View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by <intR>²Dok

You shall not pass – Die CoronaWarnApp als Einlassticket? (Teil 1)

Jan Keesen 2020-07-02T14:57:31

von FLORIAN ZUMKELLER-QUAST

Darf von potenziellen Kund*innen verlangt werden, dass diese die aktive Nutzung der CoronaWarnApp des Bundes belegen? Diese Frage beschäftigt den digitalaffinen juristischen Diskurs schon länger als es die App konkret überhaupt gibt. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ist der Ansicht, dass dies unzulässig sei. Eine ausführliche Begründung veröffentlicht es allerdings nicht. Grund genug, sich die rechtliche Lage näher anzusehen.

In Ihren FAQ stellt das BayLDA klar: Nach ihrer Auffassung ist eine solche Einlasskontrolle auf Basis des Vorzeigens der CoronaWarnApp rechtswidrig. Denn die Einwilligung des*der Nutzer*in gegenüber dem RKI zum Betrieb der App selbst decke diese Nutzung nicht. Vielmehr sei nun der*die Betreiber*in des Geschäftes datenschutzrechtlich Verantwortlicher, verstoße aber mangels Rechtsgrundlage gegen die DSGVO.

Mit dieser Ansicht steht das BayLDA nicht alleine da. Allerdings ist diese Ansicht auch alles andere als unumstritten. Anlass genug, sich mit der Frage zu beschäftigen: Verbietet das Datenschutzrecht derartige Einlasskontrollen?

Dies könnte nach Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 Satz 1 DSGVO der Fall sein: Danach ist eine Verarbeitung personenbezogener Daten nur erlaubt, wenn eine der in Art. 6 Abs. 1 DSGVO aufgelisteten Rechtsgrundlagen gegeben ist. Zweifellos handelt es sich bei der Information, dass ein*e Smartphonenutzer*in die App installiert hat und in den letzten X Tagen aktiv genutzt hat, um auf diese*n Nutzer*in personenbezogene Daten. Mit dem Ablesen vor Einlass findet auch eine Verarbeitung in Form des Erhebens dieser Daten im Sinne von Art. 4 Nr. 2 DSGVO

statt: Schließlich werden die dargebotenen Daten erfasst und gerade aufgrund dieser erfassten Informationen das weitere Vorgehen entschieden.

Anwendbarkeit der DSGVO?

Deutlich problematischer ist ein anderer Punkt: Die Anwendbarkeit der DSGVO. Denn diese ist nicht auf jede Verarbeitung personenbezogener Daten anwendbar. Sie ist gerade kein generelles Regulierungsrecht potenziell unerwünschter Vorgänge im Bereich der Digitalisierung. Vielmehr ist sie nach ihrem Art. 2 Abs. 1 nur für ganz oder teilweise automatisierte Verarbeitungen oder solche Verarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, anwendbar.

Offensichtlich liegt eine ganz automatisierte Verarbeitung beim manuellen Ablesen vom Bildschirm eines Smartphones nicht vor. Anders könnte es schon für eine teilweise automatisierte Verarbeitung aussehen. Eine Verarbeitung ist nach Art. 4 Nr. 2 schließlich jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Die Dashboardanzeige der App ist jedenfalls ein automatisiertes Verfahren. Mach das menschliche Ablesen dieser ebendiesen Gesamtvorgang zu einer teilautomatisierten Verarbeitung?

Teilautomatisierte Verarbeitung durch Ablesen vom Bildschirm?

Fernliegend wäre dies jedenfalls nicht: Das Vorzeigen des aktivierten Smartphone-Bildschirms sowie das Ablesen der dargestellten Informationen von ebendiesem stellen jedenfalls eine Vorgangsreihe dar. Hier zwischen App, für die das RKI verantwortlich sein soll, und dem Ablesen zu trennen ignoriert, dass das Ablesen nur aufgrund des aktivierten Smartphonedisplays möglich ist. Zudem spricht datenschutzrechtlich nichts dagegen, die Anzeige einerseits als Teil der gänzlich automatisierten Verarbeitung unter Verantwortung des RKI zu sehen und zudem gleichzeitig als Teil eines anderen, getrennten Vorgangs, zu sehen.

Betrachtet man die Anzeige nicht separat als Teil beider Vorgänge, gibt es lediglich zwei Möglichkeiten: Entweder ergäbe sich entweder die Situation, dass die automatisiert erzeugte Anzeige von Informationen keine Rolle für einen Vorgang spielen würde während das nichtautomatisierte Ablesen aus einem Dateisystem relevant wäre und den Anwendungsbereich der DSGVO eröffnen würde. Oder man rechnet, wie Siedenburg, die der Verwendung der automatisierten Anzeige gegenüber Dritten weiter nur dem Anzeigesystembetreiber zu. Damit würde aber ein Dritter, der auf den konkreten Vorgang keinen tatsächlichen Einfluss hat, von den rechtlichen Auswirkungen getroffen. Überzeugender ist daher die separate Betrachtung der Anzeige als Teil beider Vorgänge.

Zudem sprechen auch teleologische Wertungen für dieses Ergebnis: In einem parallelen Fall, in dem eine solche Anzeige sensiblere Daten wie etwa einen tatsächlichen Krankheitsverlauf offenbaren würden, würden wohl die meisten intuitiv diese Subsumtion bejahen. Denn unabhängig davon, ob man das Schutzziel des Datenschutzrechts als „Schutz aller persönlichen Freiheiten und Grundrechte“, als

informationelle Selbstbestimmung, als allgemeiner Schutz der Privatsphäre oder als Grundrecht auf den Erlass von Gesetzen zum effektiven Schutz personenbezogener Daten sieht, wäre es in allen Fällen diesem Ziel stark abträglich, den Schutz auf das parallele Beispiel nicht zu übertragen. Dann muss dies aber auch schon für die als geringer invasiv qualifizierten Informationen gelten. Denn personenbezogen sind auch diese.

Letztlich fügt sich die Einbeziehung des automatisierten Teilvorgangs der App-Anzeige in einen Gesamtvorgang der Einlasskontrolle sich auch gut in die Rechtsprechung des EuGH ein: Der EuGH fasst den Anwendungsbereich des Datenschutzrechts zum effektiven Schutz des Grundrechts aus Art. 16 Abs. 1 AEUV, Art. 8 GrCh tendenziell weit und bezieht etwaige entgegenstehende Rechte und Rechtsgüter im Rahmen der weiteren Auslegung oder einer Abwägung ein. Daher sprechen die besseren Argumente dafür, eine teilautomatisierte Verarbeitung zu bejahen.

Abgrenzbare Orte als Dateisystem?

Täte man dies allerdings nicht, müsste eine der Varianten der nichtautomatisierten Verarbeitung erfüllt sein. Bock hält die Speicherung in einem Dateisystem für einschlägig. Sie sieht das Innere des Geschäftsraums als strukturierten Datencontainer. Über alle dort Anwesenden sei schließlich die Information bekannt, dass diese Personen die App installiert haben. Auch wenn der Begriff der Speicherung in einem Dateisystem mit Sicherheit weit zu verstehen ist (wie ich schon im Rahmen der Klingelschilder-Debatte hier dargelegt habe), scheint ein derartiges Verständnis doch über die Grenzen des Begriffes zu gehen. Zwar sind die Anforderungen an die Strukturierung möglicherweise erfüllt, den bloßen Aufenthalt von Einzelpersonen an einem geografischen Ort als Speicherung zu deuten, dürfte allerdings zu weit gehen und den Anwendungsbereich der DSGVO zu stark ausdehnen.

Zudem würde dann jede Einlasskontrolle zur nichtautomatisierten Datenverarbeitung. Die so strukturierten Menschengruppen, etwa nach Alter oder Besitz eines Tickets für eine Veranstaltung, wären dann in einem Dateisystem gespeicherte Daten. Dies hätte die Folge, dass auch Dritte bei Betrachtung der Personen im Raum die entsprechenden Informationen erheben würden. Denn wenn schon die mit Blick auf den Rauminhalt gewinnbaren Informationen als im Dateisystem gespeichert gelten sollen, muss umgekehrt der Blick auf ebendiesen Raum auch als Auslesen und Erheben der dort gespeicherten Informationen gelten. Die Dritten wären dann, sofern Sie sich nicht auf eine der Ausnahmen nach Art. 2 Abs. 2 berufen können, auch vollständig der DSGVO unterworfen. Diese so dann vorgenommene Verarbeitung wäre ggf. rechtswidrig, in jedem Fall unterlägen diese Dritten aber den datenschutzrechtlichen Informationspflichten nach Artt. 13, 14 DSGVO . Eine derartig weiter Anwendungsbereich wäre nicht mehr handhabbar und kann vom Gesetzgeber nicht gewollt sein.

Keine Speicherung durch Anwesenheitslisten

Die Variante der geplanten Speicherung in einem Dateisystem ist daher nicht einschlägig, solange keine sonstige Speicherung, etwa im Rahmen einer Anwesenheitsliste erfolgt. Besonders in der Gastronomie, die derzeit zumindest teilweise zur Erhebung von Informationen über die Besucher verpflichtet sind (vgl. etwa § 2 Abs. 3 CoronaVO Gaststätten Baden-Württemberg), läge daher die Annahme nahe, dass die Information über die Installation der App in einem Dateisystem gespeichert wird. Allein schon wegen der Löschungspflicht werden diese Zettel nach Besuchsdatum strukturiert abgelegt werden. Allerdings ergibt sich die Information der App-Installation erst wieder aus dem Rückschluss über die Kenntnis des Faktes der Einlasskontrolle. Die DSGVO reguliert aber nur direkt gespeicherte Informationen, nicht auch noch daraus erschließbare Informationen. Daher ist durch die Anwesenheitslisten keine Speicherung gegeben.

Ebenso ergibt sich eine Speicherung der Information auch nicht etwa aus einer Kartenzahlung. Die Kartenzahlung als zusätzliche, von der Einlasskontrolle unabhängige Entscheidung des*der Kund*in, kann dabei schwerlich als ein zusammenhängender (dann aber teilautomatisierter) Vorgang gesehen werden. Es bliebe theoretisch noch die Variante der bereits in einem Dateisystem gespeicherten Daten. Das Dateisystem des Smartphones kommt dabei allerdings nicht in Betracht, denn dann wäre dies eine teilautomatisierten Verarbeitung. Die geordnete Bildschirmanzeige wird allerdings wohl kaum als für die „Speicherung in einem Dateisystem“ genügen, sodass keine der nichtautomatisierten Varianten einschlägig wäre.

Wie die verschiedenen im Diskurs befindlichen Schutzgüter am Parallelbeispiel zeigen, wäre ein gänzlicher abgelehnter Regulierungsschutz allerdings kaum konsequent erklärbar. Daher ist es letztlich überzeugender, die Anwendbarkeit der DSGVO qua teilautomatischer Verarbeitung zu bejahen. Die Frage, ob die DSGVO nun aber tatsächlich diese Einlasskontrolle verbietet, muss in einem zweiten Teil analysiert werden.

(cc) BY-NC-ND