH[1] erwartet. Während es in „Schrems I“[2] um die Gültigkeit der „Safe Harbour“-Entscheidung ging, betraf das „Schrems II-Urteil“ die Gültigkeit der sogenannten „Privacy Shield“-Entscheidung der Europäischen Kommission, sozusagen die Nachfolgerin von „Safe Harbor“. Inhaltlich betrafen jedoch beide Verfahren – wenn auch unter unterschiedlichem ‚Etikett‘ – letztlich die Frage nach der Gewährleistung eines im Verhältnis zu europäischen Standards angemessenen Datenschutzniveaus bei Datentransfers aus der EU in die USA.

Bereits im Vorhinein machte man sich wohl auf ein erneutes mögliches Scheitern vor dem EuGH gefasst und setzte sich mit Alternativen im Falle einer Ungültigkeitserklärung des „Privacy Shields“ auseinander.[3] Insbesondere die Standardvertragsklauseln galten als mögliche Alternative für den befürchteten Ernstfall.

II. Das Urteil

Zu ebendiesem Ernstfall kam es: Mit Urteil vom 16.07.2020 erklärte der EuGH nun auch den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild („Privacy Shield“) gebotenen Schutzes für ungültig.[4] Hinsichtlich des Beschlusses 2010/87 der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern stellte der EuGH fest, dass die Prüfung anhand der Charta der Grundrechte der Europäischen Union nichts ergeben habe, was seine Gültigkeit berühren könne.

In Bezug auf die Standardvertragsklauseln sieht der EuGH keine Probleme aufgrund ihres Vertragscharakters, die somit Behörden eines Drittlandes nicht binden; entscheidend sei bei diesen vielmehr, ob wirksame Mechanismen enthalten seien, die tatsächlich sicherstellen könnten, dass das durch das Unionsrecht vorgesehene Schutzniveau personenbezogener Daten eingehalten werde und dass auf diese Klauseln gestützte Übermittlungen ausgesetzt oder verboten werden, wenn Verstöße festgestellt werden sollten oder diese nicht eingehalten werden könnten.[5] Datenexporteure sowie -importeure müssten im Zuge einer Übermittlung vorab prüfen, ob das notwendige Schutzniveau im betreffenden Drittstaat eingehalten werde. Datenempfänger müssten den Datenexporteuren mitteilen, falls diese die Standardvertragsklauseln nicht einhalten könnten, daraufhin müsse die Übermittlung ausgesetzt werden und/oder die Exporteure müssten von den entsprechenden Verträgen mit den Empfängern zurücktreten. Folglich beinhalte der Beschluss 2010/87 die notwendigen Maßnahmen.

Obwohl der EuGH somit hinsichtlich des Beschlusses 2010/87 über die Standardvertragsklauseln nicht an dessen Gültigkeit zweifelt, muss das aber nicht bedeuten, dass eine Datenübermittlung auf deren Grundlage nun stets unproblematisch erfolgen kann. Der EuGH richtet sich an die Aufsichtsbehörden – und das sollte der Praxis eine Warnung sein –, indem er ausführt, *„dass die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, verpflichtet ist, eine auf Standarddatenschutzklauseln, die von der Kommission erarbeitet wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn die Behörde im Lichte aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.“*[6] Zwar könne es Situationen geben, in denen eine Übermittlung in Anbetracht der Rechtslage und der Praxis mit dem erforderlichen Datenschutz im betreffenden Drittland allein auf Grundlage der Standarddatenschutzklauseln garantiert werden könne, aber auch Situationen, in denen die in diesen enthaltenen Regelungen möglicherweise kein ausreichendes Mittel darstellten, um effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten.[7]

1 *EuGH*, Urt. v. 16.07.2020 – C-311/18 („Schrems II“).

2 *EuGH*, Urt. v. 06.10.2015 – C-362/14 („Schrems I“).

3 Siehe dazu die Antwort des EU-Kommissars für Justiz und Rechtsstaatlichkeit, Didier Reynders, auf eine parlamentarische Anfrage des Europaabgeordneten Moritz Körner, *Reynders*, Parlamentarische Anfrage, 19. Mai 2020, Antwort von Didier Reynders im Namen der Europäischen Kommission, Bezugsdokument E-001120/2020, letzter Abruf am 07.09.2020, dort auch zum Folgenden.

4 *EuGH*, siehe Fn. 1, dort auch zum Folgenden.

5 *EuGH*, siehe Fn. 1, Rn. 122–149, dort auch zum Folgenden.

6 *EuGH*, siehe Fn. 1, Rn. 121.

7 *EuGH*, siehe Fn. 1, Rn. 126.

Somit nimmt der EuGH die in der Union ansässigen Verantwortlichen beziehungsweise Auftragsverarbeiter in die Pflicht, es ist so,

„dass es gemäß Art. 46 Abs. 1 DSGVO, falls kein Angemessenheitsbeschluss der Kommission vorliegt, Sache des in der Union ansässigen Verantwortlichen bzw. des dort ansässigen Auftragsverarbeiters ist, insbesondere geeignete Garantien vorzusehen. Die Erwägungsgründe 108 und 114 dieser Verordnung bestätigen, dass der Verantwortliche oder gegebenenfalls sein Auftragsverarbeiter, wenn sich die Kommission nicht zur Angemessenheit des Datenschutzniveaus in einem Drittland geäußert hat, ‚als Ausgleich für den [im] Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Personen vorsehen [sollte]' und dass ‚[d]iese Garantien … sicherstellen [sollten], dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessenen Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen … in der Union oder in einem Drittland'"[8].

Aufgrund dessen, dass die Standardvertragsklauseln keine drittstaatlichen Behörden binden könnten, das durch DSGVO vorgesehene Schutzniveau jedoch nicht beeinträchtigt werden dürfe, könne es sich als notwendig erweisen, die in den Klauseln enthaltenen Garantien zu ergänzen.[9] Die von der Kommission erlassenen Standarddatenschutzklauseln zielten somit nur darauf ab, den in der Union ansässigen Verantwortlichen bzw. ihren dort ansässigen Auftragsverarbeitern vertragliche Garantien zur Verfügung zu stellen, die in allen Drittländern einheitlich gälten – unabhängig vom dort jeweiligen Schutzniveau; sie könnten jedoch keine Garantien, für das unionsrechtlich verlangte Schutzniveau zu sorgen, bieten, die über die vertraglichen Verpflichtungen hinausgingen, es könne daher – je nach Lage – erforderlich sein, zusätzliche Maßnahmen zu ergreifen.[10] *„Folglich obliegt es vor allem diesem Verantwortlichen bzw. seinem Auftragsverarbeiter, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren. Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden. Dies ist insbesondere dann der Fall, wenn das Recht dieses Drittlands dem Empfänger aus der Union übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und daher geeignet sind, die vertragliche Garantie eines angemessenen Schutzniveaus hinsichtlich des Zugangs der Behörden dieses Drittlands zu diesen Daten zu untergraben."*[11]

„Insoweit muss […] die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, […] eine solche Übermittlung aussetzen oder verbieten, wenn sie im Licht aller Umstände der Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet."[12]

III. Reaktionen und Konsequenzen

Nach dieser Entscheidung ist die Verunsicherung in der datenverarbeitenden Praxis groß: Viele Unternehmen fragen sich, ob sie selber aufgrund der entschiedenen Aspekte zur Anpassung ihrer Datenverarbeitungsprozesse – womöglich gar zur Einstellung – aufgefordert sind. Zwar wurde direkt und ausdrücklich lediglich das „Privacy Shield" als Datentransfergrundlage in die USA für ungültig erklärt, jedoch äußerte sich der EuGH auch zu den Anforderungen im Zuge der Verwendung von Standardvertragsklauseln, für deren rechtmäßigen Einsatz gegebenenfalls Maßnahmen zur Gewährleistung eines entsprechenden Sicherheitsniveaus vorzusehen sind. In Folge der Ungültigkeitserklärung des „Privacy Shields" ist jedoch nicht ganz klar, ob und wie die Praxis diesen gestellten Anforderungen im Falle von USA-Datentransfers unter Verwendung von Standardvertragsklauseln überhaupt gerecht werden kann.[13]

1. Drastische oder sehr vage Ansichten und Ratschläge

Die vertretenen Ansichten reichen von Extrempositionen mit drastischen Handlungsaufforderungen über eher gemäßigte, zurückhaltende Stellungnahmen bis zu lediglich vagen und oberflächlichen Ratschlägen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit forderte datenverarbeitende Stellen in Berlin auf, „in den USA gespeicherte personenbezogene Daten nach Europa

8 *EuGH*, siehe Fn. 1, Rn. 131.

9 *EuGH*, siehe Fn. 1, Rn. 132.

10 *EuGH*, siehe Fn. 1, Rn. 133

11 *EuGH*, siehe Fn. 1, Rn. 134f.

12 *EuGH*, siehe Fn. 1, Rn. 146.

13 Vgl. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegenüber Golem.de bei *Greis*, Keine Schonfrist mehr beim Datenschutz, 22.07.2020, Golem.de, letzter Abruf am 07.09.2020.

zu verlagern".[14] Der EuGH habe zu weitreichende Zugriffsmöglichkeiten der US-Behörden auf Daten europäischer Bürgerinnen und Bürger festgestellt, was zur Folge habe, dass personenbezogene Daten bis zu einer Änderung der Rechtslage – abgesehen von bestimmten gesetzlichen Ausnahmen – in aller Regel nicht mehr wie bisher in die USA übermittelt werden dürften. Auf eine der Alternativen zum „Privacy Shield", die Standardvertragsklauseln, geht die Berliner Datenschutzbeauftragte zwar ebenfalls ein und sieht eine grundsätzliche Einsatzmöglichkeit zur Herstellung eines gleichwertigen Datenschutzniveaus – bei Erfüllung der durch den EuGH betonten Anforderungen –, fordert aber dennoch: „Verantwortliche, die – insbesondere bei der Nutzung von Cloud-Diensten – personenbezogene Daten in die USA übermitteln, sind nun angehalten, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln."[15] Ihrer Ansicht nach hat der EuGH „grundsätzlich klar gemacht, dass die Übermittlung personenbezogener Daten in die USA weder mit dem Privacy Shield, [sic] noch mit Standardvertragsklauseln oder Binding Corporate Rules (BCR) möglich ist".[16]

Der Vorsitzende des Bundesverbandes IT-Sicherheit (TeleTrusT), Karsten Bartels, erklärte, dass das Urteil „für die betroffenen Unternehmen große Rechtsunsicherheit" schaffe und bemängelte, dass nun eine „langfristige und verlässliche Absicherung des Datentransfers in die USA fehlt".[17] Wolle man die nun bestehenden Risiken gänzlich vermeiden, müsse man eine „Verarbeitung in Europa unter ausschließlicher Kontrolle europäischer Unternehmen" sicherstellen.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Prof. Ulrich Kelber, äußerte sich folgendermaßen: „Standardvertragsklauseln sind weiterhin eine mögliche Grundlage für den Datentransfer. Eine Übermittlung von Daten in die USA kann allerdings nur dann über Standardvertragsklauseln begründet werden, wenn zusätzliche Maßnahmen getroffen werden, die das gleiche Datenschutzniveau wie in der Europäischen Union gewährleisten. Dabei müssen die Umstände der Datentransfers von Fall zu Fall betrachtet werden. Das gilt auch für die Übermittlung in andere Länder".[18]

Der Europäische Datenschutzausschuss hat in Reaktion zum Urteil und zur Beantwortung der nun akut aufgeworfenen Fragen FAQs erstellt, die im Verlauf der weiteren Auseinandersetzung mit dem Urteil fortlaufend ergänzt werden sollen.[19] Zwar wird im Rahmen dieses Dokumentes sowohl auf den Einsatz von Standardvertragsklauseln als auch von verbindlichen internen Datenschutzvorschriften eingegangen, insgesamt bleibt es dabei jedoch auf einer sehr allgemeinen Ebene und stellt lediglich fest, dass – je nach konkretem Fall – entsprechende Maßnahmen getroffen werden müssten; welche konkret diese sein könnten oder sollten, wird (derzeit) weiteren Ausführungen, die noch folgen sollen, vorbehalten.[20] Mithin geht die Hilfestellung des Europäischen Datenschutzausschusses durch diese FAQs (momentan) noch nicht wesentlich über die Feststellungen des EuGH hinaus. Die Aussagen zu den Ausnahmen nach Art. 49 DSGVO erschöpfen sich in knappen Hinweisen zur Einwilligung, zur Vertragserfüllung gegenüber dem Betroffenen sowie zu den wichtigen Gründen des öffentlichen Interesses; im Großen und Ganzen wird auf die maßgeblichen Leitlinien[21] des Europäischen Datenschutzausschusses verwiesen.[22] Hervorgehoben wird aber – und das wird der entscheidende Knackpunkt in der Praxis sein, die sich nicht auf die weitere Verwendung der Standardvertragsklauseln mit ihren derzeit notwendigen, aber ungewissen Maßnahmen im Zusammenhang mit Datentransfers in die USA verlassen will –, dass „der allgemeine Grundsatz beachtet werden [muss], wonach die Ausnahmen gemäß Artikel 49 DSGVO in der Praxis nicht zur ‚Regel' werden dürfen, sondern auf bestimmte Situationen beschränkt bleiben müssen, wobei jeder Datenexporteur sicherstellen muss, dass die Übermittlung der strengen Notwendigkeitsprüfung entspricht."[23]

2. Erste Abhilfemöglichkeiten

„Einsicht ist der erste Schritt zur Besserung", das besagt ein Sprichwort. Um nun als für die Datenverarbeitung Verantwortlicher festzustellen, ob man aufgrund des „Schrems II-Urteils" Anpassungen vornehmen oder Abhilfe im Rahmen der eigenen Datenverarbeitung schaffen muss, ist es zunächst wichtig, „Einsicht" – im Sinne von Einblick – in die eigenen zu verantwortenden Datentransferprozesse zu nehmen. Lobenswert ist, dass Max Schrems nicht nur mit dem ‚erhobenen Zeigefinger' gegenüber Datenverarbeitenden agiert, sondern auch konstruktiv zur Datenschutzpraxis beiträgt. Sehr anschaulich hat das Europäische

14 *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Pressemitteilung 711.424.1 vom 17.07.2020, letzter Abruf am 13.08.2020, S. 1, dort auch zum Folgenden.

15 *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, siehe Fn. 14, S. 2.

16 So auf Nachfrage gegenüber Golem.de bei *Greis*, siehe Fn. 13.

17 So bei *Krempl*, Datenschutzbeauftragte zum Privacy Shield: Nutzer können Schmerzensgeld verlangen, 20.07.2020, Heise.de, letzter Abruf am 07.09.2020, dort auch zum Folgenden.

18 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, EDSA beschließt FAQ zu Schrems II, Pressemitteilung 19/2020 vom 24.07.2020, letzter Abruf am 07.09.2020.

19 *EDPB – European Data Protection Board*, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems, Angenommen am Donnerstag, 23. Juli 2020 (allerdings noch nicht geprüfte Übersetzung), letzter Abruf am: 07.09.2020.

20 *EDPB – European Data Protection Board*, siehe Fn. 19, insbesondere S. 6.

21 Siehe *EDPB – European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, angenommen am 25. Mai 2018, letzter Abruf am 07.09.2020.

22 *EDPB – European Data Protection Board*, siehe Fn. 19, S. 4 f.

23 *EDPB – European Data Protection Board*, siehe Fn. 19, S. 5.

Zentrum für digitale Rechte (NOYB), die Datenschutz-NGO von Max Schrems, FAQs hinsichtlich der Konsequenzen durch das Urteil, Handlungsempfehlungen sowie Musterfragebögen für US-Anbieter oder Anbieter mit US-Bezug veröffentlicht[24], die den nun möglicherweise betroffenen für die Datenverarbeitung Verantwortlichen die ersten notwendigen Schritte erleichtern und dabei helfen können, einen Überblick über die eigenen Datentransferprozesse zu gewinnen sowie Handlungsoptionen zu evaluieren.

IV. Nach dem Urteil ist (hoffentlich nicht) vor dem Urteil

Während der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kurz nach der Entscheidung noch davon ausging, es liege im aufsichtsbehördlichen „Ermessen, zunächst auf Änderungen hinzuwirken, ohne Anordnungen oder Bußgelder zu erlassen, wenn Unternehmen nachvollziehbar darlegen, aus welchen Gründen sie noch einige Zeit benötigen, um die Gerichtsentscheidung umzusetzen“,[25] erhöht sich nun für einige Unternehmen schlagartig der Druck. Manche Unternehmen scheinen sich nämlich dem bereits oben erwähnten Satz „Einsicht ist der erste Schritt zur Besserung“ – und dieses Mal ist „Einsicht“ im Sinne von Bewusstwerdung gemeint – gänzlich zu widersetzen und an ihrer geübten Datentransferpraxis auch im Nachgang zum „Schrems II-Urteil“ unverändert festzuhalten. Max Schrems’ Datenschutz-NGO reichte in der Folge Beschwerden gegen 101 Unternehmen ein, die ihre Datenverarbeitung nicht den Vorgaben des Urteils angepasst hatten.[26] Auch Facebook zeigt sich (bisher) unbeeindruckt von den strengen Anforderungen, die der EuGH an Datenübermittlungen in die USA stellt, und beruft sich[27] auf die Alternative der Standardvertragsklauseln – und das obwohl auch deren Belastbarkeit als Übertragungsgrundlage ja derzeit mehr als umstritten und fraglich ist.[28] Die EU-Kommission möchte indessen die Standardvertragsklauseln überarbeiten und den Vorgaben des EuGH-Urteils anpassen. Es ist jedoch unklar, inwiefern diese Klauseln überhaupt einen adäquaten Schutz gewährleisten können sollen, der über den des ehemaligen „Privacy Shields“ hinausgeht, das ja gerade keine hinreichenden Sicherheiten für ein adäquates Datenschutzniveau in den USA bieten konnte. Diese Tauglichkeit bezweifelt auch Max Schrems, der sich jedoch aufgrund der immensen Bedeutung, die der europäische Markt für die US-Konzerne habe, insgesamt zuversichtlich gestimmt im Hinblick auf die Aushandlung eines neuen Abkommens der EU mit den USA zeigt.

Wir werden sehen, in welcher Form und Strenge die Aufsichtsbehörden in kommender Zeit aufgrund des Urteils – und Max Schrems’ Beschwerden – durchgreifen werden. Viele Fragen hinsichtlich der Konsequenzen des Schrems II-Urteils sowie der Zukunft im Hinblick auf Datenübertragungen in die USA sind somit derzeit offen oder nur sehr unklar und vage zu beantworten. Es bleibt spannend und hoffentlich ist diesmal nach dem Urteil nicht wieder vor dem Urteil.

Felix Sobala

24 *NOYB – Europäisches Zentrum für digitale Rechte*, Nächste Schritte für EU-Unternehmen & FAQs, 20.07.2020, letzter Abruf am 07.09.2020.

25 So bei *Greis*, siehe Fn. 13.

26 *NOYB – Europäisches Zentrum für digitale Rechte*, 101 Complaints on EU-US transfers filed, 17.08.2020, letzter Abruf am 07.09.2020.

27 *Facebook*, Updating our international data transfer mechanisms, 17.08.2020, letzter Abruf am 07.09.2020.

28 *Fanta*, Facebook schickt weiter Daten in die USA, 03.09.2020, Netzpolitik.org, letzter Abruf am 07.09.2020, dort auch zum Folgenden.

Die Daten aus Corona-Kontaktlisten sind nicht vogelfrei

Die Eindämmung der Verbreitung von SARS-CoV-2 in Deutschland darf – leider – als gescheitert bezeichnet werden. Ein (mehr oder weniger hohes) Infektionsrisiko besteht in allen Teilen des Landes. Auch wenn sich die Ausbreitung an sich nicht verhindern lässt, so sind doch Bestrebungen, die Infektionsrate in Schach zu halten, wichtig und sinnvoll. Wie der Balanceakt zwischen komplettem Lockdown und sorgloser Freiheit, zwischen Gesundheitsschutz und Schutz der Wirtschaft zu schaffen ist, ist naturgemäß nicht leicht zu beantworten.

Nachverfolgung: Richtiges Ziel, falscher Weg?

Ein wichtiger Punkt ist sicherlich die Nachverfolgung von Infektionsketten und die Benachrichtigung der Kontaktpersonen von Infizierten, sodass diese ihrerseits vermeiden können, weitere Personen anzustecken. Problematisch sind vor allem die sogenannten „Superspreader“ – häufig symptomfrei Erkrankte, die besonders viele weitere Personen anstecken.[1] Um hier schnell einschreiten zu können, werden allerorts Corona-Kontaktlisten geführt; beim Besuch von Restaurants, Fitnessstudios, Friseursalons und vielen anderen Einrichtungen müssen die Kontaktdaten hinterlegt werden.

Dass der Bedarf für eine schnelle und unkomplizierte Erfassung von Besucher- und Besucherinnendaten durch die Pandemie verhältnismäßig plötzlich auftrat, darf keine Rechtfertigung für halbgare Lösungen sein. Wie aber können die Listen datenschutz- und allgemein rechtskonform geführt werden? Einen praktischen Leitfaden finden Sie in diesem Magazin auf Seite 9.

Das Problem liegt jedoch nicht allein in der Erfassung selbst.

Das Problem des Missbrauchs der Kontaktlisten

Wie leicht die einmal erhobenen Kontaktdaten in falsche Hände geraten können, zeigte sich zuletzt durch eine Aktion des Chaos Computer Clubs (CCC), der Ende August öffentlich machte, wie leicht die Daten aus einer weit verbreiteten Gastronomie-Software abgreifbar waren, die zur Verwaltung von Reservierungen, Bestellungen und eben auch Corona-Kontaktlisten genutzt wird. Die CCC-Hackerinnen und -Hacker konnten auf über 87.000 Corona-Datensätze und knapp fünf Millionen Datensätze von Reservierungen zugreifen, die teilweise über ein Jahrzehnt zurückreichten. Der CCC wies dabei auf mehrere Schwachstellen hin: unzureichendes Rechte-Management und schlecht geschützte Passwörter sind nur zwei Sicherheitslücken, die an sich mit einem sinnvollen IT-Sicherheits-Konzept verhältnismäßig leicht geschlossen werden könnten.[2] Immerhin reagierte der Cloud-Anbieter schnell, die Lücken seien laut einem Sprecher des Unternehmens bereits geschlossen worden. Der CCC rät derweil von digitalen Listen ab, da diese oft „mit der heißen Nadel gestrickt“ und die sensiblen Daten nicht ausreichend geschützt seien.[3] Wenig später nahm sich der Club einer weiteren Software an. Auch hier konnten hunderttausende Datensätze ausgelesen werden, die aber immerhin verschlüsselt waren, sodass der Zugriff auf die bestehenden persönlichen Informationen nicht möglich war – wohl aber das Abgreifen neu zu erfassender Einträge für die Zukunft.[4]

Demgegenüber sind auch Papierlisten kein Allheilmittel. Werden fortlaufende Listen geführt, kann etwa jeder Gast eines Restaurants die Kontaktdaten früherer Besucherinnen und Besucher einsehen. Eine Stichprobenuntersuchung in Hamburg hatte im Juli ergeben, dass ein Drittel der kontrollierten Gewerbe- und Gaststättenbetriebe die Listen offen für jedermann zugänglich herumliegen ließen.[5] Da verwundert es nicht, dass so manch einer lieber einen falschen Namen und eine erfundene Adresse einträgt.

Die unzureichend geschützten Daten sind aus mehreren Gesichtspunkten problematisch. Nicht nur lassen sich – etwa bei Stammgästen – detaillierte Verhaltensprofile erstellen, um den bestmöglichen Zeitpunkt für einen Einbruch in deren pünktlich zum Mittagessen leere Wohnung zu bestimmen. In einem anderen Fall wurde eine Restaurantbesucherin unter der angegebenen Mobilfunknummer später „zu privaten Zwecken“ kontaktiert.[6] Auch die Nutzung der Daten im Rahmen polizeilicher Ermittlungen widerspricht dem erklärten Zweck der Listen. Ein Fall, der für Aufsehen sorgte, ereignete sich Anfang Juli in Hamburg:

Nachdem ein Mann in einem Lokal angeblich Gäste mit einem Teppichmesser bedroht hatte, nutzte die Polizei die Corona-Kontaktliste des Restaurants und kontaktierte die dort genannten Personen, um mögliche Augenzeugen

1 Vgl. *Furuse et al.*, Clusters of Coronavirus Disease in Communities, EID Journal, Vol. 26, No. 9 – September 2020; vgl. auch *Uhlmann*, Das Rätsel um die stillen Kranken, SZ.de, 29.05.2020, jeweils letzter Abruf am 03.09.2020.

2 Vgl. *Neumann*, CCC hackt digitale „Corona-Listen“, CCC.de, 28.08.2020; *Biselli*, Sicherheitslücke bei digitalen Coronalisten entdeckt, Golem.de, 28.08.2020, jeweils letzter Abruf am 03.09.2020.

3 Vgl. *Reuter*, CCC hackt Corona-Kontaktlisten aus beliebter Restaurantsoftware, Netzpolitik.org, 28.08.2020, letzter Abruf am 03.09.2020.

4 Vgl. *Scherschel*, CCC deckt erneut Schwachstellen in Corona-Listen auf, Heise Online, 03.09.2020, letzter Abruf am 03.09.2020.

5 Vgl. *Greis*, Polizei nutzt Corona-Kontaktlisten nach Straftat, Golem.de, 06.07.2020, letzter Abruf am 03.09.2020.

6 Vgl. *Greis*, Datenschützer kritisieren offene Gästelisten, Golem.de, 25.06.2020, letzter Abruf am 03.09.2020.

ausfindig zu machen.[7]

Der Landesdatenschutzbeauftragte Hamburgs, Johannes Caspar, bringt das Problem auf den Punkt: „Wo Daten zulässigerweise erhoben werden, [ergeben] sich immer wieder weitergehende Begehrlichkeiten" für andere, neue Zwecke.[8] Doch welche rechtlichen Rahmenbedingungen kommen hinsichtlich der Corona-Kontaktlisten zum Zuge – und sind diese überhaupt mit dem geltenden (Verfassungs-)Recht vereinbar?

Uneinheitliche Rechtsgrundlagen in den Ländern

Zur Bekämpfung übertragbarer Krankheiten sind gemäß Art. 80 Abs. 1 GG i.V.m. § 32 Satz 1 IfSG die Länder zum Erlass von Rechtsverordnungen ermächtigt. Demzufolge ergibt sich die jeweilige Verpflichtung (oder in manchen Ländern Berechtigung) der Betriebe zum Erfassen der Daten aus verschiedenen landesrechtlichen Regelungen.[9]

Teilweise verbleibt jedoch – je nach Formulierung – ein gewisser Interpretationsspielraum hinsichtlich der Pflicht zur Datenerhebung. In einigen Regelungen waren bis vor kurzem noch Soll-Vorschriften oder (jedenfalls dem Wortlaut nach) eine Wahlmöglichkeit in Bezug auf die Listenführung zu finden. Inzwischen wird in den verschiedenen Neufassungen und Aktualisierungen zumindest in Bezug auf die Pflicht zur Datenerhebung durchaus auf eine eindeutige Formulierung geachtet.

Uneinheitlich sind auch die Regelungen dazu, wer zu welchen Zwecken auf die erhobenen Daten zugreifen darf. In Hamburg etwa ist gemäß § 7 Abs. 1 Nr. 3 HmbSARS-CoV-2-EindämmungsVO nur „die zuständige Behörde" zur Verarbeitung der Daten befugt, Nr. 5 zufolge sind „die Verwendung der Kontaktdaten zu anderen als den […] genannten Zwecken sowie deren Weitergabe […] untersagt". Eine dem Zweck der Erhebung widersprechende Nutzung durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung – wie im oben geschilderten Fall zur Suche nach Zeugen – wird jedoch in anderen Gesetzen durch die Hintertür wieder erlaubt.[10] Soweit der Zugriff tatsächlich aus besonders gewichtigen Gründen – bei Straftaten gegen das Leben beispielsweise – erfolgt, mag es durchaus gerechtfertigt sein. Es zeigte sich allerdings, dass die Listen z.B. in Bayern auch für Ermittlungen im Rahmen der Drogenkriminalität, bei Eigentumsdelikten oder zur Gefahrenabwehr genutzt wurden.

Der bayerische Innenminister Herrmann sprach in diesem Zusammenhang von „Kapitalverbrechen", ohne diese Behauptung näher zu belegen.[11] Äußerst fragwürdig ist diese Sichtweise nicht erst dann, wenn (wie in Baden-Württemberg und Mecklenburg-Vorpommern im Frühjahr geschehen) durch die Gesundheitsämter auch sensible Gesundheitsdaten mit übermittelt werden.[12] Inzwischen hat Herrmann seine Aussagen relativiert; es war bekannt geworden, dass die Daten auch für Ermittlungen wegen Fahrerflucht, Diebstahl oder Beleidigung genutzt wurden. Dabei sah das Innenministerium keinen Anlass, die betroffenen Gäste über die Datenauswertung zu informieren.[13]

Der Zugriff durch Ermittlungsbehörden und die Doppeltür-Rechtsprechung des Bundesverfassungsgerichts

Die grundsätzlich verbindliche – wenn auch nicht gänzlich unumstrittene – Rechtsprechung des BVerfG zur Bestandsdatenauskunft wird dabei weitestgehend ignoriert. Zwar wird die grundsätzliche Verfassungsmäßigkeit der Auskunft über Bestandsdaten nicht beanstandet. Es müsse jedoch in jedem Fall entweder eine konkrete Gefahr im Einzelfall oder der Anfangsverdacht einer Straftat vorliegen.[14] Sowohl die Übermittlung als auch der Abruf der Daten müssen jeweils für sich genommen auf verhältnismäßigen Rechtsgrundlagen beruhen, die die Verwendungszwecke der Daten ausreichend begrenzen und an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden.[15] Dieser Rechtsgedanke ist auch auf die Nutzung der Corona-Kontaktlisten-Daten zu übertragen. Insofern fehlt „den Türen der ‚Kontaktnachverfolgung' […] jeweils ein Flügel".[16]

In diesem Kontext ist auch die Entscheidung des saarländischen Verfassungsgerichtshofes zu nennen, der Art. 2 § 3 der Verordnung zur Änderung infektionsrechtlicher Verordnungen zur Bekämpfung der Corona-Pandemie (VO-CP) unter Bezugnahme auf die Bestandsdatenauskunft-II-Entscheidung des BVerfG für mit der Landesverfassung unvereinbar erklärte, da es

7 Vgl. *Greis*, Polizei nutzt Corona-Kontaktlisten nach Straftat, Golem.de, 06.07.2020, letzter Abruf am 03.09.2020.

8 *Greis*, Polizei nutzt Corona-Kontaktlisten nach Straftat, Golem.de, 06.07.2020, letzter Abruf am 03.09.2020.

9 Z.B. § 2a CoronaSchVO (Nordrhein-Westfalen), § 3 SARS-CoV-2-Infektionsschutzverordnung (Berlin), Unterpunkt 3.2.9. der Bekanntmachung des Bayerischen Gesundheitsministeriums vom 14.05.2020 zum Vollzug des IfSG (Stand 17.07.2020) (Bayern) oder § 6 Abs. 1 i.V.m. § 14 Satz 1 CoronaVO (Baden-Württemberg) (jeweils in der am 03.09.2020 geltenden Fassung).

10 Vgl. z.B. § 23 BDSG, Strafverfolgungsbehörden berufen sich i.d.R. auf §§ 160 ff. StPO.

11 Vgl. *Laufer*, Polizei nutzt Corona-Kontaktlisten für Drogenermittlungen, Netzpolitik.org, 31.07.2020, letzter Abruf am 04.09.2020.

12 Vgl. *Laufer*, Polizei sammelt in mehreren Bundesländern Coronavirus-Listen, Netzpolitik.org, 02.04.2020, letzter Abruf am 05.09.2020.

13 Vgl. *Krempl*, Bayerische Polizei: Mit Corona-Gästelisten gegen Kleinkriminalität, Heise Online, 03.09.2020, letzter Abruf am 07.09.2020.

14 BVerfG, Beschl. v. 27.05.2020 – 1 BvR 1873/13; vgl. m. Anm. *Nolte/Krenke* jurisPR-ITR-Compl 4/2020 Anm. 2.

15 Vgl. BVerfG, Beschl. v. 27.05.2020 – 1 BvR 1873/13 LS. 1

16 Vgl. *Härting*, Corona ohne „Doppeltür": Warum die Vorschriften zur Sammlung von Kontaktdaten in der Gastronomie verfassungswidrig sind., CR-online.de Blog, 02.08.2020, letzter Abruf am 03.09.2020.

einer förmlichen, parlamentarischen Ermächtigung bedürfe, die die zu erhebenden personenbezogenen Daten, den Anlass und spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regelt und den Grundsatz der Verhältnismäßigkeit wahrt.[17] Das IfSG enthalte gerade keine solche Ermächtigung.[18] Art. 2 § 3 VO-CP sei zudem geeignet, die Intensität des Eingriffs zu verharmlosen und zu verunklaren.[19] Es bleibt zu hoffen, dass diese Frage konkret auf die Corona-Kontaktlisten-Daten bezogen auch für andere landesrechtliche Regelungen (die i.d.R. zumindest sinngemäß gleich lauten) verfassungsgerichtlich geklärt wird.

Fazit

Die Verarbeitung der im Zusammenhang mit Corona-Kontaktlisten gesammelten personenbezogenen Daten muss eindeutig und vernünftig geregelt werden. Der Wunsch des hamburgischen Datenschutzbeauftragten, die Ermittlungsbehörden mögen von der Nutzung der Corona-Daten entgegen dem ursprünglichen Zweck nur „äußerst zurückhaltend“ Gebrauch machen, „um die Akzeptanz der Maßnahmen zur Eindämmung der Epidemie in der Bevölkerung nicht zu gefährden“, ist zu unverbindlich.[20]

Sowohl die Übermittlung der Listen an Gesundheitsämter und deren Befugnisse zur Nutzung der Daten als auch – insbesondere – der Zugriff durch Strafverfolgungsbehörden sind hinsichtlich des Umfangs und der zulässigen Zwecke der Abfragen zu klären. Andernfalls ist zu befürchten, dass vermehrt falsche Kontaktdaten angegeben werden – und das Ziel der Nachverfolgbarkeit und Eingrenzung künftiger Infektionsketten so ausgehebelt wird.[21]

Bei der Entwicklung der Corona-Warn-App zeigte sich, dass ein Kompromiss aus Nachverfolgbarkeit und Datenschutz durchaus machbar ist. Für die Kontaktlisten in Lokalen, Fitnessstudios usw. sollte kein geringerer Standard angestrebt werden. Bis eine – verfassungs- und DSGVO-konforme – Lösung geschaffen wird, sollten Gastronomen und Gastronominnen und Betreiber sowie Betreiberinnen anderer Einrichtungen, für die eine Kontaktdatenerhebungspflicht besteht, die Herausgabe der so gesammelten Daten an Ermittlungsbehörden zu verweigern und auf einen entsprechenden Beschlagnahmebeschluss bestehen..[22]

Priska Katharina Büttel

17 Vgl. zuletzt BVerfG, Beschl. v. 27.05.2020 – 1 BvR 1873/13.

18 VerfGH Saarbrücken, Beschl. v. 13.05.2020 – 2 B 175/20 – Lv 15/20 S. 27 f.

19 VerfGH Saarbrücken, Beschl. v. 13.05.2020 – 2 B 175/20 – Lv 15/20 S. 31.

20 Vgl. Ist das erlaubt? Hamburger Polizei nutzt Corona-Kontaktliste zur Zeugensuche, MoPo.de, 08.07.2020, letzter Abruf am 04.09.2020.

21 Vgl. *Meißner*, Corona.Kontakt-Listen als Ermittlungsansatz in Strafverfahren?, Beck-Blog, 09.07.2020, letzter Abruf am 05.09.2020.

22 Vgl. *Härting*, Corona ohne „Doppeltür“: Warum die Vorschriften zur Sammlung von Kontaktdaten in der Gastronomie verfassungswidrig sind., CR-online.de Blog, 02.08.2020, letzter Abruf am 03.09.2020.

Datenschutz- und rechtskonformer Umgang mit Corona-Kontaktlisten

Mit Beginn der kälteren Jahreszeit ist mit einer Zunahme der Innengastronomie zu rechnen.[1] Um dem erhöhten Infektionsrisiko in Räumen entgegenzuwirken, ist es notwendig, sichere Möglichkeiten der Kontaktverfolgung von Gästen zu gewährleisten. Die zuletzt bekannt gewordenen Sicherheitspannen bei der Speicherung von Corona-Kontaktlisten in Restaurants,[2] und die Nutzung der Daten für polizeiliche Ermittlungen,[3] sind geeignet, Restaurantbesucher zu Falschangaben zu motivieren. Angesichts dieser Entwicklungen stellt sich die Frage, wie eine datenschutz- und rechtskonforme Kontaktdatenerfassung aussehen könnte, die geeignet wäre, das Vertrauen der Bürger zurückzugewinnen.

Rahmenbedingungen zur Aufbewahrung von Kontaktlisten

Ungeachtet bestehender Unterschiede bei der Registrierungspflicht zwischen den Bundesländern[4] ergeben sich für Gastronomen generalisierend folgende Verpflichtungen: Die Gastronomen müssen den Vor- und Nachnamen, Kontaktdaten (Anschrift, Telefonnummer und/oder E-Mail), sowie den Zeitraum des Aufenthalts des Gastes festhalten. Diese Daten haben die Gastronomiebetriebe für drei bis vier Wochen (oder einen Monat – je nach Bundesland) aufzubewahren und anschließend zu löschen. Eine bestimmte Form ist bei der Aufbewahrung nicht zu beachten. Die Länder betonen in ihren Verordnungen, dass die Daten ausschließlich zur Kontaktverfolgung genutzt werden dürfen und dass eine Kenntnisnahme durch Dritte auszuschließen ist.[5]

Die konkrete Umsetzung dieser Vorgaben obliegt den einzelnen Gastronomiebetrieben, wobei von den Behörden und den Gastronomieverbänden zahlreiche Muster für die Datenerfassung bereitgestellt worden sind.[6] Eine Verpflichtung, diese zu nutzen, besteht jedoch nicht. Kontaktlisten können in Papierform oder digital geführt werden. Hieraus ergibt sich ein breites Spektrum möglicher Gestaltungsformen, wobei lediglich die Eintragung in fortlaufende Listen durch die Gäste selbst als unzulässig erachtet wird.[7]

Technische und rechtliche Risiken cloudbasierter Lösungen

Zur Vermeidung eines Zettelchaos gehen Restaurants vermehrt dazu über, die Daten in Cloud-Services zu speichern. Die Risiken einer solchen Vorgehensweise sind spätestens erkennbar geworden, nachdem es Hackern des Chaos Computer Clubs (CCC) gelang, in das System eines solchen Cloudanbieters ohne größere Probleme einzudringen und so zeitweise auf die Corona-Kontakterhebungen von 180 Restaurants, die das System aktiv nutzten, zuzugreifen.[8] Für Gastronomiebetreiber birgt die Nutzung solcher cloudbasierter Systeme ein oft nicht erkanntes haftungsrechtliches Risiko. Denn Cloudservices wie beispielsweise jener, der zuletzt von CCC gehackt wurde, fungieren häufig lediglich als sog. Auftragsverarbeiter (Art. 28 DSGVO).[9] Bei dieser Konstellation verarbeitet ein Auftragsverarbeiter[10] – der Cloudservice – bestimme Daten im Auftrag eines Verantwortlichen, z.B. eines Restaurants. Im Außenverhältnis behält der Verantwortliche, in unserem Beispiel das Restaurant, jedoch die volle datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten.[11] Für Restaurants als Verantwortliche der Datenverarbeitung besteht daher im Falle einer nicht ordnungsgemäßen Datenverarbeitung durch den Auftragsverarbeiter ein Risiko von Sanktionen nach Art. 83 Abs. 4 i.V.m. Art. 28 DSGVO.[12] Aufgrund dieser Risiken, muss gegenwärtig generell von der Nutzung bestehender Cloud-Systeme abgeraten werden.

Apps anstatt Gästelisten?

Eine echte Alternative zur Führung von Gästelisten entsteht derzeit in Österreich. Dort ist vor kurzem eine App entwickelt worden, die eine anonyme, digitale Gästeregistrierung ermöglicht.[13] Mit der App scannen die Gäste einen zu einem Tisch gehörigen QR-Code, wodurch verschlüsselt gespeichert wird, welches Smartphone sich zu welcher Zeit an welchem Tisch befunden hat. Im Falle eines bestätigten Corona-Infizierten im Restaurant kann der Wirt Besucher, die zur selben Zeit im Restaurant waren, durch die App mittels Pushnachricht warnen. So innovativ und datensparsam dieser

1 Der Artikel bezieht sich auf die Sach- und Rechtslage v. 07.09.2020.

2 Vgl. *Meyer-Fünffinger et.al.*, Daten von Restaurantbesuchern einsehbar, Tagesschau.de, 28.08.2020, letzter Abruf am 07.09.2020.

3 Siehe dazu der vorangegangene Beitrag von *Büttel*.

4 Eine nützliche Übersicht zu den unterschiedlichen Regelungen ist die diesbezügliche Synopse der DEHOGA, letzter Abruf am 07.09.2020.

5 Vgl. z.B. § 6 Abs. 1, 2 CoronaVO Baden-Württemberg v. 23.06.2020.

6 z.B. das Musterformular für die Gastronomie zur Erhebung von Kontaktdaten von Gästen des Bayerischen Landesamts für Datenschutzaufsicht, letzter Abruf am 07.09.2020.

7 Vgl. die Nachweise bei *Haschert*, in: Schmidt, COVID-19, Rechtsfragen zur Corona-Krise, 2. Auflage 2020, § 20, Rn. 147 ff.

8 Vgl. hierzu und zu den folgenden Darstellungen die Pressemitteilung des CCC vom 28.08.2020, letzter Abruf am 07.09.2020.

9 Zu weiteren Gestaltungsmöglichkeiten vgl. *Schumacher*, in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Aufl. 2019, B. Datenschutzrechtliche Aspekte bei Outsourcing-Projekten, Rn. 52.

10 Vgl. die Legaldefinition in Art. 4 Nr. 8 DSGVO.

11 *Petri*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 28 DS-GVO, Rn. 3.

12 *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 28 DS-GVO, Rn. 29.

13 *Wimmer*, Österreichische App ersetzt unsichere Coronalisten in Restaurants, futurezone.at, 13.08.2020, letzter Abruf am 07.09.2020.

Ansatz erscheinen mag, so stößt er doch auf die gleichen Bedenken, die auch gegen eine allgemeine Verpflichtung zur Nutzung der Corona-Warn App der Bundesregierung vorgetragen werden: Zum einen kann die fortwährende Nutzung der App schwer überwacht werden. Zum anderen muss es eine Alternative für Gäste geben, die über kein kompatibles Smartphone verfügen. Nicht zuletzt ist die rechtliche Zulässigkeit einer Verpflichtung zur Nutzung der Corona-Warn App umstritten.[14] Eine verpflichtende Nutzung von Apps, sei es einer eigenen App für Restaurants oder der Corona-Warn App, kann daher kurzfristig keine Lösung sein.

Datenschutzkonforme Gestaltung papiergeführter Listen

Aktuell ist die sicherste Lösung immer noch die Nutzung von Papier und Stift. Aber auch hier sind mehrere Ansätze denkbar. So plädiert der CCC dafür, dass Gäste einen gesonderten Zettel ausfüllen, der vom Wirt zusammen mit den anderen Zetteln des Tages in einem versiegelten Umschlag verwahrt wird. Täglich wird dann, nach Ablauf der Aufbewahrungsfrist, je ein Umschlag vernichtet.

Doch dieser Ansatz erscheint wenig praxistauglich. Zum einen entsteht bereits durch die parallele Aufbewahrung von 30 Umschlägen ein gewisses Risiko für Chaos. Wirkliche Unordnung dürfte jedoch entstehen, wenn die Umschläge im Fall der Fälle geöffnet und die Zettel wieder geordnet werden müssen. Geht man von einem Restaurant aus, das 50 eintragungspflichtige Gästegruppen im Laufe des Tages bewirtet, müssten im Falle einer bestätigten Infektion erst 50 Zettel geordnet und ausgewertet werden, bis die betroffenen Gäste kontaktiert werden könnten. Bedenkt man, dass dieses Problem sich mit mehr Zetteln noch vergrößert und das gleichzeitig bei mehr Gästen von einer erhöhten Ansteckungsgefahr ausgegangen werden kann, werden die Nachteile dieser

„Zettellösung“ deutlich. Im Ergebnis würde wertvolle Zeit verloren gehen und dem Infektionsschutz kein Gefallen getan.

Vorzugwürdig erscheint daher ein Konzept, das u.a. der Landesbeauftrage für Datenschutz in Mecklenburg-Vorpommern empfiehlt:[15] Danach sollen die personenbezogenen Daten bei der Bestellung durch eine Servicekraft aufgenommen werden, die diese in eine fortlaufende Liste einträgt. Die Gäste könnten so nichts von den personenbezogenen Daten der anderen Gäste mitbekommen. Am Ende des Tages könnten die fortlaufend erstellten Listen sicher verwahrt werden. Durch ein solches Vorgehen wird ein Zettelchaos vermieden und gleichzeitig im Ernstfall eine zielgerichtete Zugriffsmöglichkeit auf die Daten gewährleistet.

Wichtig ist, dass Gastronomiebetreiber nicht mehr Daten erfassen, als sie nach der jeweiligen Corona-Verordnung dürfen. Denn nur die Erfassung der von der Verordnung vorgesehenen Daten ist nach Art. 6 Abs. 1 Satz 1 lit. c) DSGVO zulässig. Zudem sollte ein Rhythmus gefunden werden, um die alten Listen zu entsorgen. Empfehlenswert ist, dies zu Beginn des Tages vorzunehmen, an dem die Aufbewahrungspflicht abgelaufen ist. Die Listen sollten nicht schlicht weggeworfen, sondern vorher geschreddert werden. Mit diesen einfachen Schritten lässt sich ein ausreichendes Niveau an Datenschutz gewährleisten.

Ausblick

Sofern die Bundesländer nicht – wie etwa der Freistaat Sachsen[16] – die Registrierungspflicht in Restaurants auflockern, sollte eine einheitliche Regelung zur Führung der Coronalisten angestrebt werden. Vorzugwürdig sind weiterhin Papierlösungen, wobei zur Vermeidung von zu vielen Zetteln Verfahren mit fortlaufenden Listen am geeignetsten sind. Denkbar sind aber auch digitale Alternativen, soweit Datensicherheit und Datenschutz gewährleistet werden. Hier sind nicht zuletzt auch die Regierungen von Bund und Ländern gefordert, Alternativen zu entwickeln und zu formulieren, um die den Gastronomien auferlegten Belastungen abzumildern. Ob und wie es mit den Coronalisten weitergeht, ist vorrangig keine juristische, sondern eine politische Frage.

Peter Fischer

14 Zur Diskussion: *Haschert*, in: Schmidt, COVID-19, Rechtsfragen zur Corona-Krise, 2. Auflage 2020, § 20, Rn. 94 ff.

15 Vgl. die Hinweise zu Corona und Datenschutz auf der Website des Landesbeauftragen für Datenschutz in Mecklenburg-Vorpommern, letzter Abruf am 07.09.2020.

16 In Sachsen greift diese Pflicht erst bei 35 Corona-Neuinfektionen auf 100.000 Einwohner innerhalb von 7 Tagen; vgl. § 7 Abs. 1 SächsCoronaSchVO v. 25.08.2020.

Leiter des Forschungsprojekts und AutorInnen

Prof. Dr. Dirk Heckmann

Dirk Heckmann (Jahrgang 1960) ist seit Oktober 2019 Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München, wo er sowohl der TUM School of Governance als auch der Fakultät für Informatik angehört. Zuvor hatte der in Freiburg i. Br. habilitierte Staatsrechtler von 1996 bis 2019 den Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau inne, wo er als Affiliate Professor nach wie vor die Forschungsstelle für IT-Recht und Netzpolitik (For..Net) und das Forschungsprojekt BayWiDI leitet.

Seine Lehr- und Forschungsschwerpunkte liegen im Schnittfeld von IT und Recht mit besonderem Fokus auf Datenschutzrecht, IT-Sicherheitsrecht, Legal Tech, E-Government, E-Health und Künstliche Intelligenz. Aus seiner Feder stammen der juris Praxiskommentar Internetrecht (6. Aufl. 2019) sowie weitere rund 200 Publikationen zu Recht und Digitalisierung.

2003 wurde Heckmann zum nebenamtlichen Verfassungsrichter am Bayerischen Verfassungsgerichtshof gewählt, 2007 in den Expertenkreis des Nationalen IT-Gipfels der Bundesregierung berufen. Seit 2014 ist er Vorsitzender der Deutschen Gesellschaft für Recht und Informatik, seit 2018 Direktor am Bayerischen Forschungsinstitut für Digitale Transformation bidt.

2015 wurde er in die Hauptjury des deutschen Computerspielpreises, 2016 in die Ethikkommission des Bundesverkehrsministeriums zum automatisierten und vernetzten Fahren und 2018 in die Datenethikkommission der Bundesregierung berufen.

Felix Sobala

Felix Sobala forschte von 2016 bis 2019 als Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg 1681/2 „Privatheit und Digitalisierung“ der Universität Passau im Fachbereich Rechtswissenschaften zu datenschutz- und privatheitsrechtlichen Themen. Seit 2019 ist er Wissenschaftlicher Mitarbeiter am Bayerischen Wissensnetzwerk Digitale Infrastrukturen, IT-Sicherheit und Recht für Unternehmen (BayWiDI) und promoviert zu Regulierungsansätzen des datenschutzrechtlichen Verarbeitungsgrundsatzes der Datensparsamkeit.

Priska Katharina Büttel

Priska Katharina Büttel betreut seit Oktober 2019 als geschäftsführende Wissenschaftliche Mitarbeiterin der Forschungsstelle For..Net unter anderem das Projekt BayWiDI an der Universität Passau. Sie beschäftigt sich gegenwärtig im Rahmen ihrer Promotion mit Rechtsfragen im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz und Robotik zu medizinischen Zwecken.

Peter Fischer

Peter Fischer studiert Rechtswissenschaften an der Universität Passau im siebten Semester. Er ist Studentische Hilfskraft an der Forschungsstelle für IT-Recht und Netzpolitik (For..Net).

Impressum

Sämtliche Abbildungen sind gemeinfrei-ähnlich freigegeben via Unsplash.com

Impressum

Universität Passau
Innstraße 41
94032 Passau

Telefon: 0851/509-0
Telefax: 0851/509-1005

E-Mail: praesident@uni-passau.de
Internet: www.uni-passau.de

USt.-Id-Nr.: DE 811193057

Organisation

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung

Die Universität Passau wird vom Vorsitzenden des Leitungsgremiums, Präsident Prof. Dr. Ulrich Bartosch, gesetzlich vertreten. Verantwortlicher im Sinne des § 5 TMG (Telemediengesetz) ist der Präsident. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.

Herausgeber

Prof. Dr. Dirk Heckmann
Leiter der Forschungsstelle für IT-Recht und Netzpolitik (For..Net)

Redaktion und Produktion

Priska Katharina Büttel, Dipl.-Jur.
Felix Sobala, Jurist (Univ.)

Layout und Satz

Moritz Rowold,
Studentische Hilfskraft

Das nächste Magazin erscheint Mitte Dezember 2020. Sie finden das Magazin und die Möglichkeit, sich für den kostenlosen Versand an- und abzumelden, unter www.baywidi.de.

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter baywidi@uni-passau.de.