Öffentliches Recht

Jahrbuch 2021

herausgegeben

von

Univ.-Prof. Dr. Gerhard Baumgartner

Institut für Rechtswissenschaften,
Alpen-Adria-Universität Klagenfurt

NWV

Wien 2021

Inhaltsverzeichnis

Teil C

Berichte über die Rechtsprechung zur EMRK im Jahr 2020

Clemens THIELE/Jessica WAGNER

Datenschutzrechtliche Fragen der Pandemiebekämpfung

Inhaltsübersicht

I. Einleitung

Nach dem Hype zum Wirksamwerden der Datenschutz-Grundverordnung mit 25. Mai 2018 hat das Interesse an Datenschutz durch das „Pandemiejahr" 2020 einen neuerlichen Höhenflug erfahren. Die öffentlich-rechtlichen Maßnahmen des Gesundheitsschutzes im Zusammenhang mit COVID-19 haben sich nicht nur an den Grundrechten, sondern vor allem an der geänderten Datenschutzrechtslage messen müssen. Der folgende Beitrag beschäftigt sich daher mit datenschutzrechtlichen Fragen der Pandemiebekämpfung. Dabei werden privatrechtliche Aspekte ebenso wie jene des Arbeits-, Sozial- und Steuerrechts ausgespart.[1] Die Erörterungen fokussieren sich auf die durchaus wechselvolle Entwicklung der Corona-App, behandeln die pandemischen Screeningprogramme und beleuchten die Kontaktnachverfolgung durch die Gesundheitsbehörden im Gastronomiebereich ebenso. Ein Blick auf herausragende datenschutzrechtliche Entscheidungen der Pandemiebekämpfung sowie die Verarbeitung personenbezogener Daten im Katastrophenfall nach § 10 DSG runden den Blick auf einen turbulenten Berichtszeitraum ab.

II. Die unterschätzte Norm: Katastrophen-/Pandemiebestimmung des § 10 DSG

A. Grundlagen und Hintergrund

Selbst nach über einem Jahr hat COVID-19 die gesamte Weltbevölkerung fest im Griff. Diese Krise ist ein Ereignis, das dem Umfang nach eine außergewöhnliche Situation für die Menschen darstellt. Die COVID-19-Krise ist im Vergleich zu Naturereignissen (zB Flutwellen, Lawinen oder Erdbeben) geeignet, ein gravierendes Ausmaß zu erreichen, indem durch die hohe Ansteckungsgefahr die Gesundheitssysteme der ganzen Welt lahmgelegt werden können. Obwohl die Bewältigung dieser außergewöhnlichen Situation im vergangenen Jahr durchaus im Vordergrund stand, bedeutete dies nicht, dass der Datenschutz und die DSGVO zurücktraten oder obsolet wurden.

1. Anwendungsbereich der DSGVO

Grds legt Art 2 Abs 2 lit a DSGVO fest, dass die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten findet, welche im Rahmen einer Tätigkeit erfolgt, die nicht in den unionsrechtlichen Anwendungsbereich fällt. Ein Teil der Lehre vertritt die Ansicht, dass Verarbeitungstätigkeiten im Rahmen der „*öffentlichen Sicherheit*", worunter insb auch der Schutz von Personen

1 Vgl instruktiv dazu bereits *Schmidl*, Datenschutzrechtliche Fragestellungen im Zusammenhang mit einer Pandemie wie COVID 19, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht 2020 (2020), 43.

im Katastrophenfall zählt, nicht in den Anwendungsbereich der Verordnung fallen und Art 23 DSGVO, der den Mitgliedsstaaten die Möglichkeit einräumt, Beschränkungen zur Sicherstellung bestimmter nationaler Interessen vorzusehen, überflüssig sei.[2] Diese Ansicht kann allerdings nicht geteilt werden. Im Hinblick auf die Rsp des EuGH, wonach Verarbeitungstätigkeiten zum Zwecke des Schutzes der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit nicht eo ipso aus dem Anwendungsbereich der Richtlinie 2002/58/EG für elektronische Kommunikation fallen würden – da sonst den Regelungen über die Beschränkungen von Rechten und Pflichten im Rahmen dieser Tätigkeiten jede praktische Wirksamkeit genommen wäre –,[3] ist auch auf die damalige Datenschutzrichtlinie und somit auf die DSGVO zu übertragen. Von einer gänzlichen Ausnahme der DSGVO für den Katastrophenschutz kann daher nicht ausgegangen werden. Um diesen Rechtsunsicherheiten entgegenzuwirken, hat der nationale Gesetzgeber mit der Bestimmung des § 4 Abs 1 DSG die generelle Anwendbarkeit der Bestimmungen der DSGVO vorgesehen, um auch Datenverarbeitungen außerhalb des Anwendungsbereichs des Unionsrechts zu erfassen, sofern nicht spezifischere Bestimmungen im Dritten Hauptstück des DSG vorgesehen sind.[4]

Die unmittelbar und sachlich anwendbare DSGVO darf daher auch in COVID-19-Zeiten keineswegs unberücksichtigt bleiben oder sogar übergangen werden.

2. Nationale Katastrophenbestimmung

Der österreichische Gesetzgeber hat von der Möglichkeit in Art 23 DSGVO iVm ErwGr 73 DSGVO, nämlich gewisse datenschutzrechtliche Verpflichtungen bzw Betroffenenrechte zur Sicherstellung der „öffentlichen Sicherheit" zu beschränken, Gebrauch gemacht und (wiederholt) eine datenschutzrechtliche Ermächtigung zur Verarbeitung im Rahmen des Katastrophenschutzes in das (neue) DSG aufgenommen.

Geschaffen wurde die nunmehr in § 10 DSG verankerte Datenschutzvorschrift, die die Verarbeitung im Katastrophenfall regelt, allerdings nicht im Zuge der Anwendbarkeit der DSGVO bzw der Neunovellierung des DSG oder in der COVID-19-Krise, sondern – nahezu wortgleich – bereits 2004 unter dem Eindruck der in Thailand eingetretenen Tsunami-Katastrophe, um erkennungsdienstliche Daten von Abgängigen, insb Fingerabdruckdaten, Abbildungen

2 Siehe *Gola* in Gola (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar[2] Art 23 Rz 6 (2018); aA *Bäcker* in Kühling/Buchner (Hrsg), Datenschutz-Grundverordnung/BDSG: Kommentar[3] Art 23 Rz 13, 16 (2020).

3 EuGH 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige), jusIT 2017/10, 31 (*Jahnel*) = ÖJZ 2017/37, 281 (*Lehofer*) = NLMR 2016, 571 = ZIIR-Slg 2017/12 = ZIIR 2017, 165 = ecolex 2017, 176 = ZTR 2017, 46.

4 *Schweighofer/Zanol/Gojmerac*, Interoperabilität im Katastrophenmanagement und Datenschutz, in Schweighofer ua (Hrsg), IRIS 2019 (2019) 143 (145f).

oder sonstige Feststellungen äußerlicher körperlicher Merkmale, an andere Staaten bzw Dienstleister zu übermitteln, sodass diese einen Abgleich mit den erkennungsdienstlichen Daten an Verstorbenen durchführen können.[5] § 10 DSG hat somit im Rahmen des Art 6 Abs 2 sowie Art 23 DSGVO und Kapitel IX der DSGVO iVm ErwGr 10 die Vorgängerregelung des § 48a DSG 2000 in adaptierter Form abgelöst.

B. § 10 DSG als taugliche Pandemiebestimmung?

1. Ermächtigung und Voraussetzungen

Nach § 10 Abs 1 DSG sind Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen im Katastrophenfall ermächtigt, personenbezogene Daten gemeinsam zu verarbeiten, soweit die in Abs 1 leg cit genannten Voraussetzungen erfüllt sind.

Die privilegierte Datenverarbeitung setzt das Vorliegen einer „**Katastrophe**" voraus, die sich im In- oder Ausland ereignet hat. Als Katastrophe iSv § 10 DSG kann jedenfalls die COVID-19-Pandemie angesehen werden. Eine konkrete Definition zum Begriff „Katastrophe" findet sich zwar weder im Gesetz noch in den Materialien zum Datenschutzanpassungsgesetz 2018, jedoch wurde in den Gesetzesmaterialien zu § 48a DSG 2000 dargelegt, dass eine Katastrophe jedenfalls dann vorliegt, wenn durch ein Naturereignis oder ein sonstiges Ereignis dem Umfang nach eine außergewöhnliche Schädigung von Personen und Sachen eingetreten[6] ist oder unmittelbar bevorsteht. Ein Ereignis mit entsprechendem Gefahrenpotential sind zB auch Lawinen, Flutwellen, Terrorangriffe oder Erdbeben.

Für die Anwendbarkeit dieser Bestimmung ist die Betroffenheit einer **großen Anzahl von Personen** erforderlich. Dies ist in der aktuellen COVID-19-Krise gegeben. Von der aktuellen Krise ist nicht nur die österreichische Bevölkerung, sondern die gesamte Weltbevölkerung betroffen. Sie lässt sich daher jedenfalls als schwerwiegender Katastrophenfall unter § 10 DSG subsumieren.

Soll eine Datenverarbeitung auf diese Bestimmung gestützt werden, müssen jedoch, neben dem Vorliegen einer Katastrophe, weitere Voraussetzungen erfüllt sein. Nach dem Wortlaut dieser Norm muss die Datenverarbeitung in der Katastrophe jene Menschen unmittelbar betreffen und zur Hilfeleistung notwendig sein.

Von der Katastrophe **unmittelbar betroffen** ist jedoch nicht die gesamte österreichische Bevölkerung, sondern ausgehend vom allgemeinen Sprachgebrauch der unmittelbaren Betroffenheit lediglich jene Personen, welche auf COVID-19 positiv getestet wurden. Die Erfassung von allen Personen („*zur*

5 *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG. Datenschutzgesetz § 10 Rz 1 (2018).

6 *Thiele* in Thiele/Wagner, Praxiskommentar zum DSG § 10 Rz 4 (2020).

Auffindung und Identifizierung [...] und zur Information von Angehörigen“) würde die Wortlautgrenze überspannen.[7]

Als Ermächtigungsgrundlage kommt § 10 DSG daher lediglich in Betracht, wenn neben einer Ermächtigung zur Datenverarbeitung bzw Datenübermittlung (1) eine Katastrophe, (2) die unmittelbare Betroffenheit und (3) der Hilfeleistungszweck vorliegen.

2. Datenübermittlung

Eine Datenübermittlung an die in Abs 1 leg cit genannten Ermächtigten ist rechtmäßig, wenn (1) die Daten beim Verantwortlichen rechtmäßig erhoben worden sind und (2) die zu übermittelnden Daten zu Bewältigung der Katastrophe benötigt werden. Der Datenübermittlung muss jedoch stets ein Hilfeleistungszweck zugunsten der unmittelbar betroffenen Personen zugrunde liegen.

Ein Verantwortlicher, der rechtmäßig über personenbezogene Daten verfügt, ist nur bei Vorliegen eines Hilfeleistungszwecks und der Voraussetzung der unmittelbaren Betroffenheit berechtigt, diese an Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen zu übermitteln. So sind zB alle Personen, wie insb Personal von Gemeinschaftseinrichtungen oder Ärzte, berechtigt Informationen über konkrete Infektionsfälle an die Gesundheitsbehörde oder an das Rote Kreuz als Hilfsorganisation nach Art 9 Abs 2 lit i DSGVO iVm § 10 Abs 2 DSG zu übermitteln.

Zudem erlaubt § 10 Abs 3 DSG eine Datenübermittlung in das Ausland, sofern diese für die Erfüllung der in Abs 1 genannten Zwecke unbedingt notwendig ist.

C. Ausblick

Die Katastrophenbestimmung umfasst lediglich unmittelbar betroffene Personen, also auf COVID-19 positiv Getestete. Mittelbar betroffene Personen sind durch § 10 DSG nicht mit umfasst. Eine allgemeine Erweiterung der Katastrophenbestimmung auf mittelbar betroffene Personen würde allerdings zu weit gehen und ist nicht verhältnismäßig. Dies wäre zwar für die Eindämmung der COVID-19-Krise zu begrüßen, jedoch nicht zur Eindämmung anderer Katastrophenfälle (zB Erdbebenunglück) erforderlich. Eine Ergänzung des § 10 DSG auf „*von der Corona-Pandemie mittelbar betroffene Personen, [...]*“ könnte eine Kontaktnachverfolgung zB im Zusammenhang mit der „Stopp Corona“-App erleichtern und als Rechtfertigungsgrundlage dienen.[8] Die Katastrophenbestimmung könnte zwar in der COVID-19-Krise zum Teil eine „taugliche“ Rechtsgrundlage darstellen, sollte jedoch nicht dazu führen, dass die strengen Eingriffsvoraus-

7 *Bisping*, Corona-Tracking und Datenschutz, Zak 2020/266, 170 (171).
8 *Bisping*, Zak 2020/266, 170 (172).

setzungen in das Grundrecht auf Geheimhaltung iSv § 1 DSG übergangen werden.

III. „Stopp Corona"-Apps

Die COVID-19-Pandemie stand erst an ihrem Anfang und schon wurde der Ruf nach technischen Mitteln zu ihrer Bekämpfung laut. Das „Leuchtturm-Projekt"[9] einer App[10] zur anonymisierten Verständigung, um Infektionsketten rasch zu unterbrechen, wurde als „Schlüssel" zu einer raschen Rückkehr in die Normalität gepriesen.[11] Dabei wurden die Dauer und Intensität der COVID-19-Krise ebenso unterschätzt, wie die grund- und datenschutzrechtlichen Anforderungen an die Technik.[12]

Seit dem Wirksamwerden der DSGVO muss nämlich jede „Stopp Corona"-App den Datenschutz schon eingebaut haben,[13] also gewissermaßen in ihrer technologischen DNA tragen, um privatsphäreverträglich eingesetzt werden zu können. Die vom EDSA veröffentlichten Richtlinien behandeln zum einen die Verarbeitung von Gesundheitsdaten zu Forschungszwecken und zum anderen die Nutzung von Standortdaten und Tracing-Tools im Kontext der COVID-19-Pandemie. Damit sind die wesentlichen Pflöcke einer – besser jeder – den unionsrechtlichen Standards entsprechenden Tracing- oder Tracking-Technologie definiert:

---

9 So zutr *Tschohl*, Die österreichische „Stopp Corona"-App. Von Datenschutz und dem Propheten im eigenen Land, ÖGZ 7-8/2020, 64.

10 Abkürzung für engl „*Application*", also eine Anwendungssoftware, die auf jedem Smart-Phone installiert werden kann.

11 *Schönberger*, zit gem Interview vom 30.03.2020 <https://futurezone.at/netzpolitik/experte-gesundheit-geht-vor-datenschutz/400796960> (05.04.2021).

12 Vgl den durchaus bunten Meinungsstrauß in der Lit: *Knyrim/Gabauer*, Datenschutz & Coronakrise: Wie viel Überwachung von Bürgern und Mitarbeitern ist zulässig?, ecolex 2020, 390; *Thiele*, Stopp Corona – Thesen und Antithesen zum Einsatz von Tracking-Apps in der Coronakrise, ZIIR 2020, 152; *Bisping*, Zak 2020/266, 170; *Leissler*, Die COVID-19-Krise: Ein Paradigmenwechsel im Datenschutzrecht? Im Zeitalter der globalen Vernetzung bedingt die Bekämpfung von Pandemien auch die Nutzung von Daten. In manchen Bereichen bedeutet dies eine Abkehr vom traditionellen datenschutzrechtlichen Denken, AnwBl 2020/196, 412; *Gamper*, Verpflichtende Corona-Trac(k)ing-Apps: von der „demokratischen Zumutung" zum „Rand der Demokratie", NLMR 2020, 155; *Thiele*, „Stopp Corona"-App und flächendeckendes Screening, jusIT 2020/32, 85; *Gosch*, Veranstaltungsbericht: Grazer Datenschutz-Gespräche - „Datenschutz in der Corona-Krise (?)" – ONLINE, jusIT 2020/60, 168 jeweils mwN.

13 Der Europäische Datenschutzausschuss (EDSA) veröffentlichte am 21.04.2020 zwei Richtlinien für die datenschutzgerechte Entwicklung von Corona-Tracing-Apps in der EU <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf> (05.04.2021) und <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf> (05.04.2021).

Für die **Verarbeitung von Gesundheitsdaten**[14] ist Folgendes zu beachten:

- Der nationale Gesetzgeber jedes Mitgliedsstaates kann gem Art 9 Abs 2 lit i und j DSGVO spezielle Gesetze erlassen, um die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke zu ermöglichen. Die Verarbeitung von Gesundheitsdaten zum Zwecke der wissenschaftlichen Forschung muss ebenfalls durch eine der Rechtsgrundlagen in Art 6 Abs 1 DSGVO abgedeckt sein. Daher sind die Bedingungen und der Umfang für eine solche Verarbeitung je nach den in den einzelnen Mitgliedsstaaten geltenden Gesetzen unterschiedlich.
- Angesichts der Verarbeitungsrisiken im Zusammenhang mit dem Ausbruch von COVID-19 ist die Einhaltung von Art 5 Abs 1 lit f, Art 32 Abs 1 und Art 89 Abs 1 DSGVO unerlässlich. Hierdurch wird festgelegt, dass die Gesundheitsdaten nur in einer Weise verarbeitet werden dürfen, die durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der Daten gewährleistet. Bei einer Datenverarbeitung zu wissenschaftlichen Zwecken sollen darüber hinaus geeignete Garantien gegeben werden, dass solche technischen und organisatorischen Maßnahmen bestehen.
- Es sind verhältnismäßige Aufbewahrungsfristen für die Daten festzulegen. Bei der Festlegung solcher Speicherfristen sind Kriterien wie die Länge und der Zweck der Forschung zu berücksichtigen. Nationale Bestimmungen können auch Regeln bzgl der Aufbewahrungsdauer festlegen und müssen daher berücksichtigt werden.
- Prinzipiell dürfen Situationen wie der aktuelle COVID-19-Ausbruch die Möglichkeit der betroffenen Personen, ihre Rechte gemäß Art 12 bis 22 DSGVO auszuüben, nicht ausschließen oder einschränken. Art 89 Abs 2 DSGVO erlaubt es dem nationalen Gesetzgeber jedoch, (einige) der Rechte der betroffenen Person, wie sie in Kapitel III der DSGVO festgelegt sind,[15] einzuschränken. Aus diesem Grund können die Einschränkungen der Rechte der betroffenen Personen je nach den geltenden Gesetzen des jeweiligen Mitgliedsstaates variieren.

Bei der **Verarbeitung von Standortdaten**[16] gilt es für Entwickler von Tracing-Apps hauptsächlich zu beachten:

---

14 Näher zur Begriffsbestimmung der Gesundheitsdaten iZm COVID-19 siehe unten Pkt V.

15 Die Betroffenenrechte nach den Art 12 ff DSGVO, also insb Auskunft oder Löschung, aber auch die Einschränkung der Verarbeitung und die Datenübertragbarkeit.

16 Davon zu unterscheiden ist die mit dem 2. COVID-19-Gesetzespaket (BGBl I 16/2020) eingefügte Regelung des § 98a TKG 2003 mit Geltung ab 22.03.2020. Diese soll es im Krisenfall ermöglichen, Telekommunikationsbetreiber aus Zeitgründen auch formlos im Wege der BReg zu verpflichten, Warnungen, dh Inhaltsdaten, an ihre Kunden weiter zu verbreiten. Diese Kompetenz kann gem Abs 4 des neuen § 98a TKG 2003 je nach Gefährdungslage auf andere oberste Organe, wie etwa einzelne BM, andere bundesstaatliche Organe wie Behörden oder ein

- Die Verwendung einer solchen App muss freiwillig sein und darf den Zugang zu gesetzlich garantierten Rechten nicht einschränken. Der Einzelne muss jederzeit volle Kontrolle über seine Daten haben und soll die Möglichkeit haben, sich frei für die Verwendung einer solchen App zu entscheiden.
- Grds lehnt der EDSA die Verwendung von Standortdaten ab. Informationen über die räumliche Nähe zwischen Nutzern der App zur Unterbindung von Infektionsketten können ohne deren Standort eingeholt werden. Bei dieser Art der Verwendung ist die Erhebung von Standortdaten nicht erforderlich und sollte daher auch nicht erfolgen.
- Ist bei einem Nutzer der App eine COVID-19-Erkrankung diagnostiziert worden, sollen nur die Personen, mit denen der Nutzer der App innerhalb des epidemiologisch relevanten Zeitraums für die Ermittlung von Kontaktpersonen in engem Kontakt gestanden hat, informiert werden.
- Der Betrieb dieser Art von Apps kann den Einsatz eines zentralen Servers erfordern. In diesem Fall und in Übereinstimmung mit den Grundsätzen der Datenminimierung und des Datenschutzes sollten die vom zentralen Server verarbeiteten Daten auf das absolute Minimum beschränkt werden.

Die am Beginn ihrer Entwicklung durchaus unter diesen Standards liegende „Stopp Corona"-App des Österreichischen Roten Kreuzes (OeRK) kann inzwischen als vorbildlich angesehen werden.[17] Die nach und nach verbesserten Releases haben ein Datensicherheits- und Datenschutzniveau erreicht, das sogar zu internationaler Anerkennung geführt hat.[18]

IV. COVID-Screening: Testen, Testen, Testen

A. Screening

Einen weiteren Schwerpunkt für den Datenschutz in den Zeiten der Pandemie bildet nach wie vor der Komplex des Screenings, Testens und im Grunde auch des Impfens.

Im Berichtszeitraum hat der Gesetzgeber dafür die notwendigen Voraussetzungen geschaffen, indem er das EpidemieG (mehrfach) novelliert und um datenschutzrechtliche Regelungen ergänzt hat.

---

speziell ernanntes Organ, etwa einen Krisenkoordinator, delegiert werden. Krit aus verfassungsrechtlicher Sicht dazu *Bernsteiner*, Das öffentliche Warnsystem nach § 98a TKG 2003 – Diskussionsstoff für Grundsätzliches, ZfV 2020/13, 125; ebenso *Bußjäger/Egger*, Verfassungs- und verwaltungsrechtliche Grundlagen staatlicher Krisenkommunikation, ÖJZ 2021/8, 63 jeweils mwN.

17 Vgl den DSFA-Bericht Version 2.0 <https://www.roteskreuz.at/fileadmin/user_upload/PDF/Datenschutz/Datenschutz-Folgenabschaetzung-Bericht_OeRK_StopCoronaApp_04-08-2020_V2.0_final.pdf> (05.04.2020).

18 Vgl die Nw bei *Tschohl*, Die „Stopp Corona"-App des Österreichischen Roten Kreuzes – Erfahrungsbericht über ein DS-GVO-Leuchtturmprojekt, ZD 2020, 329.

Am Ende der „ersten Welle“[19] hat sich die Durchführung von großangelegten Screeningprogrammen als ein Mittel der Pandemiebekämpfung zu etablieren begonnen. Zunächst hat alles mit flächendeckenden PCR-Tests in Seniorenheinrichtungen begonnen. Dieses **Screening 1.0** beruhte ausschließlich auf Einwilligungserklärungen der Betroffenen nach Art 9 Abs 2 lit a DSGVO[20] mangels ausreichend determinierter gesetzlicher Grundlagen.[21] Es dauerte nicht lange und die ersten – unter Erwachsenenvertretung stehenden – Heimbewohner beschwerten sich bei den Gerichten.[22]

Mit dem – ebenfalls als Sammelgesetz – verabschiedeten 16. COVID-19-Gesetz[23] ist erstmals eine gesetzliche Bestimmung für Screeningprogramme zur Bekämpfung von COVID-19 geschaffen worden. Dieses **Screening 2.0** verfügt mit § 5a EpidemieG über eine ausdrückliche gesetzliche Grundlage für die Verarbeitung, insb die Ermittlung, von bestimmten (auch gesundheitsbezogenen) Datenkategorien und deren Weiterverarbeitung zur Führung des Registers für Screeningprogramme nach § 5b EpidemieG. Ob diese Bestimmungen allerdings den Vorgaben des Art 9 Abs 2 lit i DSGVO bzw der Verfassungsbestimmung des § 1 Abs 2 DSG entsprechen, ist fraglich,[24] kann aber letztlich dahin gestellt bleiben. Denn auch diese vor allem in der „zweiten Welle“ iZm freiwilligen Testungen vor den Weihnachtsfeiertagen im Dezember 2020 eingesetzten Screeningprogramme haben die Freiwilligkeit betont.

Gemäß § 5a Abs 3 EpidemieG sind die Vorsorgeuntersuchungen durch Antigen-Schnelltests „*unter größtmöglicher Schonung der Privatsphäre der betroffenen Person durchzuführen*“. Die Teilnahme bedarf der ausdrücklichen Einwilligung der betroffenen Person; die Abstrichnahme qualifizierten Gesundheitspersonals.[25] Das war aber auch schon vorher der Fall. In medizinischer Hinsicht ist es ebenfalls bei einem Nasen-Rachen-Abstrich, also einem Eingriff in die körperliche Integrität verblieben. Aus datenschutzrechtlicher Sicht hat sich der Anwendungsbereich der Screenings nicht unerheblich verändert. Neben den behördlich veranlassten (individuellen) Testungen und den spezifischen

19 Rückblickend nehmen sich die Infektions- und Inzidenzzahlen aus dem März und April 2020 eher als leises Plätschern aus, denn als grollende Welle.

20 Ausführlich dazu mit Mustererklärungen und den erforderlichen datenschutzrechtlichen Dokumentationsmaßnahmen vgl *Thiele*, Datenschutzrechtliche Begleitung von Screeningprogrammen zur Bekämpfung von COVID-19 in Seniorenheimeinrichtungen, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht 2020 (2020), 63 ff.

21 Zum Fehlen einer qualifizierten Rechtsgrundlage des Bundes oder der Länder vgl die Mitteilung der DSB vom 27.04.2020 an den Magistrat der Stadt Salzburg, zit nach *Thiele*, jusIT 2020/32, 85 (86).

22 Rechtskräftige Entscheidungen sind dem *Verfasser* aber bislang nicht bekannt geworden.

23 BGBl I 43/2020, kundgemacht am 14.05.2020, in Kraft getreten mit 15.05.2020.

24 Krit bereits *Thiele*, jusIT 2020/32, 85 (87).

25 Instruktiv *Hausreither/Lust*, COVID-19: Informationen zu Gesundheitsberufen und Neues aus dem Berufsrecht, ÖZPR 2020/57, 103.

Screeningprogrammen (zB in Senioreneinrichtungen) sind bevölkerungsweite Screenings dazugekommen. Ein positiver Antigen-Test löst die Meldeverpflichtung nach §§ 2 und 3b EpidemieG[26] und daher eine vorherige Informationsverpflichtung[27] bereits bei der Testung aus:

Weitergabe personenbezogener Daten an die Gesundheitsbehörden

Für den Fall, dass der Antigen Schnelltest positiv ausgefallen ist, wird am selben Tag ergänzend ein PCR-Test durchgeführt. Nach erfolgter PCR-Testung werden Ihre Testung, die Identifikationsdaten, Ihre Kontaktdaten sowie die Probematerialkennung an ein Medizinisch-diagnostisches Laboratorium übermittelt.

Im Falle eines positiven PCR-Testergebnisses ist das Labor zur Anzeige der Krankheit verpflichtet (Art 9 Abs. 2 lit i und g DSGVO iVm § 3 Abs. 1a EpG iVm Verordnung des Bundesministers für Gesundheit betreffend elektronische Labormeldungen in das Register anzeigepflichtiger Krankheiten). Diese Anzeige erfolgt im Register der Anzeigepflichtigen Krankheiten (§ 4 Epidemigesetz). Dadurch kann die Bezirksverwaltungsbehörde, in deren Sprengel sich die erkrankte Person aufhält, die nach dem Epidemiegesetz vorgesehenen Maßnahmen setzen.

Die Meldeverpflichtung der die Testungen, maW Screenings, durchführenden Verantwortlichen an das Screeningregister des Gesundheitsministeriums steht nach § 5b EpidemieG – auch im Fall eines negativen Testergebnisses – außer Frage. Damit verbunden ist eine klare Aufklärungsverpflichtung der Stelle, die freiwillige SARS-CoV-2 Antigen-Schnelltests anbietet. Die Betroffenen müssen vor bzw bei der Anmeldung zu den in Teststraßen von Mitarbeitern des OeRK abgenommenen Tests über die Weitergabe der personenbezogenen Daten und deren Zweck nachweislich informiert werden. Bspw erfolgt dies über das vom Land Salzburg eingerichtete Online-Portal „Salzburg testet“[28].

Weitergabe personenbezogener Daten an das Register für Screeningprogramme

Da es sich bei dem Angebot von freiwilligen SARS-CoV-2 Antigen Schnelltests um ein Screeningprogramm gemäß § 5b Epidemiegesetz 1950 handelt, werden die von Ihnen eingegebenen Daten mit einem bereichsspezifischen Personenkennzeichen sowie dem Testergebnis (positiv bzw. negativ) im Register für Screeningprogramme des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz gespeichert.

Der direkte Personenbezug (Name und Kontaktdaten) ist vom Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz unverzüglich unumkehrbar zu löschen, sobald das Testergebnis vorliegt und im Fall einer bestätigten Infektion mit SARS-CoV-2 die Datenübertragung in das Register anzeigepflichtiger Krankheiten erfolgt ist.

26 Vgl zur datenschutzrechtlichen Rollenverteilung iZm der elektronischen Übermittlung von Negativbefunden bereits DSB 15.02.2021, 2021-0.101.211 (Negativer PCR-Test).

27 Vgl etwa die Website „Salzburg testet“ <https://www.salzburg-testet.at> (05.04.2021).

28 Abrufbar unter <https://www.salzburg-testet.at> (05.04.2021).

Diese vorherige Aufklärung ist wesentlicher Wirksamkeitsbestandteil der geforderten ausdrücklichen Willenserklärung nach Art 9 Abs 1 lit a DSGVO.[29]

In den Berichtszeitraum fällt schließlich eine weitere Novellierung der Screeningvorschrift des § 5a EpidemieG, die ab 29.12.2020 in Kraft gesetzt worden ist. Aus datenschutzrechtlicher Sicht ist darin mit Abs 6 leg cit eine ausdrückliche gesetzliche Möglichkeit geschaffen worden, die – andernfalls nicht nutzbar[30] zu machenden – Daten aus dem Zentralen Melderegister (ZMR) mit den Personenidentifikationsdaten der Testwilligen durch Verknüpfungsanfrage nach § 16a Abs 3 MeldeG abzugleichen. Gleichzeitig erweitert der neu eingefügte § 5a Abs 5 EpidemieG die Screeningprogramme auf den Schulbereich. Damit ist am Ende des Berichtszeitraums ein **Screening 3.0** erreicht.[31]

V. Contact-Tracing (Gastroregistrierungspflichten)

A. Hintergrund und Verordnungen der Länder

Zur Eindämmung der COVID-19-Erkrankungen, insb zur Gewährleistung und Nachvollziehbarkeit von Kontakten in der COVID-19-Krise wurde Ende September 2020 zunächst in Wien sowie zeitnah in anderen Bundesländern bzw Bezirken eine – lediglich für kurze Zeit anhaltende – verpflichtende COVID-19-Registrierungspflicht der Gäste in der Gastronomie eingeführt. Eine bundesweit einheitliche Regelung zur Registrierungspflicht setzte sich mangels Zweckmäßigkeit nicht durch, sondern brachte aufgrund der kompetenzbegründeten Rechtszersplitterung die unterschiedlichsten Lösungen in den Bundesländern hervor. Aus den unterschiedlich erlassenen Ausführungsverordnungen der Länder mit zum Teil Verordnungsermächtigungen für die BVB oder landesweit einheitlichen Regelungen, primär gestützt auf §§ 5 Abs 3 oder 43a EpidemieG bzw §§ 3, 4 COVID-19-MG, kristallisierten sich im Berichtszeitraum zwei Registrierungsmodelle – Betreiberpflichten- sowie das Gästepflichtenkonzept – heraus.[32]

29 Statt vieler EuGH 29.07.2019, C-40/17 (Fashion ID), jusIT 2019/73, 208 (*Thiele*) = ZIIR 2019, 428 (*Stadler/Chochola*) = ÖBl 2019/76, 291 (*Horak/Spring*) = ZIIR-Slg 2019/71 = RdW 2020/50, 29 = VbR 2019/116, 188 = ecolex 2019, 923 = EuGRZ 2019, 343 = ZfRV-LS 2019/42, 212 = Dako 2020/24, 41 (*Gabauer*) = ZIIR-Slg 2020/83 = ZTR 2019, 165.

30 Ständige Spruchpraxis der Datenschutzbehörden, deutlich bereits DSK 14.12.2012, K121.879/0014-DSK/2012 (BürgerInnenumfrage Stadt Graz), jusIT 2013/8, 17.

31 Im Jahr 2021 ist aufgrund des Rein-Testens, Frei-Testens odgl sowie den Impfungen mit einer ähnlich dynamischen Entwicklung zu rechnen.

32 *Thiele/Wagner*, COVID-19-Registrierungspflichten in der Gastronomie, jusIT 2020/85, 228 (228).

B. Anwendungsbereich und Verantwortlicher

Im Rahmen der Gastroregistrierungspflicht fand eine Erhebung von personenbezogenen Daten der Gäste, insb Name, Telefonnummer, E-Mail-Adresse, Tischnummer, Datum sowie Verweildauer oder -zeit statt. Bei den von den Gästen erhobenen oder bereitgestellten personenbezogenen Daten handelt es sich zweifelsfrei um personenbezogene Daten iSv Art 4 Z 1 DSGVO, sodass der datenschutzrechtliche Anwendungsbereich jedenfalls eröffnet war. Dabei spielte es auch keine Rolle, ob die durch die verpflichtende Registrierung erhobenen Daten nach bestimmten Merkmalen iSv Art 4 Z 6 DSGVO strukturiert oder unstrukturiert waren, denn auch unstrukturierte Daten unterliegen dem Grundrecht auf Geheimhaltung iSv § 1 Abs 1 DSG. Fest steht jedenfalls, dass jede Datenverarbeitung ausnahmslos einen Rechtfertigungstatbestand nach Art 6 oder Art 9 DSGVO bzw § 1 Abs 2 DSG bedarf.

Das **Betreiberpflichtenmodell** unterschied sich vom Gästepflichtenmodell insb darin, dass dieses unmittelbar den Gastronomiebetreiber bzw -inhaber zur Datenerhebung verpflichtete. Das **Gästepflichtenmodell** hingegen legte dem Gast, bereits vor dem Betreten von Betriebsstätten bzw vor der Konsumation auf, seine personenbezogenen Daten dem Gastronomiebetreiber bzw -inhaber bekannt zu geben. Bei beiden Modellen blieb die datenschutzrechtliche Verantwortung iSv Art 4 Z 7 DSGVO beim Gastronomiebetreiber bzw -inhaber, sodass dieser für die Einhaltung der datenschutzrechtlichen Vorgaben zuständig war. Gegenüber der Außenwelt – also den Gästen – trat der Gastronomiebetreiber bzw -inhaber als Verfügungsberechtigter der erhobenen Daten auf.

Die von den Bundesländern bzw BVB erlassenen Verordnungen regelten allesamt, dass die Gaststättenbetreiber gewisse personenbezogene Daten der Gäste lediglich im COVID-19-Verdachts- bzw Anlassfall an die Gesundheitsbehörden auf Verlagen zum Contact-Tracing zu übermitteln hatten.

C. Erfasste Daten als Gesundheitsdaten?

Betrachtet man die im Zuge der Gästeregistrierung erhobenen personenbezogenen Daten losgelöst vom konkreten Verarbeitungszweck – nämlich diese ausschließlich zum Schutz von Leben und Gesundheit der Mitarbeiter und der Gäste des Gastronomiebetreibers bzw -inhabers iZm COVID-19 bzw der COVID-19-Epidemie sowie zur Unterstützung der Gesundheitsbehörden bei der Ermittlung von Kontaktpersonen bei Auftreten eines Infektionsfalles – wären diese lediglich als nicht-sensible Daten zu werten. Nach Art 4 Z 15 DSGVO handelt es sich um Gesundheitsdaten, wenn sich die personenbezogenen Daten auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen aus deren Gesundheitszustand hervorgehen. Im Lichte des Art 9 DSGVO sind Gesundheitsdaten zweifelsfrei besonders schüt-

zenswerte Daten. Der Begriff ist iSd Rsp des EuGH weit auszulegen.[33] Im Zusammenschau mit ErwGr 35 DSGVO können daher auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, unter Gesundheitsdaten fallen, sofern diese für gesundheitliche Zwecke zur eindeutigen Identifizierung herangezogen werden. Die DSB hielt bereits mehrmals fest, dass aus Gesundheitsdaten jedenfalls Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen müssen.[34]

Im Zusammenhang mit der Gastroregistrierung vertritt die DSB die Ansicht, dass bereits die Datenermittlung in den Gastrobetrieben in einem rein gesundheitlichen Kontext erfolgte und die erhobenen Daten auch nur in einem solchen genutzt werden sollten, sodass diese als besondere Kategorie personenbezogener Daten zu qualifizieren seien und lediglich einer der in Art 9 Abs 2 DSGVO taxativ aufgezählten Tatbestände heranziehen sei.[35] Übersehen wurde dabei allerdings, dass es sich bei der Datenverarbeitung „Gastroregistrierungspflicht" um zwei voneinander getrennte Datenverarbeitungsschritte, nämlich die Ermittlung bzw Erhebung und die Übermittlung, handelt und diese in diesem Sinne getrennt voneinander zu beurteilen sind.[36] Bei der Datenerhebung handelt es sich zunächst um potenziell sensible Daten, sodass erst ab der Information, eine mögliche COVID-19-Infektion könnte stattgefunden haben, Art 9 Abs 2 DSGVO greift.

D. Ermittlung einer tauglichen Rechtsgrundlage für die Datenerhebung

Eine Rechtfertigung zB nach Art 6 Abs 1 lit c DSGVO iVm § 5 Abs 3 EpidemieG, nämlich zur Erfüllung einer rechtlichen Verpflichtung gem der Wr Contact-Tracing V, auf die sich die Stadt Wien stützte, hielt[37] nicht stand. Als rechtliche Grundlage für die COVID-19-Registrierungspflicht samt Kontaktnachverfolgung im Verdachtsfall kommt nach Ansicht der DSB eine Rechtfertigung nach Art 6 DSGVO aufgrund des gesundheitlichen Kontexts nicht in Betracht und kann letztlich dahin gestellt bleiben. Ausgehend davon bedarf es daher für mit der Gästeregistrierung im Zusammenhang stehende Datenverarbeitungen zu diesem besonderen Zweck ausnahmslos einer tauglichen Grundlage iSd Art 9 DSGVO.

33 EuGH 06.11.2003, C-101/01 (Lindqvist), MR 2004, 83 (*Kronegger*) = ÖJZ 2004/45, 741 (*Hörlsberger*) = EuGRZ 2003, 714 = ZER 2004/330, 93.

34 DSB 09.04.2019, DSB-D123.526/0001-DSB/2019 (nrk), jusIT 2020/21, 60 (*Gerhartl).*

35 DSB 19.11.2020, 2020-0.743.659 (Gästeregistrierung), ecolex 2021/66, 82 (*Kröpfl*).

36 Vgl *Thiele/Wagner*, jusIT 2020/85, 228 (230).

37 Vgl DSB 19.11.2020, 2020-0.743.659 (Gästeregistrierung).

Keine taugliche Rechtsgrundlage bildet die ausdrückliche Einwilligung iSv Art 9 Abs 2 lit a DSGVO, die von der betroffenen Person einer aktiven und unmissverständlichen Willenshandlung bedarf. Dieser Tatbestand scheitert idR an den zwingenden Voraussetzungen der Freiwilligkeit. Nachdem insb bei Verweigerung der Bekanntgabe der personenbezogenen Daten der Zutritt zur Betriebsstätte unter Berufung des Hausrechts verweigert werden kann, ist bei Nichtabgabe der Einwilligung ein klarer Nachteil zu erwarten. Zudem setzt die Freiwilligkeit voraus, dass im Falle einer Nichteinwilligung in die Datenverarbeitung der betroffenen Person eine zumutbare Alternative zur Verfügung steht. Selbst wenn der betroffenen Person eine zumutbare Alternative zur Verfügung steht (zB Konsumationsrabatte udgl), wäre eine Berufung auf Art 9 Abs 2 lit a DSGVO in keinem Fall zweckmäßig, da die Einwilligung jederzeit widerrufen werden kann.

Als möglicher Rechtfertigungsgrund könnte insb Art 9 Abs 2 lit i DSGVO, der eine Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, erlaubt, in Frage kommen. Bei diesem Tatbestand handelt es sich allerdings um eine Öffnungsklausel. Das bedeutet, dass eine Verarbeitung von sensiblen Daten nur dann zulässig ist, wenn im Recht der Union oder der Mitgliedsstaaten eine gerade jenen Zwecken dienende Verarbeitungsnorm enthalten ist. Die Durchführungs- bzw Ausführungsverordnungen der Länder können grds eine solche Norm darstellen. In datenschutzrechtlicher Sicht ist allerdings bei der Schaffung einer Rechtsgrundlage iSv Art 9 Abs 2 lit i DSGVO zwingende Voraussetzung, dass die nationale Norm klar und präzise determiniert sein muss.

Ob zB § 5 Abs 3 EpidemieG eine taugliche Grundlage iSd Art 9 Abs 2 lit i DSGVO für eine Verordnung (wie zB die Wr Contact-Tracing Verordnung als Betreiberpflichtenmodell) bzw Datenerhebung bzw -übermittlung an die Gesundheitsbehörde zur Kontaktnachverfolgung im Verdachtsfall darstellte, ist nach wie vor fraglich. Der VfGH hat zwar im Hinblick auf die von der Stadt Wien geschaffene Verordnung bereits festgehalten, dass diese aufgrund der fehlenden Nachvollziehbarkeit bzw Verhältnismäßigkeitsprüfung gesetzwidrig war, hat allerdings nicht explizit die Frage, ob die angefochtene Verordnungsbestimmung in § 5 Abs 3 EpidemieG überhaupt eine taugliche Grundlage für eine Verordnungsermächtigung darstellt, beantwortet.[38]

Oberösterreich oder Niederösterreich stützten etwa ihre Verordnungen auf §§ 3, 4 iVm 7 Abs 2 COVID-19-MG[39] sowie § 5 Abs 3 iVm §§ 43 Abs 4a und 43a Abs 2 EpidemieG und unterwarfen „*bestimmte*“, iSv „*bestimmte einge-*

38 Vgl *Kriwanek/Tuma*, VfGH: COVID-19 – Wiener Contact Tracing Verordnung 2020 (22.03.2021, LexisNexis Rechtsnews 30626 <lexis360.at>).

39 Vgl Bundesgesetz betreffend vorläufige Maßnahmen zur Verhinderung der Verbreitung von COVID-19 (COVID-19-Maßnahmengesetz – COVID-19-MG), BGBl I 12/2020 idF I 104/2020.

schränkte" Orte aus epidemiologischer Sicht notwendigen Betretungserfordernissen.[40] Es ist nach wie vor diskussionswürdig, ob durch die in Anspruch genommenen Rechtsgrundlagen, insb, wie und ob ein Gast eine Betriebsstätte betreten durfte, die Einführung der verpflichtenden Gästeregistrierung gedeckt war. Die Verhältnismäßigkeit des Gästepflichtenmodells war auf den ersten Blick eher zu verneinen, als die Änderungen der COVID-19-MV vom 22.10.2020 ua bereits vorsahen, dass der Betreiber (mit mehr als 50 tatsächlich zur Verfügung stehenden Sitzplätzen) auf Basis einer Risikoanalyse ein dem Stand der Wissenschaft entsprechendes COVID-19-Präventionskonzept zur Minimierung des Infektionsrisikos auszuarbeiten und umzusetzen hatte. Zudem war vorgesehen, dass ein datenschutzkonformeres System zur Nachvollziehbarkeit von Kontakten, wie bspw ein System zur Erfassung von Anwesenheit auf freiwilliger Basis der Gäste mit echten Alternativangeboten, etwa einem günstigeren Menüpreis, vorgesehen werden kann. Dies sowie die Differenzierung auf die Eingriffstiefe spiegelten sich allerdings in keinem Gästepflichtenmodell wider.

E. Datenübermittlung an Dritte

Der Zweck der Gastroregistrierung im Berichtszeitraum bestand ausschließlich in der Kontaktnachverfolgung im Verdachtsfall durch die zuständige **Gesundheitsbehörde**. Eine Datenübermittlung von Personen, die im Zuge der Registrierungspflicht rechtmäßig erfasst wurden, an die Gesundheitsbehörde war jedenfalls iSv Art 9 Abs 1 lit i DSGVO iVm § 5 Abs 3 EpidemieG zulässig. Zu beachten ist jedoch, dass § 5 Abs 3 EpidemieG lediglich jene Personen adressiert, die zur Kontaktnachverfolgung einen Beitrag leisten könn(t)en und keine ausdrückliche Verpflichtung darstellt. Der Gastronomiebetreiber hatte daher lediglich jene Daten zu übermitteln, über welche er tatsächlich verfügte.

Ein **strafbehördlicher Zugriff** auf COVID-19-Gästelisten und somit eine Übermittlungspflicht eines Gastronomiebetreibers zum Zweck der Aufklärung einer Straftat im Wege eines polizeilichen Auskunftsersuchens nach § 152 StPO bestand bzw besteht idR nicht. Fest steht, dass jegliche Weitergabe von rechtmäßig erhobenen personenbezogenen Gästedaten eine Zweckänderung darstellt, die mit dem ursprünglichen Verarbeitungszweck – Kontaktnachverfolgung – keinesfalls iSv Art 6 Abs 4 DSGVO vereinbar ist. Eine Weitergabe der rechtmäßig erhobenen und im Verantwortungsbereich des Gastronomiebetreibers verfügbarer Gästedaten wäre lediglich unter Einhaltung der Erlaubnistatbestände des § 4 Abs 3 Z 1 (ausdrückliche gesetzliche Ermächtigung) oder Z 2 DSG (Interessenabwägung) möglich gewesen. Der Gastronomiebetreiber hätte zB dann datenkonform gehandelt, wenn das Warum und Wofür der behördlichen Datenanforderungen klar hervorgegangen wäre, die Daten rechtmäßig erhoben wurden und, sofern keine ausdrückliche gesetzliche Verpflichtung zur

40 Näheres dazu *Thiele/Wagner*, jusIT 2020/85, 228 (232).

Datenherausgabe zur Anwendung kam (§ 4 Abs 3 Z 1), eine umfassende Interessensabwägung samt Verhältnismäßigkeitsprüfung ergeben hätte, dass die Betroffenensphäre bestmöglich geschützt wird.

F. Ausblick zur Gästeregistrierung

Insgesamt bedarf es für das Einführen von verpflichtenden Gästeregistrierungen einer qualifizierten Rechtsgrundlage im nationalen Recht, wie zB einer verfassungskonformen Verordnungsermächtigung.

Am 19.12.2020 wurde daher der gesetzlichen Unsicherheit zur verpflichtenden Gästeregistrierung entgegengewirkt. In § 5c EpidemieG wurde nun zum Zweck der Ermittlung von Kontaktpersonen bei Umgebungsuntersuchungen, soweit dies aufgrund der COVID-19-Pandemie unbedingt erforderlich und verhältnismäßig ist, die Möglichkeit zur Gästeregistrierung befristet bis 31.12.2021 gesetzlich verankert. In § 5 c Abs 1 letzter Satz EpidemieG wurde nun ausdrücklich die Verpflichtung der betroffenen Person zur Bekanntgabe der in Abs 1 Z 1 bis Z 8 leg cit aufgezählten personenbezogenen Daten aufgenommen. Die personenbezogenen Daten sind für die Dauer von 28 Tagen aufzubewahren und nach Ablauf dieser Zeit unverzüglich zu löschen. Ausdrücklich festgehalten ist, dass eine Verarbeitung der Daten zu anderen Zwecken nicht zulässig ist und die zur Aufbewahrung datenschutzrechtlich Verantwortlichen sicherzustellen haben, dass die ermittelten Daten nicht durch Dritte einsehbar sind.

Eine verpflichtende Gästeregistrierung kann jedoch nur dann standhalten, wenn durch den Verordnungsgeber vor Verordnungserlassung notwendige und dokumentierte prognosehafte Beurteilungen zur Ausbreitung von COVID-19, der in Geltung stehenden übrigen Maßnahmen (zB Maskenpflicht, Abstandsregelungen) sowie eine Prüfung der Geeignetheit, Erforderlichkeit und Angemessenheit im Hinblick auf die in Aussicht genommene Erhebung von Kontaktdaten zur Verhinderung der Verbreitung von COVID-19 stattfinden. Der Verordnungsgeber hat somit schlussendlich zu beurteilen, ob und inwieweit er zur Verhinderung der Verbreitung von COVID-19 die Kontaktdatenerhebung für erforderlich hält, und hat dabei zwingend eine Abwägung der grundrechtlich geschützten Interessen der betroffenen Gastronomiebetreiber bzw -inhaber zu treffen.[41]

41 VfGH 10.03.2021, V 573/2020-16 (Contact Tracing Stadt Wien).

VI. Ausgewählte COVID-19-Rsp zum Datenschutz

A. VfGH

1. Maskenpflicht in Schulgebäuden

Lediglich am Rande befasste sich der VfGH im Berichtszeitraum mit den datenschutzrechtlichen Aspekten iZm der Pandemiebekämpfung. In seinem Erk[42] zur Feststellung der Gesetzwidrigkeit der Anordnung einer Maskenpflicht in Schulgebäuden und der Klassenteilung im Frühjahr 2020 führte das Höchstgericht – datenschutzrechtlich – lediglich aus, dass das Epidemiologische Meldesystem (EMS) primär den BVB zur Erfüllung der Aufgaben zur Durchführung von Erhebungen über das Auftreten anzeigepflichtiger Krankheiten, zur Verhütung der Weiterverbreitung und Bekämpfung anzeigepflichtiger Krankheiten und der Erfüllung der Aufgaben der Landeshauptmänner im Rahmen ihrer Koordinierungsfunktion dient. Eine Verarbeitung durch andere Behörden oder zu anderen Zwecken verstößt gegen § 1 DSG. Der Schulverwaltung sind diese Daten daher nicht zur Verfügung gestanden.[43]

2. Wiener Contact-Tracing

Im Rahmen der Feststellung der Gesetzwidrigkeit zur Verordnung des Magistrats der Stadt Wien betr der Auskunftserteilung für Contact-Tracing iZm Verdachtsfällen von COVID-19 hielt der VfGH in seinem Erk fest, dass die – am 19.12.2020 in Kraft getretene – Verordnungsermächtigung in § 5c EpidemieG zur Erhebung vorgesehener Daten schwerwiegende Eingriffe in das Grundrecht auf Datenschutz nach Art 8 EMRK und § 1 DSG ermöglicht. Dies vor dem Hintergrund, dass die vorgesehene Datenerhebung zum Zweck der Ermittlung von Kontaktdaten bei Umgebungsuntersuchungen große Teile der Bevölkerung betrifft und die Zusammenschau der erhobenen Daten Rückschlüsse über die persönliche Lebensführung der Betroffen zulässt. Der VfGH führte aus, dass bei einer weitreichenden Verordnungsermächtigung, die schwerwiegende Grundrechtseingriffe ermöglicht, der Verordnungsgeber im Verordnungserlassungsverfahren nachvollziehbar darzulegen hat, auf welcher Informationsbasis über die nach dem Gesetz maßgeblichen Umstände die Verordnungsentscheidung fußt und die gesetzliche Abwägungsentscheidung erfolgt ist. Die Wr Contact-Tracing-V betr Auskunftserteilung erfüllte die Anforderungen nicht, insb war die Entscheidungsgrundlage nicht nachvollziehbar dokumentiert.[44]

42 VfGH 10.12.2020, V 436/2020 (Maskenpflicht in Schulgebäuden), NLMR 2020, 531.
43 Vgl Rz 40 des Erk.
44 VfGH 10.03.2021, V 573/2020-16 (Contact Tracing Stadt Wien).

B. Datenschutzbehörde

1. Öffentliche Kritik am Gesundheitssystem in COVID-Zeiten

In den Berichtszeitraum fällt eine bemerkenswerte Entscheidung der DSB, deren Zusammenhang mit der Pandemiebekämpfung aber nicht gesichert ist. Der von der Behörde anonymisierte Sachverhalt lässt nicht erkennen, ob die vom Beschwerdeführer mit seiner Aktion beabsichtigte Kritik am (versagenden) Gesundheitssystem bereits einen COVID-19-Bezug aufgewiesen hat. Da aber (auch) künftig sowohl von COVID-19-Leugnern als auch von Impfbefürwortern medizinische Einzelschicksale durchaus in plakativer Weise zur Untermauerung ihrer (konträren) Standpunkte eingesetzt werden können, sei auf die datenschutzrechtlichen Konsequenzen an dieser Stelle bereits hingewiesen.

Im Anlassfall[45] veröffentlichte ein Arzt auf seiner privaten Facebook-Seite medizinische Daten seiner Patienten. Er postete Ausschnitte aus Patientenbriefen, Befunddaten, medizinische Diagnosen, Aufnahme- und Entlassungsdaten von Krankenhäusern, Sozialversicherungsnummern von Patienten oder die Namen der behandelnden Ärzte auf seiner Pinnwand – allesamt öffentlich einsehbar. Aufgrund von zahlreichen Beschwerden leitete die DSB ein Verfahren nach den Art 58, 57, 55 iVm Art 1 DSGVO („amtswegiges Prüfverfahren") ein. Dieses führte unverzüglich zu einem sog Mandatsbescheid nach § 22 Abs 4 iVm § 57 AVG. Die DSB untersagte dem Arzt wegen Gefahr im Verzug die Offenlegung von Patienten- und Gesundheitsdaten. Dass der Tatbestand der „Gefahr im Verzug" erfüllt war, ergab sich daraus, dass der datenschutzrechtlich Verantwortliche bereits begonnen hatte, sensible Daten elektronisch zu veröffentlichen.[46] Unterlassungsaufforderungen der Ärztekammer sowie ein Disziplinarverfahren hätten den Verantwortlichen bisher nicht davon abgehalten, Gesundheitsdaten seiner Patienten weiterhin auf öffentlich zugänglichen Social-Media-Plattformen zu verbreiten.

Mit Mandatsbescheid wurde dem Verantwortlichen daher die Offenlegung personenbezogener Gesundheits- und Patientendaten auf der persönlichen Facebook-Seite sowie auf dem offiziellen Facebook-Auftritt der Ärztekammer für Wien sowie sonstigen öffentlichen Facebook-Gruppen/Seiten und Social-Media-Plattformen mit sofortiger Wirkung untersagt.

Das amtswegige Prüfungsverfahren mündete schließlich in ein Bußgeldverfahren nach Art 83 DSGVO. Aufgrund der mehrfachen Datenschutzverletzungen[47] verurteilte die DSB den Arzt, weil er personenbezogene Daten sowie auch Gesundheitsdaten zu Unrecht verarbeitet hatte, rechtskräftig zu einer

45 DSB 30.03.2020, 2020-0.0.203.677 (Patientendaten auf Facebook).

46 Vgl *Thiele/Wagner* in DSG § 22 Rz 19 mHw auf DSK 27.07.2007, K213.009/0002-DSK/2007 (Patientenbefragung Hörminderung) und DSK 15.03.2010, K213.051/0004-DSK/2011 (Google Street View I), jusIT 2011/49, 106 (*König*).

47 Art 5 Abs 1 lit a, Art 9 Abs 1 und Abs 2 iVm Art 83 Abs 5 lit a DSGVO.

Geldstrafe in Höhe von 600,- EUR, im Fall der Uneinbringlichkeit zu einer Ersatzfreiheitsstrafe von 36 Stunden.[48]

2. Gästeregistrierung bei Lokalbesuch

Im aus Wien stammenden Anlassfall[49] reichte der Gast eines Restaurants bei der DSB eine Beschwerde gegen die X-GmbH als Gastronomiebetreiberin ein, worin er einen Verstoß gegen § 1 DSG und Art 6 DSGVO geltend machte: Das Restaurant hatte nämlich vom Gast verlangt, seinen Namen, seine Telefonnummer (optional seine E-Mail-Adresse) und seine Tischnummer anzugeben, wenn er bedient werden wollte. In seinem Datenschutzhinweis gab das Restaurant an, dass es diese Daten „zum Schutz des Lebens und der Gesundheit unserer Mitarbeiter und unserer Gäste im Zusammenhang mit dem Auftreten von COVID-19 und der COVID-19-Epidemie“ erheben würde.

Der Beschwerdeführer stellte seine Daten am 2. Oktober 2020 mittels eines QR-Code-Scanners zur Verfügung und schickte anschließend eine Auskunftsanfrage nach Art 15 DSGVO. In seiner Antwort gab das Restaurant an, dass die Verarbeitung auf der Grundlage der Wr Contact-Tracing-V[50] erfolgt. Die DSB hatte daher (umfassend) zu prüfen, ob es gem Art 6 und 9 DSGVO rechtmäßig wäre, Daten über den Kunden für die vom Restaurant angegebenen Zwecke zu verarbeiten?

Die DSB gab der Beschwerde statt und stellte fest, dass die X-GmbH den Beschwerdeführer im Recht auf Geheimhaltung verletzt hatte, indem sie dessen personenbezogene Daten, nämlich Vorname, Nachname, Telefonnummer, für Zwecke der Kontaktnachverfolgung verarbeitet hatte. Soweit sich die Beschwerde gegen die Verarbeitung anderer als der in der Auskunft angeführten Daten des Beschwerdeführers richtete, erwies sie sich mangels tatsächlicher Verarbeitung als unbegründet.

Nach Ansicht der DSB handelte es sich bei den erfassten Daten bereits um gesundheitsbezogene Daten iSv Art 9 Abs 1 DSGVO, für deren Verarbeitung zu Zwecken der Kontaktnachverfolgung weder eine gesetzliche Grundlage existiere noch eine gültige Einwilligung bestehen würde. Die Datenverarbeitung konnte nicht auf Art 9 Abs 2 lit a DSGVO gestützt werden, weil aus Sicht des Durchschnittskunden bei Nichtabgabe der Einwilligung klar ein Nachteil (hier: Nichtbewirtung) zu erwarten gewesen war. Die einschlägigen Bestimmungen des EpidemieG iVm der Wr Contact-Tracing-V normierten eine Pflicht zur Auskunftserteilung gegenüber der BVB, aber gerade keine Verpflichtung

48 DSB 19.10.2020, 2020-0.111.488 (Patientendaten auf Facebook II).

49 DSB 19.11.2020, 2020-0.743.659 (Gästeregistrierung), ecolex 2021/66, 82 (*Kröpfl*) = ZIIR 2021, 68 (*Thiele*).

50 Verordnung des Magistrats der Stadt Wien betreffend Auskunftserteilung für Contact Tracing im Zusammenhang mit Verdachtsfällen von COVID-19, ABl 41/2020 (Wr Contact-Tracing-V).

zur Erhebung und Verarbeitung der Gästedaten. Die Auskunftspflicht wiederum könnte sich nach § 5 Abs 3 EpidemieG nur auf solche Daten beziehen, die dem Inhaber einer Betriebsstätte der Gastronomie ohne besonderen Ermittlungsaufwand zur Verfügung stünden. Schließlich verstieß die datenschutzrechtliche Erklärung für die Gäste aufgrund ihrer Widersprüchlichkeit bzw irreführenden Passagen gegen den Datenverarbeitungsgrundsatz von Treu und Glauben. Dies führte fallkonkret zu einer Verletzung von § 1 DSG.

Die Entscheidung aus dem November 2020 ist in ihrem Ergebnis nach der damaligen Gesetzeslage[51] zutreffend, in ihrer Begründung, die den Begriff der Gesundheitsdaten überspannt, aber abzulehnen.[52] Zur noch am 19.12.2020 in Kraft getretenen Einfügung von § 5c EpidemieG siehe oben (Pkt V.F.).

VII. Zusammenfassung

Weder die Politik noch der Gesetzgeber sind auf die durch COVID-19 ausgelöste Pandemie in datenschutzrechtlicher Hinsicht vorbereitet gewesen. Die einzige nationale Bestimmung, die jemals ein Katastrophenszenario antizipiert hat, beruht auf einem historischen Tsunami-Ereignis in Thailand aus dem Jahr 2004.[53] Der erste Teil des Beitrages heftet sich auf die Spur der nahezu identen Nachfolgevorschrift des § 10 DSG.

Die als „Schlüssel" zur Normalität gepriesene „Stopp Corona"-App ist nach holprigen Anfängen zu einem mustergültigen Beispiel des *privacy by design* geworden. Das auch von der Politik unter medialem Getöse zerschlagene Porzellan hat eine populäre Verbreitung und einen effektiven Einsatz aber verhindert.

Mehr Erfolg ist den Screeningprogrammen beschieden, die durch eine konsequente datenschutzrechtliche Begleitung und flankierende gesetzliche Maßnahmen zu wirksamen Maßnahmen der Pandemiebekämpfung geworden sind. Künftig bleibt allerdings die Frage nach der Speicherbegrenzung, maW den Löschfristen iZm dem Screeningregister nach § 5b EpiedmieG offen und ist letztlich von den Gerichten zu klären.

Ein eher kurzes „Gast"-Spiel im Berichtszeitraum hatten die Gästeregistrierungen im Contact-Tracing. Ebenso heftig wie so manche Diskussion darüber, ob es sich beim Lieblingslokal um ein Gasthaus oder ein Wirtshaus handeln würde, fiel die Schelte der DSB zur fehlenden Rechtmäßigkeit der Gästekontaktdatenlisten aus. Für den VfGH scheiterte eine inhaltliche Prüfung schon an der fehlenden Dokumentation des Verordnungsgebers, die eine Verhältnismäßigkeit der Gästeerfassungen nachvollziehbar gemacht hätte.

Im Ergebnis hat sich auch in der Pandemie die DSGVO bewährt, denn der grundrechtlich determinierte Datenschutz macht auch in Krisenzeiten keine Pause.

51 Dazu bereits *Thiele/Wagner*, jusIT 2020/85, 228 ff.
52 Ausführlich dazu *Thiele*, Entscheidungsanmerkung, ZIIR 2021, 75 ff.
53 § 48a DSG 2000 idF BGBl I 13/2005.