You shall not pass – Die CoronaWarnApp als Einlassticket? (Teil 2)

Jan Keesen 2020-07-03T10:15:04

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 das Datenschutzrecht die einschlägige Regulierung darstellt und die danach erforderliche Rechtsgrundlage fehle. Doch ist das wirklich so?

In Teil 1 der Analyse hatte ich die Anwendbarkeit der DSGVO auf diesen Fall dargelegt. Da die DSGVO anwendbar ist, muss der*diejenige, der*die über Mittel und Zwecke der Verarbeitung bestimmt, für ihre Rechtmäßigkeit einstehen, Art. 5 Abs. 2, Art. 4 Nr. 7 DSGVO. Naheliegender Zweck der Einlasskontrolle als Zugangsbeschränkung ist der Infektionsschutz insbesondere für Mitarbeiter*innen und Kund*innen. Diesen sowie das in der Verarbeitung verwendete Mittel, das abzulesende Smartphone, wird von dem*der Geschäftsinhaberin festgelegt, sodass diese*r der*die Verantwortliche ist. Dass das RKI Verantwortlicher der App und damit der Anzeige über die aktive App-Nutzung selbst ist, ist hier unschädlich: Die Anzeige ist sowohl Teil des Vorgangs „Dashboard-Anzeige der App“ als auch „Ablesen des Dashboard-Inhalts“ vom vorgezeigten Smartphone-Bildschirm.

Mögliche Rechtsgrundlagen

Als Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 DSGVO kommen drei Varianten in Betracht: Zunächst die Einwilligung nach lit. a, sodann der Schutz lebenswichtiger Interessen nach lit. d und zuletzt ein überwiegendes Interesse nach lit. f. Die Rechtsgrundlage Vertrag nach lit. b wird in der Regel ausscheiden, da in den

typischen Fällen die Einlasskontrolle aus Basis der CoronaWarnApp nicht als für die etwaige Vertragserfüllung erforderlich angesehen werden kann. Und mangels eines bereits erlassenen Begleitgesetzes zur CoronaWarnApp, wie verschiedentlich gefordert, kommt eine gesetzliche Verpflichtung nach lit. c ebenfalls nicht in Betracht. Die reine Fürsorgepflicht für Mitarbeiter wird hierfür jedenfalls nicht ausreichen, da die entsprechenden gesetzlichen Grundlagen aus allgemeinen Regelungen der Schuldverhältnisse bestehen und daher nicht spezifisch genug hinsichtlich der Datenverarbeitung sind. Ob sie für ein überwiegendes Interesse ausreichen könnten, könnte aber dahinstehen, wenn die Einwilligung die üblichen Anforderungen der Geschäftsbetreiber*innen ausreichend erfüllen würde.

Bei den angezeigten Informationen der CoronaWarnApp handelt es sich allerdings um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO, sodass zusätzlich eine der Varianten von Art. 9 Abs. 2 DSGVO erfüllt sein muss. Denn die App zeigt neben der reinen Aktivität selbst auch an, wie hoch das aktuelle Infektionsrisiko des*der Nutzer*in eingeschätzt wird.

Freiwilligkeit der Einwilligung?

Für die Einwilligung wäre dies unproblematisch, aus Art. 9 Abs. 2 lit. a DSGVO folgen hier mangels eines expliziten speziellen Verbotsgesetzes keine weitergehenden Einschränkungen. Das BayLDA lehnt die Rechtmäßigkeit der Einwilligung wegen Mängeln in der erforderlichen Freiwilligkeit ab. Im Beispiel eines Monopolsupermarktes bzw. anderen Monopolgeschäften in einer Region wäre dies sicher der Fall. In der wohl deutlich üblicheren Situation der Vielfalt der möglichen Geschäfte ist dies allerdings deutlich schwieriger. Es gibt schlicht kein allgemeines Recht auf Zugang zu einem speziellen Supermarkt oder einer spezifischen Bar. Der*die Betreiberin hat immer noch das Hausrecht und darf daher Menschen vom Betreten ausschließen.

Kein Kopplungsverbot

Auch wenn die DSGVO die tatsächliche Freiwilligkeit der Einwilligung besonders betont und sie auch von privatautonomen Entscheidung für einen (zweiseitigen) Vertrag unterscheidet, so klingt aus der pauschalen Behauptung der Nichtfreiwilligkeit eher die wohl nur scheintote Idee des Kopplungsverbotes: Eine unmittelbare Verknüpfung von datenschutzrechtlicher Einwilligung und anderweitigem rechtlichen Entgegenkommen des*der Verantwortlichen soll die Freiwilligkeit der Einwilligung negieren. Insbesondere die deutschen Datenschutzaufsichtsbehörden sehen in Art. 7 Abs. 4 DSGVO ein solches Verbot. Allerdings ist diese Ansicht schon kaum mit dem Wortlaut des Absatzes vereinbar. Auch hat die bisherige Rechtsprechung ein solches striktes Kopplungsverbot durchweg ablehnt, so etwa das OLG Frankfurt am Main (27.06.2019 – 6 U 6/19) und jüngst der französische Conseil d'État (CR N° 434684). Denn ein*e Kund*in entscheidet auch bei Anforderung einer solchen Einwilligung immer noch selbst, ob ihm*ihr die Erlangung der geschäftlichen Leistungen die Preisgabe der persönlichen Daten wert ist.

Auch mit dem EG 16 der RL 2018/1972 wäre ein Kopplungsverbot kaum vereinbar, wird dort doch explizit vom Bezahlen mit Daten gesprochen. Ebenso baut die RL 2019/770 mitunter auf dem Konzept von Daten als Gegenleistung auf. Wenn aber personenbezogene Daten schon die Hauptleistung sein können, kann die Preisgabe personenbezogener Daten als Nebenleistung nicht pauschal unzulässig sein. Als sinnvoller Maßstab für die Beurteilung der Freiwilligkeit nach Art. 7 Abs. 4 bleibt daher lediglich, keine Ausnutzung von Zwangssituationen oder andere, ähnliche Eingriffe in die Privatautonomie zu dulden.

Übermäßiger Druck von Außen?

Ein derartiger Eingriff bzw. derartige externer Druck auf den*die potenzielle*n Kund*in wird bei der Verfügbarkeit von alternativen, ähnlichen Geschäften vor Ort oder dem zumutbaren Verweis auf Onlinebestellungen aber in der Regel nicht gegeben sein. Denn anders als etwa konkretere und dadurch meist noch sensiblere Gesundheitsdaten ist die reine Installation der App inkl. Ablesen des Infektionsrisikos ohne weitere Speicherung ein weitgehend eher weniger invasiv wahrgenommener Vorgang. Die Sinn und Zweck der CoronaWarnApp besteht gerade in einer erheblichen Vereinfachung und Verbesserung der Möglichkeiten der Verfolgung und frühzeitigen Eindämmung der Virenverbreitung. Unabhängig von der letztendlichen Effektivität der App in diesem Bereich ist die Anforderung der aktiven App-Nutzung diesem Zweck in jedem Fall unmittelbar dienlich, und dies auch gerade im Interesse der Geschäftsinhaber*innen, die so nicht unbegründet hoffen, einen Beitrag zur Vermeidung eines neuerlichen Lockdowns zu leisten.

Die Entscheidung, ob ein*e Kund*in der App diesbezüglich in gleichem Maße vertraut und ob ihm*ihr die Bestätigung dessen durch Preisgabe der Daten persönlich wert ist, ist angesichts eines nicht vorhandenen allgemeinen Anspruchs auf die ebendiese Leistungen nicht anders denn als freiwillig bezeichenbar. Dabei macht es auch keinen Unterschied, ob es sich beim fraglichen Geschäft um das bisherige Lieblings- oder Stammrestaurant oder auch nur den naheliegendsten Supermarkt handelt. Aus rechtlicher Sicht sind Alternativen vorhanden, mögen diese einem selbst ansonsten tatsächlich auch noch so nachteilig erscheinen. Der externe Druck, in diese Datenverarbeitung einzuwilligen, übersteigt das sonst übliche und omnipräsente Ausmaß an sozialem Einfluss auf eigene Entscheidungen nicht. Und ein Erfordernis für eine weitergehende Freiheit der Entscheidung ist der DSGVO nicht entnehmbar.

Folgen der Einwilligung als Basis

Damit wäre die Einwilligung eine taugliche Rechtsgrundlage. Neben den Informationspflichten nach Art. 13, 14 DSGVO, die durch einen Aushang am Eingangsbereich erfüllbar wären, bleibt daher nur die Frage, welche Aufwände aus Art. 5 Abs. 2 DSGVO erwachsen. Aufgrund der Rechenschaftspflicht, die der*die Verantwortliche für die Einhaltung der Rechtmäßigkeit hat, wird im Rahmen der Einwilligung oft empfohlen, immer schriftliche oder andere beständige Dokumentationen der Einwilligung anzulegen. Dies wäre ein beträchtlicher Mehraufwand.

Allerdings ist ein derartiger Mehraufwand nicht im Sinne des Datenschutzrechtes. Denn schon nur zur Dokumentation müsste der*die Verantwortliche noch weitere Daten wie etwa den Namen erheben. Im Sinne der Datenminimierung wäre dies jedenfalls nicht. Im konkreten Fall der Erhebung vom Smartphonedisplay des*der Kund*in kommt allerdings ein einfacher Faktor ins Spiel: Allein das Verfahren stellt schon sicher, dass die Erhebung freiwillig erfolgt. Denn andernfalls bräuchte der*die Kund*in das Smartphone nicht vorzeigen. Im Vorzeigen kommt die Freiwilligkeit gerade zum Ausdruck. Und nach Ende des Vorzeigens ist die Verarbeitung auch schon beendet, sodass es auch nicht mehr auf weitere Freiwilligkeit ankommt. Dies hat zudem den Vorteil, dass ein etwaiger Widerruf der Einwilligung auch keine Folgeprobleme auslösen kann.

Auf die weiteren denkbaren Rechtsgrundlagen kommt es daher außer für die benannten Monopolgeschäfte schon gar nicht an. Und bei diesen wäre ein überwiegen der Datenverarbeitungsinteressen der besonders geschützten Gesundheitsdaten (Art. 9 Abs. 1 DSGVO) aufgrund der Versorgungsfunktion wenn überhaupt, so wohl nur erschwert begründbar. Im Normalfall kann allerdings ein*e Geschäftsinhaber*in über das Hausrecht tatsächlich den Zugang zum eigenen Geschäft vom Beleg der aktiven Nutzung der CoronaWarnApp abhängig machen. Sollte die Bundesregierung zu ihrem Wort stehen, dass dies nicht erwünscht ist und nicht stattfinden darf, muss sie ein entsprechendes Gesetz in die Wege leiten, dass dieses Vorgehen nach Art. 9 Abs. 2 Nr. 1 DSGVO verbietet.
