Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt Prof. Dr. Hermann Weber, Schriftleiter von 1982–2001

Herausgegeben von *Prof. Dr. Martin Burgi,* München – *Prof. Dr. Christian Calliess,* Berlin – *Dr. Josef Christ,* Richter des BVerfG, Karlsruhe – *Prof. Dr. Klaus-Peter Dolde,* Rechtsanwalt, Stuttgart – *Dr. Frank Fellenberg,* Rechtsanwalt, Berlin – *Prof. Dr. Andreas Heusch,* Präsident des VG, Düsseldorf – *Prof. Dr. Thomas Mayen,* Rechtsanwalt, Bonn – *Prof. Dr. Hubert Meyer,* Geschäftsf. Vorstandsmitglied des Niedersächsischen Landkreistages, Hannover – *Prof. Dr. Janbernd Oebbecke,* Münster – *Prof. Dr. Joachim Scherer,* Rechtsanwalt, LL.M., Frankfurt a. M. – *Dr. Heribert Schmitz,* Ministerialrat a. D., Berlin – *Prof. Dr. Friedrich Schoch,* Freiburg – *Dr. Thomas Schröer,* Rechtsanwalt, Frankfurt a. M. – *Prof. Dr. Rudolf Streinz,* München

Schriftleitung: Rechtsanwalt Prof. Dr. Achim Schunder und Rechtsanwältin Dr. Christiane Prause, Beethovenstraße 7 b, 60325 Frankfurt a. M.

12 2021

Seite 1–8
40. Jahrgang
15. Juni 2021

Professor Dr. Christof Muthers und Professor Dr. Marc Röckinghausen*

COVID 19 – die Pandemie macht an der Grenze nicht Halt

Zum Austausch von grenzüberschreitenden Gesundheits- und Meldedaten

Die COVID 19 Pandemie stellt nicht nur die Gesundheitswissenschaften vor viele neue Fragen, sondern auch die Rechtswissenschaft, die sich sowohl mit verfassungs- und datenschutzrechtlichen Fragen als auch solchen rund um das Infektionsschutzgesetz befassen muss. Dass daneben auch das Melderecht eine Rolle spielen kann, wird der vorliegende Beitrag zeigen.

I. Einleitung

Da das Virus an der Grenze nicht Halt macht, stellen sich zudem immer Fragen auch nach der grenzüberschreitenden Zusammenarbeit von Behörden zur Bekämpfung der Pandemie. Zur Veranschaulichung soll folgender einfacher Sachverhalt dienen: Aufgrund dem Gesundheitsamt gemeldeter einzelner positiver Testergebnisse bei in niederländischen Betrieben beschäftigten Arbeitsmigranten mit Unterkunft in Deutschland wurde das Wohn- und Arbeitsumfeld dieser Personen seitens der Kommunen ermittelt. Dabei fanden umfangreiche Testungen in Sammelunterkünften sowie kleineren Unterkünften von Leiharbeitern aus der niederländischen Fleischindustrie statt. Schon nach wenigen Tagen war den Verantwortlichen klar, dass die seitens des jeweiligen Gesundheitsamtes angeordneten Maßnahmen und Auflagen oftmals vorsätzlich umgangen wurden. Dazu schien ganz bewusst die grenzüberschreitende Trennung von Unterbringung in Deutschland und Arbeitsstätte in den Niederlanden eingesetzt zu werden.[1] Der transnationale Austausch von Gesundheits- und Meldedaten ist insofern aus infektionsschutzrechtlicher Sicht erforderlich, da beispielsweise der Verdacht besteht, dass den Meldepflichten nicht immer nachgekommen wird. Es wurden wiederholt Personen in Unterkünften angetroffen, die sich dort zwar aufhielten, jedoch nicht gemeldet waren. Zudem wurden zum Teil infizierte und nicht infizierte Personen nachträglich in andere Unterkünfte verbracht, so dass die zwingend erforderliche, verlässliche Kontrolle der Ausbreitung der Infektion nicht gewährleistet werden konnte. Darüber hinaus ist die Zuständigkeit für den Erlass und die Überwachung etwaiger Quarantäneverfügungen und sonstiger infektionsschutzrechtlicher Maßnahmen festzustellen. Aus infektionsschutzrechtlicher Sicht scheint ein Datenaustausch über Melde- sowie Gesundheitsdaten zwingend erforderlich. Unklar ist, ob und auf welcher Grundlage solche Daten über die Grenze hinweg ausgetauscht werden können.

II. Melderechtliche Grundlagen für eine grenzüberschreitende Weitergabe von Meldedaten

1. Anwendungsvoraussetzungen des § 35 Bundesmeldegesetz

§ 35 BMG sieht eine Datenübermittlung an ausländische öffentliche Stellen vor, sofern es sich um Tätigkeiten handelt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Union fallen. Die Datenübermittlung erfolgt dabei im Rahmen dessen, was § 34 I 1 BMG erlaubt. Danach darf eine Meldebehörde einer anderen öffentlichen Stelle aus dem Melderegister die unter Nr. 1–14 aufgeführten Daten übermitteln, soweit es zur Erfüllung der Aufgaben der Meldebehörde oder des Empfängers der Daten erforderlich ist. Wenn also die Voraussetzungen des § 35 BMG erfüllt sind, dann entspricht der Umfang der Datenübermittlung genau dem, der zwischen inländischen Behörden zulässig ist.[2]

§ 35 BMG setzt zum einen voraus, dass es sich um Tätigkeiten handelt, die ganz oder teilweise im Anwendungsbereich des Rechts der Europäischen Union liegen. Zum anderen kommt § 34 I 1 BMG lediglich nach Maßgabe der für diese Tätigkeiten geltenden Gesetze und Vereinbarungen zur Anwendung. Auslegungsbedürftig ist dabei vorrangig die

* Die *Verf.* sind Professoren an der Hochschule für Polizei und öffentliche Verwaltung des Landes Nordrhein-Westfalen und beraten das Euregionale Informations- und Kompetenzzentrum – EURIEC (www.euriec.eu). Der Beitrag entstand im Rahmen eines Gutachtens für das Euregionale Informations- und Kompetenzzentrum – EURIEC (www.euriec.eu).

1 Vgl. Neue Ruhr Zeitung v. 28.6.2020 – Grenzüberschreitende Taskforce zu Leiharbeitern gebildet.

2 Vgl. auch *Süßmuth/Laier*, Bundesmeldegesetz, 2. Aufl. (Stand Sept. 2015), § 35 BMG Rn. 1.

erste Voraussetzung. Nach dem Wortlaut lassen sich verschiedene Bedeutungen vertreten. Zum einen kann damit – sehr restriktiv – gemeint sein, dass die Norm nur dann zur Anwendung kommen kann, wenn ein einschlägiger Sekundärrechtsakt existiert. Etwas weiter wäre der Anwendungsbereich, wenn man zwar auf diesen Sekundärrechtsakt verzichten könnte, zumindest aber eine ausdrückliche Kompetenznorm im AEUV für einen spezifischen Politikbereich verlangte. Gänzlich offen wäre der Anwendungsbereich, wenn man auch auf eine derartig spezifische Kompetenznorm verzichten könnte und allein die Harmonisierungsbefugnis der Union zur Verwirklichung des Binnenmarkts ausreichen würde.

2. Genese des § 35 Bundesmeldegesetz

Die Fassung des § 35 BMG geht zurück auf die Vorgängerregelung in § 18 I 2 Melderechtsrahmengesetz (MRRG). Eine inhaltliche Übernahme dieser Vorgängerregelung entsprach auch der ausdrücklichen Absicht beim Erlass des Bundesmeldegesetzes.[3] § 18 I 2 MRRG wiederum wurde im Kontext der Umsetzung der Datenschutz-Richtlinie[4] neu in das Gesetz aufgenommen. Vorrangig erfolgte die Umsetzung durch eine Anpassung der unmittelbar dem Datenschutz dienenden Gesetze, in erster Linie war das Bundesdatenschutzgesetz betroffen.[5] Durch die Datenschutz-Richtlinie wurde erstmalig ein einheitliches Datenschutzniveau für die Ausführung und Anwendung des Gemeinschaftsrechts durch die Mitgliedstaaten der Europäischen Union geschaffen. Der innergemeinschaftliche Datenverkehr musste dem inländischen Datenverkehr gleichgestellt werden. Um einer Kompetenzüberschreitung entgegenzutreten, war der Anwendungsbereich der Datenschutz-Richtlinie in Art. 3 II eingeschränkt worden. Keine Anwendung sollte die Richtlinie auf die Verarbeitung personenbezogener Daten finden, die (1) für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen sowie (2) von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. Dieser zweite Ausnahmebereich spielt für die Übermittlung von Meldedaten keine Rolle. Sowohl § 4 b I BDSG in seiner Fassung aus dem Jahr 2001 als auch § 35 BMG in seiner immer noch geltenden Fassung[6] greifen die erste Ausnahme aus Art. 3 II Datenschutz-Richtlinie auf und wenden den Anwendungsausschluss in eine positive Anwendungsvoraussetzung („Tätigkeiten, die … in den Anwendungsbereich … fallen"). Ausweislich der Gesetzesbegründung zu § 4 b BDSG sollte die Datenübermittlung innerhalb der ersten Säule der Europäischen Union, also im vergemeinschafteten Bereich, privilegiert werden.[7] Eine Datenübermittlung außerhalb der ersten Säule war nach § 4 b II BDSG ebenfalls möglich, stand jedoch unter der Voraussetzung eines schutzwürdigen Interesses sowie eines angemessenen Datenschutzniveaus im Empfängerstaat. Diese Form der Datenübermittlung sah § 18 I 2 MRRG nicht vor und sieht § 35 BMG ebenfalls nicht vor.

3. Unionsrechtskonforme Auslegung des § 35 Bundesmeldegesetz

Damit steht außer Zweifel, dass die Auslegung des § 35 BMG in Bezug auf die Voraussetzung „*im Anwendungsbereich des Rechts der Europäischen Union*" vor dem Hintergrund der unionsrechtlichen Grundlage erfolgen muss. Denn der Zweck der Regelung besteht in der Übernahme der unionsrechtlichen Vorgaben. Die insoweit relevante Regelung des Art. 3 Datenschutz-Richtlinie sowie die Kompetenznorm, auf die sich die Richtlinie stützt, sind in der Zwischenzeit jedoch von Nachfolgeregelungen abgelöst worden, so dass sich vorab die Frage stellt, ob Erkenntnisse auf der Grundlage der Altregelungen überhaupt noch Aussagekraft haben.

a) *Aktuelle Relevanz der Datenschutz-Richtlinie.* Die primärrechtliche Grundlage der Datenschutz-Richtlinie war Art. 100 a EGV idF des Maastrichter Unionsvertrags, der durch den Vertrag von Amsterdam zu Art. 95 EGV wurde. Diese Regelung lebt im AEUV in Art. 114 weiter, so dass sich die Kompetenzgrundlage inhaltlich nicht verändert hat. Nimmt man den Sekundärrechtsakt in den Blick, so stellt sich die Rechtslage ähnlich dar. Die Datenschutz-Richtlinie wurde aufgehoben und ersetzt durch die Datenschutz-Grundverordnung.[8] Die Vorschrift des Art. 3 der Datenschutz-Richtlinie findet nunmehr ihre Entsprechung in Art. 2 der DS-GVO.[9] Nach Art. 2 II Buchst. a findet die Datenschutz-Grundverordnung keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

Während die Datenschutz-Richtlinie noch den Anwendungsbereich des Gemeinschaftsrechts als Grenze markierte, konnte dies die Datenschutz-Grundverordnung nicht mehr tun, da mit dem Inkrafttreten des Lissabonner Vertrags die Union zur Rechtsnachfolgerin der Europäischen Gemeinschaft geworden war (Art. 1 III 3 EUV). Nimmt man die Anwendungsausschlüsse in Art. 3 II Datenschutz-Richtlinie und Art. 2 II DS-GVO genauer in den Blick, wird deutlich, dass der Anwendungsbereich durch die gewählten Formulierungen der Reichweite der Kompetenznormen angeglichen werden sollte. In diesem Sinne haben die Formulierungen lediglich klarstellende Funktion,[10] da ein Sekundärrechtsakt keine Rechtswirkungen erzeugen kann, die über die Kompetenznorm hinausgehen, auf die er sich stützt. Dem steht das grundlegende unionsrechtliche Prinzip der begrenzten Einzelermächtigung entgegen.

Ganz entsprechend hatte Art. 3 II Datenschutz-Richtlinie seine Anwendung auf das Binnenmarktziel begrenzt, da sich die Richtlinie auf Art. 100 a EGV (jetzt Art. 114 AEUV) gestützt hat, der ausdrücklich dieses Ziel benennt. Da sich die Datenschutz-Grundverordnung auf Art. 16 AEUV stützt, der sich als Kompetenzgrundlage (deklaratorisch) auf den Anwendungsbereich des Unionsrechts beschränkt, übernimmt auch Art. 2 II DS-GVO diese Formulierung. Dadurch, dass die Kompetenzgrundlage dem Ersten Teil des AEUV entstammt, entfällt hier sogar der zuvor notwendige Bezug auf das Binnenmarktziel.[11] Die Kontinuität der An-

3 Vgl. die Begründung des Gesetzesentwurfs der Bundesregierung, BR-Drs. 524/11, 81.
4 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281 v. 23.11.1995, 31 ff.
5 Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze v. 18.5.2001, BGBl. I 2001, 904.
6 Vgl. auch *Süßmuth/Laier*, Bundesmeldegesetz, 2. Aufl. (Stand Sept. 2015), § 35 BMG Rn. 2.
7 Vgl. die Begründung des Gesetzesentwurfs der Bundesregierung, BR-Drs. 461/00, 83.
8 Art. 94 der VO (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung RL 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119 v. 4.5.2016, 1 ff.
9 Vgl. auch: *Kühling* in *Kühling/Buchner*, DS-GVO, 2017, Art. 2 Rn. 4.
10 So auch: *Kieck/Pohl*, DuD 2017, 567 (568 f.).
11 Vgl. dazu auch: *Kühling/Raab* in *Kühling/Buchner*, DS-GVO, 2017, Einl. Rn. 75.

wendungsausschlüsse in der Datenschutz-Richtlinie und der Datenschutz-Grundverordnung zeigt sich darin, dass sowohl der Bereich der Strafverfolgung einschließlich Strafvollstreckung, als auch der Bereich der Gemeinsamen Außen- und Sicherheitspolitik als auch ausschließlich persönliche oder familiäre Tätigkeiten von der Anwendung ausgenommen sind. Damit lässt sich festhalten, dass Erkenntnisse zur Reichweite des Anwendungsbereichs der Datenschutz-Richtlinie auch unter Geltung der Datenschutz-Grundverordnung weiterhin ihre Gültigkeit behalten.

b) *Anwendungsbereich der Datenschutz-Richtlinie*. Derartige Erkenntnisse lassen sich aus der Rechtsprechung des *EuGH* zur Datenschutz-Richtlinie gewinnen. In seiner Entscheidung in der Rechtssache C-465/00 hatte der *EuGH* im Rahmen einer Vorlage unter anderem darüber zu befinden, ob die Datenschutz-Richtlinie überhaupt anwendbar sei.[12] Zugrunde lag ein Rechtsstreit vor dem *Österreichischen Verfassungsgerichtshof*. Der Österreichische Rechnungshof begehrte entsprechend einem innerstaatlichen Rechtsakt Auskünfte über Einkünfte von bei öffentlichen Arbeitgebern Beschäftigten, die eine definierte Einkommensgrenze überschreiten. Streitgegenstand war die Frage, ob Europäisches Datenschutzrecht einer Weitergabe derartiger personenbezogener Daten entgegensteht. Das wiederum konnte nur dann der Fall sein, wenn auf den Sachverhalt die Datenschutz-Richtlinie anwendbar war.

Aus dem Zusammenhang zwischen der Kompetenznorm des Art. 100 a EGV (Art. 114 AEUV) und der Definition des Anwendungsbereichs in Art. 3 Datenschutz-Richtlinie lasse sich nach Ansicht des *EuGH* nicht ableiten, dass in jedem Einzelfall, der von dem auf dieser Kompetenznorm ergangenen Rechtsakt erfasst wird, tatsächlich ein Zusammenhang mit dem freien Verkehr zwischen Mitgliedstaaten bestehen müsse.[13] Für die Rechtfertigung der Heranziehung des Art. 100 a EGV (Art. 114 AEUV) komme es entscheidend darauf an, dass der auf dieser Grundlage erlassene Rechtsakt tatsächlich die Bedingungen für die Errichtung und das Funktionieren des Binnenmarktes verbessern *solle*.[14] Diesen Zusammenhang hatte der *Gerichtshof* bereits in einem früheren Verfahren herausgestellt, in dem es um die Nichtigkeit der Tabakwerbe-Richtlinie[15] ging.[16] Art. 100 a EGV (Art. 114 AEUV) sei keine allgemeine Kompetenzgrundlage zur *Regelung* des Binnenmarktes, erforderlich sei vielmehr die Absicht einer *Verbesserung* des Funktionierens des Binnenmarktes.[17] Während der *EuGH* diese Voraussetzung für die Tabakwerbe-Richtlinie als nicht erfüllt ansah, stehe dies für die Datenschutz-Richtlinie außer Zweifel, da sie vorrangig den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten sicherstellen *solle*. Wenn es aber allein auf die Zielsetzung der Richtlinie ankomme, könne die Anwendbarkeit nicht davon abhängen, dass auch tatsächlich ein hinreichender Zusammenhang mit der Ausübung der Grundfreiheiten bestehe.[18] Andernfalls wäre die Abgrenzung des Anwendungsbereichs ungewiss und hinge von Zufälligkeiten ab.

Die Weite des Anwendungsbereichs der Datenschutz-Richtlinie lasse sich darüber hinaus auch daraus ableiten, dass die positive Formulierung in Art. 3 I einen unmittelbaren Zusammenhang der Datenverarbeitung mit der Ausübung der Grundfreiheiten gerade nicht verlange. Bestätigt werde dies durch die in Absatz 2 normierten Ausnahmen, die nicht in dieser Weise formuliert wären, wenn die Richtlinie ausschließlich für Sachverhalte gelten würde, die einen hinreichenden Zusammenhang mit der Ausübung der Grundfreiheiten aufwiesen.[19] Ausgeschlossen waren nämlich ausdrücklich die nicht vergemeinschafteten Bereiche, wie der Gemeinsamen Außen- und Sicherheitspolitik, der Landesverteidigung und der Strafverfolgung.

Ausgehend von diesem Befund kam der *EuGH* zu dem eindeutigen Ergebnis, dass der Sachverhalt des Ausgangsverfahrens (Übermittlung von Informationen über Einkünfte bei öffentlichen Arbeitgebern) in den Anwendungsbereich der Datenschutz-Richtlinie falle.[20] Ein weiteres Argument fand das Gericht in den Zielen, die in Art. 7 und Art. 13 zum Ausdruck kämen. Danach kann eine Datenverarbeitung zB für die Wahrnehmung einer Aufgabe zulässig sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 7 Buchst. e). Das vorgeschriebene Maß des Datenschutzes kann sich reduzieren, wenn es um Kontroll-, Überwachungs- und Ordnungsfunktionen geht, die mit der Ausübung öffentlicher Gewalt verbunden sind (Art. 13 I Buchst. f.). Festhalten lässt sich damit, dass der notwendige Binnenmarktbezug weder verlangt, dass eine Kompetenznorm für spezifische Bereiche/Politiken, noch ein einschlägiger Sekundärrechtsakt vorliegt. Binnenmarktbezug liegt schon dann vor, wenn es um den freien Verkehr von Waren, Personen, Dienstleistungen oder Kapital geht (wobei dies unter Geltung der Datenschutz-Grundverordnung nicht mehr erforderlich ist). Sämtliche Bereiche des mitgliedstaatlichen Ordnungsrechts, die im Zusammenhang mit diesem freien Verkehr Anforderungen an wirtschaftliche Betätigungen stellen, erfüllen damit das Erfordernis des Binnenmarktbezugs und fallen in den Anwendungsbereich des Gemeinschafts-/Unionsrechts.

c) *Auswirkungen auf das nationale Recht*. Die Privilegierung der Datenübermittlung an andere Mitgliedstaaten in § 4 b I BDSG erstreckte sich somit auf sämtliche Fälle mit einem so verstandenen Binnenmarktbezug. Auf Meldedaten sollte diese Form der Privilegierung durch § 18 I 2 MRRG ausgeweitet werden. Mit der Neufassung in § 35 BMG sollte daran nichts geändert werden. Von den eingangs genannten drei Auslegungsmöglichkeiten stellt sich also diejenige als zutreffend heraus, die den Anwendungsbereich am weitesten fasst.

Ob das Meldewesen selbst zu den Politiken der Europäischen Union gehört, kann also nicht die Frage sein, an der sich entscheidet, ob § 35 BMG zur Anwendung kommt oder nicht. Die Tätigkeit, wegen der eine Datenübermittlung an eine ausländische öffentliche Stelle erfolgt, muss den aufgezeigten Binnenmarktbezug haben, um von § 35 BMG erfasst zu werden. Werden Meldedaten für eine Tätigkeit benötigt, die einen Bezug zum freien Verkehr von Waren, Personen, Dienstleistungen oder Kapital haben, so greift § 35

12 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378.
13 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378 Rn. 46.
14 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378 Rn. 46.
15 RL 98/43/EG des Europäischen Parlaments und des Rates v. 6.7.1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über Werbung und Sponsoring zugunsten von Tabakerzeugnissen, ABl. 1998 L 213, 9 ff.
16 *EuGH*, C-376/98, ECLI:EU:C:2000:544 = EuZW 2000, 694 = NJW 2000, 3701.
17 *EuGH*, C-376/98, ECLI:EU:C:2000:544 = EuZW 2000, 694 = NJW 2000, 3701 Rn. 85.
18 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378 Rn. 47; vgl. auch *EuGH*, C 101/01, ECLI:EU:C:2003:596 = EuZW 2004, 245 = CR 2004, 286.
19 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378 Rn. 48.
20 *EuGH*, C-465/00, ECLI:EU:C:2003:294 = EuGRZ 2003, 232 = BeckRS 2004, 77378 Rn. 52.

BMG auch dann, wenn es um die Wahrung eines öffentlichen Interesses oder die Ausübung öffentlicher Gewalt geht. Für die – rein innerstaatliche – Übermittlung der Einkommensdaten hat der *EuGH* dies ohne weiteres angenommen. Für die Tätigkeit der Gesundheitsbehörden im Zusammenhang mit Arbeitsmigranten, die in der fleischverarbeitenden Industrie in den Niederlanden beschäftigt sind und in Deutschland in verschiedenen Unterkünften in mehreren Kommunen wohnen, dürfte dies in gleichem Maße gelten. Der Binnenmarktbezug liegt dabei darin, dass es sich um Arbeitnehmer handelt, deren Freizügigkeit das Unionsrecht garantiert. Ein positiver Binnenmarkteffekt kann aber nicht nur darin liegen, dass Freiheitsgarantien gewährt werden, sondern auch darin, dass sozial-, umwelt- oder auch infektionsschutzrechtliche Anforderungen unabhängig von Grenzen zwischen Mitgliedstaaten einheitlich zur Anwendung kommen.[21] Zu einem abweichenden Ergebnis kommt man auch dann nicht, wenn man die in Art. 3 II Datenschutz-Richtlinie und Art. 2 II DS-GVO normierten Ausnahmen betrachtet. Allein infrage kommt die dort jeweils genannte öffentliche Sicherheit. Nach der Rechtsprechung des *EuGH* betrifft die öffentliche Sicherheit das Schutzsystem eines Staates zur Erhaltung seines Gewaltmonopols sowie den Schutz seiner Existenz und seiner zentralen Einrichtungen.[22] Auf die Übermittlung von Meldedaten in ordnungsrechtlichen Verwaltungsverfahren trifft dies jedenfalls nicht zu. Auch die weiteren genannten Ausnahmen kommen nicht in Betracht.

4. Bestimmtheit des § 35 BMG

Zweifel an der Anwendbarkeit des § 35 BMG könnten sich darüber hinaus aus einer nicht hinreichenden Bestimmtheit ergeben. Der rechtsstaatlich gebotene Grundsatz der Normenklarheit und Bestimmtheit verlangt die Erkennbarkeit des vom Gesetzgeber Gewollten. Eine Norm muss so formuliert sein, dass die von ihr Betroffenen die Rechtslage erkennen und ihr Verhalten danach einrichten können. Ein Gesetz ist hinreichend bestimmt, wenn sein Zweck aus dem Gesetzestext in Verbindung mit den Materialien deutlich wird.[23] Wie bereits erläutert wurde, ergibt sich der Zweck der Formulierung „im Anwendungsbereich des Rechts der Europäischen Union“ aus dem Zusammenhang mit der unionsrechtlichen Grundlage und wird mithilfe der einschlägigen Rechtsprechung des *EuGH* bestimmbar. Diese Bestimmbarkeit genügt aber den Anforderungen an den Bestimmtheitsgrundsatz, so dass im Ergebnis eine Anwendung des § 35 BMG nicht am Grundsatz der Normenklarheit scheitert.

Das Maß der erforderlichen Bestimmtheit ist im Bereich des administrativen Ansatzes auch nicht so hoch wie im Bereich der Strafverfolgung. Außerdem ist mit dem hier erzielten Ergebnis die Prüfung der Zulässigkeit einer Datenübermittlung auch noch nicht abschließend beantwortet. Die datenschutzrechtliche Prüfung schließt sich an, so dass über die Prüfung der Verhältnismäßigkeit der Übermittlung im Einzelfall noch eine weitere rechtsstaatlich gebotene Grenze zu überwinden ist.

III. Datenschutzrechtliche Grundlagen der Übermittlung von Gesundheitsdaten

Da die Übermittlung personenbezogener Daten, mit der eine Behörde, die von ihr erhobenen Daten, einer anderen Stelle zugänglich macht, einen eigenen Grundrechtseingriff begründet,[24] ist zu prüfen, ob und auf welcher Grundlage dieser Eingriff und somit die Übermittlung rechtlich zulässig ist. Dieser Eingriff ist zunächst an dem Grundrecht zu messen, in das bei der ursprünglichen Datenerhebung eingegriffen wurde.[25] Als Grundrechtseingriffe bedürfen Übermittlungen einer eigenen normenklaren und hinreichend bestimmten Rechtsgrundlage.[26] Diese nationale Systematik des GG greift die Datenschutz-Grundverordnung auf, wonach jeder Austausch von Daten im Anwendungsbereich der Datenschutzgrundverordnung dem Zweckbindungsgrundsatz der Art. 5 I b, 6 IV DS-GVO genügen muss.

Wie schon Art. 1 II Datenschutz-Richtlinie schließt Art. 1 III DS-GVO grundsätzlich weitergehende nationale Maßnahmen zum Schutz personenbezogener Daten aus und stellt somit klar, dass die Datenschutz-Grundverordnung – wie schon die Datenschutz-Richtlinie[27] – das Datenschutzrecht in der EU vollständig harmonisiert, soweit die Datenschutz-Grundverordnung die Mitgliedstaaten nicht selbst zu abweichenden oder konkretisierenden Regelungen ermächtigt. Die Datenschutz-Grundverordnung bildet daher einen abschließenden legislativen Konsens innerhalb der EU ab, wie personenbezogene Daten zu schützen sind. Damit soll ausgeschlossen werden, dass die Mitgliedstaaten nationale Maßnahmen zum Schutz personenbezogener Daten ergreifen und diese Beschränkung der Grundfreiheiten als wichtiges Allgemeininteresse rechtfertigen. Ebenso dürften Mitgliedstaaten das Datenschutzniveau in einem anderen Mitgliedstaat nicht in Zweifel ziehen, sondern müssen eine Übermittlung von Daten in einen anderen Mitgliedstaat ebenso behandeln wie innerhalb des Mitgliedstaates.[28] Allerdings erlaubt die Datenschutz-Grundverordnung den Mitgliedstaaten an einer Vielzahl von Stellen, Konkretisierungen und Spezifizierungen vorzunehmen, und eröffnet ihnen hierbei gewisse Spielräume.[29]

Die Erhebung und Verwendung von Daten zur Abwehr von Gefahren, wie einer Pandemie, insbesondere auch staatlicherseits, ist nicht von vornherein ausgeschlossen. Denn der Schutz personenbezogener Daten bzw. das Recht auf informationelle Selbstbestimmung besteht nach übereinstimmender Auffassung des *EuGH*[30] und des *BVerfG*[31] nicht absolut, sondern kann eingeschränkt werden. Das gilt nach dem Willen des Gesetzgebers selbst für besonders sensible Daten wie Gesundheitsdaten, deren Verarbeitung eigentlich grundsätzlich untersagt ist.[32] Insofern begründet das Recht auf informationelle Selbstbestimmung eben keine absolute Verfügungsgewalt über die eigenen personenbezogenen Daten.

21 Vgl. auch: Calliess/Ruffert/*Korte*, 5. Aufl. 2016, AEUV Art. 114 Rn. 46.
22 Vgl. zB: *EuGH*, C-367/89, Slg. 1991, I-4621 Rn. 19 ff.; C-72/83, Slg. 1984, 2727 L 7; C-398/98, Slg. 2001, I-7915; vgl. dazu auch *Epiney* in *Bieber/Epiney/Haag/Kotzur*, Die Europäische Union, 13. Aufl. 2019, § 11 Rn. 53; *Kühling* in *Kühling/Buchner*, DS-GVO, 2017, Art. 2 Rn. 21.
23 Vgl. *BVerfGE* 65, 1 = NJW 1984, 419 = NJW 2017, 3069 Rn. 174 = NVwZ 1984, 167 Ls.
24 Vgl. *BVerfGE* 100, 313 (367) = NJW 2000, 55 = NVwZ 2000, 185 Ls.; *BVerfGE* 141, 220 (334) = NJW 2016, 1781 = NVwZ 2016, 839 Ls.; stRspr.
25 Vgl. *BVerfGE* 100, 313 (367) = NJW 2000, 55 = NVwZ 2000, 185 Ls.; *BVerfGE* 141, 220 (334) = NJW 2016, 1781 = NVwZ 2016, 839 Ls.; stRspr.
26 Vgl. *BVerfGE* 65, 1 (46) = NJW 1984, 419 = NVwZ 1984, 167 Ls.; *BVerfGE* 100, 313 (389) = NJW 2000, 55 = NVwZ 2000, 185 Ls.; stRspr.
27 Grundlegend *EuGH*, ECLI:EU:C:2003:596 = EuZW 2004, 245 Rn. 95 f. – Lindqvist; zuletzt NJW 2016, 3579 Rn. 57 ff. – Breyer.
28 BeckOK Datenschutzrecht/*Wolff/Brink*, DS-GVO, Art. 9 Rn. 9; *Paal/Pauly/Ernst*, DS-GVO Art. 1 Rn. 14; Kühling/Buchner/*Buchner*, DS-GVO Art. 1 Rn. 18.
29 EG 10 S. 3–6.
30 *EuGH*, NJW 2019, 3504 (3506).
31 *BVerfGE* 65, 1 (44) = NJW 1984, 419 = NVwZ 1984, 167 Ls.; *BVerfGE* 115, 320 (344 ff.) = NJW 2006, 1939 = NVwZ 2006, 1156 Ls.
32 Vgl. Art. 9 DS-GVO sowie ErwG 54 S. 1.

Vielmehr hat der Einzelne Beschränkungen zum Schutz überwiegender Allgemeininteressen hinzunehmen.[33]

Zu diesen überwiegenden Allgemeininteressen, die eine Beschränkung des informationellen Selbstbestimmungsrechts rechtfertigen können, zählt unzweifelhaft der Schutz der Bevölkerung vor Gesundheitsgefahren, welchen das *BVerfG* einerseits aus Art. 2 II 1 GG ableitet und der andererseits auf europäischer Ebene in Art. 2 I und Art. 3 I Charta der Grundrechte der Europäischen Union sowie Art. 168 AEUV niedergelegt ist.[34] Der Gesundheitsschutz gehört somit zu den überragend wichtigen Gemeinschaftsgütern, durch die Einschränkungen der Freiheit des Einzelnen[35] und damit sowohl des informationellen Selbstbestimmungsrechts als auch sogar der Bewegungsfreiheit[36] gerechtfertigt werden können.[37] Dies gilt vor allem dann, wenn – wie aktuell – eine Gefahr für die Gesundheit der Bevölkerung nicht nur zu besorgen, sondern schon konkret eingetreten ist: in diesen Fällen trifft den Gesetzgeber eine Pflicht, Schutzmaßnahmen zum Schutz der Bevölkerung zu ergreifen,[38] wobei ihm bei Erfüllung dieser Pflicht ein weiter Einschätzungs-, Wertungs-Gestaltungsspielraum zukommt.[39]

Entsprechend sieht auch die Datenschutz-Grundverordnung eine Reihe von rechtlichen Grundlagen vor, die die Datenverarbeitung – zT auch sensibler Daten – ohne Einwilligung der betroffenen Personen bei einem bestehenden öffentlichen Interesse gestatten und deren Tauglichkeit als Erlaubnistatbestände im Folgenden analysiert und dargestellt werden sollen.

Eine solche Regelung findet sich in Art. 9 IV DS-GVO, wonach die Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten können, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Demnach bedarf es zunächst einer Gesamtbetrachtung der potenziell einschlägigen Normen, um dann deren Anwendungsbereich zu bestimmen und zugleich miteinander in Einklang zu bringen.

Die wesentlichen datenschutzrechtlichen Rechtsgrundlagen finden sich in den nachfolgenden Normen.

1. Art. 6 Datenschutz-Grundverordnung

Da die von der Weitergabe betroffenen und somit verarbeiteten Daten im Ausgangsfall nicht als anonym zu qualifizieren sind, ist der Anwendungsbereich des unionalen Datenschutzrechts nach Art. 2 I DS-GVO eröffnet. Nach Art. 6 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der dort normierten Bedingungen erfüllt ist. In Betracht kommen hier Absatz 1 Buchst. d und e, wonach die Verarbeitung erforderlich sein kann, um *lebenswichtige Interessen* der betroffenen Person oder *einer anderen natürlichen Person zu schützen* oder für die *Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse* liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Der Begriff der *Lebenswichtigkeit* bestimmt sich dabei objektiv, wobei darunter insbesondere die körperliche Unversehrtheit und das Leben zu verstehen ist.[40] Gleichwohl ist „lebenswichtig" nicht gleichzusetzen mit lebensnotwendig, so dass Buchst. d nicht erst greift, wenn eine Lebensgefahr besteht.[41] Ein unmittelbarer Bezug zur körperlichen Integrität und Gesundheit des Betroffenen (oder einer anderen natürlichen Person) genügt.[42] EG 46 S. 3 verdeutlicht zudem, dass Datenverarbeitungen im Einzelfall zugleich zur Erfüllung öffentlicher und lebenswichtiger Interessen erforderlich sein können, so etwa in humanitären Notfällen, insbesondere bei (durch Natur und Mensch verursachten) Katastrophen. Daher wäre Art. 6 I Buchst. d DS-GVO durchaus grundsätzlich geeignet die grenzüberschreitende Datenverarbeitung in Zeiten der Pandemie zu rechtfertigen. Allerdings hat der Rechtfertigungstatbestand des Art. 6 DS-GVO nur subsidiären Charakter; er soll nach dem Willen des Gesetzgebers nur herangezogen werden, wenn die Datenverarbeitung auf keine andere Grundlage gestützt werden kann.[43] Eine solche andere Norm könnten die nachstehend angesprochen Normen aus Art. 9 DS-GVO, bzw. den nationalen Vorschriften zum Datenschutz in Form des BDSG, des LDG NRW bzw. des Infektionsschutzgesetzes sein.

Der Anwendungsbereich von Art. 6 I Buchst. d dürfte jenseits des privaten Sektors ohnehin begrenzt sein. Die Abwehr von Gefahren, die lebenswichtige Interessen bedrohen, stellt jedenfalls (zusätzlich) eine Aufgabe im öffentlichen Interesse dar (Buchst. e) und kann darüber hinaus im Einzelfall sogar eine rechtliche Verpflichtung der öffentlichen Stellen (Buchst. c) begründen.[44]

2. Art. 9 Datenschutz-Grundverordnung

Grundsätzlich untersagt Art. 9 I 1 DS-GVO die Verarbeitung von Gesundheitsdaten. Allerdings erlaubt Absatz 2 die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren. Solch massive Gefahren für die öffentliche Gesundheit können übertragbare Krankheiten, aber auch Gefahren chemischen oder unbekannten Ursprungs sein.[45] In diesen Fällen sind Einwilligungen der Betroffenen oft nicht einholbar oder zielführend.

Der Begriff der öffentlichen Gesundheit soll im Sinne der VO (EG) Nr. 1338/2008 zu verstehen sein. Nach Art. 3 c versteht man unter dem Begriff der „Öffentlichen Gesundheit" daher alle Elemente im Zusammenhang mit der Gesundheit, nämlich den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität.[46]

Als weiteren Tatbestand nennt Art. 9 I 1 Buchst. i selbst als Beispiele für öffentliche Interessen den Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren. Dies rekurriert wiederum auf Art. 168 AEUV, wonach die Tätigkeit der Union die Politik der Mitgliedstaaten ergänzt und umfasst dabei die Beobachtung, frühzeitige Meldung und Be-

33 *Kuhlmann*, GSZ 2020, 115 (119). *BVerfGE* 65, 1 (44) = NJW 1984, 419 = NVwZ 1984, 167 Ls.; *BVerfGE* 92, 191 (197) = *BVerwGE* 92, 191 (nicht amtl.) = NJW 1995, 3110 = NVwZ 1996, 157 Ls.
34 Vgl. *Kuhlmann*, GSZ 2020, 115 (119).
35 *BVerfGE* 7, 377 (414) = NJW 1958, 1035.
36 Vgl. *Di Fabio* in *Maunz/Dürig*, GG, Art. 2 II Rn. 46; *VG München*, NVwZ 2020, 651 (654) .
37 Vgl. *Kuhlmann*, GSZ 2020, 115 (119).
38 *BVerfGE* 39, 1 (42, 56) = NJW 1975, 573; *Schulze-Fielitz* in *Dreier*, GG Art. 2 II Rn. 76.
39 *BVerfGE* 85, 191 (212) = NJW 1992, 964; *Di Fabio* in *Maunz/Dürig*, GG, Art. 2 II Rn. 50.
40 Vgl. EG 112 S. 2.
41 BeckOK Datenschutzrecht/*Wolff/Brink*, DS-GVO, Art. 6 Rn. 36.
42 *Gola/Schulz*, DS-GVO, Art. 6 Rn. 45.
43 Vgl. EG 46 S. 2.
44 Kühling/Buchner/*Buchner/Petri*, DS-GVO, Art. 6 Rn. 108.
45 *Gola/Schulz*, DS-GVO, Art. 9 Rn. 40.
46 Vgl. dazu Kühling/Buchner/*Buchner/Petri*, DS-DVO, Art. 9 Rn. 116 f.

kämpfung schwerwiegender grenzüberschreitender Gesundheitsgefahren.[47]

Nach alledem lässt sich die COVID 19 Pandemie unzweifelhaft unter den Anwendungsbereich von Art. 9 I 2 Buchst. i DS-GVO subsumieren, denn die COVID 19 Pandemie erfasst nicht nur den Gesundheitszustand einschließlich Morbidität der Betroffenen, sondern betrifft auch weite Teile der Gesundheitsversorgung (Auslastung der Intensivstationen etc.) bzw. die dazu notwendigen Mittel, wie auch die potenzielle Überlastung des Systems und den allgemeinen Zugang zu (anderen) Gesundheitsversorgungsleistungen.[48]

Unklar ist, ob Art. 9 II Buchst. i DS-GVO als eigenständige datenschutzrechtliche Legitimationsnorm für die Weitergabe der Gesundheitsdaten im vorliegenden Fall angesehen werden kann. Da – anders als bisher im Art. 8 Datenschutz-Richtlinie – gesundheitsspezifische Regelungen in einer EU-Verordnung erfasst werden, hat diese gem. Art. 288 AEUV zunächst allgemeine Geltung; sie ist in allen ihren Teilen verbindlich und gilt daher unmittelbar auch in Deutschland. Nach kritischer Ansicht entfaltet die Bestimmung allerdings selbst keine eigene Legitimationswirkung, sondern ist auf „Ausfüllung" durch ergänzende Rechtsetzung angewiesen.[49] An diese stellt Art. 9 II Buchst. j DS-GVO auch materielle Anforderungen dergestalt, dass das jeweilige Recht angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsieht. Ob Art. 9 II Buchst. i DS-GVO somit als unzureichende Eingriffsnorm für den datenschutzrechtlichen Eingriff anzusehen ist, kann dahinstehen, sofern es eine ausreichende, den Vorgaben der Datenschutz-Grundverordnung genügende, nationale Vorschrift gibt.[50] Von dieser Öffnungs- bzw. Ergänzungsklausel hat der deutsche Gesetzgeber mit der Regelung des § 22 I 1 Nr. 1 c (iVm § 22 II 2) BDSG Gebrauch gemacht.

3. § 22 Bundesdatenschutzgesetz

§§ 22 I 1 Nr. 1 c) BDSG normiert, dass abweichend von Art. 9 I der VO (EU) 2016/679 die Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art. 9 I der VO (EU) 2016/679 durch öffentliche und nichtöffentliche Stellen zulässig ist, wenn diese aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist. Absatz 1 Nr. 1 c betrifft somit die Verarbeitung zugunsten öffentlicher Gesundheitsinteressen. Im Einzelnen wird mit der Vorschrift von den Öffnungsklauseln des Art. 9 II Buchst. i Gebrauch gemacht.[51]

Fraglich ist zunächst, ob § 22 BDSG nicht im Zusammenhang mit der Generalklausel des § 3 BDSG zu sehen ist. § 3 erlaubt die Verarbeitung personenbezogener Daten durch öffentliche Stellen, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Letzteres träfe wohl auf eine Kontaktverfolgung infizierter Personen zum Zwecke der Eindämmung der COVID 19 Pandemie nach dem Infektionsschutzgesetz zu (vgl. dazu unten 4.) zu. Ausweislich des Willens des Gesetzgebers soll § 3 BDSG jedoch nur für Datenverarbeitungen mit geringer Eingriffsintensität gelten, was jedenfalls kaum mehr angenommen werden kann, sobald es sich bei den zu verarbeitenden Daten um Gesundheitsdaten handelt.[52]

Es verbleibt somit bei § 22 I 1 Nr. 1 c BDSG, der es erlaubt, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auch besonders sensitive Daten wie Gesundheitsdaten zu verarbeiten, jedenfalls soweit dies erforderlich ist. Umstritten ist allerdings, ob § 22 BDSG eine ausreichende Rechtsgrundlage für die Verarbeitung zu den dort genannten Zwecken ist, denn die Norm übernimmt lediglich den Wortlaut der Datenschutz-Grundverordnung. Auf Grund dieser inhaltsgleichen Formulierung stellt sich auch im Hinblick auf Absatz 1 Nr. 1 c die Frage nach dem eigenständigen Anwendungsbereich der Bestimmung.[53]

Unterstellt man, dass die allgemeine Bestimmung des § 22 I 1 Nr. 1 c BDSG die vom *BVerfG* aufgestellten strengen Anforderungen an eine hinreichend präzise bereichsspezifische Regelung angesichts der vorliegend hohen Grundrechtseingriffsintensität nicht erfüllt,[54] wäre – zumindest unter Rechtssicherheitsgesichtspunkten – zu prüfen, ob nicht (zusätzlich) eine spezifischere Ermächtigungsgrundlage vorliegt. Ein Eingriff in das Grundrecht auf Schutz der personenbezogenen Daten bedarf nämlich einer Ermächtigung, die die zu erhebenden personenbezogenen Daten als solche, den Anlass und den spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regelt und den Grundsatz der Verhältnismäßigkeit wahrt.[55]

Dies ist bei § 22 BDSG im vorliegenden Falle zumindest unklar, da weder die zu erhebenden personenbezogenen Daten als solche, der Anlass und der spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung geregelt sind. Solche bereichsspezifischen Regelungen – abseits des § 22 BDSG – (die Anlass und den spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regeln und den Grundsatz der Verhältnismäßigkeit wahren) finden sich etwa im Recht der Arznei- oder Medizinproduktsicherheit.[56] Im vorliegenden Fall kommt als solche bereichsspezifische Vorschrift das Infektionsschutzgesetz in Betracht. Diese Verdrängung geht freilich nur so weit, wie der Regelungsgehalt der Spezialvorschrift trägt. Enthält diese nur Vorgaben zur materiell-rechtlichen Zulässigkeit einer Verarbeitung, so bleiben die prozeduralen Anforderungen aus Absatz 2 gleichwohl anwendbar.[57]

4. Infektionsschutzgesetz

Das Infektionsschutzgesetz des Bundes sieht zunächst keine offensichtliche Rechtsgrundlage für die direkte Weitergabe personenbezogener Daten durch eine deutsche Gesundheitsbehörde eines Landes an eine ausländische Behörde (hier: niederländische Behörde) vor.

47 Vgl. dazu nur Calliess/Ruffert/*Kingreen*, EUV/AEUV, Art 186 Rn. 11.
48 Wie hier auch *Kühling/Schildbach*, NJW 2020, 1545 (1547); EDSA, Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, Version 1.1 v. 5.5.2020, Rn. 33.
49 Vgl. BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 9 Rn. 84; Spindler/Schuster/*Spindler/Dalby*, DS-GVO, Art. 9 Rn. 21; anders wohl Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, angenommen am 21.4.2020 Rn. 33.
50 Die einschlägigen § 22 BDSG, § 16 LDSG NRW werden nachfolgend dargestellt.
51 Vgl. BT-Drs. 18/11325, 94.
52 Vgl. BT-Drs. 118/11325, 81 und 18/10938, 58 f.
53 Einen solchen verneinend Paal/Pauly/*Frenzel*, § 22 BDSG Rn. 8.
54 So *Kühling/Schildbach*, NJW 2020, 1545 (1549); § 22 BDSG wohl für ausreichend haltend: *Kuhlmann*, GSZ 2020, 115 (120).
55 Vgl. zuletzt *BVerfG*, NJW 2020, 2699 = ZD 2020, 580; *BVerfGE* 65, 1 = NJW 1984, 419 = NVwZ 1984, 167 Ls.
56 Für eine detailliertere Übersicht s. Kühling/Buchner/*Weichert*, DS-GVO, Art. 9 Rn. 119.
57 Kühling/Buchner/*Weichert*, DS-GVO Art. 9 Rn. 45.

a) *§ 12 II Infektionsschutzgesetz.* Einen Übermittlungsmodus von Daten der Gesundheitsbehörden eines Landes an die obersten Landesbehörden, das Robert Koch-Institut und schließlich auch an zuständige Behörden anderer Mitgliedstaaten der Europäischen Union sieht § 12 II IfSG vor. Das Robert Koch-Institut ist gem. § 12 II 4 IfSG die zuständige Behörde für Übermittlungen nach dem Beschluss Nr. 1082/2013/EU, insbesondere auch für Warnmeldungen an die zuständigen Behörden anderer Mitgliedsstaaten gem. Art. 9 Beschluss Nr. 1082/2013/EU. Im Rahmen des Early Warning and Response Systems (EWRS) darf das Robert Koch-Institut als zuständige nationale Behörde daher gem. Art. 9 III Beschluss Nr. 1082/2013/EU auch personenbezogene Daten übermitteln, da die COVID 19 Pandemie eine schwerwiegende grenzüberschreitende Gesundheitsgefahr iSv Art. 9 I Beschluss Nr. 1082/2013/EU darstellt. Diese Übertragung muss aber dem Zweckbindungsgrundsatz der Art. 5 I b, 6 IV DS-GVO genügen und die übertragenen Informationen dürfen dann auch nur zur allgemeinen Seuchenbekämpfung oder weiteren mit diesem Zweck vereinbaren Zwecken verwendet werden.

b) *§ 27 I 1 Infektionsschutzgesetz.* Nach § 27 I 1 IfSG unterrichtet das Gesundheitsamt insbesondere in den Fällen des § 25 I IfSG unverzüglich andere Gesundheitsämter oder die zuständigen Behörden und Stellen nach den §§ 54–54 b, deren Aufgaben nach diesem Gesetz berührt sind, und übermittelt ihnen die zur Erfüllung von deren Aufgaben erforderlichen Angaben, sofern ihm die Angaben vorliegen.

Die COVID 19 Pandemie ist dann ein Fall des § 25 IfSG, sofern es sich ergibt oder anzunehmen ist, dass jemand krank, krankheitsverdächtig, ansteckungsverdächtig oder Ausscheider ist oder dass ein Verstorbener krank, krankheitsverdächtig oder Ausscheider war. Dann stellt das Gesundheitsamt die erforderlichen Ermittlungen an, insbesondere über Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit. Im Falle einer (potenziellen) COVID 19 Ansteckung liegen diese Voraussetzungen unproblematisch vor, fraglich ist allerdings, ob § 27 IfSG als ausreichende Ermächtigungsgrundlage für den Datenaustauch im vorliegenden Fall dienen kann. § 27 IfSG ist dabei im Gesamtkontext des Infektionsschutzgesetzes zu betrachten:

So sieht § 9 I IfSG neben vielen anderen Daten vorrangig eine namentliche Meldung mit Angaben zu Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend: Anschrift des derzeitigen Aufenthaltsortes und weitere Kontaktdaten vor. Demnach erlaubt § 9 IfSG grundsätzlich die Verarbeitung solcher Daten. Adressat der Datenverarbeitung ist nach § 9 IV IfSG zunächst das Gesundheitsamt, in dessen Bezirk sich die betroffene Person derzeitig aufhält oder zuletzt aufhielt. Die verarbeiteten Daten zu meldepflichtigen Krankheiten und Nachweisen von Krankheitserregern werden jeweils fallbezogen mit den Daten der zu diesem Fall geführten Ermittlungen und getroffenen Maßnahmen sowie mit den daraus gewonnenen Erkenntnissen auch an das Gesundheitsamt übermittelt, in dessen Bezirk die betroffene Person ihre Hauptwohnung hat oder zuletzt hatte oder in dessen Bezirk sich die betroffene Person gewöhnlich aufhält, falls ein Hauptwohnsitz nicht feststellbar ist oder falls die betroffene Person sich dort gewöhnlich nicht aufhält.

Zusätzlich zu prüfen ist noch, ob beim Eingriff in das Grundrecht auf Schutz der personenbezogenen Daten durch die Übermittlung der personenbezogenen Gesundheitsdaten an das niederländische Gesundheitsamt die zu erhebenden personenbezogenen Daten als solche, der Anlass und der spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung durch § 27 IfSG klar geregelt sind und der Grundsatz der Verhältnismäßigkeit gewahrt ist.[58] Dabei ist insbesondere auch auf die allgemeinen Grundsätze nach Art. 5 DS-GVO einzugehen, der diese Grundsätze überwiegend zusammenfasst. (dazu zusammenfassend später). Festzuhalten ist allerdings hier schon einmal, dass § 27 IfSG die Weitergabe der in Frage stehenden Daten an das Gesundheitsamt erlaubt, an dem sich die Person aufhält oder ihren Wohnsitz hat.

5. § 16 Datenschutzgesetz Nordrhein-Westfalen

Als weitere Vorschrift ist § 16 NRWDSG zu berücksichtigen.[59] Dieser normiert, dass die Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art. 9 I der VO (EU) 2016/679 zulässig ist, soweit sie nach Absatz 1 Nr. 1 zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist oder nach Nr. 3 zum Zwecke der Gesundheitsvorsorge, zur medizinischen Diagnostik, zur Gewährleistung und Überwachung der Gesundheit oder Mitteilung von Gesundheitswarnungen, zur Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren oder zur Verwaltung von Leistungen der Gesundheitsversorgung erforderlich ist, sofern die Verarbeitung dieser Daten durch ärztliches oder sonstiges Personal erfolgt, das einer entsprechenden Geheimhaltungspflicht unterliegt.

§ 16 I NRWDSG regelt also nach der Vorstellung des Gesetzgebers die Fälle, in denen die Verarbeitung besonderer Kategorien personenbezogener Daten ohne die Einwilligung der betroffenen Person aus Gründen eines erheblichen öffentlichen Interesses zulässig ist. Nach Art. 9 II Buchst. i DS-GVO können die Mitgliedstaaten die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheitsvorsorge zulassen.[60] Insbesondere dient § 16 I Nr. 3 Var. 4 NRWDSG der Verarbeitung sensibler Daten zur Prävention oder Kontrolle ansteckender Krankheiten – wie der COVID 19 Pandemie – sofern dies erforderlich ist.[61]

Weitere Voraussetzung ist, dass die Verarbeitung dieser Daten durch ärztliches oder sonstiges Personal erfolgt, das einer entsprechenden Geheimhaltungspflicht unterliegt. Darunter fallen insbesondere Berufsgruppen, die zu einer der Gruppen des § 203 StGB zählen. Im Gesundheitsamt fallen so neben den ärztlichen Mitarbeitern auch sonstiges Personal darunter, da nach § 22 II und III des Gesetzes über den öffentlichen Gesundheitsdienst des Landes Nordrhein-Westfalen[62] die Leitung der medizinischen Dienste der unteren Gesundheitsbehörde einer Ärztin oder einem Arzt nach Absatz 1 obliegt und Amtsarzt und Amtsärztin im Sinne sonstiger bundes- und landesrechtlicher Regelungen Ärztinnen und Ärzte nach Absatz 1 sind. Damit umfassen die Berufsträgergeheimnisse nach § 203 I und II, 4 StGB die dort arbeitenden Personen, sowohl als ärztliches Personal, wie auch als Amtsträger. Insbesondere zählt dazu aber das sonstige Personal als mitwirkendes Personal iSv § 203 IV StGB.

58 Vgl. *BVerfG*, NJW 2020, 2699 = ZD 2020, 580; *BVerfGE* 65, 1 = NJW 1984, 419 = NVwZ 1984, 167 Ls.

59 Ähnliche Vorschriften finden sich in weiteren Landesdatenschutzgesetzen (wie hier zB § 16 ThürDSG); anders Art. 8 I Nr. 4 BayDSG, § 14 BlnDSG, die jeweils nur den Wortlaut des § 22 BDSG wiedergeben und somit den gleichen Bedenken unterliegen wie § 22 BDSG selbst (vgl. dazu *Kühling/Schildbach*, NJW 2020, 1545 [1549]; § 22 BDSG wohl für ausreichend haltend: *Kuhlmann*, GSZ 2020, 115 [120]).

60 Vgl. LT-Drs. 17/1981, 142.

61 Vgl. dazu auch *Schwartmann/Mühlenbeck* in *Schwartmann/Pabst*, LDSG NRW, § 16 Rn. 25 ff.

62 ÖGDG NRW v. 25.11.1997.

Geht man davon aus, dass die Daten an die niederländischen „Gesundheitsämter" bzw. wesensgleiche Institutionen übermittelt und dort ebenfalls die niederländischen Geheimhaltungsstandards für Gesundheitsdaten eingehalten werden, erlaubt § 16 I NRWDSG also die Verarbeitung dieser Daten ohne die Einwilligung der betroffenen Person, da ein erhebliches öffentlichen Interesse iSv Art. 9 II Buchst. i DS-GVO vorliegt.

6. Datenschutzrechtliche Gesamtwürdigung

Bei unterschiedlichen datenschutzrechtlich anwendbaren Normen stellt sich zusätzlich die Frage, welche der gesetzlichen Normen für die Beurteilung des hier in Frage stehenden datenschutzrechtlichen Vorgangs abschließend heranzuziehen ist. Dies hängt im Wesentlichen von zwei Faktoren ab. Zunächst ist darauf abzustellen, wer für die fragliche Maßnahme verantwortlich ist, also die Daten verarbeitet. Dies wäre hier aus deutscher Sicht das Gesundheitsamt. Da es sich dabei um eine öffentliche Stelle des Landes (NRW) handelt, findet das NRWDSG Anwendung (vgl. § 1 I BDSG).[63] Vorrang hat jedoch immer eine bundesrechtliche bereichsspezifische Bestimmung. Dies könnte hier das nationale Infektionsschutzgesetz sein. Soweit es keine einschlägigen landesrechtlichen Vorschriften gibt, ist § 1 II BDSG zu berücksichtigen, wonach das BDSG auch für öffentliche Stellen der Länder der Länder gilt, soweit der Datenschutz nicht durch Landesgesetz geregelt ist. Dabei ist der Begriff des „soweit" als Abweichung des Landesrechts vom „sachlichen Geltungsbereich" (Schutzbereich)[64] zu verstehen. Es geht also um Regelungslücken oder fehlende Regelungen (wie bei der Analogie), nicht hingegen um bewusste Nicht-Regelungen und auch nicht um inhaltlich andersartige Regelungen. „Danach, ob diese Regelung mit derjenigen des BDSG übereinstimmt oder ob sie für den Betroffenen günstiger oder weniger günstig ist, fragt das Gesetz nicht; entscheidend ist allein die Existenz einer Regelung".[65] Demnach ist im vorliegenden Fall zunächst grundsätzlich auf die Vorschrift des § 16 NRWDSG abzustellen, welche durch die spezialgesetzlichen Vorschriften des Infektionsschutzgesetzes ergänzt werden (soweit). Beide Gesetze sind aber wiederum im Lichte der Datenschutz-Grundverordnung und der allgemeinen Grundrechte zu würdigen bzw. es ist ergänzend auf die dort niedergelegten allgemeinen Grundsätze, insbesondere die Grundprinzipien aus Art. 5 DS-GVO zurückzugreifen (Rechtmäßigkeit, Transparenz, Zweckbindung, Richtigkeit, Integrität und Vertraulichkeit).

Für das nationale Ausfüllen der Öffnungsklausel des Art. 9 II Buchst. i DS-GVO durch die §§ 22 BDSG und 16 NRWDSG, sowie § 27 IfSG gilt neben dem Erforderlichkeitskriterium insbesondere die Maßgabe, dass „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person" getroffen werden müssen (vgl. Art. 5 DS-GVO). Auch wenn im Einzelnen darüber gestritten werden kann, was unter solchen Maßnahmen zu verstehen ist, ist der nationale Gesetzgeber jedenfalls verpflichtet, konkrete Schutzvorschriften zu erlassen. Als solche Maßnahme kann die Vorgabe in § 16 I Nr. 3 NRWDSG verstanden werden, da dieser die Verarbeitung nur solchen Personen überlässt, die als Berufsträger der Verschwiegenheit unterliegen, sei es als Amtsträger, sei es als medizinisches Personal. Zu prüfen wäre gegebenenfalls noch, wie die Gesundheitsämter, an die die Daten auf niederländischer Seite weitergegeben werden, aufgestellt sind. Dabei ist allerdings zusätzlich zu berücksichtigen, dass die Mitgliedstaaten – also Deutschland – das Datenschutzniveau in einem anderen Mitgliedstaat – also den Niederlanden – nicht in Zweifel ziehen dürfen. Sie müssen eine Übermittlung von Daten in einen anderen Mitgliedstaat ebenso behandeln wie innerhalb des Mitgliedstaates.[66] Demnach wäre also eine Übermittlung der in Frage stehenden Daten an die zuständige öffentliche Stelle in den Niederlanden nach § 16 I Nr. 3 Var. 4 NRWDSG rechtlich zulässig.

IV. Fazit

Damit ergibt sich folgende Gesamteinschätzung: Die Übermittlung von Meldedaten im Binnenmarkt scheitert in der Regel nicht daran, dass der Datenfluss ein grenzüberschreitender ist. Wenn und soweit Anknüpfungspunkt für eine Anfrage die wirtschaftliche Betätigung eines Marktbürgers ist, privilegiert § 35 BMG die Datenübermittlung an ausländische öffentliche Stellen im Binnenmarkt. Bei der gebotenen unionsrechtskonformen Auslegung genügt die Vorschrift auch den rechtsstaatlichen Anforderungen an die Normenklarheit.

Art. 9 II Buchst. i DS-GVO eröffnet darüber hinaus grundsätzlich die Möglichkeit Gesundheitsdaten in Zeiten der Pandemie auszutauschen. Es handelt sich um einen Fall des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, da nicht nur der Gesundheitszustand der Bevölkerung einschließlich der Morbidität betroffen ist, sondern auch weite Teile der allgemeinen Gesundheitsversorgung (wie beispielsweise die Auslastung der Intensivstationen/Schutz vulnerabler Gruppen/Überlastung des Systems insgesamt und der allgemeine Zugang zu Gesundheitsversorgungsleistungen[67]) belastet werden.

National wird Art. 9 II Buchst. i ergänzt durch Art. 16 I Nr. 3 NRWDSG, der sich inhaltlich auf Art. 9 DS-GVO beruft und diesen insofern spezifiziert als er nicht nur allgemein auf öffentliche Interessen im Bereich der öffentlichen Gesundheit bzw. den Schutz vor grenzüberschreitenden Gesundheitsgefahren abstellt, sondern konkret die Prävention und Kontrolle ansteckender Krankheiten und schwerwiegender Gesundheitsgefahren als datenschutzrechtlich rechtfertigenden Eingriffsgrund normiert.

Die Übermittlung von COVID 19 bedingten Gesundheitsdaten ist daher gem. Art. 9 II Buchst. i DS-GVO iVm § 16 I Nr. 3 NRWDSG grundsätzlich zulässig, da der Austausch von Gesundheits- und Meldedaten angesichts einer transnationalen Pandemie öffentlichen Gesundheitsinteressen dient (Art. 9 II Buchst. i DS-GVO) und nach § 27 IfSG eine Weitergabe der Daten an die (niederländischen) zuständigen Stellen für die Bekämpfung der Pandemie vor Ort iSd § 27 IfSG zulässig ist. Dabei ist davon auszugehen, dass das niederländische Datenschutzniveau der Datenschutz-Grundverordnung entspricht und daher grundsätzlich auch nicht infrage zu stellen ist und die Grundprinzipien aus Art. 5 DS-GVO, wie Rechtmäßigkeit, Transparenz, Zweckbindung, Richtigkeit, Integrität und Vertraulichkeit dort ebenso eingehalten werden. ■

63 Vgl. dazu nur *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. Rn. 209; Gola/Heckmann/*Gola/Reif*, BDSG, § 1 Rn. 6.
64 BeckOK DatenschutzR/*Gusy*, BDSG, § 1 Rn. 72; Simitis/*Dammann*, § 1 BDSG Rn. 125.
65 Simitis/*Dammann*, § 1 BDSG Rn. 125; BeckOK DatenschutzR/*Gusy*, BDSG § 1 Rn. 72.
66 BeckOK Datenschutzrecht/*Albers/Veit*, DS-GVO, Art. 9 Rn. 9; Paal/Pauly/*Ernst*, DS-GVO, Art. 1 Rn. 14; Kühling/Buchner/*Buchner*, DS-GVO Art. 1 Rn. 18.
67 Wie hier auch *Kühling/Schildbach*, NJW 2020, 1545 (1547); EDSA, Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, Version 1.1 v. 5.5.2020 Rn. 33.