Bundesministerium
Justiz

Republik Österreich
Datenschutz
behörde

REPUBLIK ÖSTERREICH DATENSCHUTZRAT

DATENSCHUTZTAG 2021

Vorwort des Vorsitzenden des Datenschutzrates

Abg.z.NR Mag. Friedrich Ofenauer

Das Jahr 2020 war in jeder Hinsicht ein besonderes. Nicht nur das Thema Gesundheit, sondern auch der Datenschutz standen im vergangenen Jahr im Mittelpunkt des Interesses. Und auch wenn die Pandemie es leider nicht erlaubt, den Europäischen Datenschutztag 2021 als Präsenzveranstaltung abzuhalten, möchte ich als Vorsitzender des Datenschutzrates diese Gelegenheit für einen kurzen datenschutzrechtlichen Rückblick auf die Tätigkeit des Datenschutzrates im Jahr 2020 nutzen.

Die vergangenen Monate haben eine überdurchschnittliche Anzahl an Sitzungen des Datenschutzrates notwendig gemacht. COVID-19 stellte den Datenschutzrat dabei vor gänzlich neue Herausforderungen, da für zahlreiche Datenverarbeitungen im Gesundheitsbereich personenbezogene Daten benötigt werden. Der Datenschutzrat hat in diesem Zusammenhang Änderungen des Epidemiegesetzes 1950 und des COVID-19-Maßnahmengesetz geprüft und dazu Stellung genommen. Zudem wurden in den Sommermonaten durch einen Arbeitsausschuss des Datenschutzrates Prinzipien für die Verwendung von Contact Tracing und Contact Tracing-Apps vor dem Hintergrund der COVID-19-Pandemie sowie Grundsätze für die Verarbeitung von Gesundheitsdaten vor dem Hintergrund der COVID-19-Pandemie ausgearbeitet und im Datenschutzrat beschlossen. Im weiteren Zusammenhang mit der Pandemie stand auch die Prüfung der Änderung des Gesundheitstelematikgesetzes 2012, mit welcher der Elektronische Impfpass bzw. das zentrale Impfregister gesetzlich verankert werden. Auch die eHealth-Verordnung wurde in diesem Zusammenhang vom Datenschutzrat geprüft. Neben diesen Datenverarbeitungen im Gesundheitsbereich hat sich der Datenschutzrat insbesondere auch mit dem Anti-Doping-Bundesgesetz 2021, dem Hass-im-Netz-Bekämpfungs-Gesetz und dem Kommunikationsplattformen-Gesetz befasst.

Als Vorsitzender dieses Gremiums bin ich dankbar dafür, dass der Datenschutzrat mit seinen Mitgliedern und Ersatzmitgliedern auch in diesen schwierigen Zeiten handlungsfähig geblieben ist und mit seiner Arbeit auch aufgezeigt hat, dass die Bekämpfung der Pandemie und die Wahrung des Datenschutzes nicht im Widerspruch stehen müssen.

Auch in diesem Jahr ist zu erwarten, dass herausfordernde datenschutzrechtliche Fragen an den Datenschutzrat herangetragen werden. In diesem Sinne wäre es mir eine besondere Freude, wenn der Europäische Datenschutztag 2022 wieder im Rahmen eines persönlichen Austausches stattfinden könnte!

Bleiben Sie gesund!

Wien, 21. Jänner 2021

Friedrich Ofenauer

Vorwort des Leiters der Stabsstelle Datenschutz im Bundesministerium für Justiz

Mag. Dr. Eckhard Riedl

Mit Ausnahme des in jeder Hinsicht besonderen Jahres 2020 haben zuvor 13 Jahre in Folge Vortrags- und Diskussionsveranstaltungen zu datenschutzrechtlichen Themenstellungen anlässlich der Unterzeichnung der Datenschutzkonvention des Europarats am 28. Jänner 1981 im Bundeskanzleramt und zuletzt im Bundesministerium für Justiz – gemeinsam vom Verfassungsdienst, der Datenschutzbehörde und dem Datenschutzrat organisiert – stattgefunden. Der Part des Verfassungsdienstes und der dortigen vormaligen Datenschutzabteilung wird im Lichte der Änderungen durch die Bundesministeriengesetz-Novelle vom Jänner 2020 nunmehr von der im Bundesministerium für Justiz eingerichteten Stabsstelle für Datenschutz übernommen. Die COVID 19-Pandemie mit den damit einhergehenden Restriktionen verhindert in diesem Jahr leider die Abhaltung der gewohnten traditionellen Veranstaltung zum Datenschutztag. Gerade für das Jahr 2021 ist dies gleich in mehrerlei Hinsicht besonders bedauerlich.

Am 28. Jänner 2021 jährt sich die Unterzeichnung der Datenschutzkonvention des Europarats zum vierzigsten Mal. Österreich hat die Datenschutzkonvention und das Zusatzprotokoll 1988 bzw. 2008 ratifiziert. Die im Jahr 2012 aufgenommenen Verhandlungen auf Europaratsebene zur Modernisierung der Datenschutzkonvention konnten mit der Annahme des Änderungsprotokolls zur Datenschutzkonvention durch das Ministerkomitee des Europarats anlässlich der 128. Ministertagung am 18. Mai 2018 abgeschlossen werden. Unter österreichischem EU-Ratsvorsitz wurden die notwendigen Schritte zur Ermöglichung der Ratifikation dieses Änderungsprotokolls durch die EU-Mitgliedstaaten eingeleitet. Dementsprechend hat Österreich das Protokoll zum frühestmöglichen Zeitpunkt am 10. Oktober 2018 unterzeichnet. Wenn nun schon das 40-jährige Bestehen der Datenschutzkonvention pandemiebedingt nur mit kleineren symbolischen Akten geehrt werden kann, sollte es in diesem Jubiläumsjahr aber gelingen, die Ratifikation des Änderungsprotokolls zur Datenschutzkonvention in Österreich abzuschließen.

Die vergangenen Monate haben gezeigt, dass die Bekämpfung einer weltweiten Gesundheitskrise notgedrungen auch massive Eingriffe in grundrechtliche Positionen bedingt, wie sie bis vor Kurzem in einer auf rechtlichen Grundwerten basierenden und demokratisch geprägten Gesellschaft noch nicht vorstellbar gewesen wären. Neben dem Recht auf Freizügigkeit, dem Recht auf Erwerbsfreiheit und Eigentum sowie dem Recht auf Achtung des Privat- und Familienlebens zählt auch das Grundrecht auf Datenschutz zu jenen Grundrechten, die im Rahmen der Pandemiebekämpfung weitreichenden Beschränkungen unterworfen wurden. Selbst unter Berücksichtigung der zweifellos außergewöhnlichen Umstände, die zweifellos außergewöhnliche Maßnahmen erfordern, und in Anerkennung des (rechts)politischen Beurteilungs- und Gestaltungsspielraums des Gesetzgebers muss die Achtung und Einhaltung grundrechtlicher Positionen von ungebrochener und unerschütterbarer Wichtigkeit sein. Die vielbeschworene Krisenfestigkeit der Grundrechte gilt es auch im Hinblick auf die Achtung des Grundrechts auf Datenschutz unter Beweis zu stellen. Das macht aus datenschutzrechtlicher Sicht eine fachliche, auch kritische Auseinandersetzung mit der einen oder anderen Maßnahme zur Krisenbewältigung unumgänglich.

Nicht zuletzt haben die traditionellen Veranstaltungen zum Datenschutztag der „Datenschutz-Community“ aus dem öffentlichen und privaten Bereich in großem Rahmen und schönem Ambiente die seltene Möglichkeit zum einschlägigen und gehaltvollen Informations- und Meinungsaustausch geboten. Wie hoch der Wert von unmittelbaren, nicht

technikbasierten Sozialkontakten in fachlich ausgewiesenem und dennoch ungezwungenem Rahmen einzuschätzen ist, ist in Ermangelung solcher Möglichkeiten spätestens seit den pandemiebedingt langanhaltenden Kontakt- und Bewegungsbeschränkungen leidvoll bekannt.

In diesem Sinne ist auf eine rauschende Veranstaltung zum Datenschutztag 2022 zu hoffen, bei der wir auf die österreichische Ratifikation des Änderungsprotokolls zur Datenschutzkonvention und auf die erfolgreiche Bewältigung der Gesundheitskrise in Einklang mit grund- und datenschutzrechtlichen Werten in altbekannter, noch nicht vergessener Geselligkeit anstoßen können.

Wien, am 25. Jänner 2021

Eckhard Riedl

Vorwort der Leiterin der Datenschutzbehörde

Dr. Andrea Jelinek

Sehr geehrte Leserinnen und Leser, liebe Freundinnen und Freunde des Datenschutzes!

Am 28. Jänner wird europaweit der Datenschutztag gefeiert, mit welchem an den 28. Jänner 1981 erinnert werden soll: An diesem Tag wurde die Datenschutzkonvention des Europarates zur Unterschrift aufgelegt. Somit feiern wir heuer 40 Jahre Datenschutz in Europa!

Die Datenschutzkonvention spielt im täglichen Bewusstsein zu Unrecht keine große Rolle. Die tragenden Prinzipien des Datenschutzes, wie die Rechtmäßigkeit der Datenverarbeitung und Grundsätze wie Datenminimierung und Zweckbindung sind bereits in der Datenschutzkonvention verankert.

Wir sollten uns daher alle daran erinnern, dass sie die Grundlage für das europäische Verständnis des Datenschutzes ist und die unionsrechtlichen Regelungen zum Datenschutz – zunächst die Richtlinie 95/46/EG und schließlich die DSGVO und die Richtlinie (EU) 2016/680 – inhaltlich darauf aufbauen.

Zudem ist die – zwischenzeitig modernisierte – Datenschutzkonvention nach wie vor der einzige multilaterale Staatsvertrag, der ausschließlich dem Schutz personenbezogener Daten gewidmet ist, dem mittlerweile auch außereuropäische Staaten der Datenschutzkonvention beigetreten sind. Dies zeigt, dass das europäische Verständnis des Datenschutzes nicht nur auf Europa begrenzt ist, sondern auch andere Länder die Notwendigkeit erkannt haben, diese Rechtsmaterie verbindlich zu regeln.

Für die Datenschutzbehörde stellen das Jahr 2020 und auch das laufende Jahr sicherlich die bis dato herausforderndsten Jahre seit 1980 – jenem Jahr, in welchem die Datenschutzkommission ihre Tätigkeit aufnahm – dar.

Aufgrund der anhaltenden Pandemie wurde die Entscheidung getroffen, den jährlichen Datenschutztag, der üblicherweise als Präsenzveranstaltung des Datenschutzrates, des Bundeministeriums für Justiz und der Datenschutzbehörde stattfindet, dieses Jahr im Wege einer Sonderschrift zu begehen. Es wäre zwar technisch möglich, eine virtuelle Veranstaltung durchzuführen; erfahrungsgemäß führt dies bei großer Teilnehmerzahl aber dazu, dass es zu Übertragungsproblemen kommen kann, was der Qualität einer solchen Veranstaltung schadet.

In dieser Sonderschrift nehmen Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde zu insgesamt vier Themen Stellung, die im Jahr 2020 besondere datenschutzrechtliche Relevanz hatten:

- Der Zugriff auf das Ergänzungsregister für sonstige Betroffene
- Die Verarbeitung von personenbezogenen Daten für Zwecke der Kontaktnachverfolgung
- Der Zugriff auf lokale Register für Zwecke der so genannten Massentestungen
- Der BREXIT und seine Auswirkungen

Dabei ist zu berücksichtigen, dass diese Beiträge Fachbeiträge darstellen und – soweit sie nicht bereits rechtkräftige Entscheidungen der Datenschutzbehörde betreffen – die Datenschutzbehörde nicht binden.

Wir alle hätten uns gewünscht, dieses runde Jubiläum anders zu begehen. Ich wünsche Ihnen viel Freude bei der Lektüre und vor allem Gesundheit und Wohlergehen im Jahr 2021!

Dr. Andrea Jelinek, 25. Jänner 2021

Inhalt

I. Das Ergänzungsregister für sonstige Betroffene

von Mag. Vanessa NEUDECKER[1]

1. Einleitung

Im Zuge der Abwicklung des „Härtefall-Fonds“ erfuhr das „Ergänzungsregister für sonstige Betroffene“ (im Folgenden ERsB) mediale Präsenz.[2] Der Härtefall-Fonds - als Teil des umfassenden Hilfspakets der Österreichischen Bundesregierung - ist eine Förderung für Selbstständige.[3] Um Geld aus dem Fonds zu lukrieren, war bei dessen Beantragung - zur Erleichterung des Datenabgleichs - mitunter die Angabe der Kennzahl des Unternehmensregisters (KUR) oder die Global Location Number (GLN) erwünscht.[4] Über die Website des Wirtschaftsministeriums (www.ersb.gv.at) war es möglich, die entsprechenden Kennziffern zu erfragen.[5] Durchschnittlich erfolgten über den Webzugang 50.000 Zugriffe pro Woche, wobei die Anzahl der Zugriffe eine Woche nach Einführung des Härtefallfonds auf über 7 Mio. anwuchs.[6] Nach anfänglichen Zweifeln über eine mögliche Unrechtmäßigkeit der öffentlichen Führung des Registers[7], kritisierte NEOS in der Aussendung zur Pressekonferenz am 8. Mai 2020[8] - unterstützt durch die NGO epicenter.works - die öffentliche Führung des „Ergänzungsregisters für sonstige Betroffene“.[9] Am selben Tag wurde der öffentliche Zugang zum ERsB deaktiviert.[10]

---

[1] Mag. Neudecker ist Bedienstete der Datenschutzbehörde; der Beitrag gibt ausschließlich ihre persönliche Meinung wieder. Der Beitrag ist außerdem eine verkürzte Wiedergabe der von ihr im Rahmen eines universitären Lehrganges erstellten Masterthese.

[2] Vgl uA oV "Gigantisches Datenleck" rund um Härtefall-Fonds entdeckt <https://futurezone.at/netzpolitik/gigantisches-datenleck-rund-um-haertefall-fonds-entdeckt/400835555> (20.01.2021), Vgl oV, Was wir über den Datenschutzskandal wissen <https://futurezone.at/netzpolitik/was-wir-ueber-den-datenschutzskandal-wissen/400835993> (20.01.2021); Vgl Laufer, Hunderttausende Adressen von Bürgern in Onlineregister auffindbar <https://www.derstandard.at/story/2000117351903/gigantisches-datenleck-hunderttausende-adressen-von-buergern-im-netz-auffindbar> (20.01.2021).

[3] <https://www.wko.at/service/haertefall-fonds-phase-2.html> (20.01.2021).

[4] <https://www.wko.at/service/haertefall-fonds-phase-2.html#heading_3__Welche_Unterlagen_soll_ich_fuer_die_Beantragung_vorbereiten_> (20.01.2021).

[5] <https://futurezone.at/netzpolitik/was-wir-ueber-den-datenschutzskandal-wissen/400835993> (20.01.2021).

[6] Vgl Anfragebeantwortung 2016/AB XXVII.GP, 6f.

[7] Vgl *Hoyos*, Das größte Datenleck der Republik <https://www.douglas-hoyos.at/post/das-gr%C3%B6%C3%9Fte-datenleck-der-republik> (20.01.2021).

[8] Vgl *oV,* AVISO: NEOS-PK: Massives Datenschutz-Leck um Wirtschafts- und Finanzministerium und WKO aufgedeckt, Morgen Freitag 10:30 <https://www.ots.at/presseaussendung/OTS_20200507_OTS0134/aviso-neos-pk-massives-datenschutz-leck-um-wirtschafts-und-finanzministerium-und-wko-aufgedeckt-morgen-freitag-1030> (20.01.2021).

[9] Vgl *Laufer,* Hunderttausende Adressen von Bürgern in Onlineregister auffindbar <https://apps.derstandard.at/privacywall/story/2000117351903/gigantisches-datenleck-hunderttausende-adressen-vonbuergern-im-netz-auffindbar> (20.01.2021).

[10] Vgl Anfragebeantwortung 2016/AB XXVII GP, 3.

In der Folge wurde über ein „*gigantische[s] Datenleck*“[11], vom „*größten Datenskandal der Republik*“[12], einem „*sorglosen Umgang des Staates mit unseren Daten*“[13] sowie von einem „*löchrigen Datenschutzverständnis der Ministerien*“[14] berichtet.[15]

Der Fokus der im Zuge der Abwicklung des Härtefall-Fonds ausgelösten Debatte lag auf der Frage der Rechtmäßigkeit der öffentlichen Führung – und folglich der möglichen Einsehbarkeit Daten natürlicher Personen – des ERsB. Vor diesem Hintergrund soll in diesem Beitrag das Ergänzungsregister für sonstige Betroffene beleuchtet werden.

2. Ergänzungsregister für sonstige Betroffene

Das Ergänzungsregister, geführt durch die Stammzahlenregisterbehörde, gliedert sich in das Ergänzungsregister für natürliche Personen (ERnP) und das Ergänzungsregister für sonstige Betroffene (ERsB).[16] Die Führung des Ergänzungsregisters oblag bis Ende 2018 der Datenschutzbehörde.[17] Angesichts der Bundesministeriengesetz-Novelle 2017, kam es zu Änderungen der Zuständigkeiten der Bundesministerien.[18] Im Zuge dessen fiel die Zuständigkeit betreffend die Stammzahlenregisterbehörde in den Wirkungsbereich des BMDW. 2018 wurde diese Änderung im E-Government-Gesetz verankert, sodass die Aufgaben der Stammzahlenregisterbehörde seit 28. Dezember 2018 durch die Bundesministerin für Digitalisierung und Wirtschaftsstandort wahrgenommen werden.[19]

---

[11] *oV,* "Gigantisches Datenleck" rund um Härtefall-Fonds entdeckt <https://futurezone.at/netzpolitik/gigantisches-datenleck-rund-um-haertefall-fonds-entdeckt/400835555> (20.01.2021).
[12] *oV,* "Größter Datenskandal der Republik" <https://www.w24.at/News/2020/5/Groesster-Datenskandal-der-Republik> (20.01.2021).
[13] *Neubauer,* Der sorglose Umgang des Staates mit unseren Daten <https://www.diepresse.com/5810852/der-sorglose-umgang-des-staates-mit-unseren-daten> (28.12.2020).
[14] *oV,* Löchriges Datenschutzverständnis in Ministerien <https://www.wienerzeitung.at/nachrichten/politik/oesterreich/2059907-Register-nach-Neos-Alarmruf-offline.html> (20.01.2021).
[15] *Laufer,* Hunderttausende Adressen von Bürgern in Onlineregister auffindbar <https://www.derstandard.at/story/2000117351903/gigantisches-datenleck-hunderttausende-adressen-von-buergern-im-netz-auffindbar> (20.01.2021).
[16] § 1 ERegV 2009.
[17] Vgl *oV* <https://www.dsb.gv.at/stammzahlenregisterbehorde> (20.01.2021).
[18] Bundesgesetz, mit dem das Bundesministeriengesetz 1986 geändert wird (Bundesministeriengesetz-Novelle 2017), BGBl 164/2017.
[19] Vgl Bundesgesetz, mit dem das E-Government-Gesetz, das IKT-Konsolidierungsgesetz, das Signatur- und Vertrauensdienstegesetz, das Unternehmensserviceportalgesetz, das Bundesgesetzblattgesetz, das Zustellgesetz, die Bundesabgabenordnung, das Bundesfinanzgerichtsgesetz, das Meldegesetz 1991, das Passgesetz 1992 und das Personenstandsgesetz 2013 geändert werden BGBl. I Nr. 104/2018; *oV,* Stammzahlenregisterbehörde <https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde.html> (20.01.2021).

2.1. Hintergrund

Geprägt durch das mit 1. März 2004 in Kraft getretene und zuletzt 2018 novellierte E-GovG[20] - als rechtliche Grundlage elektronischer Behördendienste[21] - trägt das Ergänzungsregister zur Umsetzung des Bürgerkartenkonzepts (nunmehr E-ID) bei, indem es Betroffenen, welche aus rechtlichen Gründen nicht in ein Basisregister (ZMR, Firmenbuch, Vereinsregister) eingetragen werden können,[22] die Möglichkeit bietet, mit einem eindeutigen Ordnungsbegriff am E-Government teilnehmen zu können[23] und deckt somit den verbleibenden „Rest" an Betroffenen ab.[24]

2.2. Rechtsgrundlage

Das E-GovG sieht die Führung des Registers gemäß § 6 E-GovG seit 2004 vor,[25] behält jedoch nähere Angaben über Inhalt sowie Art und Weise der Handhabung zu erlassenden Verordnungen vor.[26] So fanden sich nähere Ausführungen zum Ergänzungsregister zunächst in der „*Verordnung des Bundeskanzlers über das Ergänzungsregister nach dem E-Government-Gesetz*" aus dem Jahre 2005,[27] welche durch die „*Verordnung des Bundeskanzlers über das Ergänzungsregister (Ergänzungsregisterverordnung 2009 – ERegV 2009)*" abgelöst wurde.[28] Die Ergänzungsregisterverordnung erfuhr zuletzt am 10. Juli 2020, durch die „*317. Verordnung der Bundesministerin für Digitalisierung und Wirtschaftsstandort mit der die Ergänzungsregisterverordnung 2009 (ERegV 2009) geändert wird",* eine Modifikation.[29]

2.3. Eintragung

Entsprechend § 10 ERegV 2009 darf eine Eintragung ins ERsB nur aus nachstehenden Gründen erfolgen:[30]

- Aufgrund einer Selbstregistrierung, anhand einer Antragstellung des Betroffenen selbst.

[20] E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004 idF BGBl. I Nr. 104/2018.
[21] Vgl § 1 Abs 1 E-GovG.
[22] Vgl *Bundesministerium für Digitalisierung und Wirtschaftsstandort* (Hrsg), österreichisches E-Government ABC, 166.
[23] Vgl Ebd., 164.
[24] Vgl *Liebenwein/Bittermann*, AnwBl 2020, 415.
[25] E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004 idF BGBl. I Nr. 104/2018; § 6 E-GovG.
[26] Vgl *Jahnel*, jusIT 2020, 33 (88); Vgl. § 6 E-GovG.
[27] Ergänzungsregisterverordnung – ERegV, BGBl. II Nr. 2005/241.
[28] Ergänzungsregisterverordnung 2009 – ERegV 2009, StF: BGBl. II Nr. 331/2009.
[29] Ergänzungsregisterverordnung 2009 – ERegV 2009, BGBl. II Nr. 331/2009 idF BGBl. II Nr. 317/2020.
[30] Vgl § 10 Abs 1 ERegV 2009.

- Auf Ersuchen eines Auftraggebers des öffentlichen Bereichs im Zuge der Ausstattung einer Datenanwendung mit Stammzahlen.

- Zudem kann eine Eintragung aufgrund eines Ersuchens einer Institution, die unmittelbar durch Gesetz oder Verordnung eingerichtet ist, bewirkt werden.

- Schließlich darf eine Eintragung in das ERsB zur Vornahme von Änderungen erfolgen.[31]

2.4. Öffentliche Einsehbarkeit

Während das ERnP nicht öffentlich geführt wird, war das ERsB bis vor Kurzem, entsprechend § 14 ERegV 2009 (alt), im Internet öffentlich zugänglich.[32] Bereits die Erstfassung der Verordnung aus dem Jahre 2005 sah die Führung eines im Internet zugänglichen öffentlichen Registers sowie die für jedermann bestehende Möglichkeit, sich für seine Zwecke einen mit Amtssignatur versehenen elektronischen Auszug anfertigen zu lassen, vor.[33] Über den Webzugang https://www.ersb.gv.at konnte jeder eine direkte sowie indirekte Abfrage tätigen.[34] Der Auszug aus dem Ergänzungsregister enthielt dabei unter anderem folgende Daten:

- die rechtsgültige Bezeichnung des Betroffenen,

- Anschrift,

- Sitz,

- soweit vorhanden, Angaben über die eindeutige Identität der Personen, die für den Betroffenen vertretungsbefugt sind, samt Umfang der Vertretungsbefugnis.[35]

Hierbei handelt es sich zweifelsohne um personenbezogene Daten iSd Art. 4 DSGVO.[36] Seit der jüngsten Modifikation der Ergänzungsregisterverordnung am 10. Juli 2020 ist eine allgemeine öffentliche Verfügbarkeit des ERsB nicht mehr durch die Rechtsgrundlage gedeckt.[37]

---

[31] Vgl § 10 Abs 1 Z 1 – 3 ERegV 2009.
[32] § 14 ERegV 2009.; §6 Abs 4 E-GovG.
[33] BGBl 2005/241; §16 ERegV 2005.
[34] Vgl *Bundesanstalt Statistik Österreich* (Hrsg), Unternehmens Register für Zwecke der Verwaltung,12f.
[35] Vgl § 11 ERegV; *Jahnel*, jusIT 2020, 33 (88); ERsB: Geschwärzte Auszüge prominenter Leute <https://epicenter.works/document/2583 > (20.01.2021).
[36] Vgl *Hödl* in DSGVO Art 4 Rz 9.
[37] Ergänzungsregisterverordnung 2009 – ERegV 2009, BGBl II 331/2009 idF BGBl II 317/2020.

3. Datenschutzrechtliche Problemstellung

3.1. Problemstellung

Ausgehend vom derzeit bekannten und insoweit, diesem Beitrag zugrundeliegenden Sachverhalt, stellt sich die Frage, ob die Veröffentlichung der im ERsB enthaltenen Datensätze natürlicher Personen datenschutzkonform war. Da im Zuge der Modifikation der Ergänzungsregisterverordnung im gegebenen Zusammenhang die entsprechende Rechtsgrundlage zur öffentlichen Führung und somit zur Veröffentlichung der im Register enthaltenen Datensätze wegfiel - sowie das Register auch tatsächlich nicht mehr öffentlich einsehbar ist -, kommt es im Folgenden ausschließlich zur Darstellung eines Prüfungsansatzes, jedoch zu keiner abschließenden Beurteilung.[38]

3.2. Darstellung eines Prüfungsansatzes

Für die Verarbeitung personenbezogener Daten besteht grundsätzlich ein Verarbeitungsverbot, demnach bedarf die Verarbeitung einer entsprechenden Rechtsgrundlage.[39] Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Behörden zu schaffen,[40] kommt insoweit ausschließlich eine qualifizierte gesetzliche Grundlage als Erlaubnistatbestand in Betracht.[41] § 6 E-GovG iVm der ERegV 2009 (alt) wäre grundsätzlich eine taugliche Rechtsgrundlage kraft objektiven Rechts gewesen, die eine rechtliche Verpflichtung enthielt, das ERsB als ein im Internet öffentliches Register zu führen.

In einem zweiten Schritt wäre daher zu prüfen, ob die Veröffentlichung der im ERsB enthaltenen Datensätze - konkret jene mit Personenbezug - Deckung in dieser Verpflichtung findet. Dabei stellt sich insbesondere die Frage, ob allen voran überhaupt die Eintragung natürlicher Personen ins ERsB von der Rechtsgrundlage umfasst ist. Hierzu haben sich im Zuge der öffentlichen Diskussion grundsätzlich unterschiedliche Meinungen herausgebildet:

- Einerseits wird vertreten, dass kein Erlaubnistatbestand bestehe.[42] Die datenschutzrechtliche Unzulässigkeit wird dahingehend begründet, dass durch die in § 6 Abs. 4 E-GovG vorgesehene getrennte Führung des Ergänzungsregisters nach

[38] Für eine weiterreichende datenschutzrechtliche Beurteilung siehe auch die sich derzeit im Stadium der Einreichung befindliche Masterthese, verfasst von Mag. iur. Vanessa Neudecker mit dem Arbeitstitel: „*Die Causa Härtefall-Fonds „Österreichs größter Datenschutzskandal?“ “ (Universität Wien).*

[39] Vgl *Hödl* in DSGVO Art 4 Rz 113.

[40] Vgl ErwGr 47 Verordnung (EU) 2016/679; *Kastelitz/Hötzendorfer/Tschohl* in DSGVO Art 6, Rz 51.

[41] Vgl. DSB, 28.11.2014, GZ: DSB-D215.548/007-DSB/2014.

[42] Vgl *oV,* Neos-Gutachten zu Register erhöht Druck auf Regierung <https://www.derstandard.de/story/2000117559144/neos-gutachten-zu-register-erhoeht-druck-auf-regierung> (20.01.2021).

„natürlichen Personen“ und „sonstigen Betroffenen“ davon auszugehen sei, dass eine Eintragung von „natürlichen Personen“ ausschließlich im ERnP zu erfolgen habe und eine Eintragung von „natürlichen Personen“ ins ERsB folglich unzulässig sei.[43] Zudem wird angeführt, dass bereits nach dem klaren und unmissverständlichen Wortlaut des § 6 Abs. 4 E-GovG und des § 1 ERegV nur jene betroffenen natürlichen Personen in das Ergänzungsregister eingetragen werden dürfen, welche nicht bereits im Zentralen Melderegister aufscheinen. Daraus könne geschlossen werden, dass ein Mensch, der bereits im Zentralen Melderegister eingetragen ist, als betroffene natürliche Person weder in das ERnP noch in das ERsB eingetragen werden dürfe.[44]

- Eine andere Ansicht vertritt das BMDW. Im Gegensatz zum zuvor erläuterten Ansatz wird zwischen natürlichen Entitäten und juristischen Entitäten unterschieden und die Auffassung vertreten, dass ein und dieselbe natürliche Person – ein „Mensch“ – sowohl eine natürliche und juristische Entität besitzen und folglich mehrfach Betroffener iSd § 2 Z 7 E-GovG sein könne. Begründet wird dies durch den Umstand, dass ein berechtigtes Interesse daran bestehe, dass in elektronischen Verfahren unverwechselbar unterschieden werden könne, ob eine natürliche Person als natürliche oder juristische Entität agiere.[45] Folglich findet nach dieser Ansicht die Eintragung natürlicher Personen im ERsB Deckung in der Rechtsgrundlage.

- Zudem wurde vor allem in der Lehre die Verfassungswidrigkeit der öffentlichen Führung des Registers an sich, – sowohl für die im Register eingetragen natürlichen, wie auch juristischen Personen – aufgrund eines Verstoßes gegen das Gebot des gelindesten Mittels vertreten. Denn auch unter der Prämisse einer gesetzlich zugelassenen Beschränkung, ist der konkrete Eingriff in das Grundrecht unzulässig, wenn er nicht in der jeweils gelindesten, zum Ziel führenden Art vorgenommen wird.[46] Begründet wurde dies insbesondere, durch die bestehende Möglichkeit, das Register ebenso wie das ERnP nicht öffentlich zu führen. Auch sei nicht ersichtlich, inwiefern eine nicht öffentliche Führung dem Zweck im Wege stehen würde.[47]

Je nach zu folgender Ansicht ist daher von datenschutzkonformer, datenschutzwidriger bzw. verfassungswidriger Veröffentlichung auszugehen.

Eine Entscheidung der Datenschutzbehörde in diesem Zusammenhang ist noch nicht erfolgt.

[43] Vgl Jahnel, jusIT 2020, 33 (88).
[44] Vgl *Jung*, Gutachterliche Stellungnahme, 4f.
[45] Vgl Anfragebeantwortung 2016/AB XXVII.GP, 9.
[46] Vgl VfGH 28.11.2001, B 2271/100; *Thiele/Wagner* in DSG §1 Rz 106.
[47] Vgl Jahnel, jusIT 2020, 33 (88).

II. Entscheidung der DSB zur Erhebung von Kundendaten in der Gastronomie aufgrund der Wiener Contact-Tracing-Verordnung

von Mag. Clemens Trauner[48]

1. Abstract

Gegenstand dieses Beitrages ist die **Entscheidung der Datenschutzbehörde GZ 2020-0.743.659 (VZ: D124. 3093) vom 19. November 2020**. Die Datenschutzbehörde (DSB) hat infolge der Beschwerde einer betroffenen Person ausgesprochen, dass eine Gastronomin das Recht des Betroffenen auf Geheimhaltung durch Erhebung seiner personenbezogenen Daten im Rahmen eines Restaurantbesuches verletzt hat und der Wiener Contact-Tracing Verordnung[49] keine gesetzliche Verpflichtung zur Erhebung von Kundendaten durch GastronomInnen zu entnehmen war. Die DSB hat in dieser Entscheidung überdies § 5 Abs. 3 EpiG[50] iVm der Wiener Contact-Tracing VO für gegenständlich unanwendbar erklärt und dabei ausgesprochen, dass es sich bei Kontaktdaten (Name, Telefonnummer) sowie der Information über potenziellen Kontakt zu einer an Sars-Cov-2 erkrankten Person um Gesundheitsdaten iSd Art. 4 Z 15 DSGVO[51] handeln kann, sofern diese in ausschließlich gesundheitsbezogenem Kontext verarbeitet werden.

Gegen diese Entscheidung wurde kein Rechtsmittel eingelegt, sodass sie in Rechtskraft erwachsen ist.

2. Sachverhalt

Der Beschwerdeführer besuchte am 2. Oktober 2020 eine Betriebstätte der Beschwerdegegnerin, welche als Gastgewerbe in der Betriebsart Kaffee-Restaurant betrieben wurde. Im Eingangsbereich des Lokals befanden sich Hinweistafeln, die auf die „Datenerhebung für die COVID-19 Gästeregistrierung“ verwiesen. Den KundInnen wurde die Möglichkeit geboten, ihre Kontaktdaten über einen QR-Scan oder mittels Papierformular

[48] Mag. Clemens Trauner ist Bediensteter der Datenschutzbehörde und hat diesen Fall federführend bearbeitet. Die daraus getroffenen Ableitungen geben ausschließlich seine persönliche Meinung wieder.
[49] Verordnung des Magistrats der Stadt Wien betreffend Auskunftserteilung für Contact Tracing im Zusammenhang mit Verdachtsfällen von COVID-19, ABl 2020/41.
[50] Epidemiegesetz 1950 (EpiG), StF: BGBl. Nr. 186/1950 idF BGBl. Nr. 104/2020.
[51] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L119 vom 4.5.2016 S. 1.

anzugeben. In der Datenschutzerklärung verwies die Beschwerdegegnerin auf Art. 6 Abs. 1 lit. c DSGVO iVm mit der Wiener Contact-Tracing VO und gab an, dass sie zur Erhebung der KundInnendaten gesetzlich verpflichtet sei. Weiters wurde darin auf das Hausrecht der Beschwerdegegnerin und die Möglichkeit eines Lokalverweises bei Weigerung, seine Daten zur Verfügung zu stellen, verwiesen. Der Beschwerdeführer nutzte die Variante des QR-Scans und gab seinen Namen sowie seine Telefonnummer an.

3. Allgemeines zur Wiener Contact-Tracing VO

Der Magistrat der Stadt Wien (MA 15) erließ am 28. September 2020 auf Grundlage des § 5 Abs. 3 EpiG eine Verordnung betreffend Auskunftserteilung für Contact-Tracing im Zusammenhang mit Verdachtsfällen von COVID-19 (Wiener Contact-Tracing Verordnung). Die Verordnung des Magistrats der Stadt Wien trat mit 31. Dezember 2020 außer Kraft.

Mit dieser Verordnung präzisierte der Verordnungsgeber die in § 5 Abs. 3 EpiG normierte Auskunftspflicht gegenüber der Bezirksverwaltungsbehörde im Rahmen von Erhebungen über das Auftreten anzeigepflichtiger Krankheiten. Demnach sind *alle Personen […] die zu den Erhebungen einen Beitrag leisten können […] der Bezirksverwaltungsbehörde, zur Auskunft verpflichtet.*

Wenngleich die Auskunftspflicht des § 5 Abs. 3 EpiG schon nach dem Wortlaut ohnehin alle Personen, die einen Beitrag zur Ermittlung von Verdachtsfällen leisten können, erfasst, wurde in § 1 Z 1 und Z 2 der Wiener Contact-Tracing VO eine Konkretisierung der auskunftspflichtigen Stellen sowie des Inhalts der Auskunft normiert.

Nach § 1 Z 2 lit. e Wiener Contact-Tracing Verordnung hatte eine Auskunft durch eine Betriebsstätte der Gastronomie Vorname, Name, Telefonnummer, E-Mail-Adresse und Tischnummer der Kundinnen zu enthalten.

Im Rahmen des Verfahrens stellten sich für die DSB bei der Auslegung dieser Bestimmung insbesondere die Fragen, wie die Daten im gegenständlichen Kontext zu qualifizieren waren, ob es sich bei § 5 Abs. 3 iVm § 1 Z 2 lit. e Wiener Contact-Tracing Verordnung um ausreichend klare Eingriffsnormen iSd 1 Abs. 2 DSG[52] handelte und ob die Vorgehensweise der Verantwortlichen gegenüber ihren KundInnen nachvollziehbar und zulässig war.

4. Zur Frage des Vorliegens von Gesundheitsdaten

Um beantworten zu können, ob die Verarbeitung der Daten des Beschwerdeführers zulässig war, hatte sich die DSB vorweg die Frage zu stellen, ob es sich - wie auf den ersten Blick

[52] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl. I Nr. 165/1999 idF BGBl. Nr. 14/2019.

anzunehmen - bei Namen und Telefonnummer „lediglich“ um personenbezogene Daten iSd Art. 4 Z 7 DSGVO oder womöglich um Daten besonderer Kategorien gemäß Art. 9 DSGO handelte.

Gemäß Art. 4 Z 15 DSGVO sind Gesundheitsdaten *personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.*

Diesen kommt im Gegensatz zu personenbezogenen Daten insbesondere deshalb eine erhöhte Schutzwürdigkeit zu, *da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können*[53]*.*

Der Rechtsprechung des EuGH[54] folgend legte die DSB ein weites Verständnis an den Begriff Gesundheitsdatum an. In Zusammenschau mit ErwGr 35 Satz 2 sind unter Gesundheitsdaten ebenso Nummern, Symbole oder Kennzeichen zu verstehen, die einer natürlichen Person zugeteilt wurden, um diese Person für gesundheitliche Zwecke eindeutig zu identifizieren. In Fortentwicklung ihrer Rsp, wonach aus Gesundheitsdaten jedenfalls *Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen müssen*[55] kam die DSB zum Ergebnis, dass Name und Telefonnummer des Beschwerdeführers als Gesundheitsdaten iSd Art. 4 Z 15 DSGVO zu sehen waren, da sie nicht als bloßer Identifikator, sondern ausschließlich in einem gesundheitlichen Kontext und zwar ausschließlich zum Zweck des *„Schutz[es] von Leben und Gesundheit [der] Mitarbeiter und [der] Gäste [der Beschwerdegegnerin] im Zusammenhang mit dem Auftreten des Coronavirus bzw. der COVID-19-Epidemie“* sowie zum Zweck der *„Unterstützung“* der Bezirksverwaltungsbehörde bei der Ermittlung von Kontaktpersonen bei Auftreten eines Infektionsfalles erhoben wurden.

5. Zu den Erlaubnistatbeständen des Art. 9 Abs. 2 DSGVO

5.1. Einwilligung

Nach Art. 9 Abs. 2 lit. a DSGVO ist die Verarbeitung von Daten besonderer Kategorien, wie Gesundheitsdaten dann zulässig, wenn die betroffene Person in die Verarbeitung eingewilligt hat. Die DSB kam im gegenständlichen Verfahren jedoch zum Ergebnis, dass unter den

[53] Siehe ErwGr 51 der DSGVO; Vgl. dazu auch *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 9 DSGVO Rz 3 (Stand 7.5.2020, rdb.at).
[54] Vgl. EuGH 6. 11. 2003, C-101/1, Lindqvist, Rz 49 ff.
[55] Siehe ErwGr 35 der DSGVO; Vgl. in Bezug auf die Sozialversicherungsnummer etwa den Bescheid vom 9.4.2019, GZ: DSB-D123.526/0001-DSB/2019; dazu auch *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 9 DSGVO Rz 18/2 (Stand 7.5.2020, rdb.at).

gegebenen Umständen von keiner gültig erteilten Einwilligung ausgegangen werden konnte, da an eine solche ein strenger Maßstab anzulegen ist. In einer rezenten Entscheidung hat der EuGH hierzu festgehalten, dass es sich bei einer Einwilligung um eine *aktive* und unmissverständliche Willenshandlung handeln muss.[56] Auch ErwGr 42 der DSGVO hält dazu fest, dass nur dann von einer freiwillig erteilten Einwilligung ausgegangen werden soll, wenn die betroffene Person *eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden*. Die DSB hat bereits ausgesprochen, dass Freiwilligkeit überdies das Bestehen einer zumutbaren Alternative erfordert.[57]

Hierbei war zu berücksichtigen, dass sich der Anwendungsbereich der Wiener Contact-Tracing VO auf das gesamte Gemeindegebiet erstreckte und dem Beschwerdeführer sohin auch keine echten Wahlmöglichkeiten oder Alternativen zur Verfügung standen. Wobei die zur Verfügung stehende Wahlmöglichkeit an der vom Beschwerdeführer in Anspruch genommenen Art der (Dienst-)Leistung zu beurteilen war. Zwar mag es zutreffen, dass dieser die Speisen lediglich bei der Beschwerdegegnerin oder andernorts ohne Angabe seiner Daten abholen hätte können, doch wäre ein Restaurantbesuch und der Verzehr von Speisen in der Betriebsstätte, also dem Lokal, auch bei anderen GastronomInnen nur unter denselben Bedingungen möglich gewesen. Schließlich hätte er bei allen anderen Gastronomiebetrieben im Wiener Gemeindegebiet ebenso mit der Erhebung seiner Daten rechnen müssen. Weiters drohte diesem gleichsam für den Fall, dass er die Angabe seiner Daten verweigerte, der Lokalverweis, mithin also ein Nachteil, womit von keiner freiwillig erteilten Einwilligung auszugehen war.

5.2. Zur gesetzlichen Grundlage und deren normativem Gehalt

Da sohin keine gültige Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO vorlag, stellte sich die Frage, ob ein anderer Erlaubnistatbestand die Verarbeitung rechtfertigen konnte. Nach Art. 9 Abs. 2 lit. i DSGVO ist die Verarbeitung personenbezogener Daten besonderer Kategorien auf Grund einer gesetzlichen Verpflichtung u.a. dann zulässig, *wenn die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsieht, erforderlich* ist.

[56] Vgl. EuGH 11.11.2020, C-61/19 Orange România Rz 52 mwN.
[57] Vgl. dazu den Bescheid vom 30.11.2018, GZ: DSB-D122.931/0003-DSB/2018.

Die Beschwerdegegnerin vermeinte nach § 5 Abs. 3 EpiG iVm § 1 Abs. 2 lit. e der Wiener Contact-Tracing VO zur Verarbeitung und Speicherung der Daten verpflichtet gewesen zu sein.

Bei genauer Betrachtung des Wortlauts des § 5 Abs. 3 EpiG konnte aus diesem eine solche Verpflichtung nach Ansicht der DSB jedoch nicht abgeleitet werden. Dies, weil die Gesetzesbestimmung ausschließlich jene, die zu den Erhebungen über das Auftreten einer (ansteckenden) Krankheit beitragen können und nur auf Verlangen der Bezirksverwaltungsbehörde, zur Auskunft verpflichtet.

Zwar enthielt die Wiener Contact-Tracing VO eine Präzisierung wer aller unter die in § 5 Abs. 3 EpiG genannten Personen fällt und welchen Inhalt eine Auskunft an die BvB zu enthalten hatte, doch war dem Wortlaut des in Rede stehenden Gesetzes- bzw. Verordnungstextes kein darüberhinausgehender normativer Gehalt zu entnehmen, der eine Verpflichtung zur Verarbeitung personenbezogener Daten enthielt. So ließ nach Ansicht der DSB insbesondere der Wortlaut des § 1 der Wiener Contact-Tracing VO, demzufolge die auskunftspflichtigen Stellen Daten gemäß § 1 leg. cit. ausschließlich zum Zwecke der Nachverfolgung der Kontakte bei Auftreten eines Verdachtsfalles von COVID-19 gespeichert und verarbeitet werde durften, ableiten, dass eine „Verarbeitungspflicht“ gerade nicht bestand. Die Auskunftsplicht und die strafbewährte Verletzung selber konnte sich daher lediglich auf schon vorhandene Daten erstrecken.

5.3. Mangelnde Transparenz

Die DSB kam darüber hinaus zum Ergebnis, dass die Wiener Contact-Tracing VO iVm § 5 Abs. 3 EpiG gegenständlich unangewendet zu bleiben hatte. Dabei hat die DSB erwogen, dass es sich hierbei um Eingriffsnormen iSd § 1 Abs. 2 DSG handelte. Zu Beschränkungen bzw. Eingriffen in die Rechte nach Art. 7 bzw. Art. 8 GRC[58] hat der EuGH bereits wiederholt ausgesprochen, dass solche Regelungen *klare und präzise Regeln für die Tragweite und die Anwendung dieser Maßnahme vorsehen und Mindestanforderungen aufstellen müssen, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauch sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung, ermöglichen*.[59]

[58] Charta der Grundrechte der Europäischen Union, ABl. Nr. 2016/C 202/389.
[59] Vgl. EuGH vom 6.10.2015, C-362-14, Rz. 91 Schrems mwN).

Umso bedeutender sind diese Garantien nach Ansicht des EuGH jedoch, wenn Daten automationsunterstützt verarbeitet werden und es sich um „sensible“ Daten handelt.[60] Zudem ist es nach der Rechtsprechung des EuGH erforderlich, dass eine Datenverarbeitung nicht nur auf einen Erlaubnistatbestand gestützt werden kann, sondern sind dabei kumulativ alle Grundsätze für die Verarbeitung personenbezogener Daten einzuhalten.[61] In diesem Zusammenhang war insbesondere auf den in Art. 5 Abs. 1 lit a DSGVO normierten Grundsatz der Transparenz abzustellen. In Hinblick auf den nur unklar umrissenen normativen Gehalt und den daraus ableitbaren Folgen für die Betroffenen genügte § 5 Abs. 3 EpiG iVm § 1 Z 2 lit. e der Wiener Contact-Tracing VO diesem nicht, da den Betroffenen die Tragweite des Eingriffes nicht zweifelsfrei erkennbar gewesen ist.[62] Da die DSB, wie alle österreichischen Behörden, bei einem offenkundigen Widerspruch zwischen nationalem- und Unionsrecht, das nationale Recht unangewendet zu lassen hat, war § 5 Abs. 3 EpiG iVm der Wiener Contact Tracing VO auf den gegenständlichen Sachverhalt nicht anzuwenden.[63]

5.4. Verletzung von Treu und Glauben

Neben dem Grundsatz der Transparenz verletzte die Vorgehensweise der Verantwortlichen auch den Grundsatz von Treu und Glauben gemäß Art. 5 Abs. 1 lit. a DSGVO, hatte sich diese doch darauf berufen, gesetzlich zur Verarbeitung der Daten ihrer Kunden verpflichtet zu sein und dennoch behauptet, die Verarbeitung sei von der „freiwilligen“ Angabe durch die Kunden abhängig gewesen. Wo jedoch eine gesetzliche Verpflichtung zur Erhebung besteht, verbleibt nach Auffassung der DSB kein Raum für eine freiwillige Angabe. Sohin erwies sich die Vorgehensweise der Verantwortlichen als irreführend und mit dem Grundsatz von Treu und Glauben nicht vereinbar.

6. Novelle des Epidemiegesetzes

Der Gesetzgeber hat mit einer jüngeren Novelle des EpiG und dem damit am 19. Dezember 2020 in Kraft getretenen § 5c EpiG[64] nunmehr eine gesetzliche Grundlage zur Erhebung von Kontaktdaten zum Zweck der Ermittlung von Kontaktpersonen geschaffen. Gemäß § 5c Abs. 1 leg. cit. kann, soweit und solange dies aufgrund der COVID-19-Pandemie unbedingt erforderlich und verhältnismäßig ist, längstens jedoch bis 30. Juni 2021, mit Verordnung bestimmt werden, dass BetreiberInnen von Gastronomiebetrieben verpflichtet sind, personenbezogene Daten zu erheben und der Bezirksverwaltungsbehörde auf Verlangen zu

[60] Vgl. EuGH vom 6.10.2020, verb. Rs C-511/18, C-512/18 und C-520/18, La Quadrature du Net u.a., Rz 132.
[61] Vgl. noch zur Rechtslage nach der RL 95/46/EG EuGH vom 11.12.2019, C-708/18, Rz 36 Asociaţia de Proprietari bloc M5A-ScaraA.
[62] Vgl. dazu sinngemäß VfSlg. 12.420/1990.
[63] Vgl. *Mayer/Kucsko -Stadlmayer/Stöger*, Bundesverfassungsrecht 11 [2015] Rz 246/9.
[64] Epidemiegesetz 1950 (EpiG), StF: BGBl. Nr. 186/1950 idF BGBl. Nr. 23/2021.

übermitteln. Überdies wird klargestellt, dass betroffene Personen diese Daten angeben müssen. Um welche konkreten Daten es sich dabei handelt, ist jedoch den entsprechenden Verordnungen selbst zu entnehmen. So legt § 5c Abs. 3 EpiG zwar fest, dass mit Verordnung die Erhebung von Name, Kontaktdaten (E-Mail und Telefonnummer), Datum Ort und Uhrzeit des Aufenthalts und sonstige nähere Angaben zum Aufenthaltsort angeordnet werden kann, doch ergibt sich aus dem Gesetzestext, dass eine auf § 5c EpiG gestützte VO nicht zwingend alle der genannten Daten enthalten muss. Es bleibt dem Verordnungsgeber sohin weiterhin ein Spielraum zur Ausgestaltung des Umfangs der Erhebungs- und Auskunftspflicht. Gleichzeitig wird diesem jedoch in § 5 Abs. 4 leg. cit. zwingend vorgegeben[65], dass eine solche VO eine auf 28 Tage begrenzte Aufbewahrungsdauer vorzusehen hat, nach deren Ablauf die Daten unverzüglich zu löschen sind. Weiters wird dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO Rechnung tragend klargestellt, dass in einer entsprechenden VO zu normieren ist, dass die erhobenen Daten für keine anderen Zwecke als die der Kontaktnachverfolgung verarbeitet werden dürfen.

Der Vollständigkeit ist festzuhalten, dass neben GastronomInnen auch Betreiber von Beherbergungsbetrieben, BetreiberInnen von nicht öffentlichen Freizeiteinrichtungen, von Kultureinrichtungen, von nicht öffentlichen Sportstätten, von Krankenanstalten und Kuranstalten, von Alten-, Pflege- und Behindertenheimen und VeranstalterInnen iSd § 15 EpiG von dieser Norm erfasst sind.

Die durch Verordnung zu statuierende Verpflichtung greift jedoch nur dann, wenn sich die betroffenen Personen länger als 15 Minuten im Betrieb aufgehalten haben. Weiters wurde klargestellt, dass der private Wohnbereich, Versammlungen nach dem Versammlungsgesetz sowie Veranstaltungen zur Religionsausübung nicht von auf § 5c EpiG gestützten VO erfasst sind.

6.1. Resümee

Die gegenständliche Beschwerde erwies sich im Ergebnis somit aus mehreren Überlegungen als begründet. Es gilt jedoch zu beachten, dass die DSB in dieser Entscheidung eine nicht länger in Kraft stehende Rechtslage anzuwenden hatte bzw. diese aufgrund ihres unklaren Gehalts und dem Vorrang des Unionsrechts unangewendet lassen musste. Mit Schaffung des oben dargestellten § 5c EpiG hat der Gesetzgeber eine eindeutige gesetzliche Verordnungsermächtigung zur Anordnung umfangreicher Erhebungs- und Auskunftspflichten gegenüber der Bezirksverwaltungsbehörde im Zusammenhang mit COVID-19 Verdachtsfällen eingeführt und erweist sich die nunmehr geltende Rechtslage somit als klarer. So besteht weder an der Verpflichtung – das Tätigwerden des

[65] Arg „*ist vorzusehen*“; Vgl. § 5c Abs. 4 EpiG.

Verordnungsgebers vorausgesetzt – zur Erhebung personenbezogener Daten durch ua GastronomInnen noch an der Verpflichtung von KundInnen, diese Daten anzugeben, nach geltender Rechtslage ein Zweifel.

III. Datenschutzrechtliche Fragestellungen im Zusammenhang mit COVID-19-Massentestungen

von Dr. Matthias Schmidl[66]

1. Allgemeines

Die gegenständliche Abhandlung betrifft die bereits durchgeführten bzw. geplanten Zielgruppen- und Massentestungen im Zusammenhang mit COVID-19, wobei auf die Rechtslage im November 2020 abgestellt wird.

Zwischenzeitig wurde das EpiG novelliert[67] und in § 5a Abs. 6 eine Rechtsgrundlage für den Zugriff „der zuständigen Behörden" auf das ZMR geschaffen.

Die Frage, ob Gemeinden für diese Zwecke auf das ZMR zugreifen können, bleibt dennoch von Relevanz, weil die „zuständige Behörde" im Sinne des EpiG, auf welche auch § 5a Abs. 6 Bezug nimmt, im Regelfall die Bezirksverwaltungsbehörde und nicht eine Gemeindebehörde ist (siehe § 43 Abs. 4 EpiG).

In einigen Bundesländern lag und liegt die faktische Zuständigkeit für die Vorfeldorganisation, v.a. für die Verständigung der Bevölkerung sowie die Unterteilung des Gemeindegebietes in Sprengel, vorrangig bei den Gemeinden.

Vorauszuschicken ist, dass die vorliegende Abhandlung keine verbindliche Auslegung gesetzlicher Bestimmungen darstellt, sondern eine fachliche Einschätzung.

Aus Gründen der Praktikabilität wird davon Abstand genommen, Ausführungen dahingehend zu treffen, ob und unter welchen Voraussetzungen eine Datenverarbeitung auf Basis einer Einwilligung betroffener Personen möglich ist.

2. Datenschutzrechtliche Beurteilung

2.1. Fragestellung

Es sollen folgende Fragestellungen näher beleuchtet werden.

a) Erfassung der Gemeindebürger einer Gemeinde und Unterteilung in „Sprengel" (Straßenzügen etc.),

[66] Dr. Matthias Schmidl ist stv. Leiter der Datenschutzbehörde. Der Beitrag fußt auf einer Rechtsauskunft gegenüber dem Österreichischen Städtebund vom November 2020.
[67] Siehe BGBl. I Nr. 136/2020.

b) Erfassung der Personen- und Adressdaten der Gemeindebürger durch Mithilfe von kommunalen IT-Providern,
c) Einladung der erfassten Gemeindebürger eines Sprengels zu den „zugeordneten“ Teststraßen mittels Zusendung eines Briefes.

2.2. Beurteilung

a) Soweit es die (geographische) Unterteilung eines Gemeindegebietes in mehrere Sprengel betrifft, um die Testungen geordnet durchzuführen, dürften hiefür keine personenbezogenen Daten erforderlich sein. Datenschutzrechtliche Fragestellungen stellen sich diesfalls erst dann, wenn Gemeindebürger einem Sprengel zugeordnet werden sollen.

b) Auch die Beiziehung von Auftragsverarbeitern iSd Art. 4 Z 8 DSGVO zur Abwicklung des Vorhabens erscheint aus datenschutzrechtlicher Sicht unproblematisch, sofern die Vorgaben des Art. 28 DSGVO eingehalten werden. Die Verarbeitung durch einen Auftragsverarbeiter bedarf jedenfalls einer geeigneten Rechtsgrundlage, vorwiegend eines Vertrages. Standardvertragsklauseln für Verträge nach Art. 28 Abs. 3 DSGVO sind auf der Website der Datenschutzbehörde abrufbar.[68]

c) Voraussetzung für die Zuordnung von Gemeindebürgern zu bestimmten Sprengeln, für die Information derselben sowie für die Heranziehung eines Auftragsverarbeiters ist jedoch, dass die Verarbeitung rechtmäßig ist.

Da im vorliegenden Kontext die Datenverarbeitung ausschließlich für Zwecke der öffentlichen Gesundheit erfolgt, ist davon auszugehen, dass es sich bei den hiefür verarbeiteten Daten um Gesundheitsdaten nach Art. 4 Z 15 DSGVO handelt; dies auch dann, wenn die einzelnen Datenkategorien (bspw. Vor- und Nachname, Adresse) für sich alleine noch nicht als Gesundheitsdaten zu qualifizieren wären.[69]

Die Datenverarbeitung richtet sich daher nach Art. 9 Abs. 2 DSGVO, wobei lit. i eine Datenverarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, auf Basis des Rechts der Mitgliedstaaten oder des Unionsrechtes ausdrücklich zulässt.

Im Folgenden geht es im Wesentlichen um die Frage, woher die erforderlichen personenbezogenen Daten stammen können und ob diese seitens der Gemeinden für

[68] Siehe https://www.dsb.gv.at/download-links/dokumente.html.
[69] Vgl. dazu den im vorherigen Beitrag ausführlich dargestellten Bescheid vom 19. November 2020, GZ 2020-0.743.659.

Zwecke der Information von Gemeindebürgern über die anstehenden Testungen herangezogen werden können.

In Betracht kommen hiefür vor allem Register, in welchen personenbezogene Daten von Gemeindebürgern strukturiert verarbeitet und welche von den Gemeinden geführt werden.

Dies sind vor allem

- die **Wählerevidenz** gemäß Wählerevidenzgesetz 2018 – WEviG, BGBl. I Nr. 106/2016
- das **Lokale Melderegister/Zentrale Melderegister** gemäß Meldegesetz 1991 – MeldeG, BGBl. Nr. 9/1992

Beide Register sind von den Gemeinden (§ 1 WEviG) bzw. dem Bürgermeister (§§ 13, 14 MeldeG) im übertragenen Wirkungsbereich zu führen und dürfen nur für bestimmte Zwecke verwendet werden.

Träger des übertragenen Wirkungsbereiches der Gemeinde ist der Bürgermeister (Art. 119 Abs. 2 B-VG).

§ 8 DSG regelt die Zulässigkeit der Verarbeitung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen. Unter bestimmten Voraussetzungen können Daten desselben Verantwortlichen (weiter-)verarbeitet werden.

Es wäre daher denkbar, dass Bürgermeister als Melde- bzw. Wahlbehörden Daten in den genannten Registern weiterverarbeiten, um Personen im jeweiligen Gemeindegebiet über die anstehenden Testungen zu benachrichtigen (§ 8 Abs. 2 Z 1 DSG). Allerdings ist zu beachten, dass § 8 Abs. 2 Z 1 DSG nur dann zur Anwendung gelangt, sofern nicht Spezialnormen, die die Verarbeitung von Adressdaten regeln, der Vorrang einzuräumen ist.

Die Zulässigkeit der Verarbeitung von Meldedaten im zentralen Melderegister (für andere Zwecke) richtet sich – ausschließlich – nach § 16a und § 20 MeldeG.

§ 4 Abs. 3 WEviG normiert, dass jede im ZeWaeR (Zentrales Wählerregister) und jede auf Daten des ZeWaeR aufbauende Datenverarbeitung einer ausdrücklichen bundesgesetzlichen oder in Ausführung von Art. 26a Abs. 2 B-VG erlassenen ausdrücklichen landesgesetzlichen Grundlage bedarf und alle Zugriffe auf das ZeWaeR und auf die auf das ZeWaeR aufbauenden Datenverarbeitungen zu protokollieren sind.

Sowohl im WEviG als auch im MeldeG ist ein Zugriff auf Datensätze zur Benachrichtigung von Personen über anstehende Massentestungen udgl. nicht vorgesehen, wobei die

genannten Gesetze einen Zugriff aber auch dann zulassen, wenn dies gesetzlich – dh. in einem anderen Gesetz – vorgesehen ist (§ 4 Abs. 3 WEviG, § 16a Abs. 3 MeldeG). § 20 Abs. 3 MeldeG enthält darüber hinaus die Einschränkung, dass die Bürgermeister (als Meldebehörden) ermächtigt sind, die in ihrem Melderegister enthaltenen oder ihnen gemäß Abs. 2 übermittelten Meldedaten zu verarbeiten, sofern diese zur Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden.

Die Datenschutzbehörde/Datenschutzkommission hat bereits mehrmals ausgesprochen, dass der Zugriff auf lokale Register ohne ausreichende Rechtsgrundlage einen Verstoß gegen datenschutzrechtliche Vorgaben darstellt.[70]

In diesem Zusammenhang fällt auf, dass das MeldeG die Weiterverarbeitung von Meldedaten an strengere Voraussetzungen knüpft als das WEviG: So darf gemäß § 20 Abs. 3 MeldeG eine Weiterverarbeitung durch Bürgermeister nur dann erfolgen, wenn diese eine zur Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben wesentliche Voraussetzung bildet. § 20 Abs. 3 MeldeG stellt diesbezüglich eine Spezialnorm dar, die § 8 Abs. 2 Z 1 DSG vorgeht.[71]

Allerdings ist den parlamentarischen Materialien zu § 4 Abs. 3 WEviG zu entnehmen, dass ein Zugriff für Zwecke von Meinungsumfragen oder Bürgerbefragungen außerhalb des Vollzugsbereichs von Wahlbehörden nicht intendiert war.[72] Dies wird auch durch Art. 26a Abs. 2 B-VG erhärtet, der anordnet, dass die Speicherung der Daten der Wählerevidenzen in einem zentralen Wählerregister erfolgt, in dem auch Wählerevidenzen aufgrund der Landesgesetzgebung gespeichert werden können; die Länder und Gemeinden können diese Daten für solche Verzeichnisse in ihrem Zuständigkeitsbereich verwenden. In verfassungskonformer Interpretation ist § 4 Abs. 3 WEviG daher eng auszulegen und es ist darüber hinaus davon auszugehen, dass § 4 Abs. 3 WEviG – ebenso wie § 20 Abs. 3 MeldeG – eine Spezialnorm im Verhältnis zu § 8 Abs. 2 Z 1 DSG darstellt.

Als Zwischenschritt ist somit festzuhalten, dass ein Zugriff der Bürgermeister als Melde- bzw. Wahlbehörde auf die entsprechenden Register für andere Zwecke nur dann als zulässig erachtet werden kann, wenn der Zweck des Zugriffs in einer Aufgabe begründet ist, die im Vollzugsbereich dieser Behörden liegt.

---

[70] Vgl. dazu den Bescheid vom 14. Dezember 2012, GZ K121.879/0014-DSK/2012, betreffend Zugriff auf das Melderegister, sowie die Empfehlung vom 28. November 2014, GZ DSB-D215.548/0007-DSB/2014, betreffend Zugriff auf das Wählerverzeichnis, in beiden Fällen für Zwecke einer Bürgerbefragung.

[71] Siehe *Kunnert*, in *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG § 8 Rz 9 mwN.

[72] Siehe AB 1298 der Beilagen XXV. GP S. 6.

In diesem Zusammenhang hat die Datenschutzbehörde beispielsweise den Zugriff einer Meldebehörde auf Daten des Melderegisters für Zwecke der Benachrichtigung von Eltern einzuschulender Kinder bejaht, da die Gemeinde für die Erhaltung der Pflichtschulen zuständig war.[73]

Fraglich ist im vorliegenden Zusammenhang daher, ob Gemeinden bzw. dem Bürgermeister im Zusammenhang mit Massentestungen in Bezug auf COVID-19 eine Vollzugszuständigkeit zukommt.

Art. 118 Abs. 3 Z 7 B-VG gewährleistet, dass Gemeinden Angelegenheiten der örtlichen Gesundheitspolizei, insbesondere auf dem Gebiet des Hilfs- und Rettungswesens sowie des Leichen- und Bestattungswesens, im eigenen Wirkungsbereich besorgen können. Davon umfasst sind Maßnahmen, die zur Abwehr lokaler Gesundheitsgefährdungen erforderlich sind.[74]

Wie der Verfassungsgerichtshof in Bezug auf die Bekämpfung der Tuberkulose festgehalten hat, fallen diese Maßnahmen wegen ihres überörtlichen Charakters nicht unter die gemäß Art. 118 Abs. 3 Z 7 angeführten Angelegenheiten der örtlichen Gesundheitspolizei, die der Gemeinde zur Besorgung im eigenen Wirkungsbereich übertragen sind, sondern unter Art. 10 Abs. 1 Z 12 B-VG.[75]

Aufgrund der Vergleichbarkeit der Auswirkungen ist daher von auszugehen, dass der Bekämpfung von COVID-19 ebenfalls überörtlicher Charakter zukommt. Dies wird auch dadurch erhärtet, dass sowohl das Epidemiegesetz 1950 – EpiG, BGBl. Nr. 186/1950, als auch das COVID-19-Maßnahmengesetz, BGBl. I Nr. 12/2020, auf welchen die Bekämpfung von COVID-19 maßgeblich beruht, kompetenzrechtlich auf Art. 10 Abs. 1 Z 12 B-VG fußen. Vollzugsbehörden der genannten Gesetze sind grundsätzlich die Bezirksverwaltungsbehörden im Rahmen der mittelbaren Bundesverwaltung.

Eine Weiterverarbeitung auf Basis von § 8 Abs. 2 Z 1 DSG dürfte demnach ausscheiden.

Die Verarbeitung von Adressdaten könnte auch auf § 8 Abs. 2 Z 2 lit. a DSG gestützt werden.

Dieser verlangt, dass es keiner Einwilligung der betroffenen Personen für die Verarbeitung von Adressdaten bedarf, wenn eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des

[73] Bescheid vom 1. Oktober 2019, GZ DSB-D202.238/0001-DSB/2019.
[74] *Muzak*, B-VG[6] Art. 118 Rz 9 mwN.
[75] VfSlg. 5485/1967.

Gegenstands der Benachrichtigung unwahrscheinlich ist und wenn bei einer beabsichtigten Übermittlung der Adressdaten an Dritte an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht.

Ein solches öffentliches Interesse – nämlich die Benachrichtigung über die Möglichkeit einer COVID-19-Testung im eigenen Gemeindegebiet – kann im vorliegenden Fall zwar bejaht werden. Auch hat die Datenschutzkommission/Datenschutzbehörde bereits ausgesprochen, dass eine Beeinträchtigung von Betroffeneninteressen nicht vorliegt, wenn betroffene Personen anhand von Wohnsitz und Alter oder überhaupt nur anhand des Wohnsitzes ausgewählt werden.[76]

Fraglich ist allerdings, ob eine „Übermittlung an Dritte" vorliegt. Gemäß Art. 4 Z 10 DSGVO handelt es sich bei einem „Dritten" um eine natürlich oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Voraussetzung ist demnach, dass die Daten einem anderen Verantwortlichen als dem Bürgermeister als Melde- bzw. Wahlbehörde übermittelt werden.

Ob die Aussendung der Information über die geplanten Testungen an die Gemeindebürger von einem anderen Gemeindeorgan als dem Bürgermeister zu besorgen ist, richtet sich nach landesgesetzlichen Vorgaben.

Liegt auch diese Voraussetzung nicht vor, käme eine Verarbeitung von Adressdaten nur unter den Voraussetzungen des § 8 Abs. 3 und 4 DSG in Betracht.

3. Zusammenfassung

Zusammenfassend ist daher festzuhalten, dass die Rechtmäßigkeit der Verarbeitung von Daten im (zentralen) Melderegister bzw. in der Wählerevidenz durch Gemeinden für Zwecke der Benachrichtigung von Personen über die geplanten Massentests sowie der Zuweisung dieser Personen an bestimmte Testsprengel nicht schlichtweg bejaht werden kann.

Eine Berufung auf § 8 Abs. 2 Z 1 DSG scheint nicht möglich.

Allenfalls in Städten mit eigenem Statut, in welchem dem Bürgermeister auch Aufgaben einer Bezirksverwaltungsbehörde übertragen sind, könnte ein Zugriff für die genannten Zwecke Deckung in den erwähnten Bestimmungen finden.

[76] Vgl. nochmals *Kunnert*, aaO Rz 7 mwN.

Allerdings gestattet § 8 Abs. 2 Z 2 lit. a DSG in engen Grenzen eine – bewilligungsfreie – Weiterverarbeitung von Adressdaten für Zwecke der Benachrichtigung von betroffenen Personen.

§ 8 Abs. 3 und 4 DSG kommt als Rechtsgrundlage ebenso in Betracht: Demnach ist die Übermittlung von Adressdaten an Dritte mit Genehmigung der Datenschutzbehörde unter bestimmten Voraussetzungen – vorliegend: wichtiges öffentliches Interesse an der Befragung selbst – möglich.

IV. Der „Brexit“ und die Zukunft des grenzüberschreitenden Datenverkehrs

von Mag. Marek Gerhalter, LL.M.[77]

1. Einleitung

Der Austritt des Vereinigten Königreichs aus der Europäischen Union zum 31. Jänner 2020 (medial vorab als „Brexit“ bezeichnet) läutete das in vielerlei Hinsicht bewegte Jahr 2020 ein. Der vorliegende Beitrag bietet eine überblicksmäßige Darstellung dieses einschneidenden Ereignisses und betrachtet wesentliche datenschutzrechtliche Folgen, insbesondere in Zusammenhang mit Datenübermittlungen.

2. Rückblick

“*Should the United Kingdom remain a member of the European Union or leave the European Union?*” Auf diese Frage hin stimmte das Vereinigte Königreich im Rahmen eines am 23. Juni 2016 abgehaltenen Referendums mit einer Mehrheit von knapp 52% für einen Austritt aus der Europäischen Union und betrat mit dem am 29. März 2017 als Folge des Abstimmungsergebnisses an den Europäischen Rat gemäß Art. 50 EUV[78] gestellten Austrittsgesuch[79] völliges Neuland.

Nach intensiven Verhandlungen, gepaart mit mehreren Verlängerungen der in der primärrechtlichen Austrittsbestimmung grundsätzlich vorgesehenen Zweijahresfrist[80], hat das Vereinigte Königreich mit Ablauf des 31. Jänners 2020 die Europäische Union verlassen. Zuvor haben die Europäische Union und das Vereinigte Königreich ein Austrittsabkommen[81] unterzeichnet, welches mit 1. Februar 2020 in Kraft getreten ist und wesentliche Aspekte des Austritts des Vereinigten Königreichs aus der Europäischen Union und der Europäischen Atomgemeinschaft regelt. Gemäß der Art. 126 ff des Austrittsabkommens wurde bis zum 31. Dezember 2020 ein Übergangszeitraum festgelegt, in welchem das Unionsrecht (und folglich auch die DSGVO[82]) für das Vereinigte Königreich sowie im Vereinigten Königreich

---

[77] Mag. Gerhalter ist Bediensteter der Datenschutzbehörde und auf internationalen Datenverkehr spezialisiert. Der Beitrag gibt ausschließlich seine persönliche Meinung wieder.
[78] Vertrag über die Europäische Union (konsolidierte Fassung), ABl. C 2016/202, S. 1.
[79] Abrufbar in deutscher Sprache unter <https://data.consilium.europa.eu/doc/document/XT-20001-2017-INIT/de/pdf>.
[80] Art. 50 Abs. 3 des Vertrages über die Europäische Union.
[81] Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft, ABl. L 2020/29, S. 7 idF. L 2020/225, S. 53.
[82] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 2016/119, S. 1 idF. L 2018/127, S. 2.

grundsätzlich weitergalt. Im Ergebnis wurde das Vereinigte Königreich bis zum Ende der Übergangsperiode weiterhin wie ein Mitgliedstaat behandelt und wurde seine Zugehörigkeit bzw. sein Zugang zum europäischen Binnenmarkts und zur Zollunion bis Ende 2020 verlängert; demgegenüber war es seit seinem Austritt nicht mehr in den Institutionen der Europäischen Union vertreten.

Da mit dem Auslaufen der Übergangsperiode das Vereinigte Königreich nunmehr am 1. Jänner 2021 aus dem Binnenmarkt und der Zollunion ausscheiden sollte, wurden am 2. März 2020 formale Verhandlungen zwischen der Europäischen Union und dem Vereinigten Königreich hinsichtlich der künftigen Beziehungen zueinander aufgenommen[83], welche am 24. Dezember 2020 zu einer grundsätzlichen Einigung auf ein neues Handels- und Kooperationsabkommen[84] führten.[85] Da die Einigung erst sehr spät und kurz vor Ende des im Austrittsabkommen festgelegten Übergangszeitraums erzielt wurde, hat die Europäische Kommission eine vorläufige Anwendung des Handels- und Kooperationsabkommens für einen begrenzten Zeitraum vom 1. Jänner 2021 bis zum 28. Februar 2021 vorgeschlagen.[86] Dem Start des Abkommens zum 1. Jänner 2021 wurde die Zustimmung erteilt und wird es ab diesem Zeitpunkt vorläufig angewendet.[87]

---

[83] Das diesbezügliche Verhandlungsmandat der Europäischen Kommission gründet auf dem Beschluss (EU, Euratom) 2020/266 des Rates vom 25. Februar 2020 über die Ermächtigung zur Aufnahme von Verhandlungen mit dem Vereinigten Königreich Großbritannien und Nordirland über ein neues Partnerschaftsabkommen, ABl. L 2020/58, S. 53.

[84] Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, ABl. L 2020/444, S. 14.

[85] Darüber hinaus wurde Einigung über weitere Abkommen erzielt, vgl. etwa das Abkommen zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland betreffend Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen, Abl. L 2020/444, S. 1463; sowie das Abkommen zwischen der Regierung des Vereinigten Königreich Großbritannien und Nordirland und der Europäischen Atomgemeinschaft über die Zusammenarbeit auf dem Gebiet der sicheren und friedlichen Nutzung der Kernenergie, ABl. L 2020/445, S. 5.

[86] Vorschlag für einen BESCHLUSS DES RATES über die Unterzeichnung des Handels- und vorläufige Anwendung des Kooperationsabkommens im Namen der Union zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits und über den Abschluss des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland über die Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen, KOM (2020) 855 endg.; vgl. auch Artikel FINPROV.11 Abs. 2 lit. a) des Handels- und Kooperationsabkommens.

[87] Vgl. den Beschluss (EU) 2020/2252 des Rates vom 29. Dezember 2020 über die Unterzeichnung im Namen der Union und über die vorläufige Anwendung des Abkommens über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits und des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland über die Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen, ABl. 2020/444, S. 2; sowie den Beschluss (Euratom) 2020/2253 des Rates vom 29. Dezember 2020 über die Zustimmung zum Abschluss – durch die Europäische Kommission – des Abkommens zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Europäischen Atomgemeinschaft über die Zusammenarbeit auf dem Gebiet der sicheren und friedlichen Nutzung der Kernenergie und zum Abschluss – durch die Europäische Kommission im Namen der Europäischen Atomgemeinschaft – des Abkommens über Handel und Zusammenarbeit

3. Das Handels- und Kooperationsabkommen aus datenschutzrechtlicher Sicht

Die Europäische Union und das Vereinigte Königreich bilden ab dem 1. Jänner 2021 zwei getrennte Märkte sowie zwei juristisch sowie regulatorisch getrennte Einheiten und endet diesbezüglich auch der freie Personen-, Waren-, Dienstleistungs- und Kapitalverkehr.[88] Die Zusammenarbeit zwischen der Europäischen Union und dem Vereinigten Königreich wird daher in Zukunft weniger eng als während dessen EU-Mitgliedschaft ausfallen, nichtsdestotrotz werden im Handels- und Kooperationsabkommen Fragen in wesentlichen Bereichen wie etwa Waren- und Dienstleistungshandel, Investitionen, Regulierung, öffentliches Beschaffungswesen, Wettbewerb und Beihilfenkontrolle, Energie und Nachhaltigkeit, Koordinierung von Programmen der sozialen Sicherheit, Luft- und Straßenverkehr sowie Fischerei geregelt.[89]

Datenschutzrechtliche Fragen werden indes nicht als eigener Punkt im H behandelt – dies reflektiert die grundsätzliche Haltung der Europäischen Union, Vorschriften über die Verarbeitung personenbezogener Daten nicht als Teile von (Frei-)Handelsabkommen zu verhandeln[90]. Sie finden sich aber dennoch in themenspezifischen Regelungen des Abkommens wieder, wie etwa in Form von Bekenntnissen beider Vertragsparteien zum Schutz personenbezogener Daten[91].

Praktisch am bedeutsamsten ist aus datenschutzrechtlicher Sicht wohl die Bestimmung, dass im Zeitraum von maximal sechs Monaten nach Inkrafttreten des Handels- und Kooperationsabkommens, d.h. spätestens bis zum 30. Juni 2021, die Übermittlung

---

zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, ABl. L 2020/444, S. 11; vgl auch die Mitteilung über die vorläufige Anwendung des Abkommens über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland über die Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen und des Abkommens zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Europäischen Atomgemeinschaft über die Zusammenarbeit auf dem Gebiet der sicheren und friedlichen Nutzung der Kernenergie, ABl. L 2021/1, S. 1.

[88] Vgl. *Europäische Kommission*, Das Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich. Eine neue Beziehung – mit großen Veränderungen, S.1, abrufbar in deutscher Sprache unter <https://ec.europa.eu/info/files/eu-uk-trade-and-cooperation-agreement-new-relationship-big-changes-brochure_de>.

[89] Weiterführend siehe etwa *Europäische Kommission*, Fragen und Antworten: Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich Großbritannien und Nordirland, abrufbar in deutscher Sprache unter <https://ec.europa.eu/commission/presscorner/detail/de/qanda_20_2532>.

[90] Siehe etwa MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Handel für alle Hin zu einer verantwortungsbewussteren Handels- und Investitionspolitik, KOM (2015) 497 endg., S. 9; sowie MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Austausch und Schutz personenbezogener Daten in einer globalisierten Welt, KOM (2017) 7 endg., S. 6.

[91] Vgl. etwa Artikel DIGIT.7 Abs. 1 des Handels- und Kooperationsabkommens.

personenbezogener Daten aus der Europäischen Union an Empfänger im Vereinigten Königreich nicht als Übermittlung an ein Drittland im Sinne des Unionsrechts (insb. des Kapitels V der DSGVO) gilt; diese „Überbrückungsklausel“ steht unter dem Vorbehalt, dass sich das derzeit im Vereinigten Königreich geltende Datenschutzrecht in jenem Zeitraum nicht ändert (d.h. dass in diesem Bereich sozusagen ein „Einfrieren“ der aktuellen Rechtslage stattfindet) und dass das Vereinigte Königreich in jenem Zeitraum keine seiner neuen Befugnisse im Bereich internationaler Datenübermittlungen (wie z.B. den Erlass von eigenen Angemessenheitsbeschlüssen oder anderen geeigneten Garantieinstrumenten) ausübt.[92] Der Überbrückungszeitraum kann auch früher enden, sofern die Europäische Kommission für das Vereinigte Königreich einen Angemessenheitsbeschluss gemäß Art. 45 Abs. 3 DSGVO bzw. Art. 36 Abs. 3 DSRL-PJ[93] erlässt. Die Arbeiten der Europäischen Kommission an entsprechenden Angemessenheitsbeschlüssen laufen seit März 2020.[94]

Für Datenübermittlungen aus der Europäischen Union an Empfänger im Vereinigten Königreich bedeutet die im Handels- und Kooperationsabkommen vorgesehene Überbrückungslösung, dass personenbezogene Daten vorerst ohne Rückgriff auf geeignete Garantien[95] oder auf Ausnahmetatbestände[96] übermittelt werden können.[97] Diese Erleichterung fällt künftig jedoch weg, sofern spätestens bis zum 30. Juni 2021 von der Europäischen Kommission keine entsprechenden Angemessenheitsbeschlüsse für das Vereinigte Königreich erlassen werden. In einem solchen Fall obliegt es dann den Datenexporteuren, die Verwendung anderweitiger Übermittlungsgrundlagen zu prüfen. Sofern hierfür zivilrechtliche Garantieinstrumente[98] herangezogen werden, ist auf die gegebenenfalls gebotene Schaffung zusätzlicher technischer, organisatorischer oder vertraglicher Maßnahmen hinzuweisen,[99] um für aus der Europäischen Union an Empfänger

---

[92] Art. FINPROV.10A Abs. 1, Abs. 4 und Abs. 5 des Handels- und Kooperationsabkommens.
[93] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 2016/119, S. 89 idF. L 2018/127, S. 9.
[94] Siehe die Information der *Europäische Kommission*, Fragen und Antworten: Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich Großbritannien und Nordirland, unter Punkt „Sicherheit und Zusammenarbeit im Bereich der Strafverfolgung und Justiz im Bereich Strafsachen“.
[95] Art. 46 DSGVO; Art. 37 DSRL-PJ.
[96] Art. 49 DSGVO; Art. 38 DSRL-PJ.
[97] Vgl. auch *Europäischer Datenschutzausschuss*, Information note on data transfers under the GDPR to the
United Kingdom after the transition period (updated on 13 January 2021), abrufbar in englischer Sprache unter <https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-data-transfers-under-gdpr-united-kingdom-after-0_en>
[98] Wie z.B. Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO oder verbindliche interne Datenschutzvorschriften gemäß Art. 46 Abs. 2 lit. b) iVm. Art. 47 DSGVO.
[99] Vgl. dazu *Europäischer Datenschutzausschuss*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,

im Vereinigten Königreich übermittelte personenbezogene Daten ein der Sache nach gleichwertiges Schutzniveau[100] sicherzustellen.

Weitaus detailliertere datenschutzrechtliche Bestimmungen enthält das Handels- und Kooperationsabkommen im Bereich der Übermittlung personenbezogener Daten bei der Zusammenarbeit im Bereich der Strafverfolgung und Justiz hinsichtlich Strafsachen.[101] Beispielhaft zu nennen sind etwa die diesbezüglichen Regelungen zur Übermittlung von Fluggastdaten (PNR-Daten), welche insbesondere sicherstellen sollen, dass solche Daten ausschließlich für die festgelegten Zwecke (z.B. zur Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Terrorismus oder schweren Straftaten) verwendet,[102] entsprechende Datensicherheitsmaßnahmen ergriffen,[103] Fluggäste transparent über die Verarbeitung solcher Daten informiert[104] und PNR-Daten nach bestimmten Zeiträumen zunächst teilweise de-personalisiert und letztendlich auch gelöscht werden.[105]

4. Ausblick

Die von manchen als „Weihnachtsgeschenk" bezeichnete Einigung über ein neues Handels- und Kooperationsabkommen stellt aus datenschutzrechtlicher Sicht einen letzten Aufschub für (erleichterte) Datenflüsse aus der Europäischen Union an Empfänger im Vereinigten Königreich dar, nachdem sich in diesem Bereich aller Voraussicht nach bis zum 30. Juni 2021 wenig ändern wird. Die künftige Ausgestaltung jener Datenflüsse wird vor allem vom Bestehen oder Nichtbestehen entsprechender Angemessenheitsbeschlüsse abhängig sein, weshalb die diesbezüglichen Bemühungen der Europäischen Kommission mit großer Spannung erwartet werden dürfen, nicht zuletzt, da ein solches Vorhaben insbesondere aufgrund der traditionell engen Zusammenarbeit zwischen britischen und U.S.-amerikanischen Sicherheitsbehörden zum Teil als schwierig angesehen wird.[106] Ein weiterer, auch für die aufsichtsbehördliche Praxis bedeutsamer Einschnitt ist ferner darin zu erblicken, dass die Aufsichtsbehörde des Vereinigten Königreichs („Information Commissioner's Office", kurz „ICO") seit dem Austritt nicht mehr Teil des sog. „One-Stop-Shop"-Mechanismus gemäß Art. 56 DSGVO ist und dass sie grundsätzlich auch nicht mehr an Sitzungen des Europäischen Datenschutzausschusses teilnimmt. Hat sich der sog. „Brexit" im Jahr 2020

---

abrufbar in englischer Sprache unter <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en>.

[100] EuGH 16.07.2020, C-311/18, Rz. 94, 96 und 105.

[101] Siehe Teil Drei des Handels- und Kooperationsabkommens.

[102] Art. LAW.PNR.20 des Handels- und Kooperationsabkommens.

[103] Art. LAW.PNR.25 leg. cit.

[104] Art. LAW.PNR.26 leg. cit.

[105] Art. LAW.PNR.28 leg. cit.

[106] Siehe z.B. bei *Botta*, Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II", CR 2/2020, S. 82 (88); vgl. allgemein auch *Hoeren*, Datenschutz: Jetzt wird's ernst – Großbritannien wird Drittland, MMR 2018, S. 53 (54).

aus datenschutzrechtlicher Sicht vorwiegend noch in Verhandlungen über den künftigen Kooperationsrahmen niedergeschlagen, so wird es an 2021 sowie den folgenden Jahren liegen, zu lernen, mit seinen Auswirkungen in der Praxis umzugehen.