Schlussbericht für das BMBF-Verbundprojekt

„Echtzeitdienste für die Maritime Sicherheit – Security (EMSec)“ –

Begleitforschung für die maritime Sicherheit/Rechtliche Aspekte

Ostseeinstitut für Seerecht, Umweltrecht und Infrastrukturrecht der Universität Rostock (Hrsg.)

INHALT

I. Kurzdarstellung des Projekts

Das Verbundprojekt „Echtzeitdienste für die Maritime Sicherheit – Security“ (EMSec) wurde innerhalb des Programms „Forschung für die Zivile Sicherheit“ - Bekanntmachung „Maritime Sicherheit“ vom Bundesministerium für Bildung und Forschung (BMBF) als größtes jemals gefördertes Projekt finanziert.

1. Aufgabenstellung

Unter der Prämisse, maritimen Risiken und Gefahren aus im Vorfeld definierten Bedrohungsszenarien („Kriminelle Handlungen“, „Gefahrstoffe/Gefahrgüter“, Havarie/Großschadenslage“ und „Naturkatastrophen“), künftig frühzeitig(er) zu begegnen und damit Rettungsprozesse auf See zu optimieren sowie kritische Infrastrukturen zu sichern, hat sich der Forschungsverbund EMSecs[1] unter der Koordination des Deutschen Zentrums für Luft- und Raumfahrt (DLR) der Grundlagenforschung im vorgenannten Bereich verschrieben. Letztere war dabei von dem Gedanken getragen, dass gezielte Informationen notwendig sind, um adäquat auf bevorstehende oder bereits eingetretene Risiken/Gefahren reagieren zu können. Hierbei ist es ebenso erforderlich, bestehende und neu erhobene Daten aus den verschiedenen Quellen[2] dergestalt zu bündeln, dass im konkreten Einzelfall für den Endnutzer[3] keine Zeitverluste durch die Suche nach brauchbaren Informationen entstehen. Ziel der Forschung war es daher, zu untersuchen, inwieweit es möglich ist, den in erster Linie behördlichen Nutzern die Daten und Lagebilder in einer verständlichen, den jeweiligen Anforderungen gerechten Weise schnell und sicher in Form eines ganzheitlichen Lagebildes zur Verfügung zu stellen, durch das sie in die Lage versetzt werden, maritimen Gefahren bereits im Vorfeld zu begegnen bzw. effizientere Maßnahmen bzgl. eingetretener Schadensfälle zu ergreifen.

In rechtlicher Hinsicht wurde das Vorhaben durch die Begleitforschung des Ostseeinstituts für Seerecht, Umweltrecht und Infrastrukturrecht (OSU) unter der Leitung des geschäftsführenden Direktors Prof. Dr. Wilfried Erbguth abgesichert. Die Aufgabe bestand sowohl in der Bearbeitung von – zumeist datenschutzrechtlichen - Anfragen der

[1] Der Forschungsverbund setzt sich wie folgt zusammen: für das DLR sind das Institut für Flugführung, das Deutsche Fernerkundungsdatenzentrum, das Institut für Methodik der Fernerkundung, das Institut für Raumfahrtsysteme, das Institut für Kommunikation und Navigation und das Institut für Optische Sensorsysteme beteiligt; Partner des DLR sind ATLAS ELEKTRONIK GmbH, AIRBUS DS GmbH, AIRBUS DS Airborne Solutions GmbH, das Technische Hilfswerk, das Ostseeinstitut für Seerecht, Umweltrecht und Infrastrukturrecht der Universität Rostock und weitere assoziierte Partner.

[2] Etwa Satellitendaten oder solche aus luftgestützten Diensten etc.

[3] Nutzer des Projekts sind dabei vor allem die Bundespolizei See, die Wasserschutzpolizeien, die Deutsche Gesellschaft zur Rettung Schiffsbrüchiger und das Havariekommando.

Projektpartner als auch in der gutachterlichen Darstellung des bestehenden Rechtsrahmens zur Gewährleistung maritimer Sicherheit.

2. Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Projekt lief von Oktober 2013 bis September 2016 und umfasste ein Fördervolumen von insgesamt 9,76 Millionen Euro, von denen 250.000 Euro auf das OSU entfielen.

In fachlicher Hinsicht konnten die Mitarbeiter des OSU in erster Linie von der langjährigen Erfahrung des geschäftsführenden Direktors Prof. Dr. Wilfried Erbguth im vorliegend interessierenden Bereich profitieren. So ergingen aus seiner Feder zahlreiche Publikationen zum Thema „maritimes Raumordnungs- und Infrastrukturrecht“. Dies lässt sich sowohl Monographien als auch Beiträgen in Sammelwerken und Abhandlungen in Zeitschriften entnehmen. Insoweit sei exemplarisch auf die

Monographien

- Raumordnungs- und Landesplanungsrecht, 2. Aufl. 1992, Köln u. a., mit Jörg Schoeneberg
- Rechtsfragen der Zulassung und planerischen Steuerung schwimmender und pfahlgestützter Häuser in Küsten- und Binnengewässern – anhand des Bundesrechts und des Landesrechts Mecklenburg-Vorpommern, Rostocker Schriften zum Seerecht und Umweltrecht, Bd. 34, Baden-Baden 2006, mit Matthias Schubert
- Rechtsfragen der Errichtung und Erweiterung von Binnenhäfen - unter Berücksichtigung städtebaulicher Nutzungsinteressen an Hafenflächen, Rostocker Schriften zum Seerecht und Umweltrecht, Baden-Baden 2011, mit Matthias Schubert

Beiträge in Sammelwerken

- Rechtsfragen der Planung und Genehmigung von Offshore-Windenergieanlagen, in: Koch/Lagoni (Hrsg.), Meeresumweltschutz für Nord- und Ostsee, 1996, S. 281
- Zum Planungsrecht für Küsten und Meere; in: Jörg Ennuschat/ Jörg Geerlings/ Thomas Mann/ Johann-Christian Pielow (Hrsg.), Wirtschaft und Gesellschaft im Staat der Gegenwart, Gedächtnisschrift für Peter J. Tettinger, Köln 2007, S. 397-415
- Terrorismusabwehr in Häfen: rechtliche Entwicklungen; in: Rolf Stober (Hrsg.), Jahrbuch des Sicherheitsgewerberechts 2007, Hamburg 2008, S. 41-75

und Abhandlungen in Zeitschriften

- Raumplanung im Meer – unter besonderer Berücksichtigung des Natur- und Umweltschutzrechts; in: NuR 1999, S. 491-497

- Raumordnung in der Ausschließlichen Wirtschaftszone; in: DVBl. 2003, S. 625-684, mit Chris Müller
- Steuerung von Offshore-Windenergieanlagen in der Ausschließlichen Wirtschaftszone - Raumordnerische Handlungsmöglichkeiten des Bundes und der Länder -; in: DÖV 2003, S. 665-672, mit Stefan Mahlburg
- Neues Hafensicherheitsrecht: Erstellung der Risikobewertung und des Gefahrenabwehrplans; in: DVBl. 2007, S. 1202-1211
- Gefahrenabwehr in Häfen: Indiepflichtnahme der Hafenbetreiber, Begriff des Hafens und des Hafenbetreibers im neuen Hafensicherheitsrecht; in: LKV 2007, S. 533-537
- Nationales Infrastrukturrecht zur See; in: DVBl. 2009, S. 265-274
- Gesamtplanerische Abstimmung zu Wasser – Rechtslage und Rechtsentwicklung; in: Die Verwaltung 2009, S. 179-213
- Maritime Raumordnung – Entwicklung der internationalen, supranationalen und nationalen Rechtsgrundlagen; in: DÖV 2011, S. 373-382
- Raumordnungspläne für die deutsche Ausschließliche Wirtschaftszone – Inhalte und rechtliche Beurteilung –; in: UPR 2011, S. 207-211
- Perspektiven der Raumordnung in Europa, in: RuR 2011, S. 359-365
- Europarechtliche Vorgaben für eine maritime Raumordnung: Empfehlungen; in: NuR 2012, S. 85-91[4]
- Europäisches Raumordnungsrecht: Neue Regelungskompetenzen der EU im Gefolge des Vertrages von Lissabon?; in: AöR 2012, 72-91 mit Matthias Schubert

hingewiesen. Insbesondere aber mit seinem umfangreichen Gutachten für den Landtag Mecklenburg-Vorpommern, in denen Fragen der maritimen Sicherheit behandelt wurden,[5] hat Prof. Dr. Wilfried Erbguth zusätzlich wertvolle Vorarbeiten geleistet. Daneben konnte im Rahmen der Projektbearbeitung auf die Fachliteratur in der eigenen Bibliothek des OSU zurückgegriffen werden.

[4] Die Aufzählung ist nicht abschließend.

[5] Vgl. *Landtag Mecklenburg-Vorpommern* (Hrsg.) Maritime Sicherheit im Ostseeraum 2001/ Maritime Sicherheit Band II 2002 und Band III 2003.

3. Planung und Ablauf des Vorhabens

Die Ablaufplanung des Teilvorhabens richtete sich nach im Vorfeld definierten Arbeitspaketen Nr. 3000-3300. Zusammengefasst stellte sich dies für das Arbeitspaket Nr. 3300 folgendermaßen dar:

Teil-AP-Nr. 3300 „Rechtliche Begleitforschung in Teilfeldern des Forschungsverbundes“ (24 Monate)

- Ermittlung der datenschutzrechtlichen Fragestellungen und Bezugnahme auf die technischen Teilvorhaben
- Literaturrecherche zu den datenschutzrechtlichen Fragestellungen, die im ersten Schritt ermittelt wurden
- Bewertung der datenschutzrechtlichen Fragestellungen

4. Wissenschaftlicher Stand

Für das Projekt war an den wissenschaftlichen Stand zum Zeitpunkt der Antragstellung anzuknüpfen. Bezüglich des Arbeitspakets Nr. 3300 mussten allerdings zunächst die datenschutzrechtlichen Fragestellungen ermittelt werden, sodass der wissenschaftliche Stand insofern unklar war.

5. Zusammenarbeit mit anderen Stellen

Das OSU hat im Wesentlichen eng mit den Projektkoordinatoren des DLR und den übrigen Projektpartnern zusammengearbeitet. Darüber hinaus konnte etwa einer Einladung zur Bundespolizei See (Neustadt in Holstein) gefolgt werden. Hier wurden wertvolle Gedanken zu den Themen „maritime Sicherheit“ und „AIS-Daten“ ausgetauscht. Auf den verschiedenen besuchten Veranstaltungen zu ebenjenen Aspekten wurden ferner zahlreiche Kontakte geknüpft.

II. <u>Vertiefte Darstellung</u>

1. Verwendung der Zuwendungen

Die Zuwendungen wurden entsprechend der im Projektantrag bezeichneten Zielsetzung verwendet.

Für die Arbeitspakete Nr. 3100 und 3200 entfiel ein Großteil der Arbeiten auf die gezielte Informationsrecherche, -beschaffung und -auswertung. Die gewonnenen Ergebnisse waren anschließend auf die konkreten Fragen des Forschungsvorhabens und hier insbesondere auf die im Vorfeld ermittelten Bedrohungsszenarien „Kriminelle Handlungen“, „Gefahrstoffe/Gefahrgüter“, Havarie/Großschadenslage“ und „Naturkatastrophen“ zu übertragen. Letztere mussten dabei vorab einer umfangreichen Bedrohungsanalyse zugeführt werden, welche die Beschreibung der jeweiligen Szenarien sowie der sich daraus ergebenden Bedrohungen für die zivile maritime Sicherheit zum Gegenstand hatte.

Bezüglich des Arbeitspaketes Nr. 3300 waren zunächst die relevanten datenschutzrechtlichen Fragestellungen herauszuarbeiten. Dies ging mit einer gezielten Darstellung des Datenkontakts der Projektpartner zueinander und der hieraus resultierenden rechtlichen Probleme einher. Auch dies erforderte eine intensive Literaturrecherche, -beschaffung, -auswertung und -anwendung, die schließlich in einem Einzeldokument über die Zulässigkeit der Erhebung von AIS-Daten zu Forschungszwecken und in einem ausführlichen Datenschutzkatalog mündete.

2. Resultate im Einzelnen - Arbeitspaket Nr. 3300

Im Arbeitspaket Nr. 3300 wurde sodann auf die datenschutzrechtlichen Fragestellungen und die Anfragen der Projektpartner eingegangen.

2.1. Datenkontakt der Projektpartner

Um zu ermitteln, welche Themenschwerpunkte insofern zu behandeln waren, musste zunächst der Datenkontakt der Projektpartner untereinander geklärt werden. Diese beabsichtigten, unter Nutzung multisensoraler Daten und deren interaktiver Auswertung ein gemeinsames Lagebild zu erproben, welches durch bedarfsgerechtes Einspeisen von aktuellen Informationen bspw. Standorte von Schiffen in nahe Echtzeit überträgt, um einerseits eine Früherkennung und Beurteilung komplexer Bedrohungs- oder Schadenslagen zu ermöglichen und andererseits die Reaktionszeit bis zum Erreichen der Rettungskräfte am Einsatzort auf ein Minimum zu reduzieren.

Im Hinblick auf die Gewinnung besagter Daten untersuchte der Projektpartner AIRBUS Defence & Space (ehem. CASSIDIAN GmbH) luftgestützte Sensorplattformen, welche - insbesondere durch den Einsatz von maritimen Radarsensoren - eine hochauflösende Seeverkehrserfassung innerhalb der AWZ ermöglichen sollen.

In enger Zusammenarbeit mit AIRBUS Defence &Space (ehem. CASSIDIAN GmbH) konstruierte das Institut für Raumfahrtsysteme des DLR im Rahmen seines Teilvorhabens „weiträumige luftgestützte AIS-Erfassung“ einen AIS-Demonstrator, zusammengesetzt aus einem Boden- und Flugsegment. Dabei sollte das vom Projektpartner AIRBUS Defence &Space (ehem. CASSIDIAN GmbH) entwickelte Flugsystem an die AIS-Sensorik des Instituts

für Raumfahrsysteme gekoppelt werden. Sodann war geplant, dass die „Diamond“ Bodenkontrollstation des Partners AIRBUS die Datenkommunikation übernimmt und die während des Fluges gewonnenen Datenprodukte an die Bodenkontrollstation des Instituts für Raumfahrtsysteme überträgt.

Letzteres erforschte darüber hinaus luftgestützte Verfahren zur zeitlichen und räumlichen Erfassung des Seeverkehrs durch die Verwendung von AIS-Daten, um die Bestimmung der Schiffspositionen und die Darstellung von bestehenden Verhaltensanomalien zu verbessern. Angestrebt war die Erfassung und endnutzergerechte Aufbereitung der Daten. Des Weiteren sollten AIS-Datenbanken, welche schiffsspezifische Informationen bereithalten, erstellt und ein Verfahren entwickelt werden, welches eine automatisierte Weitergabe der AIS-Daten an die Verbundpartner ermöglicht.

Überdies prüfte das DLR – konkret: das Institut für Methodik der Fernerkundung in Zusammenarbeit mit dem Deutschen Fernerkundungsdatenzentrum DFD - neuartige Methoden für großflächige Beobachtungen auf Basis von hochaufgelösten Satelliteninformationen. Diese sollten eine Detektion von Schiffen und Gefahrstoffen in einer bisher nicht erzielten Eindeutigkeit, Verfügbarkeit und Schnelligkeit erreichen. Die hierbei gewonnenen Produkte aus Satellitendaten sollten als weitere Grundlage für das Echtzeitlagebild dienen. Zur Ergänzung dieser Satellitendienste arbeitete das Institut für Flugführung des DLR an der Entwicklung neuartiger Flugführungskonzepte zur Einsatzplanung von sensortragenden Flugzeugen und Hubschraubern, um eine exakte Situationserfassung und deren Bewertung zu optimieren, wobei die Luftfahrzeuge über einen Datenlink mit einer Bodenkontrollstation verbunden und von dieser geführt werden sollte, sodass die Datenerfassung auch durch unbemannte Flugsteuerung erfolgen konnte.

Das Institut für Optische Sensorsysteme des DLR trug zur Projektumsetzung durch die Erprobung eines multispektralen Mehrkamerasystems bei, welches nach Fertigstellung an die Flugsysteme des Instituts für Flugführung montiert werden sollte. Der Projektpartner ging davon aus, dass die durch den Einsatz gewonnenen Datenprodukte die maximalen Anforderungen an Informationsgehalt und Lagegenauigkeit erfüllen und daher einen beträchtlichen Beitrag zur Erstellung eines Echtzeitlagebildes leisten können.

Im Zentrum der Arbeiten des Instituts für Kommunikation und Navigation stand die Entwicklung von Maßnahmen und Methoden zur nachhaltigen Unterbindung des illegalen Einsatzes von Störgeräten unterschiedlicher Art sowie der Entwurf von Algorithmen, um die Ortung und Identifikation solcher Signalquellen zu ermöglichen. Für diese Zwecke strebte das Institut den Aufbau einer störrobusten und flexiblen Multi-Antennen-GNSS-Empfängerplattform an. Die so empfangenen Signale sollten im Ergebnis in das Lagebild integriert werden.

Die Schnittstelle zwischen der Lagebilddarstellung und den luftgestützten sowie satellitengestützen Sensordiensten wurde von AIRBUS Defence & Space (eh. ASTRIUM GmbH) durch die Entwicklung eines Realtime Maritime Situation Awarness System (RMSAS) bereitgestellt. Das System gestattet eine intelligente Steuerung der Kontroll- und Datenflüsse und soll die Endanwender dergestalt bei der Generierung von Nutzersichten

situationsgerecht, optimal und in nahe Echtzeit unterstützen. Die Koordination der Flugplattformen und der Entgegennahme sowie Weiterleitung der erfassten Daten an das RMSAS übernahm das Institut für Flugführung.

Zur Realisierung der Nutzerintegration und -sicht untersuchte die ATLAS Elektronik GmbH ein intelligentes Mensch-Maschine-System (MMS), welches die optimale Nutzung von Echtzeitsystemen ermöglichen soll, indem es insbesondere Radar- und Satellitendaten, aber auch Schiffs- und Steuerdaten anhand eines digitalen Situationsbildes darstellt.

Als Endnutzer dieses Echtzeitdienstes befasste sich das THW schließlich mit der Evaluation von bemannten und unbemannten Technologien zur Erfassung von räumlich und zeitlich hochaufgelösten Situationsbildern, um die daraus gewonnenen Daten im Schadensfall für eine effektive und effiziente Einsatzkoordinierung nutzen und auswerten zu können.

Die Verwendung solch umfassender Echtzeitsysteme und die Speicherung der erhobenen Informationen mussten jedoch insbesondere in datenrechtlicher Hinsicht abgesichert sein. Zur rechtlichen Überprüfung, ob eine Zusammenführung der Daten zu einem Echtzeitlagebild mit den gesetzlichen Bestimmungen im Einklang steht, bedurfte es zunächst der Darstellung der relevanten Gesetze und der damit an die Projektpartner gestellten Vorgaben im Hinblick auf die Erhebung und Verwendung der Daten.

Im Rahmen der Datenverwendung war insbesondere danach zu fragen, ob der Erhebung bzw. Nutzung der Daten zu Forschungszwecken rechtliche Vorgaben entgegenstehen.

Aus der Bearbeitung dieser Fragestellungen ergab sich der nachfolgende Datenschutzkatalog. Ein eigenständiges Dokument hinsichtlich der rechtlichen Zulässigkeit der Erhebung von AIS-Daten zu Forschungszwecken durch das DLR-RY konnte insofern in die Ausarbeitung integriert werden.

2.2. Datenrechtliche Vorgaben

Für die Frage der anwendbaren Vorschriften kam es entscheidend auf die Art der gewonnenen Informationen an, da an die Erhebung und Verarbeitung einiger Daten besondere Anforderungen zu stellen sind. Dies gilt insbesondere für Geodaten, für die unter weiteren Voraussetzungen das Satellitendatensicherheitsgesetz[6] (SatDSiG) gilt, und solche, die personenbezogen oder zumindest – beziehbar sind. Letztere unterliegen dem Schutzbereich des Bundesdatenschutzgesetzes[7] (BDSG).[8]

[6] Satellitendatensicherheitsgesetz vom 23. November 2007 (BGBl. I S. 2590), zuletzt geändert durch Art. 4 Abs. 59 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154).

[7] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814).

[8] Vgl. § 1 Abs. 1 BDSG. Zum Begriff des Personenbezugs vgl. § 3 Abs. 1 BDSG.

Unter dem Begriff „Geodaten“ versteht man Informationen, mittels derer eine bestimmte räumliche Lage auf der Erdoberfläche lokalisiert werden kann. Die Ortung erfolgt bspw. über Ablesungen der Breiten- und Längenkreise.[9]

Die von den Projektpartnern zur Echtzeitortung von Schiffen bzw. Gefahrgütern und für die Einspeisung geographischer Gegebenheiten in das Echtzeitlagebild benötigten Daten lassen sich stets einem konkreten Raum auf der Erdoberfläche zuordnen, sodass es sich hierbei um Geodaten im vorgenannten Sinne handelt und daher grds. die Möglichkeit bestünde, dass das SatDSiG zur Anwendung gelangt.

Vor dem Hintergrund, dass auch Geodaten einen Personenbezug aufweisen können, war darüber hinaus an eine parallele Anwendbarkeit des BDSG zu denken. Aufgrund des Umstandes, dass sich das SatDSiG insofern als spezieller erweist, wurde jedoch zunächst untersucht, ob dessen weitere Voraussetzungen und ggf. diejenigen anderer Spezialgesetze im Hinblick auf die im Rahmen des Projekts genutzten Daten vorlagen. Im Anschluss daran wurde auf die allgemeinen Vorgaben des BDSG eingegangen.

2.2.1 Satellitendatensicherheitsgesetz (SatDSiG)

Ausweislich des allgemeinen Teils der Begründung zum Gesetzesentwurf (BT Drs. 16/4763) wurde das SatDSiG vom 23.11.2007 mit der Zielrichtung erlassen, die sicherheits- und außenpolitischen Interessen der Bundesrepublik Deutschland beim Umgang mit Erdfernerkundungsdaten zu bewahren; es bezieht sich dementsprechend auf die Erhebung und Verbreitung von Satellitengeodaten. Grund des Erlasses war die Errichtung außergewöhnlich leistungsfähiger Erdbeobachtungssatelliten („TerraSAR-X“ und „RapidEye“ - beide Start 2007, „TanDEM-X“ – Start 2009, „EnMap“ - Start 2011) mit der Absicht, die Daten weltweit zu vermarkten.[10]

2.2.1.1 Anwendungsbereich

Fraglich war, ob das SatDSiG im vorliegenden Fall in persönlicher, räumlicher und sachlicher Hinsicht zur Anwendung gelangen konnte.

Persönlicher Anwendungsbereich

In den persönlichen Anwendungsbereich des SatDSiG fallen natürliche Personen deutscher Staatsangehörigkeit bzw. juristische Personen oder Personenvereinigungen mit deutscher Staatszugehörigkeit, vgl. § 1 Abs. 1 Nr. 1a) SatDSiG. Letztere lässt sich durch die

[9] *Weichert*, Der Personenbezug von Geodaten, DuD 2007 Heft 31, 1.

[10] Vgl. BT Drs. 16/4763, S. 15.

Gesellschaftserrichtung nach deutschem Recht begründen, kann aber auch an den Sitz der juristischen Person im Bundesgebiet anknüpfen, vgl. § 1 Abs. 1 Nr. 1b) SatDSiG.

Als eingetragener Verein iSd §§ 21 ff. BGB ist das DLR eine juristische Person des Privatrechts.[11] Der persönliche Anwendungsbereich ist daher eröffnet.

Auch bei den Projektpartnern ATLAS GmbH und AIRBUS Defence & Space, bestehend aus der ASTRIUM GmbH und CASSIDIAN GmbH, handelt es sich gem. § 13 Abs. 1, 3 GmbHG i. V. m. § 6 Abs. 1 HGB um juristische Personen des Privatrechts. Soweit sie die erhobenen Satellitendaten zur Erstellung des Lagebildes nutzen wollen, ist auch diesbezüglich der persönliche Anwendungsbereich des SatDSiG eröffnet.

Im Hinblick auf eine spätere Verwendung der Daten durch die Bundespolizei See und das THW findet das SatDSiG indes keine Anwendung, da sie weder juristische Personen des Privatrechts noch des öffentlichen Rechts sind.

Die Bundespolizei wird gem. § 1 Abs. 1 S. 1 BPolG in bundeseigener Verwaltung geführt, welche dadurch gekennzeichnet ist, dass sich der Bund eigener nicht rechtsfähiger Behörden zur Aufgabenwahrnehmung bedient, also solcher Stellen, die selbst nicht Verwaltungsträger sind, aber einem solchen Organ zugeordnet werden.[12] Da § 1 Abs. 1 S. 2 BPolG die Bundespolizei dem Geschäftsbereich des Bundesministeriums des Innern (BMI) zuweist, ist sie mangels Rechtsfähigkeit keine juristische Person des öffentlichen Rechts.[13]

Beim THW handelt es sich um eine Anstalt des Bundes, die zwar grds. juristische Personen des öffentlichen Rechts sein kann,[14] jedoch ebenfalls nur, sofern sie Träger von Rechten und Pflichten ist.[15] Dies trifft auf das THW als Organ der bundeseigenen Verwaltung allerdings gerade nicht zu, vgl. § 1 Abs. 1 THW-Gesetz[16].[17]

Räumlicher Anwendungsbereich

Untersuchungsbedürftig war ferner, ob der Anwendungsbereich des SatDSiG auch in räumlicher Hinsicht eröffnet ist. Mit Blick auf den Betrieb eines hochwertigen

[11] Daran ändert sich auch dann nichts, wenn dem DLR als sog. Beliehener durch das Raumfahrtaufgabenübertragungsgesetz (BGBl. 1998 I S. 2510) hoheitliche Aufgaben zur Wahrnehmung im eigenen Namen übertragen worden sind.

[12] Vgl. *Erbguth*, Wilfried, Allgemeines Verwaltungsrecht, 7. Aufl., S. 79.

[13] Vgl. zum Erfordernis der Rechtsfähigkeit *Detterbeck*, Steffen, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 11. Aufl., Rn. 180 f.

[14] Vgl. *Peine*, Allgemeines Verwaltungsrecht, 8. Auflage, S. 18, Rn. 80.

[15] Vgl. *Berg*, Die öffentlich-rechtliche Anstalt, NJW 1985, 2294 (2296).

[16] THW-Gesetz vom 22. Januar 1990 (BGBl. I S. 118)

[17] Das THW ist daher keine juristische Person des öffentlichen Rechts, vgl. *Tholen*, Technisches Hilfswerk, FHArbSozR 3 Nr. 5811.

Satellitensystems ergibt sich dieser aus § 1 Abs. 1 Nr. 1c) SatDSiG. Da sich das Erdfernerkundungssystem im internationalen Weltraum befindet, der wegen Art. II des Weltraumvertrages[18] keinerlei staatlicher Hoheitsmacht unterliegt, knüpft die Vorschrift an den Ort des unveränderbaren Absetzens der Befehlsfolgen zur Kommandierung des Orbitalsystems vom Bundesgebiet an.

Hinsichtlich des Verbreitens der Daten ist das SatDSiG darüber hinaus anwendbar, soweit dies „vom Bundesgebiet aus erfolgt". Das ist bereits dann der Fall, wenn wesentliche Betriebsteile – etwa ein Datenarchiv oder eine Datenverarbeitungsanlage – in der Bundesrepublik gelegen sind.[19]

Da die Standorte der Projektpartner auf deutschem Hoheitsgebiet liegen, gelang das SatDSiG folglich auch insofern zur Anwendung.

Sachlicher Anwendungsbereich

In den sachlichen Anwendungsbereich fallen gem. § 1 Abs. 1 Nr. 1 und 2 SatDSiG der „Betrieb von hochwertigen Erdfernerkundungssystemen" (Nr. 1) sowie der „Umgang mit den Daten" (Nr. 2) desselben.

Um festzustellen, ob das SatDSiG auch diesbezüglich einschlägig ist, bedurfte es der weiteren Untersuchung, was unter den Begriffen „Daten" und „hochwertiges Erdfernerkundungssystem" zu verstehen ist

Datenbegriff nach dem SatDSiG

„Daten" sind ausweislich der Legaldefinition des § 2 Abs. 1 Nr. 2 SatDSiG „Signale eines Sensors oder mehrerer Sensoren eines Orbital- oder Transportsystems und alle daraus abgeleiteten Produkte, unabhängig vom Grad ihrer Verarbeitung und der Art ihrer Speicherung oder Darstellung".

Die Definition betrifft lediglich einen begrenzten Ausschnitt des sonst weit gefassten Datenbegriffs, da ausschließlich solche Informationen erfasst werden, die durch einen Satellitensensor erzeugt wurden. Auf die Art der Speicherung oder Darstellung kommt es indes nicht an, sodass sowohl analoge als auch digitale Datenprodukte und Rohdaten darunter zu subsumieren sind.[20]

[18] Vertrag über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraumes einschließlich des Mondes und anderer Himmelskörper vom 27.01.1967, BGBl. 1969 II S. 1967ff.

[19] Vgl. BT Drs. 16/4763, S. 18.

[20] Vgl. BT Drs. 16/4763, S. 19.

Begriff des hochwertigen Erdfernerkundungssystems

Daneben müssen die Daten über ein „hochwertiges Erdfernerkundungssystem“ gewonnen werden. Hierunter ist ein „raumgestütztes Erdfernerkundungssystem“, also ein „Orbital- oder Transportsystem einschließlich des Bodensegments, mit dem Daten über die Erde erzeugt werden“, zu verstehen.[21] Bei Orbitalsystemen handelt es sich um Vorrichtungen, die sich auf einer Umlaufbahn befinden; Transportsysteme hingegen sind solche, die im Grundsatz allein der Überführung von Orbitalsystemen in die Umlaufbahn dienen. Ausnahmsweise werden sie auch zur Erdfernerkundung eingesetzt wie bspw. durch Space-Shuttle oder Raumfähren.[22]

Kann danach die Eigenschaft als Erdfernerkundungsanlage bejaht werden, muss diese ferner „hochwertig“ iSd Gesetzes sein. Für die Bestimmung der Hochwertigkeit legt § 2 Abs. 2 S. 2 SatDSiG Kriterien fest, welche aufgrund von § 2 Abs. 2 S. 1 SatDSiG[23] durch § 1 SatDSiV[24] konkretisiert werden. Anknüpfungspunkt hierbei ist der Informationsgehalt der erzeugten Daten.

Nach § 1 Abs. 1 SatDSiV ist „ein Sensor eines Erdfernerkundungssystems alleine oder in Kombination mit einem oder mehreren Sensoren technisch in der Lage, Daten mit besonders hohem Informationsgehalt zu erzeugen, wenn in mindestens einer Raumrichtung eine geometrische Auflösung von 2,5 Metern oder weniger erzeugt werden kann“. Der Begriff der „geometrischen Auflösung“ beschreibt die kleinste trennbare geometrische Einheit auf allen drei Achsen im Raum.

Darüber hinaus wird nach § 1 Abs. 2 SatDSiV ein besonders hoher Informationsgehalt auch dann angenommen, wenn „im Spektralbereich von 8 bis 12 Mikrometern (thermisches Infrarot) in mindestens einer Raumrichtung eine geometrische Auflösung von 5 Metern oder weniger erzeugt werden kann“ (Nr. 1), „im Spektralbereich zwischen 1 Millimeter und 1 Meter (Mikrowellen) in mindestens einer Raumrichtung eine geometrische Auflösung von 3 Metern oder weniger erzeugt werden kann“ (Nr. 2) oder „die Zahl der Spektralkanäle 49 übersteigt (super- und hyperspektrale Sensoren) und in mindestens einer Raumrichtung eine geometrische Auflösung von 10 Metern oder weniger erzeugt werden kann“ (Nr. 3).

Wie einleitend beschrieben, basierten die Untersuchungen des Instituts für Methodik der Fernerkundung des DLR auf hochaufgelösten Satelliteninformationen.[25] Zur Akquirierung der benötigten Daten dienten in erster Linie die Satellitensysteme „TerraSAR-X“ und „TanDEM-

[21] Vgl. BT Drs. 16/4763, S. 19

[22] Vgl. BT Drs. 16/4763, S. 19.

[23] das BMWi hat durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zu erlassen, unter welchen Voraussetzungen Daten einen besonders hohen Informationsgehalt haben. Dieser Verpflichtung ist es mit dem Erlass der Satellitendatensicherheitsverordnung (SatDSiV) vom 26. März 2008 (BGBl. I S. 508) nachgekommen.

[24] Vgl. Fn. 23.

[25] S. o.

X“. Vor dem Hintergrund, dass das SatDSiG eigens aufgrund der vorgenannten Satellitenanlagen erlassen wurde, sind diese ohne weiteres als „hochwertige Erdfernerkundungssysteme“ zu qualifizieren, sodass sowohl deren Betrieb als auch die weitere Datenverwendung den Vorgaben des SatDSiG unterliegen.

Zwischenergebnis

Innerhalb der Teilvorhaben, die eine Verbreitung der fraglichen Satelliteninformationen zum Gegenstand hatten, waren die Maßgaben des SatDSiG folglich zu beachten.

2.2.1.2 Vorgaben des SatDSiG

Das SatDSiG knüpft an den Betrieb eines Erdfernerkundungssystems sowie an die Übermittlung der gewonnenen Satellitendaten strenge Voraussetzungen.

Inbetriebnahme eines Erdfernerkundungssystems

Der Betrieb eines hochwertigen Erdfernerkundungssystems bedarf zunächst einer Genehmigung, vgl. § 3 Abs. 1 SatDSiG, die im Falle des Vorliegens der formellen und materiellen Voraussetzungen zu erteilen ist, vgl. § 4 Abs. 1 SatDSiG.

Formelle Genehmigungsvoraussetzungen

Die formellen Genehmigungsvoraussetzungen lassen sich dabei in „Zuständigkeit“, „Verfahren“ und „Form“ unterteilen.

Soweit nicht anders bestimmt, ist gemäß § 24 Abs. 1 SatDSiG grundsätzlich das Bundesamt für Wirtschaft und Ausfuhrkontrolle die im vorliegenden Kontext zuständige Behörde. Ausnahmsweise ergibt sich eine abweichende Zuständigkeit des Bundesministeriums für Wirtschaft und Technologie, namentlich für die Durchführung der Sicherheitsüberprüfung nach §§ 4 Abs. 2, 12 Abs. 2 oder die Meldung iSv § 10 Abs. 1 S. 1, vgl. § 24 Abs. 2, 3 S. 1 SatDSiG.[26]

Die Genehmigung stellt eine hoheitliche Maßnahme einer Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts dar, die auf unmittelbare Rechtwirkung nach außen gerichtet ist. Es handelt sich folglich um einen Verwaltungsakt (VA) iSd § 35 S. 1 Verwaltungsverfahrensgesetz (VwVfG). Für das Genehmigungsverfahren könnten daher die

[26] Das Bundesministerium für Wirtschaft und Technologie ist darüber hinaus im Einvernehmen mit dem Auswärtigen Amt und dem Bundesministerium für Verteidigung zuständig für eine Untersagung des Erwerbs von Unternehmen oder Unternehmensbeteiligungen nach § 10 Abs. 1 S. 4 SatDSiG, vgl. § 24 Abs. 3 S. 2 SatDSiG.

allgemeinen Vorgaben des VwVfG zu berücksichtigen sein. Soweit das SatDSiG indes seinerseits Verfahrens-Bestimmungen enthält, sind diese als leges speciales vorrangig heranzuziehen.

So sieht § 25 Abs. 1 SatDSiG für die Erteilung der Genehmigung einen vorherigen schriftlich gestellten Antrag des potentiellen Betreibers eines Erdfernerkundungssystems vor. Gem. § 25 Abs. 1 S. 3 SatDSiG sind dem Antrag „die zur Prüfung der Erteilungsvoraussetzungen notwendigen Unterlagen beizufügen". Regelungen zum Umgang mit elektronischen Dokumenten hält das SatDSiG allerdings nicht bereit, sodass es für den Fall der elektronischen Übermittlung eines Rückgriffs auf § 3a VwVfG bedarf,[27] wonach das Schriftform entsprechend ersetzt werden kann.

Nach § 25 Abs. 3 SatDSiG ist die Genehmigung schriftlich oder elektronisch zu erteilen. Aus Gründen der Rechtssicherheit ist dabei das Begründungserfordernis des § 39 VwVfG zu beachten, wobei sich die Geheimhaltungsbedürftigkeit bestimmter Tatsachen als für den Begründungsumfang einschränkend auswirken kann.[28]

Materielle Genehmigungsvoraussetzungen

In materieller Hinsicht galt es insbesondere § 4 Abs. 1 SatDSiG zu beachten. Danach ist dem Betreiber des hochwertigen Erdfernerkundungssystems die Genehmigung zu erteilen, wenn die in den Nr. 1-4 genannten Voraussetzungen kumulativ vorliegen.[29] Betreiber in diesem Sinne ist derjenige, der das Erdfernerkundungssystem in eigener Verantwortung steuert, vgl. § 2 Abs. 1 Nr. 1 SatDSiG. Verantwortlich für den Betrieb des TerraSAR-X Satelliten ist das Deutsche Raumfahrt-Kontrollzentrum des DLR in Oberpfaffenhofen.[30]

Der Betreiber müsste gem. § 4 Abs. 1 Nr. 1 SatDSiG zunächst die „erforderliche Zuverlässigkeit" besitzen. Ob dies der Fall ist, ergibt sich aus einer Prognoseeinschätzung bzgl. der dauerhaften und ordnungsgemäßen Erfüllung seiner (künftigen) gesetzlichen Pflichten.[31]

Zweifel an der ordnungsgemäßen Pflichterfüllung bestehen nach dem Willen des Gesetzgebers etwa dann, wenn der Antragsteller in der Vergangenheit bereits gegen Vorschriften des SatDSiG bzw. sachnaher anderer Gesetze (zB die §§ 80 bis 109k StGB) verstoßen hat oder entsprechende Hinweise darauf bestehen.[32] Bei der Beurteilung der

[27] Vgl. dazu BT Drs. 16/4763, S. 29.

[28] Die Begründung muss jedoch mit Blick auf Art. 19 Abs. 4 GG so überzeugend sein, dass sie im Falle einer gerichtlichen Überprüfung noch als triftig anzuerkennen ist. Ein Hinweis auf die Geheimhaltungspflicht und deren Notwendigkeit wird allerdings als ausreichend erachtet, vgl. zu alledem BT Drs. 16/4763, S. 29f.

[29] Das Erfordernis des „kumulativen Vorliegens" der Voraussetzungen ergibt sich aus dem Wortlaut der Norm („und").

[30] Der Betrieb des Radarinstruments obliegt dem Institut für Hochfrequenztechnik und Radarsysteme des DLR in Oberpfaffenhofen, vgl. DLR, TerraSAR-X: Das deutsche Radarauge im All, S. 39f.

[31] Vgl. BT Drs. 16/4763, S. 22.

[32] Vgl. BT Drs. 16/4763, S. 22

Zuverlässigkeit sind daneben Zuwiderhandlungen gegen allgemeine Gesetze zu berücksichtigen, die Rückschlüsse auf das berufliche Verhalten des Betreibers zulassen (zB Steuervergehen).[33] Handelt es sich um eine juristische Person, so bezieht sich die Prognoseentscheidung auf die hinter ihr stehenden natürlichen Personen.[34]

Besitzt der Betreiber die erforderliche Zuverlässigkeit, muss nach § 4 Abs. 1 Nr. 2 SatDSiG weiterhin sichergestellt sein, dass „die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems“ (lit.a), „Steuerung des Sensors oder der Sensoren“ (lit.b), „Steuerung der Übermittlung der Daten durch das Obital-oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person“ (lit.c) „und [zur] „Steuerung des Verbreitens der Daten unmittelbar durch das Orbital- oder Transportsystem“ (lit.d) „im Bundesgebiet hergestellt und durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen Veränderung durch Dritte geschützt werden“.

Dadurch soll die aktive Kontrolle über das Orbitalsystem und deren Ausübung vom Bundesgebiet aus gewährleistet und der jederzeitige Zugriff auf denjenigen ermöglicht werden, der über die Kommandierungsbefugnis bzgl. aller sicherheitsrelevanten Teile des Orbitalsystems innerhalb eines Erdfernerkundungssystems verfügt.[35]

Die „Kommandierung“ erstreckt sich dabei sowohl auf Satelliten-Untersysteme als auch auf die Bahnvermessung und das Kommandosystem, wobei ausschließlich letzteres der Betriebsüberwachung unterfällt, weil der Betriebsablauf nur hierdurch dergestalt beeinflusst werden kann, dass eine Sicherheitsgefährdung möglich erscheint.[36]

§ 4 Abs. 1 Nr. 2 SatDSiG fordert darüber hinaus, dass die Befehlsfolgen durch entsprechende Verfahren vor Veränderungen durch Dritte geschützt werden. Insofern war die technische Richtlinie des BSI zu beachten, in der geeignete Schutzprofile festgelegt sind.[37]

Gem. § 4 Abs. 1 Nr. 3 SatDSiG ist ferner sicherzustellen, dass „die Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person, die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Betreibers und die Übermittlung der Daten vom Betreiber an eine nach § 11 zugelassene Person durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte

[33] Vgl. BT Drs. 16/4763, S. 22. Darüber hinaus werden abträgliche Angaben in der Sicherheitserklärung nach § 13 Abs. 1 Nr. 13-17 Sicherheitsüberprüfungsgesetz (SÜG) in die Prognoseentscheidung mit eingestellt.

[34] Vgl. BT Drs. 16/4763, S. 22.

[35] Vgl. BT Drs. 16/4763, S. 22.

[36] Vgl. BT Drs. 16/4763, S. 22f.

[37] BSI TR-03140 Conformity assessment according to the satellite data security act (TR-SatDSiG); vgl. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03140/index_htm.html;jsessionid=71FE51704CDF708E288F872995473B28.2_cid286 [Stand: 31.03.2014]; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03140/TR03140.pdf?__blob=publicationFile [Stand: 31.03.2014].

Kenntnisnahme geschützt sind“. Die Vorschrift dient dem umfassenden Schutz derjenigen Datenbestände, die sich nach wie vor beim Betreiber befinden und noch nicht an den Datenanbieter übermittelt und verbreitet wurden.[38]

Zudem hat der Betreiber gem. § 4 Abs. 1 Nr. 4 SatDSiG erforderliche Maßnahmen zum Schutz seiner Betriebsräume sowie den dazugehörenden Anlagen vor unberechtigtem Zutritt und Zugang zu ergreifen. Während „Zutritt“ die körperliche Anwesenheit von Personen in gewissen Betriebsräumen meint, ist unter „Zugang“ neben der Einräumung von Nutzungsbefugnissen insbesondere das elektronische Eindringen in die Systeme (sog. „Hacken“) zu verstehen.[39] Das SatDSiG enthält keine Vorgaben, welche Maßnahmen konkret zu ergreifen sind, sodass dem Betreiber die Ausgestaltung seiner Schutzvorkehrungen grds. freisteht. Dabei ist freilich das gesetzlich verankerte Ziel, den Zutritt und Zugang Unbefugter zu verhindern, stets im Blick zu halten.

Erfüllt der Betreiber die vorstehenden Anforderungen, ist die Genehmigung zu erteilen. Die zuständige Behörde ist mithin in ihrer Entscheidung gebunden, sodass kein Raum für etwaige Ermessenserwägungen besteht.

Pflichten des Betreibers

Neben dem Genehmigungserfordernis treffen den Betreiber für die Zeit des Betriebes die in den §§ 5–8 SatDSiG aufgelisteten Pflichten.

Dokumentationspflicht

Aus § 5 SatDSiG ergibt sich eine Dokumentations- und Aufbewahrungspflicht. Sie dient der Überprüfung bestehender Sicherheitsmaßnahmen sowie der Ermittlung von Verstößen.[40] Nach § 5 Abs. 1 SatDSiG ist der Betreiber eines hochwertigen Erdfernerkundungssystems dazu verpflichtet, „die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems“ (Nr. 1), „die Befehlsfolgen zur Steuerung des Sensors oder der Sensoren“ (Nr. 2), „Angaben zu Verschlüsselungsverfahren, verwendeten Schlüsseln und Schlüsselmanagement“ (Nr. 3) sowie „den Zeitpunkt und den Weg der Befehlsfolgen“ (Nr. 4) zu protokollieren. Die Aufzeichnungen sind gem. § 5 Abs. 2 SatDSiG „mindestens fünf Jahre nach Ausführung der jeweiligen Befehlsfolge aufzubewahren und zur Einsichtnahme durch die zuständige Behörde bereitzuhalten“.

---

[38] Vgl. BT Drs. 16/4763, S. 23. Die Begriffe des „Übermittelns“ und „Verbreitens“ sind nicht gleichzusetzen. Das „Verbreiten“ ist das „Inverkehrbringen oder Zugänglichmachen der Daten für Dritte“, vgl. § 2 Abs. 1 Nr. 6 SatDSiG, während das „Übermitteln“ jede Art der Übertragung oder Weitergabe umfasst und mithin als Oberbegriff zu verstehen ist, vgl. BT Drs. 16/4763, S. 23.

[39] Vgl. BT Drs. 16/4763, S. 23.

[40] Vgl. BT Drs. 16/4763, S. 23.

Anzeigepflicht

Soweit sich maßgebliche Umstände ändern, besteht für den Betreiber überdies eine Anzeigepflicht ggü. der zuständigen Behörde.

Nach § 6 Abs. 1 Nr. 1 SatDSiG zählen hierzu zunächst Änderungen von Tatsachen, die der Betreiber „zur Eintragung in das Handels- oder Vereinsregister anzumelden hat".

Die Vorschrift wahrt die Sicherheitsinteressen der Bundesrepublik Deutschland, da sich bspw. ein Geschäftsführerwechsel unmittelbar auf die Beurteilung der „Zuverlässigkeit" nach § 4 SatDSiG auswirkt, sofern die über den neuen Geschäftsführer zu treffende Prognoseentscheidung negativ ausfallen sollte.[41]

Darüber hinaus sind auch „tatsächliche Anhaltspunkte dafür, dass ein Dritter die Befehlsfolgen zur Kommandierung […] oder Steuerung […] absetzt oder abzusetzen versucht" anzuzeigen, vgl. § 6 Abs. 1 Nr. 2 SatDSiG. Damit wird dem Gefährdungsrisiko durch die aktive Kontrolle über das Erdfernerkundungssystem Rechnung getragen.[42]

§ 6 Abs. 1 Nr. 3 SatDSiG erfasst daneben solche Änderungen, die Maßnahmen der betrieblichen Organisation iSd § 4 Abs. 1 Nr. 4 SatDSiG betreffen.

Gem. § 6 Abs. 2 SatDSiG ist der Betreiber schließlich verpflichtet, der zuständigen Behörde mitzuteilen, an welche nach § 11 zugelassenen Personen er Daten übermittelt.

Die Anzeige hat in jedem Fall unverzüglich zu erfolgen, wobei der Gesetzgeber offengelassen hat, was im Einzelnen darunter zu verstehen ist. In Betracht kommt daher ein Rückgriff auf die Legaldefinition des § 121 Abs. 1 BGB, wonach „unverzüglich" „ohne schuldhaftes Zögern" bedeutet. Der aus § 6 Abs. 1 SatDSiG folgende Begriff der „Unverzüglichkeit" müsste folglich an ein Verschulden[43] des Verantwortlichen anknüpfen. Dass dies der Fall ist, zeigt der Blick auf § 28 Abs. 2 Nr. 1 SatDSiG, wonach vorsätzliche[44] und mithin schuldhafte Verstöße gegen § 6 Abs. 1 SatDSiG als Ordnungswidrigkeit geahndet werden. Insofern erscheint es gerechtfertigt, die Legaldefinition des § 121 Abs. 1 BGB zur Begriffsbestimmung heranzuziehen,[45] sodass die Anzeige im Ergebnis ohne schuldhaftes Zögern vorgenommen werden muss.

---

[41] Vgl. BT Drs. 16/4763, S. 24.

[42] Vgl. BT Drs. 16/4763, S. 24.

[43] Unter schuldhaftem Handeln sind Vorsatz und Fahrlässigkeit zu verstehen, vgl. § 276 Abs. 1 S. 1 BGB.

[44] Vgl. BT Drs. 16/4763, S. 30.

[45] Anderes gilt jedoch, sofern eine Verwaltungsvorschrift die Unverzüglichkeit des Handelns eines Verwaltungsorganes fordert. In einem solchen Fall wird eine Begriffsübernahme regelmäßig nicht dem Gesetzeszweck entsprechen, da es hierbei darauf ankommt, ob die Verzögerung sachlich gerechtfertigt war und nicht darauf, ob sie schuldhaft herbeigeführt wurde; vgl. hierzu *Pieroth*/*Schlink*/*Kniesel*, Polizei- und Ordnungsrecht, 7. Auflage, S. 314, Rn. 8.

Auskunftspflicht

Der Betreiber des Erdfernerkundungssystems ist weiterhin verpflichtet, der zuständigen Behörde auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen, wenn es zur Überwachung der Einhaltung des SatDSiG oder der dazu erlassenen Rechtsverordnungen erforderlich ist, vgl. § 7 Abs. 1 SatDSiG. Es bedarf keines bestimmten Verdachts eines Verstoßes gegen das SatDSiG, die Behörde darf vielmehr auch von einem konkreten Anlass losgelöst Auskünfte verlangen, soweit sich diese auf den Nachweis der Einhaltung des Gesetzes beschränken; eine darüberhinausgehende Auskunft kann durch den Betreiber verweigert werden.[46] Gleiches gilt für Fragen, deren Beantwortung den Auskunftspflichtigen oder einer der in § 383 Abs. 1 Nr. 1 bis 3 ZPO[47] bezeichneten Personen der Gefahr einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem OWiG[48] aussetzen würde, vgl. § 7 Abs. 2 SatDSiG.

Duldungspflicht

Um eine wirksame Kontrolle zu ermöglichen, treten neben die „aktiven" Pflichten des Betreibers, Betretens- und Prüfungsrechte der Behörde, vgl. § 8 S. 1 SatDSiG. Die entsprechend beauftragten Behördenmitarbeiter sind danach „befugt, zu den üblichen Betriebs- und Geschäftszeiten die Betriebs- und Geschäftsräume […] zu betreten und die zur Erfüllung ihrer Aufgaben erforderlichen Prüfungen vorzunehmen […]". Durch den Verweis auf die Abgabenordnung in § 8 S. 2 SatDSiG wird den Behördenmitarbeitern ferner die Einsicht in gespeicherte Daten und Datenverarbeitungssysteme ermöglicht, vgl. §§ 200, 147 Abs. 6 AO.

Meldepflicht bei Betriebsübernahme

In § 10 SatDSiG finden sich weiterhin Regelungen zur Betriebsübernahme. Soweit der – wenn auch nur anteilige – Erwerb eines solchen Unternehmens durch ausländische Staatsangehörige, juristische Personen oder Personenvereinigungen ausländischen Rechts bzw. juristische Personen oder Personenvereinigungen, an denen ausländische Staatsangehörige, juristische Personen oder Personenvereinigungen ausländischen Rechts mindestens 25 % der Stimmrechte halten, geplant oder erfolgt ist, muss die zuständige Behörde unverzüglich informiert werden. Dadurch soll in erster Linie sichergestellt werden, dass die Kontrolle über das betreffende Erdfernerkundungssystem im Einflussbereich des

[46] Vgl. BT Drs. 16/4763, S. 24.

[47] Zivilprozessordnung.

[48] Gesetz über Ordnungswidrigkeiten.

SatDSiG verbleibt, da anderenfalls die erhobenen Daten ohne vorherige Prüfung gem. § 11 ff. SatDSiG verbreitet werden könnten.[49]

Vorrangige Bedienungspflicht von Aufträgen der Bundesrepublik Deutschland

Das SatDSiG beschreibt in den §§ 22 iVm. § 21 ferner Anwendungsbereiche, in denen der Betreiber verpflichtet ist, Aufträge zur Erzeugung von Daten für die Bundesrepublik Deutschland zeitlich vorrangig, d. h. zum Auftragszeitpunkt vor jeder anderen Anfrage,[50] zu behandeln. Beschränkt durch den Gesetzeszweck, vor Gefährdungen durch die Nutzung von Erdfernerkundungssystemen zu schützen, ist es der Bundesrepublik Deutschland danach ausschließlich in Fällen des Bündnisses,[51] der Verteidigung (Art. 115a GG), des inneren Notstandes (Art. 91 GG), des Spannungsfalles (Art. 80a GG) oder sofern im Ausland eingesetzte militärische bzw. zivile Kräfte gefährdet sind, gestattet, eine vorgezogene Bedienung zu verlangen, § 21 Nr. 1-5 SatDSiG.[52]

Gem. 23 Abs. 1 SatDSiG ist der Datenanbieter oder der Betreiber allerdings berechtigt, für die vorrangige Behandlung eine dem durchschnittlichen Marktpreis entsprechende Vergütung zu verlangen. Bemessungsgrundlage sind dabei die üblichen Entgeltforderungen der Datenanbieter/Betreiber und Preise, die andere Marktteilnehmer für entsprechende Dienste fordern würden.[53]

Folgen einer Pflichtverletzung

Im Falle einer Pflichtverletzung[54] ist die zuständige Behörde zur Ergreifung der erforderlichen Maßnahmen berechtigt, § 9 Abs. 1 SatDSiG. Insbesondere darf sie gem. § 9 Abs. 2 SatDSiG „vorübergehend die Übermittlung von Daten […] untersagen“ (Nr. 1) oder die vollständige bzw. teilweise Übertragung des Betriebes auf einen „geeigneten Sonderbeauftragten“

[49] Vgl. BT Drs. 16/4763, S. 25.

[50] Vgl. § 21 Abs. 1 SatDSiG.

[51] Vgl. Art. 5 des Nordatlantikvertrages vom 04.04.1949 (BGB. 1955 II S. 289).

[52] Vgl. BT Drs. 16/4763, S. 29.

[53] Vgl. BT Drs. 16/4763, S. 29.

[54] Aufgrund seiner systematischen Stellung ist davon auszugehen, dass sich § 9 SatDSiG v.a. auf die in den §§ 5-8 SatDSiG verankerten Pflichten bezieht. Da jedoch keine ausdrückliche Bezugnahme darauf erfolgt, können auch weitere – an den Betrieb eines Erdfernerkundungssystems anknüpfende – Pflichten darunterfallen. Die Gesetzesstruktur lässt indes vermuten, dass eine Verletzung der Pflichten aus dem – am Ende des Abschnitts stehenden - § 10 SatDSiG keine Maßnahmen nach § 9 SatDSiG auslöst. So stellt bspw. der dem § 9 SatDSiG weitgehend entsprechende § 16 SatDSiG den Abschluss des Abschnitts Teil 3, Kapitel 1 des SatDSiG dar und umfasst dergestalt sämtliche Pflichten, die sich aus diesem Abschnitt ergeben. Das ist bei § 9 SatDSiG hingegen gerade nicht der Fall. Die Einhaltung der Pflicht aus § 10 SatDSiG wird aber dennoch durch § 28 Abs. 1 Nr. 2, 3a SatDSiG gewährleistet.

anordnen (Nr. 2). Sämtliche durch die Bestellung eines Sonderbeauftragten entstehenden Kosten sind dann vom Betreiber zu tragen, vgl. § 9 Abs. 3 SatDSiG.

Zu beachten war, dass es sich bei den in § 9 Abs. 2 SatDSiG bezeichneten behördlichen Maßnahmen lediglich um Regelbeispiele handelt, die nicht abschließend sind.[55] Allgemeine ordnungsrechtliche Eingriffsermächtigungen - zB aus dem Polizei- und Ordnungsrecht - bestehen ebenfalls neben den Regelungen des § 9 SatDSiG fort.[56]

Zudem können entsprechende Pflichtverletzungen als Ordnungswidrigkeit mit Geldbußen von bis zu 500.000 € geahndet werden, vgl. § 28 SatDSiG.[57] Darunter fallen auch Zuwiderhandlungen gegen die nach § 9 Abs. 1 SatDSiG angeordneten vollziehbaren Anordnungen, vgl. § 28 Abs. 1 Nr. 4 SatDSiG.

Datenverbreitung

Da die durch den Einsatz eines Satellitensensors gewonnen Daten im Rahmen des Projekts für die Erstellung eines Echtzeitlagebildes genutzt werden sollten, blieb ferner zu untersuchen, welchen Anforderungen die Datenverbreitung unterlag. Als „verbreitet“ gelten solche Informationen, die den über §§ 4 ff. und §§ 12 ff. SatDSiG geschützten Bereich verlassen.[58]

Wurden die Daten durch den ordnungsgemäßen Betrieb eines Erdfernerkundungssystems erhoben und sollen sie an einen Datenanbieter übermittelt werden, bemisst sich deren Verbreitung nach den §§ 11 ff. SatDSiG.

Zulassung

§ 11 Abs. 1 SatDSiG bestimmt dabei zunächst, dass der Datenanbieter, welcher Daten iSd Gesetzes verbreiten will, einer Zulassung bedarf. Auch in diesem Kontext stellt das Gesetz formelle sowie materielle Zulassungsvoraussetzungen auf.

Formelle Zulassungsvoraussetzungen

[55] Dies wird durch das Wort „insbesondere“ deutlich.

[56] Vgl. BT Drs. 16/4763, S. 24.

[57] § 28 Abs. 1 Nr. 2, 3a SatDSiG betrifft die Pflicht aus § 10 SatDSiG. Im Falle eines Verstoßes kann dies ein Bußgeld von bis zu 500.000 € nach sich ziehen. § 28 Abs. 1 Nr. 7 SatDSiG rekurriert auf § 5 SatDSiG. Hier ist eine Geldbuße von bis zu 50.000 € möglich. Nach § 28 Abs. 2 Nr. 1, 2 SatDSiG lässt sich eine Verletzung der Pflichten aus §§ 6, 7 SatDSiG mit bis zu 25.000 € ahnden. Die Höhe der jeweiligen Bußgelder bemisst sich dabei anhand des § 28 Abs. 3 SatDSiG.

[58] Vgl. BT Drs. 16/4763, S. 26.

Hinsichtlich der formellen Anforderungen kann auf die entsprechenden Ausführungen zur Genehmigungserteilung verwiesen werden.[59]

Materielle Zulassungsvoraussetzungen

Die materiellen Zulassungskriterien ergeben sich aus § 12 Abs. 1 Nr. 1-4 SatDSiG. Die Zulassung ist zu erteilen, wenn die Voraussetzungen kumulativ vorliegen.

§ 12 Abs. 1 Nr. 1, 2 SatDSiG verlangt, dass „der Datenanbieter die erforderliche Zuverlässigkeit besitzt“ (Nr. 1) und er technische sowie „organisatorische Maßnahmen getroffen hat, die verhindern, dass Unbefugte Zugang zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung von Daten eines hochwertigen Erdfernerkundungssystems oder Zutritt zu den dafür genutzten Betriebsräumen haben“ (Nr. 2). Damit stellt die Vorschrift inhaltlich weitestgehend dieselben Anforderungen wie § 4 Abs. 1 Nr. 1 und 4 SatDSiG auf, sodass insoweit auf die entsprechende Darstellung verwiesen wird.[60]

Aus § 12 Abs. 1 Nr. 3 SatDSiG ergibt sich, dass „die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Datenanbieters und die Übermittlung der Daten an einen anderen Datenanbieter“ ferner „durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme“ zu schützen sind.

Schließlich setzt § 12 Abs. 1 Nr. 4 SatDSiG für die Erteilung der Zulassung voraus, dass „das sichere Verbreiten der von einem hochwertigen Erdfernerkundungssystem erzeugten Daten nach dem Stand der Technik gewährleistet ist“. Dies gilt auch für eine direkte Übermittlung der Daten vom Satelliten zur Bodenstation des Kunden.[61] Obschon ein zwingendes Sicherungsverfahren gesetzlich nicht vorgeschrieben ist, hat die im Einzelfall gewählte Vorgehensweise „dem Stand der Technik“ zu entsprechen, was für den Datenanbieter bedeutet, dass notwendige Aktualisierungen selbstständig vorzunehmen sind oder durch die zuständige Behörde angeordnet werden können.[62]

Pflichten des Datenanbieters

Wie beim Betrieb eines hochwertigen Erdfernerkundungssystems, sind auch dem Datenanbieter durch die §§ 13-16 SatDSiG bestimmte Pflichten auferlegt.

[59] S. o.

[60] S. o.

[61] Vgl. BT Drs. 16/4763, S. 26.

[62] Vgl. BT Drs. 16/4763, S. 26.

Anzeigepflicht

§ 13 SatDSiG regelt die Anzeigepflicht, wobei Nr. 1 und 2 dieselben Anforderungen aufstellen wie § 6 Abs. 1 Nr. 1 und 2 SatDSiG.[63]

§ 13 Nr. 3 SatDSiG normiert darüber hinaus eine unverzügliche[64] Anzeigepflicht des Datenanbieters gegenüber der zuständigen Behörde, sofern tatsächlich Anhaltspunkte dafür vorliegen, dass die Sicherung der in Rede stehenden Daten nicht mehr aufrechterhalten werden kann. Damit soll gewährleitet werden, dass von den Daten keinerlei Gefährdung ausgeht, soweit im Falle einer Betriebseinstellung ebenso die Schutzmaßnahmen aufgehoben werden.[65]

Auskunftspflicht und Duldungspflicht

Die Vorschriften der §§ 14 und 15 SatDSiG beziehen sich auf Auskunfts- und Duldungspflichten, die denjenigen des Betreibers nach §§ 7 und 8 SatDSiG entsprechen.[66]

Dokumentationspflicht

Nach § 18 SatDSiG trifft den Datenanbieter ferner eine Dokumentationspflicht. Die Vorschrift zählt systematisch betrachtet nicht mehr zu den allgemeinen Voraussetzungen des Verbreitens von Daten,[67] sondern fällt unter den Abschnitt „Verfahren des Verbreitens von Daten“.[68]

Vorrangige Bedienungspflicht von Anfragen der Bundesrepublik Deutschland

Auch für den Datenanbieter gilt gem. § 21 SatDSiG eine vorrangige Bedienungspflicht von Anfragen der Bundesrepublik Deutschland. Diese sind zum angefragten Zeitpunkt vor jeder anderen Anfrage zu behandeln. Wie bereits erwähnt, sind die in § 21 SatDSiG genannten Fälle abschließend geregelt.[69]

Ebenso wie der Betreiber kann der Datenanbieter gem. § 23 Abs. 1 SatDSiG für die vorrangige Behandlung eine Vergütung verlangen.

---

[63] S. o.

[64] Zum Begriff der „Unverzüglichkeit“ s. o.

[65] Vgl. BT Drs. 16/4763, S. 26.

[66] S. o.

[67] Teil 3, Kapitel 1 SatDSiG.

[68] Teil 3, Kapitel 2 SatDSiG.

[69] S. o.; vgl. BT Drs. 16/4763, S. 29.

Folgen einer Pflichtverletzung

Sofern der Datenanbieter eine der vorgenannten Maßgaben verletzt, kann die Behörde gem. § 16 S. 1 SatDSiG die zur ordnungsgemäßen Pflichterfüllung erforderlichen Maßnahmen anordnen. Insoweit entspricht § 16 S. 1 SatDSiG der Vorschrift des § 9 Abs. 1 SatDSiG, sodass auf die einschlägigen Feststellungen verwiesen wird.[70]

§ 16 S. 1 Nr. 1 SatDSiG betrifft die in § 12 Abs. 1 Nr. 4 SatDSiG bezeichnete Pflicht, die Sicherungsverfahren dem Stand der Technik anzupassen. Sofern diese aufgrund des stetigen technischen Wandels veraltet sind, ist die zuständige Behörde berechtigt, die entsprechenden Anpassungen an den Stand der Technik zu verlangen. Darüber hinaus darf die Behörde das Verbreiten der Daten vorübergehend untersagen, vgl. § 16 S. 1 Nr. 2 SatDSiG.

Die besagten Maßnahmen sind - wie in § 9 SatDSiG - nicht abschließend geregelt. Andere ordnungsrechtliche Ermächtigungsgrundlagen - bspw. aus dem Polizei- und Ordnungsrecht - sind neben dem SatDSiG anwendbar.[71]

Bestimmte Pflichtverletzungen können wiederum als Ordnungswidrigkeiten geahndet werden, vgl. § 28 Abs. 2 Nr. 1, 2 SatDSiG.[72]

Verfahren des Verbreitens

In Bezug auf das Verfahren des Verbreitens der Daten ergaben sich weitere zu beachtende Besonderheiten aus den §§ 17 ff. SatDSiG.

Sensitivitätsprüfung durch den Datenanbieter

So hat der Datenanbieter nach § 17 Abs. 1 SatDSiG zunächst eine Sensitivitätsprüfung durchzuführen, bevor er eine Anfrage auf Verbreiten von Daten bedienen darf. Hierbei handelt es sich um eine Voruntersuchung im Sinne einer Erheblichkeitsprüfung, für die dem Datenanbieter ein Verfahren an die Hand gegeben wird, welches es ihm ermöglicht, eindeutige Aussagen zur Sensitivität zu treffen.[73] Da dem Datenanbieter mit der Sensitivitätsprüfung ein gewichtiger Teil der Aufsicht über die Sicherheitsinteressen der

[70] S. o.

[71] Vgl. BT Drs. 16/4763, S. 26.

[72] Betroffen sind die Pflichten nach §§ 13 und 14 SatDSiG, bei deren Verletzung ein Bußgeld in Höhe von bis zu 25.000 € erhoben werden kann, vgl. § 28 Abs. 3 SatDSiG.

[73] Vgl. BT Drs. 16/4763, S. 26.

Bundesrepublik Deutschland anvertraut wird, schließt sich der dem Datenanbieter überlassenen Einschätzung eine behördliche Nachkontrolle an.[74]

Voraussetzung der Sensitivitätsprüfung

Eine der grundlegenden Voraussetzungen für die Sensitivitätsprüfung nach dem SatDSiG ist, dass Daten „angefragt" werden. Diese Anfragebezogenheit hat zur Folge, dass eine entsprechende Prüfung selbst dann zu erfolgen hat, wenn die Daten bereits früher durch einen anderen Anfragenden verbreitet wurden.[75]

Inhalt der Sensitivitätsprüfung

§ 17 Abs. 2 S. 1 SatDSiG stellt einen Kriterienkatalog auf, anhand dessen die Sensitivität einer Anfrage zu bestimmen ist. In die Prüfung sind danach der verwendete Sensorbetriebsmodus und der durch die verwendete Verarbeitung erzielte Informationsgehalt der Daten (Nr. 1), das mit den Daten dargestellte Zielgebiet (Nr. 2), der Erzeugungszeitpunkt der Daten sowie derjenige zwischen Datenerzeugung und Bedienung der Anfrage (Nr. 3) und schließlich die Bodensegmente, an welche die Daten übermittelt werden sollen (Nr. 4) einzustellen. Als sensitiv ist die Anfrage dann einzustufen, wenn die in Ansehung der Person des Anfragenden vorzunehmende Gesamtbetrachtung[76] besagter Umstände ergibt, dass ein Schadenseintritt für wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland möglich ist. Zum Zeitpunkt der Prüfung durch den Datenanbieter muss folglich noch keine konkrete Gefahr - also die Wahrscheinlichkeit eines Schadenseintritts - vorliegen, ihre Möglichkeit löst jedoch bereits das Erfordernis einer behördlichen Nachprüfung aus, innerhalb derer anschließend festzustellen ist, ob eine Gefahr tatsächlich besteht.[77]

Die Prüfung eines möglichen Schadenseintrittes bezieht sich stets auf den konkreten einzelnen Datensatz, der zum Zeitpunkt der Untersuchung jedoch nicht zwingend vorliegen muss; sie lässt sich vielmehr auch über Metadaten durchführen, sofern diese den Datensatz ausreichend konkret beschreiben und die Zulässigkeitsprüfung dementsprechend bereits vor

[74] Vgl. BT Drs. 16/4763, S. 26.

[75] Vgl. BT Drs. 16/4763, S. 26.

[76] In die Kontrolle sind jedoch auch diejenigen Personen einzubeziehen, welche „bestimmungsgemäß mit den Daten in Kontakt kommen", vgl. § 17 Abs. 2 S. 2 SatDSiG. Sollte der Anfragensteller die betreffenden Personen nicht benennen können (oder wollen), hat dies negative Auswirkungen dahingehend, dass die Möglichkeit eines Schadenseintrittes steigt und eine Datenübermittlung ohne Offenlegung der endgültigen Datenempfänger abzulehnen ist, vgl. BT Drs. 16/4763, S. 27.

[77] Zu berücksichtigen ist, dass es sich um eine Vorprüfung handelt. Anhand der Kriterien aus Abs. 2 sollen diejenigen Fälle festgestellt werden, welche einer behördlichen Prüfung zwingend bedürfen, vgl. BT Drs. 16/4763, S. 26f.

der Beobachtung des Zielgebiets durch den Satelliten möglich ist.[78] Legt der Datenanbieter den betreffenden Datensatz nicht offen, erfolgt die Bestimmung seines Informationsinhalts durch eine Prognoseeinschätzung, die darüber Aufschluss gibt, welcher Aussagehalt der Daten bei bestmöglicher Prozessierung erreichbar wäre.[79]

Gem. § 17 Abs. 3 S. 1 SatDSiG bestimmt das Bundesministerium für Wirtschaft und Technologie im Einvernehmen mit dem Bundesministerium der Verteidigung, dem Auswärtigen Amt und dem Bundesministerium des Innern durch Rechtsverordnung ohne Zustimmung des Bundesrates, Vorgaben, unter welchen Voraussetzungen nach Abs. 2 die Möglichkeit eines Schadenseintritts der geschützten Rechtsgüter gegeben ist. Dem wurde durch Erlass der SatDSiV Rechnung getragen. § 2 SatDSiV konkretisiert vor dem Hintergrund der aktuellen Sicherheitslage[80] die durch § 17 Abs. 2 SatDSiG aufgestellten Kriterien. Die SatDSiV legt etwa kritische Gebiete fest, die den Schluss auf die Sensitivität der Anfrage zulassen. Von der Sensitivität ist bspw. dann auszugehen, wenn die Anfrage von Staatsgebieten wie Armenien, Irak oder Somalia aus erfolgt, vgl. Anlage 3 zu § 2 Abs. 2 Nr. 2a) SatDSiV.[81]

Danach waren die Anfragen über die im Projekt EMSec verwendeten Daten als nicht sensitiv einzustufen, da sich das Bodensegment des DLR DFD in Neustrelitz befindet und sich das Zielgebiet auf den Nord- und Ostseeraum beschränkte. Demzufolge waren keine Gebiete des Negativkatalogs aus Anlage 3 der SatDSiV (vgl. § 2 Abs. 2 Nr. 1 und. Nr. 2a) in Verbindung mit Anlage 1 und Anlage 3 SatDSiV) betroffen.

Die Sensitivität der Anfrage konnte sich allerdings daraus ergeben, dass „die Person des Anfragenden nicht in Anlage 4 aufgeführt ist, der Zeitraum zwischen der Erzeugung der Daten und der Bedienung der Anfrage weniger als fünf Tage beträgt“ und „die Daten in mindestens einer Raumrichtung eine geometrische Auflösung von 1,2 Metern oder weniger haben“ (§ 2 Abs. 2 Nr. 2 b) aa) SatDSiV) oder „sich aus den Daten (neben der Radarintensität auch) Phaseninformation rekonstruieren lässt“ (§ 2 Abs. 2 Nr. 2 b) bb) SatDSiV) bzw. „Daten im Spektralbereich von 8 bis 12 Mikrometern (thermisches Infrarot) oder mit einem super- oder hyperspektralen Sensor erzeugt werden“ (§ 2 Abs. 2 Nr. 3 SatDSiV).

Soweit ersichtlich, handelt es sich bei den Projektpartnern, von denen entsprechende Anfragen ausgingen, um keine der in Anlage 4 aufgeführten Personen. Für die Annahme der Sensitivität blieb demzufolge zu prüfen, ob die weiteren Tatbestandsmerkmale des § 2 Abs. 2 Nr. 2 b) SatDSiV vorlagen.

Fraglich war daher zunächst, ob der Zeitraum zwischen Datenerzeugung und Bedienung der Anfrage weniger als fünf Tage betragen würde. Entsprechende Informationen werden

[78] Vgl. BT Drs 16/4763, S. 27.

[79] Vgl. BT Drs 16/4763, S. 27. Ebenso genügt eine Prognosebeurteilung, sofern Rohdaten an den Datenempfänger übermittelt werden.

[80] Vgl. § 17 Abs. 3 S. 2 SatDSiG.

[81] Sog. Gebietsnegativliste.

regelmäßig sieben Tage im Voraus bestellt. In Abhängigkeit vom Aufnahmemodus könnten die Daten dem DLR DFD in Neustrelitz, sofern sie in dessen Empfangskreis aufgenommen wurden, jedoch bereits innerhalb von 15 bis 30 Minuten zur Verfügung stehen. Die Sensitivität der Anfrage war folglich nicht von vornherein ausgeschlossen. Hinzukommen musste jedoch entweder der Umstand, dass die Daten in mindestens einer Raumrichtung eine geometrische Auflösung von weniger als 1,2 m bzw. weniger haben oder sich daraus Phaseninformation rekonstruieren ließe. Die im Rahmen des Projekts verwendeten Daten besaßen grds. eine Raumauflösung von 3 m und schlechter, sodass sich daraus die Sensitivität nicht herleiten ließ. Es besteht jedoch die Möglichkeit, aus den Satellitendaten Phaseninformationen zu rekonstruieren.[82] Da sich die Sensitivität der Anfragen bereits hieraus ergibt und die übrigen Tatbestandsvoraussetzungen des § 2 Nr. 3 SatDSiV lediglich in einem alternativen Verhältnis zu § 2 Abs. 2 Nr. 2 b) SatDSiV stehen,[83] kam es auf deren Vorliegen folglich nicht mehr an.[84]

Vorgehen bei Sensitivität

Sobald der Datenanbieter eine als sensitiv einzustufende Datenanfrage bedienen will, bedarf er gemäß § 19 Abs. 1 S. 1 SatDSiG der Erlaubnis durch die zuständige Behörde. Über § 19 Abs. 1 S. 2 SatDSiG werden hiervon auch Fälle umfasst, in denen der Datenanbieter ohne Anfrage Daten verbreitet.

Nach § 19 Abs. 2 SatDSiG ist die Erlaubnis zu erteilen, „wenn das Verbreiten der Daten im Einzelfall die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland nicht gefährdet, das friedliche Zusammenleben der Völker und die auswärtigen Beziehungen der Bundesrepublik Deutschland nicht erheblich stört“.[85] Verbleiben Zweifel an dem Vorliegen einer Gefährdung, darf die Behörde die Erlaubnis verweigern oder aber das Verbreiten der Daten unter Auflagen stellen. So kann die Behörde bspw. die Erteilung der Erlaubnis an den Abschluss eines Vertrags über den Verwendungszweck zwischen Datenanbieter und Kunden knüpfen.[86]

Liegen die Voraussetzungen vor, soll die Entscheidung spätestens einen Monat nach Eingang des Antrages auf Erlaubnis ergehen, vgl. § 19 Abs. 3 SatDSiG.

[82] Der Wortlaut der Norm lässt darauf schließen, dass es nicht darauf ankommt, ob die Phaseninformation tatsächlich rekonstruiert wird, sodass die bloße Möglichkeit ausreichen dürfte.

[83] Dies ergibt sich aus dem Wortlaut („oder“).

[84] § 2 Abs. 2 Nr. 3 SatDSiV wäre im vorliegenden Fall nicht erfüllt, da innerhalb des Projektes lediglich Radarsensoren untersucht werden und weder thermisches Infrarot noch Hyperspektral vorgesehen sind.

[85] Es handelt sich hierbei um unbestimmte Rechtsbegriffe, bei deren Auslegung die aktuelle Sicherheitslage zugrunde zu legen ist, vgl. BT Drs. 16/4763, S. 28.

[86] Vgl. BT Drs. 16/4763, S. 28.

Die Behörde kann ferner eine Sammelerlaubnis erteilen, wenn der Datenanbieter entweder „Darstellungen von Daten mit stark vermindertem Informationsgehalt oder Metadaten für jedermann zugänglich machen will“ (Nr. 1)[87] oder „sensitive Anfragen, die in gleichartiger Weise von derselben Person für eine unbestimmte Anzahl von Daten […] angefragt werden, bedienen will“ (Nr. 2). Neben der Sammelerlaubnis ist eine Einzelfallerlaubnis dann nicht mehr erforderlich. Die Behörde hat aber die Möglichkeit, die Erlaubnis zu widerrufen, sofern Tatsachen eintreten, nach denen die Einzelfallerlaubnis nicht hätte erteilt werden dürfen. In Frage kommt insbesondere der Umstand, dass sich die aktuelle Sicherheitslage ändert oder aufgrund eines Fehlverhaltens die zwingend erforderliche Zuverlässigkeit entfällt.[88]

Dokumentationspflicht

Für das Verfahren des Verbreitens der Daten legt die Vorschrift des § 18 Abs. 1 S. 1 SatDSiG weiterhin eine Dokumentationspflicht des Datenanbieters fest. Diese betrifft sämtliche Anfragen auf Verbreiten von Daten und umfasst neben deren Dokumentation auch die Aufzeichnung des Verfahrens sowie des Ergebnisses der Sensitivitätsprüfung, vgl. § 18 Abs. 1 S. 2 Nr. 3 SatDSiG.

Die Aufzeichnungen sind gem. Abs. 3 wenigstens fünf Jahre nach Erzeugung der Daten – nicht Anfrage – aufzubewahren und der zuständigen Behörde zur Einsichtnahme zugänglich zu machen.

Folgen von Verstößen beim Betrieb eines Erdfernerkundungssystems und Verbreiten der Daten

Hinsichtlich der Rechtsfolgen von Verstößen gegen das SatDSiG, kann weitestgehend auf die obigen Ausführungen verwiesen werden.[89]

Daneben war jedoch die Vorschrift des § 29 Abs. 1 SatDSiG in den Blick zu nehmen, welche die Verhängung einer Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe für denjenigen vorsieht, der eine vorsätzliche Handlung iSd § 28 Abs. 1 Nr. 1 bis 6 SatDSiG begeht, die dazu geeignet ist, die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland (§ 29 Abs. 1 Nr. 1 SatDSiG), das friedlichen Zusammenleben der Völker (§ 29 Abs. 1 Nr. 2 SatDSiG) oder die auswärtigen Beziehungen der Bundesrepublik Deutschland (§ 29 Abs. 1 Nr. 3 SatDSiG) erheblich zu gefährden.

[87] hiervon umfasst sind Vorschaubilder bzw. Miniaturansichten (Browse Images), vgl. BT Drs. 16/4763, S. 28.

[88] Vgl. BT Drs. 16/4763, S. 28.

[89] S. o.; in diesem Kontext ist ferner zu beachten, dass solche Verstöße auch Zweifel an der Zuverlässigkeit des Betreibers bzw. Datenanbieters erwecken können. Anhand der geänderten Sachlage hat die Behörde in einem solchen Fall eine erneute Zuverlässigkeitsprüfung durchzuführen. Fällt diese negativ aus, ist sie berechtigt, entsprechende Maßnahmen zu ergreifen, vgl. BT Drs. 16/4763, S. 22.

Umgang mit personenbezogenen Satellitendaten durch die zuständige Behörde

Im vorliegenden Kontext war ferner auf § 27 SatDSiG hinzuweisen, der konkrete Anforderungen an die „Übermittlung von personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen“ stellt.[90] Nach der Systematik des Gesetzes ist § 27 SatDSiG eine Spezialnorm zu § 15 BDSG; dennoch gilt das dem BDSG zugrunde liegende Verbot mit Erlaubnisvorbehalt der Verarbeitung von personenbezogenen Daten auch gegenüber der Behörde.[91] Allerdings wird die jeweils zuständige Behörde durch § 27 Abs. 1 S. 1 SatDSiG ermächtigt, zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker, einer erheblichen Störung der auswärtigen Beziehungen oder zur Verhütung bzw. Verfolgung von Straftaten personenbezogene Daten, die ihr bei der Erfüllung ihrer Aufgaben bekannt geworden sind, an eine andere Behörde zu übermitteln. Auch eine Übermittlung an den Bundesnachrichtendienst ist möglich, soweit der Zweckbindungsgrundsatz gewahrt wird. Das heißt, dass die Daten nur für das Vorhaben eingesetzt werden dürfen, zu dessen Erfüllung sie übermittelt wurden, § 27 Abs. 1 S. 2 SatDSiG.

§ 27 Abs. 2 SatDSiG hält darüber hinaus eine weitere Ermächtigungsgrundlage zur Datenübermittlung im Falle von Strafverfahren wegen eines Verstoßes gegen das SatDSiG bereit. Danach sind Gerichte und Staatsanwaltschaften aus den zu Absatz 1 genannten Gründen berechtigt, personenbezogene Daten an oberste Bundesbehörden weiterzuleiten. Zulässig ist ein solches Vorgehen allerdings nur, sofern das Interesse an der Verwendung der übermittelten personenbezogenen Daten das Interesse des Betroffenen an der Geheimhaltung erheblich überwiegt und hierdurch das Ermittlungsziel des Strafverfahrens nicht gefährdet wird, vgl. § 27 Abs. 2 S. 3 SatDSiG.

2.2.2 Geodatenzugangsgesetz (GeoZG)[92]

Für das Verbundvorhaben war ferner zu überprüfen, ob auch die Vorschriften des GeoZG von den Projektpartnern beachtet werden mussten.

[90] Zum Begriff der „personenbezogenen Daten“ später unter Punkt II. 2.2.8.

[91] Vgl. BT Drs. 16/4763, S. 30.

[92] Geodatenzugangsgesetz vom 10. Februar 2009 (BGBl. I S. 278), geändert durch Art. 1 des Gesetzes vom 7. November 2012. Das GeoZG ist am 14. Februar 2009 in Kraft getreten.

Mit dem GeoZG hat der Bundesgesetzgeber[93] die Vorgaben der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.03.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-RL)[94] in deutsches Recht umgesetzt.[95] Die INSPIRE-RL betrifft gem. Art. 4 Abs. 1 den Zugang zu und die Nutzung von bereits erhobenen Geodaten[96] zum Zwecke der Umweltpolitik[97] sowie anderer umweltbezogener Maßnahmen[98] und bildet mithin die Grundlage für den Aufbau einer europäischen Geodateninfrastruktur, vgl. Art. 1 Abs. 1 INSPIRE-RL.

Dementsprechend gestaltet das GeoZG den nationalen Rechtsrahmen für Zugangs- und Nutzungsrechte sowohl von staatlichen Behörden als auch Privatpersonen zu Geodaten, Geodatendiensten[99] und Metadaten, § 1 S. 2 GeoZG. Diese sind nach § 8 Abs. 1 GeoZG interoperabel bereitzustellen. § 9 Abs. 2 GeoZG sieht darüber hinaus die Errichtung eines Geoportals[100] vor, das der Öffentlichkeit den Zugriff auf die Geodaten ermöglicht.[101]

2.2.2.1. Anwendungsbereich

Fraglich war daher, ob die Projektpartner verpflichtet waren, Daten, die sie im Rahmen des Forschungsvorhabens erhoben haben, der Öffentlichkeit zur Verfügung zu stellen. Davon wäre auszugehen, sofern sie in den persönlichen Anwendungsbereich des GeoZG fallen.

Persönlicher Anwendungsbereich

[93] Da das Grundgesetz (GG) keine explizite Kompetenzzuweisung für den Bereich der Geodaten vornimmt, haben sowohl Bund als auch Länder überwiegend homogene Geodatenzugangsgesetze erlassen; vgl. hierzu *Martini/Damm*, Auf dem Weg zum Open Government: Zum Regimewechsel im Geodatenrecht, DVBl. 2013, 1 (6). Für den hier zu behandelnden Fall wird ausschließlich auf das Gesetz des Bundes eingegangen.

[94] ABl. Nr. L 108 S. 2.

[95] Vgl. die amtliche Anmerkung GeoZG, BGBl. I S. 278.

[96] Zum Begriff der Geodaten s. o.; weitergehend dazu *Maatsch*, Geodaten und Verwaltungstransparenz: Die Pflicht zur Veröffentlichung von Geodaten nach dem Hamburgischen Transparenzgesetz, DuD 2014, 192 (193f.), der eine Einteilung von Geodaten in „Geobasisdaten“ und „Geofachdaten“ vornimmt.

[97] Der Umweltbegriff ist in diesem Zusammenhang extensiv auszulegen, vgl. BT Drs 16/10530, S. 13.

[98] Eine zusätzliche Pflicht zur Beschaffung der Geodaten durch die Mitgliedstaaten ergibt sich daraus indes nicht, vgl. auch Erwägungsgrund 13 der INSPIRE-RL.

[99] Zum Begriff der Geodatendienste vgl. *Maatsch*, Geodaten und Verwaltungstransparenz: Die Pflicht zur Veröffentlichung von Geodaten nach dem Hamburgischen Transparenzgesetz, DuD 2014, 192 (194).

[100] Gem. § 3 Abs. 6 GeoZG bezeichnet der Begriff „Geoportal“ eine „elektronische Kommunikations-, Transaktions- und Interaktionsplattform, die über Geodatendienste und weitere Netzdienste den Zugang zu den Geodaten ermöglicht“.

[101] Vgl. *Martini*/*Damm*, Der Zugang der Öffentlichkeit zu hochauflösenden Satellitenbildern, NJW 2014, 130 (131).

DLR

Gem. § 2 Abs. 1 GeoZG gilt das Gesetz für die geodatenhaltenden Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts. Das DLR müsste folglich zunächst eine geodatenhaltende Stelle im vorgenannten Sinne sein. Ausweislich § 3 Abs. 8 GeoZG sind dies die informationspflichtigen Stellen nach § 2 Abs. 1 Umweltinformationsgesetz (UIG)[102]. Die schlichte Verweisung auf den Adressatenkreis des UIG folgt den Vorgaben des EU-Rechts: So definiert die INSPIRE-Richtlinie in Art. 3 Abs. 9 den Behördenbegriff wortgleich wie Art. 2 Nr. 2 der Richtlinie 2003/4/EG über den Zugang der Öffentlichkeit zu Umweltinformationen.[103]

Informationspflichtige (und damit zugleich geodatenhaltende) Stellen sind sonach „die Regierung und andere Stellen der öffentlichen Verwaltung" (§ 2 Abs. 1 Nr. 1 S. 1 UIG) sowie – unter bestimmten Voraussetzungen – auch natürliche oder juristische Personen des Privatrechts (Nr. 2 der Vorschrift).

Als gemeinnütziger eingetragener Verein und somit juristische Person des Privatrechts[104] gehört das DLR zwar offenkundig nicht der Regierung an.[105] Weniger gewiss war allerdings, ob das DLR nicht als *„andere Stelle der öffentlichen Verwaltung"* i.S. des § 2 Abs. 1 Nr. 1 S. 1 UIG angesehen werden musste.[106] Hierunter fallen alle Behörden i.S. des § 1 Abs. 4 VwVfG und folglich – in Übereinstimmung mit der überwiegenden Auffassung im Schrifttum und zudem mit der Entwurfsbegründung zum UIG[107] – auch Beliehene.[108] Als solche sind privatrechtlich organisierte natürliche oder juristische Personen zu verstehen, denen durch Gesetz, aufgrund eines Gesetzes oder im Wege eines Vertrags einzelne hoheitliche Aufgaben zur Wahrnehmung im eigenen Namen übertragen worden sind.[109] Als ein entsprechendes Gesetz kam – im Fall des DLR – lediglich das Raumfahrtaufgabenübertragungsgesetz

[102] Umweltinformationsgesetz vom 22. Dezember, 2004 (BGBl. I S. 3704), zuletzt geändert durch das Gesetz zur Änderung des Umweltinformationsgesetzes vom 27.10.2014 (BGBl. I. S. 1642), s. auch die Bekanntmachung der Neufassung des Umweltinformationsgesetzes vom 27.10.2014 (BGBl. I. S. 1643). Das UIG schafft den rechtlichen Rahmen für den freien Zugang zu Umweltinformationen, vgl. § 1 Abs. 1 UIG.

[103] S. RegE in BT-Drs. 16/10530, S. 13.

[104] S. o.

[105] *Martini/Damm*, NJW 2014, 130 (132).

[106] Ohne Begründung verneinend *Martini/Damm*, NJW 2014, 130 (132).

[107] Ausdrücklich BT-Drs. 15/3406, S. 14.

[108] S. *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 6; *Gurlit*, EurUP 2006, 224 (227); *Guckelberger*, UPR 2006, 89 (90); *Schreiner*, BayVBl. 2009, 332; *Schrader*, in: Schlacke/Schrader/Bunge, Aarhus-Handbuch, § 1 Rdnr. 80; ebenso anhand der Parallele in § 1 Abs. 1 S. 1 IFG *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 1 Rn. 82; a.A. *Fluck/Theuer*, in: Fluck, Informationsfreiheitsrecht, § 2 UIG Rdnr. 230 ff.; *Louis*, NuR 2013, 77 (78), der (ohne Begründung) Beliehene unter § 2 Abs. 1 Nr. 2 UIG fassen will.

[109] *Erbguth*, Wilfried, Allgemeines Verwaltungsrecht, 7. Aufl. 2014, § 6 Rn. 22.

(RAÜG)[110] in Betracht. Nach § 1 Abs. 1 RAÜG übertragen die für Raumfahrtangelegenheiten zuständigen obersten Bundesbehörden dem DLR die Befugnis, Verwaltungsaufgaben auf dem Gebiet der Raumfahrt im eigenen Namen und in öffentlich-rechtlicher Form wahrzunehmen. § 1 Abs. 2 RAÜG beschränkt die Verwaltungsaufgaben insofern auf „die Erstellung der deutschen Raumfahrtplanung“ (Nr. 1), „die Durchführung der deutschen Raumfahrtprogramme“ (Nr. 2) und „die Wahrnehmung deutscher Raumfahrtinteressen im internationalen Bereich“. Hierbei geht es in erster Linie um das politische Raumfahrtmanagement, welches strikt vom Bereich der Forschung und Entwicklung zu trennen ist, wenngleich auch in diesem Segment eine eigene Forschungsabteilung existiert, die sich mit der Raumfahrt befasst.[111] Durch das RAÜG wurden dem DLR für das Projekt „EMSec“ folglich keine öffentlichen Aufgaben zur Wahrnehmung im eigenen Namen übertragen, sodass die Eigenschaft als Beliehener zu verneinen war. Damit schied zugleich die Informationspflichtigkeit der DLR als „Stelle der öffentlichen Verwaltung“ aus.

Die Eigenschaft als datenhaltende Stelle konnte sich damit allenfalls aus § 2 Abs. 1 GeoZG i.V.m. § 2 Abs. 1 Nr. 2 UIG ergeben. Letztere Vorschrift will – wie erwähnt – u.a. auch juristische Personen des Privatrechts als informationspflichtige Stellen verstanden wissen, allerdings nur „soweit sie öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen, die im Zusammenhang mit der Umwelt stehen, insbesondere solche der umweltbezogenen Daseinsvorsorge, und dabei der Kontrolle des Bundes oder einer unter der Aufsicht des Bundes stehenden juristischen Person des öffentlichen Rechts unterliegen.“ Der Erweiterung des Anwendungsbereichs des UIG über den Behördenbereich hinaus liegen die zunehmende Verlagerung staatlicher Aufgaben auf juristische Personen des Privatrechts (formelle und materielle Privatisierung) sowie die Änderungen im Dienstleistungsbereich zugrunde.[112]

In Frage kam hier zunächst die Tatbestandsalternative der *Wahrnehmung öffentlicher Aufgaben*.[113] Als öffentliche Aufgaben werden insofern in einem weiten Sinne sämtliche Aufgaben verstanden, an deren Erfüllung die Öffentlichkeit maßgeblich interessiert ist, die also – wie etwa der gesamte Bereich der Daseinsvorsorge – gemeinwohlerheblich sind.[114] Intendiert ist also (lediglich) eine Abgrenzung zur Verfolgung rein privater Zwecke, nicht hingegen sind als öffentliche Aufgaben allein staatliche, im Allgemeinen von Trägern

[110] Gesetz zur Übertragung von Verwaltungsaufgaben auf dem Gebiet der Raumfahrt in der Fassung der Bekanntmachung vom 22. August 1998 (BGBl. I, 2510).

[111] Vgl. *Martini*/*Damm*, NJW 2014, 130 (132).

[112] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 19.

[113] Der Umweltbegriff ist dabei sehr weit gefasst; näher dazu BVerwGE 7. Senat, Urt. v. 25. März 1999 – 7 C 21/98, zitiert nach *juris*, Rn. 28.

[114] VG Berlin, Urteil vom 5. November 2012 – 2 K 167.11 –, juris, Rn. 89 unter Verweis auf *Erichsen*, Das Recht auf freien Zugang zu Informationen über die Umwelt – Gemeinschaftsrechtliche Vorgaben und nationales Recht, NVwZ 1992, 409 (411); *Fluck/Theuer*, in: *dies.* (Hrsg.), InformationsfreiheitsR, Bd. I, 29. Erg.-Lfg. (2012), § 2 UIG Rdnr. 156 m. w. Nachw.; *Martini*/*Damm*, NJW 2014, 130 (132).

öffentlicher Gewalt wahrgenommene Aufgaben zu verstehen.[115] Nicht maßgeblich ist ferner die Rechtsform des Handelns; auch privatrechtliches Handeln kann somit öffentlichen Aufgaben dienen.[116] Der Begriff der „Wahrnehmung" stellt des Weiteren lediglich auf das tatsächliche Wahrnehmen durch die Privatrechtsperson ab.[117] Keine Rolle spielt demgegenüber, ob eine (gesetzlich oder anderweitig begründete) Pflicht zur Wahrnehmung besteht.[118] Auch und gerade Verwaltungshelfer, also Personen des Privatrechts, derer sich eine Behörde zur Erfüllung ihrer Aufgaben bedient, nehmen damit öffentliche Aufgaben i.S. des § 2 Abs. 1 Nr. 2 UIG wahr.[119]

Kaum eigenständige Bedeutung kommt daneben der weiteren Tatbestandsalternative *„Erbringung öffentlicher Dienstleistungen"* zu;[120] der Gesetzgeber des UIG verfolgte mit deren Aufnahme lediglich eine Übernahme der unionsrechtlichen Terminologie der Umweltinformations-RL, die ihrerseits wiederum auf das Bestreben der EU-Kommission zurückgeht, die Dienste von allgemeinem wirtschaftlichem Interesse i.S. von Art. 14, 106 Abs. 2 AEUV in den Anwendungsbereich der Richtlinie aufzunehmen[121]. Auch bei jenen Diensten steht der weite Bereich der Daseinsvorsorge im Vordergrund, der in § 2 Abs. 1 Nr. 2 UIG in seiner umweltbezogenen Ausrichtung explizit erwähnt wird. Das Begriffsmerkmal der „öffentlichen Dienstleistungen" soll nach zutreffender Sicht nur klarstellen, dass auch Tätigkeiten, die mit Gewinnerzielungsabsicht ausgeübt werden, zu einer Informationspflicht führen können.[122]

Vorliegend stellte sich indes die forschungsbezogene Erhebung von Geodaten durch das DLR bereits als eine Tätigkeit mit Gemeinwohlbezug und somit als Wahrnehmung einer öffentlichen Aufgabe i.S. des § 2 Abs. 1 Nr. 2 UIG dar,[123] sodass sich eine nähere Auseinandersetzung mit der Alternative der öffentlichen Dienstleistung erübrigte. Diese Aufgabe musste man auch als *im Zusammenhang mit der Umwelt stehend* begreifen, wie es die Vorschrift im Weiteren verlangt.[124] Wollte man dies bestreiten, so hätte man die

---

[115] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 21; *Martini*/*Damm*, NJW 2014, 130 (132).

[116] *Reidt/Schiller*, *wie vor*; *Fluck/Theuer*, in: Fluck,Informationsfreiheitsrecht, § 2 UIG Rdnr. 156; *Turiaux*, UIG, 1995, §§ 2, 3 Rdnr. 102.

[117] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 21.

[118] *Fluck/Theuer*, in: Fluck, Informationsfreiheitsrecht, § 2 UIG Rdnr. 161; *Schomerus/Schrader/Wegener*, UIG, 2. Aufl. 2002, § 2 Rdnr. 19.

[119] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 21.

[120] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 22: „Begriff der öffentlichen Dienstleistungen entbehrlich".

[121] Dazu *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 22 unter Verweis auf KOM(2000) 402 (endg.), S. 11.

[122] *Martini*/*Damm*, NJW 2014, 130 (132).

[123] So zutreffend *Martini*/*Damm*, wie vor.

[124] Ebenso *Martini*/*Damm*, wie vor.

Sinnhaftigkeit der Überführung des Merkmals „Umweltbezug“ aus dem UIG in das GeoZG als solche in Zweifel ziehen müssen (Gleiches galt für die entsprechende EU-rechtliche Vorgehensweise).[125]

Maßgeblich für die Qualifikation des DLR als (umwelt)informationspflichtige und damit zugleich geodatenhaltende Stelle gem. § 3 VIII GeoZG war damit das Erfordernis, dass das DLR „dabei“ – d.h. bei der Aufgabenwahrnehmung – „der Kontrolle des Bundes oder einer unter der Aufsicht des Bundes stehenden juristischen Person des öffentlichen Rechts [unterliegt]“. Was unter „Kontrolle“ i.S. der Vorschrift zu verstehen ist, ergibt sich abschließend aus § 2 Abs. 2 UIG.[126] Kontrolle liegt nach Nr. 1 der Vorschrift dann vor, wenn die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe oder bei der Erbringung der öffentlichen Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt (Nr. 1). Beispielhaft führt die Vorschrift einen Kontrahierungszwang oder einen Anschluss- und Benutzungszwang auf. Das macht deutlich, dass es nicht staatlicher Aufsichtsrechte über die Person des Privatrechts bedarf, wohl aber einer besonderen Rechtsstellung derselben, „mit der eine besondere Wächterrolle des Staates korreliert“, was etwa bei einem Monopol oder gesetzlich gewährten Wettbewerbseinschränkungen der Fall ist.[127] Nur hieraus – also aus einer quasi-staatlichen Trägerschaft von Umweltbelangen[128] – rechtfertigt sich die Unterwerfung jener Privaten unter die Informationspflichten nach dem UIG.

Geht es – wie hier – ausschließlich um eine forschungs- und entwicklungsbezogene Aufgabenwahrnehmung durch das DLR, so beschränken sich die Einflussmöglichkeiten des Bundes von vornherein auf solche vertraglich begründeter Art.[129] Zu verweisen war hier insbes. auf den Rahmenvertrag zwischen der Bundesrepublik Deutschland und dem DLR zur Einräumung von Nutzungsrechten an den erhobenen Geodaten.[130] Einflussmöglichkeiten i.S. einer Kontrolle, wie sie § 2 Abs. 2 Nr. 1 UIG sieht der Vertrag hingegen nicht vor;[131] Gleiches

[125] Dazu *Martini*/*Damm*, wie vor.

[126] Zwar beschränkt sich die Verweisung in § 3 Abs. 8 GeoZG auf § 2 Abs. 1 UIG; gleichwohl findet § 2 Abs. 2 UIG auch im Rahmen der Bestimmung des persönlichen Anwendungsbereichs des GeoZG Anwendung, gibt es doch keinerlei Anhaltspunkte in den Gesetzgebungsmaterialien, welche die Annahme einer bewussten Ausklammerung der Begriffsbestimmung in § 2 Abs. 2 UIG stützen könnten, s. *Martini*/*Damm*, wie vor.

[127] *Reidt/Schiller*, UIG, in: Landmann/Rohmer, Umweltrecht, 72. Ergänzungslieferung 2014, § 2 Rn. 25.

[128] *Arzt*, ZRP 1993, 18.

[129] *Martini*/*Damm*, NJW 2014, 130 (133).

[130] Zwischen dem Bundesministerium des Innern (BMI) und dem Zentrum für satellitengestützte Kriseninformation (ZKI) als eine dem DLR-DFD zugeordnete Serviceeinheit, existiert seit dem 1. Januar 2013 ein Rahmenvertrag, wonach sich das DLR zur Erstellung und Lieferung von auf Fernerkundungsdaten basierenden Kartenprodukten sowie zur Aufbereitung der diesen zugrundliegenden Informationen verpflichtet hat, vgl. *Martini*/*Damm*, NJW 2014, 130 (131) und BT-Drs. 17/13187, S. 2. Da die Vertragspflicht unabhängig vom Ausgang des Projektes „EMSec“ besteht, soll an dieser Stelle nicht weiter darauf eingegangen werden.

[131] *Martini*/*Damm*, wie vor.

ist für etwaige sonstige vertragliche Vereinbarungen zwischen dem DLR und dem Bund anzunehmen.

Von einer Kontrolle des Bundes über die aufgabenwahrnehmende Privatrechtsperson ist nach § 2 Abs. 2 Nr. 2 UIG ferner in Fällen eines beherrschenden Einflusses i.S. gesellschaftsrechtlicher Kontrolle auszugehen.[132] Die Vorschrift führt drei Fallgestaltungen auf, in denen Derartiges unwiderleglich vermutet wird: eine oder mehrere der in § 2 Abs. 2 Nr. 1 UIG genannten juristischen Personen des öffentlichen Rechts besitzen allein oder zusammen, unmittelbar oder mittelbar die Mehrheit des gezeichneten Kapitals des Unternehmens (lit. a), sie verfügen über die Mehrheit der mit den Anteilen des Unternehmens verbundenen Stimmrechte (lit. b) oder sie können mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des Unternehmens bestellen (lit. c). All dies trifft auf das DRL nicht zu. Abgesehen vom hier nicht maßgeblichen Ausschuss für Raumfahrt stellen Vertreter öffentlich-rechtlicher Körperschaften in keinem Gremium die Mehrheit der Mitglieder. Das gilt zumal für den Senat, dem die „Verwaltung, Leitung oder Aufsicht“ des DRL obliegt und dessen Mitglieder juristische Personen des öffentlichen Rechts nicht mehrheitlich bestellen können (§ 14 DLR-Satzung).[133] Im Ergebnis unterliegt das DRL damit nicht der Kontrolle des Bundes i.S. des § 2 Abs. 2 UIG und stellt somit keine informationspflichtige Stelle i.S. des § 2 Abs. 1 UIG dar, was unmittelbar zur Folge hat, dass es ebenso wenig als geodatenhaltende Stelle nach § 2 Abs. 1 i.V.m. § 3 Abs. 8 GeoZG zu qualifizieren war. Ansprüche auf der Grundlage dieses Gesetzes gegen das DRL – bzw. seine Untereinheiten[134] – schieden somit aus.

Bundespolizei

Fraglich war sodann, ob sich etwas anderes für die Bundespolizei als Stelle der öffentlichen Verwaltung (§ 2 Abs. 1 Nr. 1 S. 1 UIG i.V.m. § 3 Abs. 8 GeoZG) ergeben konnte, da sie die vom DLR erhobenen Geodaten zu einem späteren Zeitpunkt über das Echtzeitlagebild erhalten sollte. Dieser Umstand könnte möglicherweise dazu führen, dass sie selbst als datenhaltende Stelle zu qualifizieren wäre und somit einer entsprechenden Veröffentlichungspflicht unterliegen würde.

Darauf, dass die Bundespolizei die Daten nicht eigenständig erhebt, käme es nach dem GeoZG jedenfalls nicht an; vielmehr kann sie, auch wenn die in Rede stehenden Informationen durch andere Einrichtungen – wie hier das DLR – erstellt wurden, datenhaltende Stelle sein.[135]

---

[132] *Fluck/Theuer*, in: Fluck, Informationsfreiheitsrecht, § 2 UIG Rdnr. 220 ff.

[133] *Martini*/*Damm*, NJW 2014, 130 (133).

[134] Vgl. *Martini*/*Damm*, NJW 2014, 130 (133).

[135] Vgl. BT Drs. 10530, S. 16.

Problematisch erschien in diesem Kontext jedoch, das Echtzeitlagebild dem Anwendungsbereich des GeoZG zu unterstellen, da es sich hierbei lediglich um das Resultat der Aufbereitung verschiedener Informationen zu einem Schadensereignis (allgemeine Lage, Schadenslage, eigene Lage sowie Möglichkeiten der Schadensabwehr) handelte[136] und es insofern mit weiteren Informationen, die nicht Geodaten sind, angereichert werden sollte. Das Echtzeitlagebild selbst konnte daher nicht unter den Begriff der Geodaten subsumiert werden. Schon deshalb schied die Bundespolizei als geodatenhaltende Stelle aus.

Zu beachten war ferner § 4 Abs. 1 Nr. 3a) GeoZG, wonach die datenerstellende Institution ihrerseits datenhaltende Stelle sein muss,[137] was beim DLR – in diesem Fall – gerade nicht zutraf.[138]

Zwischenergebnis

Der persönliche Anwendungsbereich des GeoZG war nach alledem nicht eröffnet, sodass auf dessen weitere Vorgaben nicht näher eingegangen werden musste.

2.2.3 Umweltinformationsgesetz (UIG)

Ein Zugangsanspruch zu den im Rahmen des Projekts erhobenen Daten auf der Grundlage des § 3 Abs. 1 S. 1 UIG bestand hinsichtlich der im Projekt erhobenen Daten nicht: Wie bereits im Zusammenhang mit dem GeoZG dargelegt worden ist, handelt es sich weder bei dem datenerhebenden DLR noch bei der Bundespolizei See um informationspflichtige Stellen i.S. des § 2 Abs. 1 UIG. Es konnte folglich dahinstehen, ob die hier in Rede stehenden Daten als Umweltinformationen i.S. des § 2 Abs. 3 UIG zu gelten haben.

2.2.4 Informationsfreiheitsgesetz (IFG)

Als weiteres möglicherweise zu beachtende Gesetz kam das IFG in Betracht, dessen Zweck darin besteht, im Dienste der demokratischen Meinungs- und Willensbildung, sowie um eine gleichgewichtige Informationsverteilung von Staat und Bürgern herzustellen, jedermann

[136] Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK-Glossar: Ausgewählte zentrale Begriffe des Bevölkerungsschutzes, Bd. 8, Stand: Oktober 2011, S. 19.

[137] Vgl. § 4 Abs. 1 S. 1 Nr. 3a) aa) GeoZG sowie BT Drs. 10530, S. 16.

[138] Siehe die vorstehenden Ausführungen. Auch fällt das DLR nicht unter den Begriff des „Dritten“ iSd § 4 Abs. 1 Nr. 3b) GeoZG, da eine vertraglich eingegangene Verpflichtung, die im Rahmen der Forschungstätigkeit erhobenen Daten öffentlich zugänglich zu machen, nicht ersichtlich ist.

einen voraussetzungslosen[139] Anspruch gegenüber den Behörden des Bundes auf Zugang zu amtlichen Informationen zu verschaffen.[140]

2.2.4.1 Anwendungsbereich

Die Anwendbarkeit des IFG war hier nicht bereits deshalb ausgeschlossen, weil nach § 1 Abs. 3 IFG Regelungen in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen (mit Ausnahme des § 29 VwVfG und des § 25 SGB X) vorgehen; wie dargelegt, waren speziellere Gesetze wie das GeoZG[141] und das UIG vorliegend nicht anwendbar, so dass es an einer Normkollision fehlte.

Persönlicher Anwendungsbereich

Anspruchsverpflichtet sind neben den in § 1 Abs. 1 S. 1 IFG explizit genannten Behörden des Bundes auch sonstige Bundesorgane und -einrichtungen, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen (Satz 2). Den Behörden gleichgestellt finden sich natürliche Personen und juristische Personen des Privatrechts, soweit eine Behörde sich dieser Person(en) zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient (Satz 3).

DLR

Soweit es um das DLR ging, schied die persönliche Anwendbarkeit des IFG aus den bereits im Zusammenhang mit dem UIG dargelegten Gründen aus: Das DLR ist – in dem hier allein interessierenden Kontext forschungs- und entwicklungsbezogener Aufgabenwahrnehmung – keine Behörde (auch nicht in Gestalt eines Beliehenen, s. o.) und nimmt insoweit auch sonst keine öffentlich-rechtlichen Verwaltungsaufgaben wahr. Auch ist es nicht als Privatrechtssubjekt zu qualifizieren, dessen sich eine Behörde zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bediente. Hierunter fallen zwar, über die Konstellation der Verwaltungshilfe hinaus, sämtliche Kooperationsformen zwischen staatlichen Behörden und Privaten, insbesondere in Gestalt der Organisationsprivatisierung und der funktionalen Privatisierung.[142] Keine dieser Formen war jedoch im Fall der hier in Rede stehenden Forschungstätigkeit des DLR einschlägig.

---

[139] Gemeint ist, dass kein rechtliches und auch kein berechtigtes Interesse dargelegt werden muss, vgl. BT-Drs.15/4493, S. 6; *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 1 Rn. 18 f.

[140] Vgl. § 1 Abs. 1 IFG; dazu *Schrader*, ZUR 2005, 568 (571).

[141] Zur Spezialität des GeoZG gegenüber dem UIG *Martini*/*Damm*, NJW 2014, 130 (134).

[142] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 1 Rn. 117 f.

Bundespolizei

Dem persönlichen Anwendungsbereich des IFG unterfällt indes die am Verbundvorhaben beteiligte Bundespolizeibehörde, die nach § 1 Abs. 1 S. 1 IFG zum Adressatenkreis des Zugangsanspruches gehört.

Sachlicher Anwendungsbereich

Die bei der Bundespolizei vorhandenen – unter Einspeisung der durch das DLR erhobenen Geodaten erstellten – Echtzeitlagebilder mussten ferner tauglicher Gegenstand des Zugangsanspruchs nach § 1 Abs. 1 S. 1 IFG sein, was der Fall gewesen wäre, wenn es sich dabei um amtliche Informationen handelte. Der Begriff der amtlichen Information finden sich in § 2 Nr. 1 S. 1 IFG legal definiert als „jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung". Der weit verstandene Begriff der Aufzeichnung deckt unzweifelhaft auch die Echtzeitlagebilder ab, sofern diese, wovon vorliegend auszugehen war, auf einem Datenträger in beliebiger Form gespeichert wurden[143].

Sinn des weiteren Begriffselements „amtlichen Zwecken dienend" ist der Ausschluss privater Informationen, wobei es zur Abgrenzung einer funktionalen Betrachtung bedarf.[144] Amtlichen Zwecken dient eine Aufzeichnung, wenn sie bei Wahrnehmung einer öffentlich-rechtlichen Verwaltungsaufgabe aufgezeichnet wurde[145] oder in anderer Weise im Zusammenhang mit der amtlichen Tätigkeit steht.[146] Dass die Lagebilder im Rahmen eines Verbundforschungsvorhabens entstehen sollten, ist insoweit unschädlich, selbst wenn man – was allerdings kaum anzunehmen sein dürfte – den Beitrag der Bundespolizeibehörde zum Forschungsvorhaben nicht als deren amtliche Tätigkeit ansehen wollte. Entscheidend war letztlich, dass jener Beitrag der Effektivierung der zukünftigen Aufgabenwahrnehmung der Bundespolizeibehörde dient, er also in einem ausreichenden Zusammenhang mit deren amtlicher Tätigkeit steht. Bei den Echtzeitlagebildern handelt es sich folglich um amtliche Informationen i.S. des IFG.

2.2.4.2 Ausschlussgründe nach § 3 IFG

Insofern musste untersucht werden, ob der Informationszugangsanspruch zum Schutz besonderer, in § 3 IFG abschließend benannter, öffentlicher Belange ausgeschlossen war.

[143] Vgl. *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 2 Rn. 20 f.

[144] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 2 Rn. 37.

[145] *Augsberg*, DVBl. 2007, 733 (739); *Sitsen*, Das Informationsfreiheitsgesetz des Bundes, 2009, S. 144.

[146] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 1 Rn. 38.

Möglichkeit nachteiliger Auswirkungen auf Belange der inneren oder äußeren Sicherheit (Nr. 1 lit. c))

Nach Nr. 1 der Vorschrift besteht der Zugangsanspruch nicht, wenn das Bekanntwerden der Information nachteilige Auswirkungen auf näher bezeichnete Bundesinteressen haben kann. In Betracht kamen hier die in lit. c) genannten „Belange der inneren oder äußeren Sicherheit". Das betrifft nach der Entwurfsbegründung den nichtmilitärischen Sicherheitsbereich, welcher eigens von Nr. 1 lit b) der Vorschrift erfasst wird.[147]

Zieht man zur Begriffsbestimmung des Schutzguts „Belange der inneren oder äußeren Sicherheit" andere einschlägige gesetzliche Regelungen heran, etwa die Strafvorschrift des § 92 Abs. 3 Nr. 2 StGB, so wird deutlich, dass nur *erhebliche* Belange der Bundesrepublik Deutschland geschützt sind.[148] Gemeint ist die Sicherheit des Staates als solche gegenüber Störungen seiner Funktionsfähigkeit und der freiheitlich demokratischen Grundordnung durch gewaltsame Einwirkungen oder die Drohung hiermit.[149] Dieser Schutz soll sich u.a. auf entsprechend sicherheitsrelevante Informationen der Nachrichtendienste und auch der Polizeibehörden des Bundes richten.[150] Die im Rahmen des Forschungsvorhabens erstellten Echtzeitlagebilder können als derartige schutzbedürftige Informationen angesehen werden, sofern die Einsichtnahme durch jedermann Rückschlüsse auf die künftige Aufgabenwahrnehmung, d.h. die Tätigkeit zur Abwehr von Gefahren für die maritime Sicherheit, gestattet.

Erforderlich, aber auch ausreichend ist im Weiteren die bloße Möglichkeit nachteiliger Auswirkungen auf das einschlägige Schutzgut, wobei die Behörde eine Darlegungs- und Begründungslast trifft.[151] Voraussetzung ist das Bestehen einer Gefährdungslage,[152] hier für die innere oder äußere Sicherheit. Davon war nach dem eben Gesagten auszugehen, so dass ein Zugangsanspruch nach dem IFG gem. § 3 Nr. 1 lit. c) IFG ausgeschlossen ist.

Gefährdung der öffentlichen Sicherheit (Nr. 2)

Es musste ferner geprüft werden, ob auch der Ausschlussgrund nach Nr. 2 einschlägig ist, wonach ein Informationszugangsanspruch nicht besteht, wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann. Der aus dem Gefahrenabwehrrecht übernommene Begriff umfasst die Unversehrtheit der Rechtsordnung und der grundlegenden Einrichtungen und Veranstaltungen des Staates ebenso wie die

[147] BT-Drs. 15/4493, S. 9.

[148] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 3 Rn. 33.

[149] *Sitsen*, Das Informationsfreiheitsgesetz des Bundes, 2009, S. 161.

[150] *Sitsen*, wie vor.

[151] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 3 Rn. 93 ff.

[152] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 3 Rn. 97.

Unversehrtheit privater Rechtsgüter der Bürger.[153] Exemplarisch führt die Entwurfsbegründung zum IFG u.a. das berechtigte Interesse an, sensible verwaltungsinterne Abläufe und Strukturen, etwa Anzahl, Art und Einsatz von Führungs- und Einsatzmitteln, Ausstattungs- und Einsatzkonzepte der Polizeien des Bundes, Vorbereitungen von Planungsentscheidungen für Alarmierungsfälle etc.) vor Bekanntwerden zu schützen.[154] Ungeachtet der Reichweite des Schutzguts der öffentlichen Sicherheit im Übrigen sind bei derart sensiblen Schutzobjekten nach zutreffender Sicht kaum gesteigerte Anforderungen an die Gefährdung dieser Belange, d.h. an die Wahrscheinlichkeit eines Schadenseintritts, zu stellen.[155] Geht man davon aus, dass das Bekanntwerden der Echtzeitlagebilder die Effektivität der Tätigkeit der Bundespolizei im Bereich der Gefahrenabwehr für die maritime Sicherheit künftig beeinträchtigen oder gar vereiteln kann, insofern also eine konkrete Gefahr besteht, dann sind die Voraussetzungen des Ausschlussgrundes nach Nr. 2 gegeben.

Zur Kollision des Zugangsanspruchs mit der Forschungsfreiheit i.S.v. Art. 5 Abs. 3 S. 1 GG

Während es sich bei den beiden vorstehend behandelten Ausschlussgründen um solche handelt, die die Wahrnehmung hoheitlicher (Gefahrenabwehr-)Aufgaben der Bundespolizeibehörde betreffen, stellte sich im Weiteren die Frage, ob und ggf. inwieweit das IFG auch dem Spezifikum Rechnung trägt, dass es vorliegend um ein Forschungsvorhaben und die in dessen Rahmen gewonnenen Informationen ging. Angesichts dessen tritt eine Spannungslage zwischen dem Informationsinteresse der Bürger einerseits und der grundrechtlich geschützten Forschungsfreiheit der Projektpartner (Art. 5 Abs. 3 S. 1 GG) deutlich zu Tage.[156]

Soweit sich die am Verbundvorhaben beteiligten Forschungsnehmer auf die Wissenschaftsfreiheit in ihrer Ausprägung als Forschungsfreiheit berufen konnten, so musste diese Grundrechtsposition bei der Entscheidung über das Bestehen eines Informationszugangsanspruchs nach § 1 Abs. 1 S. 1 IFG Berücksichtigung finden, anders gewendet: der einfachgesetzliche Anspruch kann nur in den Grenzen des verfassungsrechtlich gebotenen Grundrechtsschutzes bestehen. In erster Linie ist es Aufgabe des Gesetzgebers, ggf. betroffenen Grundrechtspositionen bei der Ausgestaltung der Zugangsvoraussetzungen des Informationsrechts zur Durchsetzung zu verhelfen und insbesondere geeignete Kollisionsregeln aufzustellen. Vorrangig musste also danach gefragt werden, ob die gesetzlichen Schutzvorschriften, die einem Zugangsanspruch entgegenstehen, diesem Erfordernis im Hinblick auf die Forschungsfreiheit genügen. Hierbei müssen, im Anschluss an das Bundesverfassungsgericht, die gesetzlichen Vorschriften im

[153] BT-Drs. 15/4493, S. 93; *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 3 Rn. 103.

[154] BT-Drs. 15/4493, S. 10.

[155] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 3 Rn. 107.

[156] Vgl. *Bretthauer*, NVwZ 2012, 1144 (1144).

Zweifel so ausgelegt werden, dass die Wirkkraft der Grundrechtsnorm so weit wie möglich entfaltet wird (Grundsatz der größtmöglichen Grundrechtseffektivität).[157]

Dieser Anforderung ist in der Rechtsprechung insoweit Rechnung getragen worden, als Tätigkeiten, die unter die Forschungsfreiheit fallen, dem Schutz geistigen Eigentums i.S. des § 6 S. 1 IFG unterstellt worden sind.[158] Für die(se) weite Auslegung des Begriffs „geistiges Eigentum“ ist zum einen auf die Begründung des Gesetzentwurfes zum IFG[159] verwiesen worden, wonach zum geistigen Eigentum – neben dem Urheberrecht und den gewerblichen Schutzrechten – auch die Tätigkeit von Hochschulen und Forschungseinrichtungen in Kunst, Wissenschaft, Forschung und Lehre nach Art. 5 Abs. 3 GG gehören soll.[160] Nichts anderes konnte dann aber für die Teilnahme der öffentlichen Hand als Forschungsnehmer an Verbundforschungsvorhaben gelten. Ferner sind die Regelungen einiger Informationsfreiheitsgesetze auf Länderebene herangezogen worden, deren Geltungsbereich sich aus Gründen des Art. 5 Abs. 3 S. 1 GG explizit nicht auf den Bereich von Forschung und Lehre erstreckt (s. § 2 Abs. 5 ThürIFG, § 2 Abs. 3 IFGNRW).[161] Unter Berücksichtigung der Ausführungen in der Begründung des Gesetzentwurfes zum IFG des Bundes ist hieraus zutreffend abgeleitet worden, dass der Bundesgesetzgeber das Grundrecht der Wissenschaftsfreiheit – trotz fehlender gesetzlicher Klarstellung im IFG – in gleichem Maße achten wollte.[162]

Dies zugrunde gelegt, ergab sich vorliegend Folgendes: Sämtliche wissenschaftlichen Erkenntnisse, die im Verlauf des Verbundforschungsprojekts gewonnen wurden, unterfallen dem sachlichen Schutzbereich des Art. 5 Abs. 3 S. 1 GG. Sie stellen sich nach Inhalt und Form als Resultate eines „ernsthaften planmäßigen Versuchs zur Ermittlung der Wahrheit“, mithin als wissenschaftliche Betätigung dar.[163] Der Schutz der Wissenschaftsfreiheit erstreckt sich indes nicht nur auf die Art und Weise der Erkenntnisgewinnung, sondern auch auf die Entscheidung, ob, wie und wann die Forschungsergebnisse anderen zugänglich gemacht, insbesondere veröffentlicht werden sollen.[164] Der persönliche Schutzbereich des Grundrechts erfasst alle wissenschaftlich Tätigen, auch wenn es sich um juristische Personen des öffentlichen Rechts handelt,[165] die sich an Verbundforschungsvorhaben beteiligen.

---

[157] BVerfGE 39, 1 (38).

[158] VG Braunschweig, Urteil v. 26.06.2013 – 5 A 33/11 -, juris.

[159] BT-Drs. 15/4493, S. 14;

[160] VG Braunschweig, Urteil v. 26.06.2013 – 5 A 33/11 -, juris, Rn. 21; auch *Bretthauer*, NVwZ 2012, 1144 (1147).

[161] VG Braunschweig, Urteil v. 26.06.2013 – 5 A 33/11 -, juris, Rn. 21.

[162] VG Braunschweig, wie vor.

[163] BVerfGE 35, 79 (113); BVerfGE 90, 1 (12).

[164] VG Braunschweig, Urteil v. 26.06.2013 – 5 A 33/11 -, juris, Rn. 24.

[165] *Jarass*, in: Jarass/Pieroth, Grundgesetz, 13. Aufl. 2014, Rn. 141.

Gebietet also eine effektive Grundrechtsverwirklichung eine Interpretation des § 6 S. 1 IFG, der zufolge auch Ergebnisse wissenschaftlicher Forschung, an deren Generierung Anspruchsverpflichtete nach § 1 Abs. 1 IFG beteiligt sind, als „geistiges Eigentum“ zu verstehen sind, und kommt es im Einzelfall zu einer Kollisionslage zwischen dem Recht am geistigen Eigentum und dem Informationszugangsanspruch, so folgt daraus unmittelbar der Ausschluss des Letzteren. Von einer Kollisionslage i.d.S. ist auszugehen, sofern das betreffende Schutzrecht seinem Inhaber ein „Informationsrestriktionsrecht“ vermittelt.[166] Das war hier der Fall: Wie vorstehend dargelegt, ist der Forschungsfreiheit ein umfassendes Selbstbestimmungsrecht im Hinblick auf die Bekanntmachung und Herausgabe von Forschungsmaterial an Dritte immanent. Der Schutz dieses verfassungskräftigen Rechts steht gem. § 6 S. 1 IFG etwaigen Informationszugangsansprüchen nach § 1 Abs. 1 IFG absolut entgegen, ohne dass es noch einer Abwägung der widerstreitenden Positionen bedürfte: § 6 S. 1 IFG enthält keine Abwägungsklausel[167], vielmehr stellt die Vorschrift ihrerseits bereits das (verfassungskonforme) Ergebnis einer gesetzgeberischen Abwägungsentscheidung zugunsten der erfassten Schutzrechte – hier der Forschungsfreiheit – dar.[168]

2.2.5 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Mit dem IT-Sicherheitsgesetz[169] vom 17. Juli 2015 wurden eine Reihe von Gesetzesänderungen für den Bereich IT-Sicherheit beschlossen. Die Einhaltung von Sicherheitsstandards sowie die Vertraulichkeit von Informationen, insbesondere im Bereich kritischer Infrastrukturen, sind dabei von zentraler Bedeutung. Vorrangig betroffen von diesen Änderungen war das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[170] (BSI – Gesetz). Im Folgenden war daher weiter zu untersuchen, ob der Betrieb eines Echtzeitlagebildes eine kritische Infrastruktur im Sinne dieses Gesetzes darstellt.

Anwendungsbereich

Persönlicher Anwendungsbereich

[166] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 6 Rn. 18.

[167] *Schoch*, Informationsfreiheitsgesetz, Kommentar, 2009, § 6 Rn. 38.

[168] Es handelt sich insoweit um die verfassungsgebotene Abwägung zwischen der schrankenlos gewährleisteten Wissenschaftsfreiheit und dem – dem Informationsanspruch zugrundeliegenden – Demokratiegebot (Art. 20 Abs. 1 GG), dazu näher VG Braunschweig, Urteil v. 26.06.2013 – 5 A 33/11 -, juris, Rn. 26 ff.

[169] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. I S. 1324 (Nr. 31).

[170] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das durch Artikel 3 Absatz 6 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist.

Der persönliche Anwendungsbereich des BSIG ist nach § 8c BSIG rechtsformunabhängig.[171] Ausnahmen bestehen lediglich in den dort genannten Fällen. Welche Unternehmen am Ende zum Kreis der Adressaten nach § 2 Abs. 10 BSIG gehören, war bisher nicht ersichtlich, da durch § 10 Abs. 1 BSIG näheres durch Rechtsverordnung bestimmt werden sollte.[172] Mit der Verabschiedung einer ersten Verordnung auf Grundlage des § 10 Abs. 1 BSIG, der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“[173] (BSI-KritisV), sind erstmals Regelungen hierzu getroffen worden. Die Anwendung des BSIG bestimmt sich demnach nach der Einordnung einer kritischen Dienstleistung in einen bestimmten Sektor sowie dem Überschreiten eines durch die Verordnung festgelegten Schwellenwertes.[174] Sofern mit dem Echtzeitlagebild eine kritische Infrastruktur betrieben wird und kein Ausschluss nach § 8c BSIG vorliegt, ist unabhängig von der Organisationform des Betreibers auch der persönliche Anwendungsbereich eröffnet. Ob die genannten Voraussetzungen vorliegen, musste die Prüfung des sachlichen Anwendungsbereichs ergeben.

Sachlicher Anwendungsbereich

In den sachlichen Anwendungsbereich fallen Betreiber kritischer Infrastrukturen nach § 2 Abs. 10 BSIG. Mögliche Infrastrukturen sind danach „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören“ (§ 2 Abs. 10 S. 1 Nr. 1 BSIG) Um als kritisch eingestuft werden zu können, müssen sie nach § 2 Abs. 10 S. 1 Nr. 2 „von hoher Bedeutung für das Funktionieren des Gemeinwesens […] [sein], weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Die somit in Betracht kommenden Infrastrukturen werden durch die Rechtsverordnung nach § 10 Abs. 1 BSIG, der BSI-KritisV, näher bestimmt (§ 2 Abs. 10 S. 2 BSIG). Diese nimmt in den §§ 2 bis 5 eine nach Sektoren gegliederte abschließende Einteilung von Dienstleistungen vor, die dem Bereich kritischer Infrastrukturen zuzuordnen sind.[175] Es handelt sich dabei um die Sektoren „Energie“, „Wasser“, „Ernährung“ sowie „Informationstechnik und Telekommunikation“. Fraglich war an dieser Stelle also, ob das Echtzeitlagebild als eine kritische Dienstleistung im vorgenannten Sinne verstanden werden konnte.

[171] Vgl. BT Drs. 18/4096, S. 29.

[172] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22.04.2016, BGBl. I S. 958 (Nr. 20).

[173] Vgl. *Bräutigam/Wilmer*, Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38, 39.

[174] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22.04.2016, BGBl. I S. 958 (Nr. 20), S. 2.

[175] Vgl. BT Drs. 18/4096, S. 31.

Denkbar war dabei eine Zuordnung zum Bereich der Informationstechnik und Telekommunikation. Als kritische Dienstleistungen für diesen Sektor benennt die BSI-KritisV Sprach- und Datenübertragungen (§ 5 Abs. 1 Nr. 1) sowie Datenspeicherung und –verarbeitung (§ 5 Abs. 1 Nr. 2).[176] Während Sprach- und Datenübertragungen dem Versorgungsbereich Telefonie und Internet zuzuordnen sind, gehören zu Nr. 2 auch der Bereich Housing (Betrieb von Rechenzentren) und IT-Hosting mittels Serverfarmen.[177] Die Schwellenwerte betragen dabei für Rechenzentren 5 Megawatt und für Serverfarmen in einer Anzahl von 25.000 Computern bzw. virtuellen Servern,[178] um als kritische Infrastruktur im Sinne der Verordnung zu gelten. Abhängig von der für den Betrieb eines Echtzeitlagebildes notwendigen IT-Infrastruktur könnte sich hieraus die Zugehörigkeit zu einer kritischen Infrastruktur im Sinne des BSIG ergeben. Dann müsste ihr Ausfall allerdings zu „erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen“ (s.o.). Das war hier allerdings nicht zu befürchten. Das Echtzeitlagebild soll zwar zur Optimierung der maritimen Sicherheit beitragen, es war jedoch nicht ersichtlich, dass ein Ausfall der (noch zu implementierenden) Technologie (künftig) zu den Beeinträchtigungen der bezeichneten Art führen würde. Es konnte folglich nicht angenommen werden, dass der Betreiber des maritimen Echtzeitlagebildes im Bereich einer kritischen Infrastruktur tätig wird. Folglich ist das BSIG weder in sachlicher noch in persönlicher Hinsicht anwendbar.

2.2.6 Telemediengesetz (TMG)

Auch das Telemediengesetz[179] (TMG) regelt den Umgang mit informationstechnischen Diensten und war daher in die Betrachtung mit einzubeziehen.

2.2.6.1 Anwendungsbereich

Persönlicher Anwendungsbereich

In den persönlichen Anwendungsbereich des TMG fallen alle Anbieter von elektronischen Informations- und Kommunikationsdiensten (Telemedien), einschließlich öffentlicher Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird. Als Anbieten wird dabei nach § 2 Nr. 1 TMG das Bereithalten von Telemedien zur Nutzung oder die Vermittlung des

[176] Vgl. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22.04.2016, BGBl. I S. 958 (Nr. 20).

[177] Vgl. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22.04.2016, BGBl. I S. 958 (Nr. 20).

[178] Vgl. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22.04.2016, BGBl. I S. 958 (Nr. 20).

[179] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist.

Zugangs zur Nutzung verstanden. Vorliegend liegt der Sinn von Echtzeitbildern gerade in der Nutzung dieser und auch in der Vermittlung zur Nutzung durch Dritte. Die Betreiber des Echtzeitlagebildes fallen dementsprechend in den persönlichen Anwendungsbereich des Gesetzes.

Räumlicher Anwendungsbereich

Nach § 3 Abs. 1 TMG findet das TMG für niedergelassene Diensteanbieter in der Bundesrepublik Deutschland Anwendung. Dabei stellt § 2 Nr. 2 TMG klar, dass der Standort der technischen Einrichtung allein keine Niederlassung des Anbieters begründet. Dieses soll sich vielmehr danach richten, an welchem Ort die Steuerung des Diensteanbieters erfolgt.[180] Von einer Steuerung innerhalb der Bundesrepublik Deutschland konnte hier ausgegangen werden. Der räumliche Anwendungsbereich des TMG war sonach eröffnet.

Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich des § 1 Abs. 1 TMG umfasst alle Informations- und Kommunikationsdienste (IuK-Dienste), soweit sie nicht Telekommunikation im Sinne des § 3 Nr. 24 des Telekommunikationsgesetzes[181] (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind. Die vom TMG erfassten Dienstleistungen sollen elektronisch erbrachte multimediale Angebote sein, deren Zweck in der Bereitstellung von Inhalten liegt.[182] Eine reine Übertragungsleistung liegt dann vor, wenn es sich nur um eine technische Transportleistung handelt.[183] In diesem Fall ist die Anwendung des TMG ausgeschlossen. Telekommunikationsgestützte Dienste im Sinne von § 3 Nr. 25 TKG sind solche Dienstleistungen, die über reine „Sprachtelefonie“ hinausgehen und während der Telekommunikationsverbindung eine Inhaltsleistung bieten.[184]

Durch das im Verbund durchgeführte Projekt sollte die Erstellung eines gemeinsamen Echtzeitlagebildes auf der Grundlage von AIS-Daten, hochaufgelösten Satelliteninformationen und multispektralen Mehrkamerasystemen ermöglicht werden. Diese Datenflüsse sollten verdichtet zu einem möglichst realitätsgetreuen Lagebild in Echtzeit für den Endanwender führen. Damit wurden nicht nur Signale durch die verschiedenen Systeme übermittelt, sondern auch Daten für einen elektronischen

[180] *Ricke*, in: Spindler/Schuster, Das Recht der elektronischen Medien, TMG, 3. Auflage 2015, § 2 Rn. 6.

[181] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 14 des Gesetzes vom 24. Mai 2016 (BGBl. I S. 1217) geändert worden ist.

[182] Vgl. *Ricke*, in: Spindler/Schuster, Das Recht der elektronischen Medien, TMG, 3. Auflage 2015, § 1 Rn. 4f.

[183] Vgl. *Schütz*, in: Beck´scher TKG-Kommentar, 4. Auflage 2013, § 3 Rn. 79.

[184] Vgl. *Ditscheid*, in: Beck´scher TKG-Kommentar, 4. Auflage 2013, § 3 Rn. 80.

Informationsdienst iSd § 1 Abs. 1 Satz 1 TMG aufbereitet. Der geplante Informationsdienst (Echtzeitlagebild) besteht weder ganz noch überwiegend in der Übertragung von Signalen, sondern zum größten Teil in der Verdichtung von Daten zu einer für den Endanwender nutzbaren Informationsquelle, um Gefahren für die maritime Sicherheit abzuwenden. Folglich liegen Telemedien im Sinne des § 1 Abs. 1 Satz 1 TMG vor. Ein Ausschluss des TMG durch die Regelungen des TKG war nicht gegeben und der sachliche Anwendungsbereich mithin eröffnet, sodass die Regelungen des Telemediengesetzes beachtet werden mussten.

2.2.6.2 Datenschutzrechtliche Regelungen

Von Interesse waren hier v.a. datenschutzrechtliche Vorgaben, die sich im Abschnitt 4 des TMG in den §§ 11 – 15 finden. Datenschutzvorschriften dieses Abschnitts betreffen indes nur das Anbieter-Nutzer-Verhältnis iSd § 11 TMG. Gemäß § 11 Abs. 2 TMG gelten als Nutzer nur natürliche Personen. Die Regelungen des 4. Abschnittes des TMG sind dagegen nicht anwendbar, soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken (§ 11 Abs. 1 Satz 1 Nr. 1) oder innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessoren erfolgt (§ 11 Abs. 1 Satz 1 Nr. 2). Durch das TMG sind jedoch nur solche personenbezogenen Daten geschützt, die erst bei der Nutzung von Telemedien entstehen und Personenbezug aufweisen.[185] Für die Zusammenführung der Daten zu einem Echtzeitlagebildes sind die datenschutzrechtlichen Vorgaben folglich nicht zu beachten. Die Daten der von der Datenerhebung betroffenen Personen werden in dieser Phase vielmehr durch die Regelungen des Bundesdatenschutzgesetzes (BDSG) geschützt.[186] Lediglich im späteren Anbieter-Nutzer-Verhältnis zwischen Betreiber und Endanwender des Echtzeitlagebildes könnte das TMG insofern Anwendung finden.

Die Regelungen zum Datenschutz im TMG waren für den Untersuchungsgegenstand daher nicht weiter zu überprüfen.

2.2.6.3 Informationspflichten

Weiter zu beachtende Regelungen zur Zulassung und zu Informationspflichten für Diensteanbieter fanden sich sodann im 2. Abschnitt des TMG. Nach § 4 TMG besteht für Telemedien keine Zulassungs- oder Anmeldepflicht. Diensteanbieter haben jedoch eine allgemeine Informationspflicht aus § 5 TMG zu beachten. Diese umfasst u.a. eine Kennzeichnung des Dienstes mit Namen und Anschrift des Diensteanbieters sowie der

[185] Vgl. *Spindler/Nink*, in: Spindler/Schuster, Das Recht der elektronischen Medien, TMG, 3. Auflage 2015

[186] *Spindler/Nink,* in: Spindler/Schuster, Das Recht der elektronischen Medien, TMG, 3. Auflage 2015, § 11 Rn. 27.

Rechtsform bei juristischen Personen. Auch Daten zur Kontaktaufnahme und die Registereintragung sind zu nennen.

2.2.7 Telekommunikationsgesetz (TKG)

Weiter war zu prüfen, ob auch das Telekommunikationsgesetz[187] (TKG) einschlägig ist. Eine Anwendung des TKG ist grundsätzlich nicht durch die Anwendung des TMG ausgeschlossen.[188] Datenschutzrechtliche Regelungen finden sich in den §§ 91ff. TKG. Nach § 91 Abs. 1 TKG werden nur personenbezogene Daten der Teilnehmer und Nutzer von Telekommunikation geschützt. Gemäß § 3 Nr. 20 TKG ist Teilnehmer jede natürliche oder juristische Person, die mit einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat. Nutzer sind nach § 3 Nr. 14 TKG natürliche oder juristische Personen, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nehmen oder beantragen, ohne notwendigerweise Teilnehmer zu sein. Beide Adressaten für den Schutz personenbezogener Daten nach dem TKG müssen damit als Teilnehmer bzw. als Nutzer in einem öffentlich zugänglichen Telekommunikationsdienst agieren.[189] Hier wurde mit dem Betrieb eines Echtzeitlagebildes nicht beabsichtigt, dieses der Öffentlichkeit zugänglich zu machen. Vielmehr soll der Zugang künftig nur durch autorisierte Stellen erfolgen.

Die datenschutzrechtlichen Regelungen des Telekommunikationsgesetzes mussten für das Verbundvorhaben folglich nicht beachtet werden.

2.2.8 Bundesdatenschutzgesetz (BDSG)[190]

Weiter mussten neben den bereits behandelten speziellen Gesetzen auch die allgemeinen Vorgaben des Bundesdatenschutzgesetzes (BDSG) bei der Erhebung von Daten sowie deren Speicherung im Rahmen eines Echtzeitsystems beachtet werden. Insbesondere galt dies mit Blick auf den Personenbezug von Geodaten. In der Praxis tritt der Personenbezug dann auf, wenn zum Beispiel durch besagte Daten die „Lokalisierung einer Person“ oder „die Lokalisierung einer beweglichen Sache, die einer bestimmten Person zugeordnet wird bzw. zugeordnet werden kann“, möglich ist.[191] Techniken, welche die Lokalisierung von Objekten ermöglichen und zum Zwecke der Sicherheit implementiert werden, sind ein

[187] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 14 des Gesetzes vom 24. Mai 2016 (BGBl. I S. 1217) geändert worden ist.

[188] *Eckhardt*, in: Spindler/Schuster, Das Recht der elektronischen Medien, TKG § 91 Rn. 8.

[189] *Eckhardt*, in: Spindler/Schuster, Das Recht der elektronischen Medien, TKG § 91 Rn. 16.

[190] Vgl. Fn. 7.

[191] *Weichert*, Der Personenbezug von Geodaten, DuD 2007, Heft 31, 1 (2).

zukunftsrelevantes Thema.[192] Neben den positiven Aspekten einer solchen neuartigen Technologie, ist stets auch auf einen adäquaten Umgang mit personenbezogenen Daten und den mit der Erhebung verbundenen Zweck zu achten.[193] Den Schutz personenbezogener Daten stellt auf nationaler Ebene v.a. das BDSG sicher, sodass dessen Vorgaben der näheren Untersuchung unterzogen werden mussten.

2.2.8.1 Anwendungsbereich

Fraglich war dabei zunächst, ob bei der Erhebung von Geodaten im vorliegenden Fall das BDSG in persönlicher, räumlicher und sachlicher Hinsicht Anwendung finden konnte.

Persönlicher Anwendungsbereich

In persönlicher Hinsicht gilt das BDSG gem. § 1 Abs. 2 für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen. Für öffentliche Stellen trifft das Gesetz eine Unterscheidung zwischen solchen des Bundes und der Länder. Letztere fallen indes nach § 1 Abs. 2 Nr. 2 BDSG nur dann in den Anwendungsbereich, wenn der Datenschutz nicht bereits durch eigene Landesgesetze geregelt ist.[194]

Nicht-öffentliche Stellen sind erfasst, sofern „sie die Daten unter Einsatz von Datenverarbeitungsanlagen bzw. in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben“, § 1 Abs. 2 Nr. 3 BDSG.

Es war folglich danach zu fragen, ob es sich beim DLR-RY, welches hier die AIS-Daten erhoben hat, um eine öffentliche oder nicht-öffentliche Stelle iSd Gesetzes handelt.

Öffentliche Stellen des Bundes sind nach der Legaldefinition des § 2 Abs. 1 S. 1 BDSG „die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.“

Als eingetragener Verein handelt es sich beim DLR um eine juristische Person des Privatrechts; auch eine Subsumtion unter den Behördenbegriff als sog. Beliehener kam

[192] So zB in der Automobilbranche, vgl. Roßnagel, Grundrechtsausgleich beim vernetzten Automobil, Datenschutz und Datensicherheit, Heft 6/2015, 353.

[193] Vgl. Roßnagel, Grundrechtsausgleich beim vernetzten Automobil, Datenschutz und Datensicherheit, Heft 6/2015, 353 (356).

[194] Da alle Bundesländer von ihrer Möglichkeit zur Regelung des Datenschutzes Gebrauch gemacht haben, ist die Vorschrift praktisch gegenstandslos, vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 1 Rn. 19a.

vorliegend nicht Betracht.[195] Bei dem DLR handelt es sich folglich um eine nicht-öffentliche Stelle iSd § 2 Abs. 4 S. 1 BDSG,[196] sodass der persönliche Anwendungsbereich des BDSG eröffnet war.

Räumlicher Anwendungsbereich

Weiter musste das BDSG auch räumlich anwendbar sein. Hier wurde es als problematisch betrachtet, dass die in EMSec empfangenen Geodaten über die räumliche Lage von Schiffen nicht nur aus dem Bereich des Küstenmeeres stammen, welches gem. Art. 2 Abs. 1 des Seerechtsübereinkommens der Vereinten Nationen[197] zum Hoheitsgebiet der Bundesrepublik Deutschland zählt, sondern die Schiffspositionen darüber hinaus auch in weiter entfernten Gebieten bestimmt werden konnten.[198]

Aus den Gesetzgebungsmaterialen zum BDSG geht indes hervor, dass es insofern bei grenzüberschreitenden Datenverkehr nicht auf den Verarbeitungsort ankommt, sondern der Sitz der verantwortlichen Stelle (Sitzprinzip) entscheidend ist.[199] Vorliegend hat das DLR-RY als verarbeitende Stelle für die erhobenen Daten seinen Sitz im Inland. Folglich war das BDSG auch räumlich anwendbar.

Sachlicher Anwendungsbereich

Schließlich musste auch der sachliche Anwendungsbereich eröffnet sein. Da das BDSG ausschließlich für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt, vgl. § 1 Abs. 2 BDSG, war in erster Linie danach zu fragen, ob Geodaten den geforderten Personenbezug aufweisen können. Gem. § 3 Abs. 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Untersuchungsbedürftig war daher zunächst, ob es sich bei den von der Datenerhebung Betroffenen um „bestimmte oder bestimmbare“ Personen handelt.

---

[195] S. o. unter Punkt II. 2.2.2.

[196] Danach sind nicht-öffentliche Stellen u.a. juristische Personen des Privatrechts, die keine öffentlichen Stellen iSd § 2 Abs. 1-3 BDSG darstellen, vgl. § 2 Abs. 4 S. 2 BDSG.

[197] Seerechtsübereinkommens der Vereinten Nationen vom 10. Dezember 1982 (BGBl. 1994 II S. 1798).

[198] Das Küstenmeer umfasst nach Art. 2, 3 SRÜ eine Zone von höchstens 12 Seemeilen gerechnet ab der Basislinie (Niedrigwasserlinie, vgl. Art. 5 SRÜ) des jeweiligen Staates. In diesem Gebiet ist die nationale Rechtsordnung des jeweiligen Staates vollumfänglich anwendbar. An das Küstenmeer schließt die ausschließliche Wirtschaftszone (AWZ) an, die sich maximal 200 Seemeilen von den Basislinien ausgehend erstreckt, vgl. Art. 57 SRÜ. In dieser Zone besitzt ein Staat lediglich souveräne Rechte und Hoheitsbefugnisse, vgl. Art. 56 Abs. 1 lit. a SRÜ und Art. 56 Abs. 1 lit. b SRÜ. Abschließend bilden der Festlandsockel (Vgl. Art. 76ff. SRÜ) und die Hohe See (Vgl. Art. 88ff. SRÜ) die weiteren Meereszonen.

[199] Vgl. BT Drs. 14/4329, S. 31.

Bestimmbarkeit

Bei Geodaten handelt es sich grds. um „digitale Informationen, deren räumliche Lage auf der Erdoberfläche ausgewiesen ist.“[200] Sie erfüllen das Merkmal der Bestimmbarkeit, „wenn sie Informationen über eine bestimmte oder bestimmbare Person vermitteln“[201]. Problematisch erschien insofern, dass im Projekt EMSec hauptsächlich Daten über das Schiff als Gegenstand und damit Sachinformationen gesammelt wurden. Ein Personenbezug konnte sich demzufolge allein über eine Beziehung der „natürlichen Person“ zu der „Sachinformation“ herstellen lassen.

Wann eine solche Verbindung vorliegt, ist jedoch umstritten.[202] Eine Ansicht sieht die Personenbezogenheit als gegeben an, wenn die verarbeitende Stelle diese selbst mit eigenen Mitteln oder unter Zuhilfenahme von externem Know-how herstellen könnte.[203] Dieses sogenannte Zusatzwissen wird jedoch nur miteinbezogen, sofern es nicht einen unverhältnismäßigen Aufwand erfordert dieses zu erwerben.[204] Die Bestimmbarkeit eines Personenbezuges wird nach dieser Auffassung weit ausgelegt und nicht nur nach den Möglichkeiten der verantwortlichen Stelle beurteilt. Dieser Ansatz wird deshalb auch als objektiver Ansatz bezeichnet.[205]

Die konträre Auffassung geht dagegen davon aus, dass ein Personenbezug nur in dem Fall vorliegt, wenn „die Stelle den Bezug mit den ihr zur Verfügung stehenden Mitteln und ohne unverhältnismäßigen Aufwand herstellen kann“.[206] Hierbei wird allein auf das Können der datenverarbeitenden Stelle abgestellt.

Fraglich war zudem, ob jede Art von zusätzlich beschafftem Wissen dazu geeignet ist, einen Personenbezug herzustellen, da zumindest in Teilen der Literatur vertreten wird, dass der Einsatz von Zusatzwissen grundsätzlich nur dann zu berücksichtigen sei, wenn sich die Verwendung weder als Vertrags- noch als Gesetzesverstoß darstelle.[207] Für die Beurteilung ob es sich um Zusatzwissen handelt, sei entscheidend, wie schwierig sich Zugang zu den relevanten Informationen verschafft werden könne, da für dieses unterschiedliche

[200] *Dammann* in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 58.

[201] *Karg*, Datenschutz für Geodaten, DuD 2010, Heft 12, 824 (828).

[202] Vgl. *Karg*, Datenschutz für Geodaten, DuD 2010, Heft 12, 824 (828).

[203] *Dammann*, in: Simitis, BDSG, 8. Auflage 2014, § 3 Rn. 26.

[204] *Dammann*, in: Simitis, BDSG, 8. Auflage 2014, § 3 Rn. 26.

[205] Vgl. *Forgó/Krügel*, Der Personenbezug von Geodaten, MMR 2010, Heft 1, 17 (18).

[206] *Karg*, Datenschutz für Geodaten, DuD 2010, Heft 12, 824 (828).

[207] *Dammann*, in: Simitis, BDSG, 8. Auflage 2014, § 3 Rn. 26.

Herkunftsarten wie u.a. frei verfügbare Quellen (z.B. Internet), kommerzielle oder solche, die der Geheimhaltung unterliegen vorstellbar seien.[208]

Der Hinweis darauf, dass die datenverarbeitende Stelle den Personenbezug „ohne unverhältnismäßigen Aufwand" herstellen können muss, deutet indes darauf hin, dass es nicht darauf ankommen soll, ob die Daten auf rechtmäßige Weise erlangt wurden, sondern vielmehr das Verhältnis von Aufwand und Nutzen in den Blick zu nehmen ist.[209] Damit würde auch illegal erworbenes Zusatzwissen in die Bewertung miteinfließen, ob ein Personenbezug besteht, sofern der Nutzen den dafür notwendigen Aufwand übersteigen würde.[210] Dem ist beizupflichten; denn würde man einen Personenbezug von vornherein verneinen, sofern dieser lediglich durch unrechtmäßig erlangtes Zusatzwissen hergestellt werden konnte, so wäre derjenige, der sich illegal Informationen beschafft, insofern begünstigt, als er bei der Datenverarbeitung nicht unter die strengen Regelungen des BDSG fiele. Der von der Datenverarbeitung Betroffene hingegen wäre schutzlos gestellt, obschon der Personenbezug in einem solchen Fall - rein faktisch durch die Existenz und Anwendbarkeit von Zusatzwissen – gegeben ist. Das würde allerdings dem Schutzzweck des BDSG, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird", zuwiderlaufen, da sich auch aus rechtswidrig erlangten Zusatzinformationen die entsprechenden Schlüsse ziehen lassen, die durch das Recht auf personelle Selbstbestimmung gerade besonders unter Schutz gestellt sein sollen. Dementsprechend darf es bei der Entscheidung, ob eine Person bestimmbar ist, im Ergebnis nicht darauf ankommen, wie der Personenbezug hergestellt wurde, sondern es „sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen", vgl. Erwägungsgrund 26 S. 2 RL 95/46/EG.

Der Ansicht, wonach ein Personenbezog nicht gegeben ist, wenn die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann[211], wurde daher nicht gefolgt. Das verfügbare Zusatzwissen war unter den genannten Kriterien miteinzubeziehen.

Damit wurde bezüglich des Begriffes der Bestimmbarkeit dem objektiven Ansatz gefolgt. In Anbetracht der vernetzten Welt und damit steigender technologischer Möglichkeiten, Bezüge zwischen Informationen und natürlichen Personen durch die Nutzung von Drittwissen zu ermöglichen, ist es sinnvoll auch Drittwissen in die Betrachtung, ob ein Personenbezug gegeben ist, miteinzubeziehen. Bei der Bestimmung des Personenbezugs wird daher das „individuell verfügbare Zusatzwissen" der jeweiligen Stelle ausgegrenzt und insofern „alle überhaupt verfügbaren Mittel" berücksichtigt.[212] Damit soll eine bessere

[208] Vgl. *Dammann* in: Simitis, BDSG, 8. Auflage, § 3 Rn. 24, 27.

[209] Vgl. *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 2015, Heft 8, 365 (370).

[210] Vgl. *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 2015, Heft 8, 365 (370).

[211] Vgl. Österreichisches Datenschutzgesetz, § 4 Nr. 1; *Dammann* in: Simitis, BDSG, § 3 Rn. 28.

[212] *Forgó/Krügel*, Der Personenbezug von Geodaten, MMR 2010, Heft 1, 17 (18).

Grundlage für die Befolgung von Datenschutzregeln ermöglicht werden, weil eine Einzelfallprüfung, ob die jeweilige datenverarbeitende Stelle mit den ihr individuell zur Verfügung stehenden Mitteln den Bezug einer Person zu einer Sache herstellten kann, mit einem solchen Vorgehen entfällt.[213]

Mit dem Betrieb von AIS werden verschiedene Daten über das jeweilige Schiff ausgesendet. Diese Daten enthalten u.a. Schiffsname, Schiffstyp, Position, Kurs, Bestimmungshafen und voraussichtliche Ankunftszeit.[214] Über verschiedene Internet-Portale[215] ist es möglich, diese Angaben problemlos zu erhalten. Mit dem Erheben von Informationen - wie zum Beispiel der Ermittlung des Schiffsnamens - wäre es unter Nutzung des Schiffsregisters damit gegebenenfalls möglich, Personendaten (Aufenthaltsort) zu erhalten. Auch ist es denkbar, dass bei der Speicherung dieser Daten, ganze Reiserouten verfolgt werden können. Jedenfalls wird es in den meisten Fällen möglich sein, anhand des Schiffnamens und der Kennung zumindest festzustellen, wer Kapitän des betreffenden Schiffes ist. Damit war für die erhobenen Geodaten eine Bestimmbarkeit gegeben.

Einzelangaben

Für die Anwendung des BDSG musste es sich bei den AIS-Daten weiter um Einzelangaben über natürliche Personen handeln. Sammelangaben über Personengruppen fallen dabei nicht in den Bereich der Einzelangabe.[216] Insofern könnte es von Belang sein, wie sich die Besatzung der von der Datenerhebung betroffenen Schiffe zahlenmäßig zusammensetzt, da nicht auszuschließen ist, dass einzelne Crewmitglieder ab Erreichen einer gewissen Personenanzahl an Bord des Schiffes nicht mehr identifizierbar sind. Untersuchungsbedürftig war dies, weil in EMSec v.a. AIS-Daten erhoben wurden, nach SOLAS Regel V 2.4 aber v.a. Schiffe mit einer BRZ[217] von mindestens 300 in der Auslandsfahrt einer AIS-Ausrüstungspflicht unterliegen, womit davon auszugehen war, dass AIS-Daten insbesondere von Schiffen mit größeren Besatzungszahlen gesendet werden. Auf die Besatzungszahl dürfte es aber zumindest dann nicht ankommen, wenn mit den erhobenen Informationen auch nur eine Person identifiziert werden kann, weil es sich dann bei den AIS-Daten um personenbezogene oder zumindest – beziehbare Daten handeln würde.

Wie gesehen, ist es möglich, anhand des Schiffnamens und der Kennung festzustellen, wer Kapitän des jeweiligen Schiffes ist (s. o.). Daher war es für die datenschutzrechtliche

[213] Vgl. *Forgó/Krügel*, Der Personenbezug von Geodaten, MMR 2010, Heft 1, 17 (18).

[214] Vgl. Entschließung A.917(22) vom 29. November 2001 (deutsche Übersetzung in: Verkehrsblatt 2002, S. 715), geändert durch Entschließung A. 956(23).

[215] http://www.marinetraffic.com; http://www.vesseltracker.com; http://www.kielmonitor.de/.

[216] *Gola/Schomerus*, BDSG, § 3 Rn. 3.

[217] Detailliert zur Berechnung dieser Größe: http://www.bsh.de/de/Schifffahrt/Berufsschifffahrt/Schiffsvermessung/Vermessungsverfahren.jsp (Abruf v. 16.09.2015)

Dimension nicht entscheidend, inwieweit aus der Personengruppe der Crew einzelne Mitglieder identifizierbar sind. Die Möglichkeit, die Identität des Kapitäns eines Schiffes festzustellen, genügte für sich allein, dass für die erhobenen Geodaten und damit für das Echtzeitsystem insgesamt datenschutzrechtliche Vorgaben beachtet werden mussten.

Persönliche oder sachliche Verhältnisse

Weiter musste es sich bei diesen Angaben um solche handeln, die Aufschluss über persönliche oder sachliche Verhältnisse geben. Die vorliegend in Rede stehenden Geodaten lassen sich in der Verknüpfung zu dem jeweiligen Schiff und dessen Besatzung über Zusatzwissen mit dem Aufenthaltsort der an Bord befindlichen Personen in Verbindung bringen.[218] Sofern es sich bei diesen Daten um sog. „Punktdaten" handelt, wird mittels der Bestimmung des Aufenthaltsorts ein sachliches Verhältnis in Bezug auf die Person beschrieben.[219] Punktdaten sind dabei „Geodaten, die einen bestimmten Ort in einem zweidimensionalen System mittels x- und y- Koordinate beschreiben, wie bei Längen- und Breitengraden."[220] Ein für das Vorliegen von Punktdaten fester Auflösungsgrad ist nicht vorhanden, lediglich Schwellenwerte werden empfohlen.[221] Einer dieser Werte sieht die Schwelle bei einem Auflösungsgrad von 1:5.000 an[222], welcher einem Maßstab von 1 cm auf der Karte zu 50 m in der Wirklichkeit entspricht.

Für den Betrieb von AIS ist eine Positionsgenauigkeit von +/- 10 m vorgesehen.[223] Hier waren die erhobenen Daten unterhalb dieser Schwelle angesiedelt und damit auch als Punktdaten zu qualifizieren. Folglich wird mittels der AIS-Daten ein sachliches Verhältnis einer Person (Aufenthaltsort) beschrieben.

Nach alledem war das BDSG auch in sachlicher Hinsicht anwendbar.

2.2.8.2 Erhebung der Daten

Weiter musste die Datenerhebung gemäß § 4 BDSG auch zulässig sein. Nach Abs. 1 ist von der Zulässigkeit auszugehen, wenn das BDSG selbst oder eine spezielle Rechtsnorm dies

[218] S. o.

[219] Vgl. *Weichert*, Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, DuD 2009, 347 (350).

[220] Behm, RDV 2010, 61 (64).

[221] Arbeitsgruppe Geodatenschutz, Behördenleitfaden zum Datenschutz bei Geodaten und –diensten vom 20.01.2014, S. 11, (abrufbar unter http://www.imagi.de/SharedDocs/Downloads/IMAGI/DE/Imagi/behoerdenleitfaden.html).

[222] Arbeitsgruppe Geodatenschutz, Behördenleitfaden zum Datenschutz bei Geodaten und –diensten vom 20.01.2014, S. 11, (abrufbar unter http://www.imagi.de/SharedDocs/Downloads/IMAGI/DE/Imagi/behoerdenleitfaden.html).

[223] Vgl. Entschließung A.917(22) vom 29. November 2001 (deutsche Übersetzung in: Verkehrsblatt 2002, S. 715), geändert durch Entschließung A. 956(23).

erlaubt oder der Betroffene eingewilligt hat. Als spezielle Vorschrift des BDSG iSd § 4 Abs. 1 BDSG kam § 28 BDSG in Betracht.

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG (eigene Geschäftszwecke, Erforderlichkeit)

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist eine Datenerhebung zulässig, wenn damit die Erfüllung eigener Geschäftszwecke bezweckt ist, diese zur Wahrung berechtigter Interessen der erhebenden Stelle erforderlich sind und die schutzwürdigen Interessen des Betroffenen nicht überwiegen. Die Abwägung war dabei für die widerstreitenden Interessen des Betroffenen auf sein Recht zur informationellen Selbstbestimmung und dem Forschungsinteresse des DLR-RY vorzunehmen.

Berechtigtes Interesse

Fraglich war daher, ob das DLR-RY ein berechtigtes Interesse an der AIS-Datenerhebung hatte. Unerheblich war dabei, ob es sich um ein Interesse wirtschaftlicher oder ideeller Natur handelt, vielmehr kam es im Wesentlichen darauf an, ob es von der Rechtsordnung als entsprechend schutzwürdig eingestuft wird.[224] Es konnte davon ausgegangen werden, dass ein solches Interesse vorlag, da die Datenbeschaffung insoweit für die Erfüllung der Verbindlichkeiten des DLR-RY ggü. dem Mittelgeber und den übrigen Verbundpartnern von Belang war. Ferner hat das Institut geplant, die Forschungsergebnisse in weiteren Projekten zu nutzen und weiterzuentwickeln, was der Sicherheit im maritimen Bereich durch den Bau leistungsfähigerer Satelliten zugutekommen sollte, sodass ein berechtigtes Interesse angenommen werden konnte.

Erforderlichkeit

Die Datenerhebung musste darüber hinaus erforderlich sein. Der Zweck der Forschung bestand im Ergebnis darin, maritime Verkehrssicherungssysteme zu optimieren. In einer Experimentalphase sollte deshalb überprüft werden, ob der Realisierung des Forschungsvorhabens Hindernisse tatsächlicher Art entgegenstehen, etwa, weil ein Abgleich der luft- und weltraumgestützten Daten nicht umsetzbar war. Die Informationsbeschaffung wurde dementsprechend auch als erforderlich eingestuft.

Interessenabwägung

Schließlich durfte auch kein Grund zur Annahme bestehen, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Datenverarbeitung das Interesse des DLR-RY überwiegt. Es war folglich eine umfassende Abwägung der beiderseitigen Belange

[224] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 28 Rn. 24.

vorzunehmen. Im Hinblick auf den Schutzzweck des BDSG war auf Seiten des Betroffenen neben weiteren Faktoren v.a. das allgemeine Persönlichkeitsrecht zu beachten.[225] In die Abwägung mit eingestellt werden musste indes, dass es sich bei den AIS-Daten um keine besonders sensitiven Angaben handelt, also um solche, die Rückschlüsse auf „rassische und ethische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“[226] des Betroffenen zulassen. Wie bereits ausgeführt, ist jedoch zumindest der Kapitän des Schiffes, also sein Aufenthaltsort bestimmbar. Als besonders gewichtig war allerdings der Umstand anzusehen, dass die betroffenen Personen ihrerseits ein Interesse an der Informationsbeschaffung durch das DLR-RY haben dürften, da gerade sie z.T. von einem optimierten System zur maritimen Verkehrssicherung und mithin einer Verbesserung der Kollisionsverhütung auf See profitieren würden. Die überwiegenden Gründe sprachen somit dafür, dem Forschungsinteresse des DLR-RY den Vorzug ggü. den Belangen der Betroffenen einzuräumen, sodass die Interessenabwägung zugunsten der in diesem Fall verantwortlichen Stelle ausfiel.

Im Ergebnis waren damit die Tatbestandsvoraussetzungen des § 28 Abs. 1 S. 1 Nr. 2 BDSG erfüllt. Die Erhebung von Geodaten in Form der AIS-Daten erfolgte daher rechtmäßig.

§ 28 Abs. 1 Satz 1 Nr. 3 BDSG (eigene Geschäftszwecke, allgemeine Zugänglichkeit der Daten)

Darüber hinaus ist eine Erhebung zur Erfüllung eigener Geschäftszwecke zulässig, wenn die erhobenen Daten allgemein zugänglich sind oder ein Recht zur Veröffentlichung durch die verantwortliche Stelle besteht. Auch ist für diesen Fall eine Abwägung der schutzwürdigen Interessen vorzunehmen.

Allgemein zugänglich

Zu untersuchen war daher zunächst, ob es sich bei den AIS-Daten um solche Informationen handelt, die aus allgemein zugänglichen Quellen stammen. Der Begriff der allgemeinen Zugänglichkeit entspricht dem des Art. 5 Abs. 1 S. 1 GG, sodass es sich um solche Quellen handelt, die „technisch geeignet und dazu bestimmt sind, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.“[227] Der Umstand, dass die AIS-Daten der Allgemeinheit über Internetseiten wie „www.vesseltracker.com“ zur Verfügung stehen, könnte darauf hindeuten, dass jedenfalls die Voraussetzungen technischer Natur erfüllt sind. Um dem Schutzzweck des BDSG

[225] Vgl. *Erbs*, Georg/*Kohlhaas*, Max, Strafrechtliche Nebengesetze, 195. Ergänzungslieferung 2013, BDSG § 28 Rn. 9.

[226] Vgl. § 3 Abs. 9 BDSG.

[227] BVerfG 1. Senat, Entscheidung v. 25. April 1972 – 1 BvL 13/67, zitiert nach *juris*, Rn. 52.

hinreichend Rechnung zu tragen, müssten die Daten indes auch in zulässiger Weise in das Internet eingestellt worden sein.[228] Klärungsbedürftig war deshalb, ob eine Veröffentlichung der Daten im Internet rechtmäßig ist. Dem steht zum einen Art. 24 RL 2002/59/EG entgegen, wonach die Mitgliedstaaten die erforderlichen Maßnahmen zu ergreifen haben, um die Vertraulichkeit der auf Grundlage der Richtlinie erhobenen Daten sicherzustellen. Zum anderen ergibt sich aus Erwägungsgrund 6 RL 2009/17/EG,[229] dass die IMO eine Veröffentlichung der AIS-Daten im Internet aus Sicherheitsgründen ausdrücklich missbilligt und die Mitgliedstaaten entsprechend angehalten sind, dagegen vorzugehen.[230] Die Verbreitung der Daten über Seiten wie „www.vesseltracker.com“ widerspricht den vorstehenden Überlegungen und erfolgt daher in unzulässiger Weise.

Denkbar war es aber, das AIS selbst als allgemein zugängliche Quelle zu betrachten, da insofern jeder, der mit einem AIS-Empfangsgerät ausgerüstet ist, die Möglichkeit besitzt, AIS-Daten zu erheben. Dem ist allerdings entgegenzuhalten, dass die gewonnenen Daten ausschließlich Navigationszwecken dienen und gerade nur denjenigen zur Verfügung stehen sollen, die sich im beschränkten Funkbereich von bis zu 50 km aufhalten, vorausgesetzt, sie sind mit einem entsprechenden System ausgestattet.[231] Gegen die allgemeine Zugänglichkeit sprach ferner, dass die Daten über UKW-Funkkanäle übertragen werden, welche eigens für den AIS-Datenaustausch reserviert sind, wobei die Frequenzen von der Bundesnetzagentur über die FreqV[232] zugeteilt wurden.[233] Wie bereits bei den AIS-Daten, die an landgestützte Einrichtungen gesendet werden, so gilt auch für die erhobenen Geodaten über Satelliten-AIS, dass diese aus den gleichen Gründen nicht für die Allgemeinheit bestimmt sind, sondern nur einem bestimmten Personenkreis zur Gewährleistung sowie zur Verbesserung der maritimen Sicherheit zugänglich gemacht werden sollen. Folglich waren diese ebenfalls nicht als allgemein zugängliche Quelle iSd § 28 Abs. 1 S. 1 Nr. 3 BDSG zu betrachten.

Befugnis zur Veröffentlichung der Daten

Weiter war zu prüfen, ob nicht eine Befugnis zur Veröffentlichung der Daten bestünde. Hier setzt wie bereits ausgeführt die Richtlinie 2009/17/EG an, die sich diesbezüglich ausdrücklich

---

[228] Vgl. *Spindler*, Gerald/*Nink*, Judith; in: *Spindler*, Gerald/*Schuster*, Fabian [Hrsg.], Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, BDSG § 28 Rn. 7.

[229] Richtlinie 2009/17/EG des Europäischen Parlaments und des Rates vom 23. April 2009 zur Änderung der Richtlinie 2002/59/EG über die Errichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr, ABl. Nr. L 131 vom 28. Mai 2009, S. 101.

[230] Vgl. dazu ebenfalls BT Drs. 16/7415, S. 24.

[231] Vgl. *Nehab*, Tobias, Veröffentlichung von Schiffspositionen im Internet: Rechtliche Bewertung und Analyse der Erhebung von AIS-Daten, ZD 2013, 382 (385).

[232] Frequenzverordnung vom 27.08.2013 (BGBl. I, 3326).

[233] Vgl. VBW Kompakt, Informationen des Vereins für europäische Binnenschifffahrt und Wasserstraßen e.V. , Ausgabe: 3.12.2013, 1 (3); § 1 iVm FreqV Anlage Teil A Nr. 216, 218, 223, (Teil B D 227A, D 228).

gegen eine Veröffentlichung von AIS-Daten – und damit auch der erhobenen Geodaten[234] – ausspricht.[235] Demzufolge lag auch keine Befugnis zur Veröffentlichung der Daten vor.

Folglich war § 28 Abs. 1 Satz 1 Nr. 3 BDSG als Rechtsgrundlage für die Erhebung von Geodaten in Form der AIS-Daten nicht einschlägig. Es wurde daher allein auf § 28 Abs. 1 S. 1 Nr. 2 BDSG abgestellt.

2.2.8.3 Weitere Anforderungen

Bei der nach § 28 Abs. 1 S. 1 Nr. 2 BDSG rechtmäßigen Datenerhebung hat der Verantwortliche indes noch weitere Anforderungen zu erfüllen.

Grundsatz der Direkterhebung

Nach § 4 Abs. 2 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen, d.h. unter seiner Mitwirkung zu erheben. Ihm muss also die Möglichkeit eingeräumt werden, darauf Einfluss zu nehmen, welche Daten er wem zu welchem Zweck preisgibt.[236] Im Hinblick auf die AIS-Daten hätte man argumentieren können, dass der Betroffene regelmäßig Kenntnis davon haben dürfte, dass das System in bestimmten Intervallen statische, dynamische und reisebezogene Daten des Schiffes, auf dem er sich befindet, übermittelt.[237] Fraglich war allerdings, ob der Kapitän diese Übermittlung dergestalt beeinflussen kann, dass eine echte Mitwirkung vorliegt.

Rein rechtlich betrachtet besteht für Schiffe seit dem 1. Juli 2004 die Pflicht, AIS fortwährend in Betrieb zu halten.[238] Nur in bestimmten Ausnahmefällen ist der Kapitän berechtigt, das AIS abzuschalten. Obschon also die tatsächliche Möglichkeit bestehen würde, die Datenübermittlung zu beenden, ginge damit ein Verstoß gegen seerechtliche Vorschriften einher, sodass von einer faktischen Bindung ausgegangen werden musste. Zudem war zu

---

[234] Zwar sind die durch Satelliten-AIS erhobenen Geodaten weltweit abrufbar, ihre Veröffentlichung im Internet erfolgt indes widerrechtlich, was gegen die Annahme einer „allgemeinen Zugänglichkeit“ spricht, s.o. Unterstützt wird dieses Ergebnis durch § 202 b StGB, wonach die Veröffentlichung grds. strafbar und „lediglich“ die strafrechtliche Verfolgung aufgrund der ausländischen Firmensitze schwer umsetzbar ist, vgl. hierzu: VBW Kompakt, Informationen des Vereins für europäische Binnenschifffahrt und Wasserstraßen e.V. , Ausgabe: 3.12.2013, 1 (4).

[235] Richtlinie 2009/17/EG des Europäischen Parlaments und des Rates vom 23. April 2009 zur Änderung der Richtlinie 2002/59/EG über die Errichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr, ABl. Nr. L 131 vom 28. Mai 2009, S. 101, s. genau Erwägungsgrund 6.

[236] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 4 Rn. 21.

[237] Das folgt bereits aus der Richtlinie über den bordseitigen Betrieb von automatischen Schiffsidentifizierungssystemen (AIS), wonach sich der Benutzer vor Gebrauch des AIS mit den Grundgedanken der Richtlinie vertraut machen soll, vgl. VkBl. 2002, S. 713.

[238] S. o.

berücksichtigen, dass der Benutzer des AIS dieses in erster Linie zu Navigationszwecken verwenden wird. Vor diesem Hintergrund ist ihm zwar bewusst, dass er die Daten seines Schiffes an andere Schiffe und Landstationen übermittelt, er wird aber prinzipiell nicht damit rechnen, dass andere als Navigationszwecke mit der Datenerhebung verfolgt werden. Da sich auch keine Rechtsvorschrift ausmachen ließ, nach der das DLR-RY ausdrücklich befugt wäre, AIS-Daten für Forschungszwecke zu erheben, konnte eine konkludente Mitwirkung durch den Betrieb des AIS unter dem geltenden Recht ebenfalls nicht bejaht werden.

Wenn das DLR-RY sich die besagten Schiffsinformationen beschaffen würde, hätte die davon betroffene Person folglich weder Kenntnis davon, wem sie die Daten übermittelt, noch zu welchem Zweck. Dergestalt konnte von einer Mitwirkung nicht mehr ausgegangen werden.

Für einen solchen Fall sieht § 4 Abs. 2 BDSG jedoch mehrere Ausnahmen vor. So bedarf es nach Nr. 1 keiner Mitwirkungshandlung, sofern eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Eine entsprechende Norm war allerdings nicht ersichtlich.

Nach Nr. 2 können die Daten auch dann ohne die Mitwirkung des Betroffenen erhoben werden, wenn „der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht“ (lit. a) oder „die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde“ (lit. b) „und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.“ Die Datenerhebung bei Dritten (lit. a) war für das Forschungsvorhaben nicht erforderlich. Dementsprechend musste allein danach gefragt werden, ob die Informationsbeschaffung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (lit. b). Dabei waren der Zeit-, Kosten- und Arbeitsaufwand, gemessen an der Sensibilität der zu erhebenden Daten, in die Ermittlung des „unverhältnismäßigen Aufwands“ einzubeziehen.[239] Aufgrund der Dichte und Fluktuation des Schiffsaufkommens in Nord- und Ostsee wäre es dem DLR-RY nicht möglich gewesen, die Mitwirkung aller betroffenen Schiffscrews einzufordern. Da durch das AIS ferner keine besonders sensiblen Daten übermittelt werden, war von einem unverhältnismäßigen Aufwand auszugehen, sodass der Ausnahmetatbestand des § 4 Abs. 2 Nr. 2b BDSG als erfüllt betrachtet werden konnte. Überdies durften jedoch keine Anhaltspunkte für die Beeinträchtigung überwiegender schutzwürdiger Interessen der Betroffenen vorliegen. Diesbezüglich wird auf die im Rahmen der Prüfung zu § 28 Abs. 1 S. 1 BDSG vorgenommene Interessenabwägung Bezug genommen.[240] Ein überwiegendes Interesse auf Seiten der Schiffscrew war demzufolge nicht gegeben und die Beschaffung der Informationen mithin auch ohne Mitwirkung des Betroffenen zulässig.

Zweckbindungsgrundsatz

[239] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 4 Rn. 28.

[240] S. o.

Darüber hinaus fordert § 28 Abs. 1 S. 2 BDSG, dass die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, bei deren Erhebung festzulegen sind. Die Vorschrift des § 40 Abs. 1 BDSG konkretisiert dies für den Fall der Forschung dahingehend, dass die Daten, welche später für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden sollen, auch nur dafür erhoben werden dürfen. Dieser Aspekt bereitete im vorliegenden Kontext keine Schwierigkeiten, da das DLR-RY beabsichtigte, AIS-Daten im Rahmen seiner Grundlagenforschung für das Projekt EMSec zu erheben.

2.2.8.4 Verarbeitung[241] und Nutzung personenbezogener Daten durch Forschungseinrichtungen

Den weiteren Umgang mit den erhobenen Daten regelt § 40 BDSG. Die Vorschrift stellt die dabei zu berücksichtigenden Grundsätze auf.

Normadressaten

§ 40 BDSG wendet sich ausschließlich an Forschungseinrichtungen. Dies setzt eine gewisse Unabhängigkeit der datenverarbeitenden Stelle voraus, was allerdings nicht bedeutet, dass sie ausschließlich wissenschaftlich tätig sein muss.[242] Als Forschungszentrum erfüllt das DLR-RY diese Kriterien jedoch ohne weiteres.

Zweckbindungsgrundsatz

Auch im Bereich der Verarbeitung oder Nutzung personenbezogener Daten ist der Zweckbindungsgrundsatz zu beachten, sodass die Informationen allein zum Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden dürfen, vgl. § 40 Abs. 1 BDSG. Aus Gründen der Bestimmtheit sind für den Begriff der „wissenschaftlichen Forschung“ strengere Anforderungen als bei Art. 5 Abs. 3 S. 1 GG zu stellen, dergestalt, dass es sich um ein Forschungsvorhaben handeln muss, bei dem der Forschungszweck bereits im Vorfeld hinreichend definiert wurde.[243] Auch diese Voraussetzungen waren erfüllt, da der Forschungsgegenstand durch die Teilvorhabenbeschreibung des DLR-RY zum Projekt EMSec insofern klar umrissen wurde.

Wenngleich sich die Zweckbindung endgültig ausgestaltet, bedeutet dies nicht, dass die Übermittlung[244] der Daten an weitere Forschungseinrichtungen für andere wissenschaftliche

[241] Vgl. zum Begriff der Datenverarbeitung § 3 Abs. 4 BDSG. Danach ist unter Verarbeiten das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten zu verstehen.

[242] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 40 Rn. 7.

[243] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 40 Rn. 7a.

[244] Vgl. zum Begriff der Datenübermittlung § 3 Abs. 4 Nr. 3 BDSG.

Zwecke ausgeschlossen ist.[245] Für die Weitergabe sind allerdings die allgemeinen Zulässigkeitsvoraussetzungen einzuhalten,[246] die sich für nicht-öffentliche Stellen wie dem DLR-RY nach § 28 Abs. 2 Nr. 3 BDSG richten.

Voraussetzungen für die Übermittlung der Daten an andere Forschungseinrichtungen

In § 28 Abs. 2 Nr. 3 wird die schon seit 2001 im BDSG enthaltene Privilegierung der wissenschaftlichen Forschung fortgesetzt.[247] Demnach ist die Übermittlung zulässig, sofern „es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann." Dabei muss die Forschungseinrichtung nicht notwendigerweise auch verarbeitende Stelle sein.[248]

Erforderlichkeit

Zunächst müsste die Übermittlung der Daten also für die Durchführung des Forschungsvorhabens erforderlich sein. Da die Ergebnisse des Teilvorhabens des DLR-RY zu einem späteren Zeitpunkt in ein umfassendes Lagebild eingepflegt werden sollten, kam es in diesem Kontext erheblich darauf an, dass die Projektpartner, die sich mit der Erstellung des Lagebildes befassen, auf die entsprechenden Daten zugreifen können. Zu berücksichtigen war ferner, dass das DLR-RY zwar in erster Linie seine eigenen Forschungsziele verfolgte, Ausgangspunkt dabei aber stets das Gesamtziel des Verbundvorhabens war. Das setze indes gerade den Austausch gewonnener Ergebnisse voraus, sodass die Übermittlung der erhobenen Daten für die Durchführung des Forschungsvorhabens notwendig und damit erforderlich im beschriebenen Sinne war.

Überwiegen des wissenschaftlichen Interesses an der Durchführung des Forschungsvorhabens

Für die Frage nach dem Überwiegen des wissenschaftlichen Interesses an der Durchführung des Forschungsvorhabens gegenüber dem Interesse des Betroffenen an dem Ausschluss der

[245] Vgl. *Erbs*, Georg/*Kohlhaas*, Max, Strafrechtliche Nebengesetze, 195. Ergänzungslieferung 2013, BDSG § 40 Rn. 2.

[246] Vgl. *Erbs*, Georg/*Kohlhaas*, Max, Strafrechtliche Nebengesetze, 195. Ergänzungslieferung 2013, BDSG § 40 Rn. 2.

[247] Zuvor: § 28 Abs. 3 S. 1 Nr. 4 BDSG a. F.

[248] Vgl. *Wolff,* Heinrich Amadeus in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, § 28 Rn. 110.

Zweckänderung konnte weitestgehend auf die Ausführungen zur Interessenabwägung innerhalb der Prüfung des § 28 Abs. 1 S. 1 Nr. 2 BDSG verwiesen werden.[249] Zu berücksichtigen war allerdings, dass das Interesse im vorliegenden Zusammenhang erheblich überwiegen musste. Aber auch davon konnte wegen der geringen Sensibilität der erhobenen Daten[250] und des Nutzens, den die Betroffenen bei einem Erfolg des Forschungsvorhabens für sich beanspruchen könnten, ausgegangen werden.

Zweck der Forschung auf anderer Weise nicht oder nur mit unverhältnismäßigem Aufwand erreichbar

Ohne die Weitergabe der Daten an die Projektpartner wäre schließlich das Ziel der Verbundforschung, ein umfassendes Lagebild zu erstellen und mithin die zivile Sicherheit im maritimen Bereich zu erhöhen, nicht erreichbar gewesen.

Die allgemeinen Zulässigkeitsvoraussetzungen für eine Datenübermittlung an andere Forschungseinrichtungen waren folglich erfüllt.

Anonymisieren der Daten

Als weniger problematisch dürfte sich die Weitergabe der Informationen jedoch gestalten, wenn sie vor ihrer Übermittlung dem Verfahren der Anonymisierung unterzogen wurden. Unter Anonymisierung versteht man die Veränderung der Daten dergestalt, dass die Wahrscheinlichkeit der Identifizierbarkeit einer Person in dem Maße reduziert wird, dass sie nach allgemeiner Lebenserfahrung und dem Stand der Forschung praktisch ausscheidet.[251] In Bezug auf AIS-Daten wäre ein Anonymisieren denkbar, indem bei ihrer Weitergabe ausschließlich Positionsdaten übermittelt und darüber hinausgehende Informationen wie bspw. Schiffsnummer, Kurs und Geschwindigkeit so verändert werden würden, dass Rückschlüsse auf das konkrete Schiff nicht mehr möglich wären. In Fällen, bei denen die Anwendbarkeit der Datenschutzanforderungen unmittelbar an den Personenbezug

[249] S. o.

[250] Wenngleich es sich um keine sensiblen Daten iSd § 3 Abs. 9 BDSG handelt, ist von einem Personenbezug und der sachlichen Anwendbarkeit des BDSG dennoch auszugehen. Dadurch ändert sich auch dann nichts, wenn für das Forschungsvorhaben EMSec lediglich optische Schiffs-Positionsdaten von Interesse sein dürften. Der Begriff des „Erhebens“ ist weit zu verstehen, sodass hiervon auch die reine zweckgerichtete Beobachtung umfasst ist; vgl. *Schild*, Hans-Hermann in: Wolf, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutzrecht in Bund und Ländern, München 2013, § 3, Rn. 51. Ähnlich verhält es sich mit dem Begriff des „Erfassens“, welcher alle Formen der Verkörperung von Signalen, unabhängig von ihrer Art (optische und akustische Signale inbegriffen) umschließt; vgl. *Schild*, Hans-Hermann in: Wolf, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutzrecht in Bund und Ländern, München 2013, § 3, Rn. 62.

[251] Vgl. *Roßnagel*, Alexander/*Scholz*, Philip, Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721 (724). Vgl. zum Begriff des Anonymisierens auch § 3 Abs. 6 BDSG.

angeknüpft hätte, wäre das BDSG in Ermangelung desselben dann nicht anwendbar gewesen.[252]

Insofern wurde überprüft, ob das DLR-RY dazu verpflichtet war, die Daten vor deren Übergang auf die übrigen Projektpartner zu anonymisieren. Eine solche Pflicht hätte sich aus § 40 Abs. 2 S. 1 BDSG ergeben können. Danach sind personenbezogene Daten zu anonymisieren, „sobald dies nach dem Forschungszweck möglich ist." In diesem Zusammenhang hat das BVerfG in seinem „Volkszählungsurteil" betont, dass „der Wissenschaftler […] regelmäßig nicht an der einzelnen Person interessiert [ist], sondern an dem Individuum als Träger bestimmter Merkmale."[253] So lag der Fall denn auch hier, da es dem DLR-RY nicht auf die Personen ankam, die sich auf dem Schiff befanden, über das die Daten erhoben wurden. Vielmehr ging es darum, den Schiffsverkehr in seiner Gesamtheit zu erfassen und einen Abgleich mit land- und weltraumgestützten AIS-Daten vorzunehmen. An den mitgesendeten personenbezogenen Daten bestand insofern kein Interesse. Sie waren also für die weitere Forschung unerheblich und folglich zu anonymisieren. Dies entspricht auch dem allgemeinen Grundsatz der Datensparsamkeit, vgl. § 3a S. 2 BDSG.

§ 40 Abs. 2 S. 2 BDSG bestimmt ferner, dass die einzelnen Merkmale bis zum Zeitpunkt des Anonymisierens separat zu speichern[254] sind, sofern der Forschungszweck dies zulässt.

Befugnis zur Veröffentlichung

Es war ebenso zu hinterfragen, ob eine projektabschließende Befugnis zur Veröffentlichung der erzielten Ergebnisse bestehen könnte. Gem. § 40 Abs. 3 Nr. 1 BDSG besteht eine solche, sofern der Betroffene eingewilligt hat. Die Probleme, die sich im Zusammenhang mit der Einwilligung ergeben, wurden bereits dargestellt.[255] Da § 40 Abs. 3 Nr. 1 BDSG jedoch unmittelbar auf personenbezogene Daten abstellt, findet diese Regelung keine Anwendung, wenn es sich um anonymisierte Daten handelt. Die Veröffentlichung der AIS-Daten in anonymisierter Form ist daher ohne weiteres zulässig.[256]

Unzulässigkeit der Verarbeitung oder Nutzung bei Widerspruch des Betroffenen

[252] Vgl. *Roßnagel*, Alexander/*Scholz*, Philip, Datenschutz durch Anonymität und Pseudonymität: Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721 (725 f.).

[253] Vgl. BVerfG 1. Senat, Urt. v. 15. Dezember 1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 – Volkszählungsurteil, zitiert nach *juris*, Rn. 209.

[254] Speichern meint dabei „das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung", vgl. § 3 Abs. 4 Nr. 1 BDSG.

[255] S. o.

[256] Vgl. *Gola*, Peter/*Schomerus*, Rudolph, Bundesdatenschutzgesetz, Kommentar, 11. Aufl. 2012, § 40 Rn. 15.

Zu beachten war ebenfalls, dass personenbezogene Daten nicht für eine automatisierte Verarbeitung erhoben, verarbeitet oder genutzt werden dürfen, „soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt“, § 35 Abs. 5 BDSG.

2.2.8.5 Weitere zu beachtende Grundsätze bei der Datenverarbeitung

Das BDSG sieht überdies weitere allgemein zu berücksichtigende Grundsätze vor.

Meldepflicht

Da das DLR-RY beabsichtigte, die AIS-Daten in automatisierter Form zu erheben, war die Vorschrift des § 4d BDSG von Bedeutung, wonach entsprechend angewandte Verfahren vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde[257] zu melden sind.[258] Dies sind in der Regel die Landesbeauftragten für Datenschutz und Informationsfreiheit, vgl. § 38 Abs. 6 BDSG.[259] Die örtliche Zuständigkeit ergibt sich aus den Verwaltungsverfahrensgesetzen der Länder, wobei für die Bestimmung des Zuständigkeitsbereichs die Lage des Betriebes maßgeblich ist, von dem die Datenverarbeitung ausgeht.[260] Der Inhalt der Meldepflicht lässt sich dabei § 4e BDSG entnehmen.

Ausnahmen von der Meldepflicht

Bestellung eines Beauftragten für den Datenschutz

Die Meldepflicht entfällt nach § 4d Abs. 2 BDSG jedoch, „wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Vorgaben hierzu finden sich in § 4f BDSG. Danach hatte das DLR-RY als nicht-öffentliche Stelle spätestens innerhalb eines Monats nach Aufnahme der Tätigkeit einen Datenschutzbeauftragten zu bestellen,[261] es sei denn, dass höchstens neun Personen ständig mit der automatisierten Datenverarbeitung

[257] Vgl. zu den Aufgaben der Aufsichtsbehörde § 38 BDSG.

[258] Vgl. § 4d Abs. 1 BDSG.

[259] Ausnahme: Bayern; in Schleswig–Holstein ist das Landeszentrum für Datenschutz zuständig; vgl. *Wolff,* Heinrich Amadeus in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, § 38 Rn. 88.

[260] *Wolff,* Heinrich Amadeus in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, § 38 Rn. 89.

[261] Vgl. § 4f Abs. 1 S. 2 BDSG.

beschäftigt waren.[262] Hiervon ausgenommen sind solche Personen, welche nur gelegentlich (bspw. aufgrund von Krankheits- oder Urlaubsvertretung) mit der automatisierten Verarbeitung personenbezogener Daten betraut wurden. Umfasst waren somit allein diejenigen, bei denen diese Tätigkeit als beständiger Teil der Arbeitsleistung anzusehen war.[263]

Bei der Bestellung des Datenschutzbeauftragten handelt es sich um ein Instrument der innerbetrieblichen Selbstkontrolle.[264] Auch, wenn es vorgesehen war, die AIS-Daten weiteren Projektpartnern – in welcher Form auch immer - zur Verfügung zu stellen, konnte dies also nicht dazu führen, dass sich die Zahl der beim DLR-RY „ständig mit der automatisierten Datenverarbeitung Beschäftigten“ dadurch erhöht, da man andernfalls den innerbetrieblichen Bereich verlassen hätte.

Vorabkontrolle

Unabhängig von der Anzahl der Beschäftigten normiert § 4f Abs. 1 S. 6 BDSG jedoch Gegenausnahmen hinsichtlich der Befreiung von der Bestellpflicht. Relevant war insoweit die Alternative „soweit die Verarbeitungen einer Vorabkontrolle unterliegen“.

Eine Vorabkontrolle ist erforderlich, sofern mit der automatisierten Datenverarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen einhergehen, vgl. § 4d Abs. 5 S. 1 BDSG. Es handelt sich bei den „besonderen Risiken“ um einen unbestimmten Rechtsbegriff,[265] dessen Inhalt durch Auslegung zu ermitteln war.

Auszugehen war grds. vom Wortlaut der Norm. Dem Wort „besondere“ in § 4d Abs. 5 S. 1 BDSG lässt sich entnehmen, dass es sich um gesteigerte Risiken handeln muss, die über die allgemeinen Gefahren der automatisierten Datenverarbeitung hinausgehen. In welchen Fällen ein solch erhöhtes Risikopotential angenommen werden kann, ergab sich daraus jedoch noch nicht.

Weiterhelfen konnte insofern der Blick auf § 4d Abs. 5 S. 2 BDSG. Die Vorschrift benennt beispielhaft Umstände, denen „besondere Risiken“ für die Rechte und Freiheiten der Betroffenen immanent sind. Die Pflicht zur Vorabkontrolle ist danach v.a. dann gegeben, wenn besondere Arten von personenbezogenen Daten verarbeitet werden (Nr. 1) oder „die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten […]“ (Nr.2). Danach war vorliegend keine vorherige Prüfung

[262] Vgl. § 4f Abs. 1 S. 4 BDSG.

[263] Vgl. *Wolff,* Heinrich Amadeus in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, § 4f Rn. 16.

[264] Vgl. *Moos*, Flemming in: Wolff, Heinrich Amadeus/Brink, Stefan[Hrsg.]: Datenschutz in Bund und Ländern, München 2013, § 4f Rn. 2.

[265] Vgl. *Spindler*, Gerald/*Nink*, Judith; in: *Spindler*, Gerald/*Schuster*, Fabian [Hrsg.], Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, BDSG § 4d Rn. 9.

vorzunehmen, da weder besonders sensible Daten erhoben wurden[266] noch das Verhalten der Betroffenen analysiert werden sollte.[267] Aus dem Wort „insbesondere“ geht indes hervor, dass die Regelung nicht abschließend ist und mithin auch weitere Faktoren ein „besonderes Risiko“ im Sinne der Vorschrift begründen können. Diese müssten jedoch zumindest ein gleichwertig starkes Risiko für die Rechte und Freiheiten des Betroffenen darstellen.[268]

Auf den ersten Blick handelte es sich hier um keinen vergleichbaren Fall, da in erster Linie Schiffspositions-Daten zu Navigationszwecken verarbeitet werden sollten, die lediglich mittels zusätzlicher Kenntnisse Rückschlüsse auf die an Bord befindliche Crew zulassen würden.[269] Ein besonderes – über die allgemeinen Gefahren der automatisierten Datenverarbeitung hinausgehendes - Risiko für das allgemeine Persönlichkeitsrecht[270] der Betroffenen bestand folglich nicht.

Unter Berücksichtigung von Sinn und Zweck der Vorschrift hätten sich aber möglicherweise andere Schlüsse ziehen lassen. § 4d Abs. 5 BDSG dient der Umsetzung von Art. 20 Abs. 1 DS-RL,[271] wonach die Mitgliedstaaten festlegen, „welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können […]“ Erwägungsgrund 53 führt dazu aus, dass bestimmte Datenverarbeitungen „aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen - oder aufgrund der besonderen Verwendung einer neuen Technologie“ besonders risikobehaftet sein können. Art. 27 Abs. 2 VO (EG) Nr. 45/2001,[272] der für die Auslegung von Art. 20 Abs. 1 DS-RL maßgebend ist,[273] konkretisiert, was im Einzelnen darunterfallen kann:

- „Verarbeitungen von Daten über Gesundheit und Verarbeitungen von Daten, die Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen“ (lit. a);

[266] S. o.

[267] Vielmehr kommt es dem DLR-RY gerade nicht auf die einzelnen Personen an, s. o.

[268] Vgl. *Spindler*, Gerald/*Nink*, Judith; in: *Spindler*, Gerald/*Schuster*, Fabian [Hrsg.], Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, BDSG § 4d Rn. 9.

[269] S. o.

[270] Es wird davon ausgegangen, dass unter „Rechte und Freiheiten der Betroffenen“ das allgemeine Persönlichkeitsrecht zu verstehen ist, welches durch das BDSG geschützt wird, s. o.

[271] Vgl. *Spindler*, Gerald/*Nink*, Judith; in: *Spindler*, Gerald/*Schuster*, Fabian [Hrsg.], Recht der elektronischen Medien, Kommentar, 2. Aufl. 2011, BDSG § 4d Rn. 1.

[272] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12. Januar 2001, S. 1-22.

[273] Vgl. EuGH Große Kammer, Urt. v. 9. November 2010 – C-92/09, C-93/09, zitiert nach *juris*, Rn. 106.

- „Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten, einschließlich ihrer Kompetenz, ihrer Leistung oder ihres Verhaltens“ (lit. b)
- „Verarbeitungen, die eine in den nationalen oder gemeinschaftlichen Rechtsvorschriften nicht vorgesehene Verknüpfung von Daten ermöglichen, die zu unterschiedlichen Zwecken verarbeitet werden“ (lit. c) sowie
- „Verarbeitungen, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen“ (lit. d).

Die Verarbeitung der AIS-Daten bietet weitreichende Verknüpfungsmöglichkeiten, sodass Art. 27 Abs. 2 lit. c) VO (EG) Nr. 45/2001 hätte im vorliegenden Fall einschlägig sein können. Dem war jedoch entgegenzuhalten, dass die Verknüpfung der AIS-Daten mit anderen Schiffsinformationen geradezu dazu vorgesehen war, um die Sicherheit im maritimen Bereich zu erhöhen[274] und deren automatisierte Verarbeitung demzufolge keinen nationalen oder gemeinschaftlichen Rechtsvorschriften zuwiderläuft.

Im Ergebnis konnte also davon ausgegangen werden, dass es keiner Vorabkontrolle bedurfte, da durch die AIS-Datenverarbeitung des DLR-RY keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen iSd § 4d Abs. 5 BDSG begründet wurden. Für die Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen, kam es daher entscheidend darauf an, ob der Schwellenwert des § 4f Abs. 1 S. 4 BDSG überschritten wurde.

Ausnahmetatbestand des § 4d Abs. 3 BDSG

Die Pflicht, das Verfahren der automatisierten Verarbeitung der zuständigen Stelle zu melden, entfällt nach § 4d Abs. 3 BDSG darüber hinaus, „wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftig und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.“ Da sich die erforderliche Einwilligung als problematisch erwies,[275] und auch keine rechtsgeschäftliche bzw. rechtsgeschäftsähnliche Beziehung zwischen DLR-RY und den von der Datenerhebung und -verarbeitung betroffenen Personen bestand, lagen die Voraussetzungen des Ausnahmetatbestandes nicht vor.

[274] Vgl. Art. 22a RL 2002/59/EG, wonach die Mitgliedstaaten lokale Seeverkehrsinformations-Managementsysteme einführen: SafeSeaNet.

[275] S. o.

Zwischenergebnis

Die Gesamtschau von § 4d Abs. 2 und 3 BDSG ergab, dass von der Meldepflicht nur bei der Bestellung eines Datenschutzbeauftragten durch das DLR-RY abgesehen werden konnte, auch wenn es hierzu beim Vorliegen der Voraussetzungen des § 4f Abs. 1 S. 4 BDSG grundsätzlich nicht verpflichtet gewesen wäre.[276]

2.2.8.6 Datensicherheit

Nach § 9 S. 1 BDSG musste das DLR-RY als nicht-öffentliche Stelle darüber hinaus die technischen und organisatorischen Maßnahmen treffen, die erforderlich waren, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Dadurch soll die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Datensysteme gesichert werden.[277] Erforderlich sind Schritte nach § 9 S. 2 BDSG allerdings nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Es genügt indes nicht, die notwendigen Vorkehrungen zu treffen, vielmehr muss die verantwortliche Stelle auch belegen können, dass sie Maßnahmen getroffen hat, die dem Schutzzweck des BDSG entsprechen.[278]

Konkretisiert wird die Vorschrift des § 9 BDSG durch die Anlage zum BDSG. Hiernach ist „die […] innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird." Ein besonderes Verfahren sieht das BDSG nicht vor. Um die umfangreichen gesetzlichen Vorgaben einhalten zu können, empfiehlt es sich aber dennoch, ein umfassendes Datenschutzmanagementsystem[279] einzurichten, welches konkrete unternehmensinterne Mechanismen und Bestimmungen enthält. Verantwortlich für die Einrichtung und Ausübung eines solchen Systems ist die Führungsebene des Unternehmens.[280]

---

[276] Vgl. auch BT Drs. 14/4329, S. 35.

[277] Vgl. *Meints*, Martin, Datenschutz nach BSI-Grundschutz?, DuD 2006, 13.

[278] Vgl. *Bizer*, Johann, Verpflichtung zum Sicherheitskonzept, DuD 2006, 44.

[279] Dies kann bspw. durch die Erstellung eines IT- und Sicherheitskonzepts unter Zugrundelegung von Risikoanalysen und Schutzbedarfskategorien realisiert werden; vgl. *Karg*, Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, § 9 Rn. 91-99. Darüber hinaus stellt auch das BSI über sein IT-Grundschutzhandbuch mehrere Möglichkeiten zur Umsetzung des Datenschutzes bereit. Um Bußgeld- und Haftungsfälle auszuschließen, wird dringend empfohlen, die in Erwägung gezogenen Maßnahmen durch den jeweiligen Landesdatenschutzbeauftragten überprüfen zu lassen.

[280] Das folgt aus dem Grundsatz, dass Vorstand, Geschäftsführung etc. zur Schadensabwendungen für das Unternehmen verpflichtet sind; vgl. *Bizer*, Johann, Bausteine eines Datenschutzaudits – Erste Schritte zu einem Schema für freiwillige Auditierungen, DuD 2006, 5.

Aus Satz 2 Nr. 1 bis 8 der Anlage ergeben sich sodann die rechtlichen Anforderungen. Verbindlich ist allein das Ergebnis. Die konkret zu treffenden Maßnahmen standen dem DLR-RY frei, mit der Einschränkung, dass sie dem Stand der Technik entsprechen mussten. Grundsätzlich sollte die Errichtung eines IT-Systems jedenfalls die wesentlichen Schutzanforderungen des BDSG umsetzen und daher über technische Möglichkeiten verfügen, die bspw. eine effektive Umsetzung der Betroffenenrechte[281] sichern.[282] Welche Maßnahmenziele hiervon im Einzelnen umfasst sind, wurde sodann dargestellt.

Nr. 1 – Zutrittskontrolle

Bei der Zutrittskontrolle handelt es sich um eine räumliche Sicherheitsmaßnahme, mit der ausgeschlossen werden soll, dass Unbefugte Zutritt zu denjenigen Datenverarbeitungsanlagen erlangen, welche für die Verarbeitung bzw. Nutzung personenbezogener Daten vorgesehen sind. Hierunter ist nicht nur die Errichtung entsprechender Zutrittssperren, sondern auch der Aufbau eines den Zutritt regelnden Konzepts und dessen Einhaltung zu subsumieren.[283]

Nr. 2 – Zugangskontrolle

Über die Errichtung einer Zugangskontrolle soll - im Gegensatz zur Zutrittskontrolle - der Zugang Unbefugter zu den Datenverarbeitungs*systemen* abgewehrt werden. Die getroffenen Vorkehrungen dürfen allerdings nicht nur den Schutz vor unberechtigter Nutzung bezwecken. Vielmehr soll allein schon die Wahrnehmung der Dateninhalte lediglich den berechtigten Personen möglich sein, was etwa durch ein System umgesetzt werden könnte, welches die Berechtigung vor einer Freigabe der Daten abfragt.[284]

Nr. 3 – Zugriffskontrolle

Im Rahmen der Zugriffskontrolle erfolgt sodann eine Überprüfung der individuellen Rechte einer grundsätzlich zutritts- und zugangsberechtigten Person. Insoweit sind Parameter festzulegen, auf welche Art und Weise der Zugang zu den geschützten Daten erfolgen darf.

[281] Insbesondere Auskunfts- und Löschungsansprüche.

[282] Dazu mehr in BfDI 23. Tätigkeitsbericht 2009-2010, 1.3 Datenschutz durch Technik und Organisation, S. 22f.

[283] Vgl. *Karg,* Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 16-17.

[284] Vgl. *Karg*, Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 20.

Vor diesem Hintergrund ließe sich bspw. an die Tätigkeitsbeschreibung der Beschäftigten oder ihre hierarchische Stellung im Unternehmen anknüpfen.[285]

Nr. 4 – Weitergabekontrolle

Über die Weitergabekontrolle soll eine Überprüfung des Übermittlungsvorganges und die Legitimation des Empfängers zur Dateneinsicht sichergestellt werden. Die Einrichtung eines solchen Verfahrens ist notwendig, um Umgehungsmöglichkeiten der Zugangs- und Zugriffsberechtigungen entgegenzuwirken.[286]

Nr. 5 – Eingabekontrolle

Unter der Eingabekontrolle ist die Verpflichtung einer umfassenden Protokollierung und Dokumentation hinsichtlich der Frage, welcher Mitarbeiter welche personenbezogenen Daten im Datenverarbeitungssystem eingegeben, verändert oder entfernt hat, zu verstehen.[287]

Nr. 6 – Auftragskontrolle

Soweit personenbezogene Daten über ein Auftragsverhältnis weitergegeben werden, hat der Auftraggeber sicherzustellen, dass die Daten weisungsgetreu verwendet und verarbeitet werden. Den Auftragsnehmer trifft seinerseits die Pflicht, zu kontrollieren, dass die übermittelten Daten derart genutzt werden, dass Gesetzesverstöße ausgeschlossen sind.[288]

Nr. 7 – Verfügbarkeitskontrolle

Über die Verfügbarkeitskontrolle sollen die Daten vor unbeabsichtigter Zerstörung gesichert und somit dem Schutzziel der Verfügbarkeit getragen werden. Es müssen daher Vorkehrungen getroffen werden, um dem Verlust der Verfügungsgewalt über die Daten -

[285] Vgl. *Karg*, Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 22.

[286] Vgl. *Karg*, Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 24.

[287] Vgl. *Karg*, Moritz in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 27-28.

[288] Vgl. *Karg*, Moritz, in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 33-34.

etwa durch Abhandenkommen von Speichergeräten oder infolge stromausfallbedingter Löschungen von Datensätzen - vorzugreifen.[289]

Nr. 8 – Trennungsprinzip

Im Hinblick auf die Einhaltung des Zweckbindungsgrundsatzes auch innerhalb eines Unternehmens ist die verantwortliche Stelle dazu verpflichtet, Maßnahmen zu ergreifen, durch die sichergestellt wird, dass Daten zu unterschiedlichen Zwecken getrennt verarbeitet werden können. Das wäre etwa durch den Einsatz verschiedener Server oder die Programmierung der Datenverarbeitungsanlagen möglich.[290]

2.2.8.7 Rechte des Betroffenen

Das BDSG räumt dem von der Datenerhebung und –verarbeitung Betroffenen gegenüber der verantwortlichen Stelle zusätzlich gewisse Rechte ein.

Recht auf Benachrichtigung

So folgt aus § 33 Abs. 1 BDSG etwa eine Benachrichtigungspflicht, wenn erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert werden. Die Benachrichtigungspflicht umfasst dabei die Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, die Verarbeitung und Nutzung sowie die Identität der datenverarbeitenden Stelle. Da AIS-Daten durch das DLR-RY ohne Mitwirkung des Betroffenen erhoben wurden,[291] hatte dieser regelmäßig keine Kenntnis von der Speicherung seiner Daten. Grundsätzlich wäre er folglich darüber zu benachrichtigen gewesen. Von einer solchen Pflicht kann hingegen abgesehen werden, wenn „die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde“, vgl. § 33 Abs. 2 Nr. 5 BDSG.

Ebenso wie bei der Einwilligung ging es mit einem übermäßigen Aufwand einher, sämtliche Betroffene entsprechend zu unterrichten.[292] Insofern war ausnahmsweise von einem Entfallen der Benachrichtigungspflicht auszugehen.

---

[289] Vgl. *Karg*, Moritz, in: Wolff, Heinrich Amadeus/Brink, Stefan [Hrsg.], Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 35

[290] Vgl. *Karg*, Moritz, in: Wolff, Heinrich Amadeus/Brink, Stefan, Datenschutz in Bund und Ländern, München 2013, Anlage zu § 9 Rn. 40-42

[291] S. o.

[292] Zur Problematik der Einwilligung s. o.

Recht auf Auskunft

Erlangt der Betroffenen dagegen Kenntnis von dem Umgang mit seinen Daten, so hat er gem. § 34 Abs. 1 S. 1 BDSG die Möglichkeit, einen Antrag auf Auskunftserteilung zu stellen. Die Anforderungen an einen solchen Antrag sowie der Umfang der Auskunftspflicht ergeben sich ebenfalls aus § 34 Abs. 1 BDSG. Die Pflicht zur Auskunftserteilung entfällt nach § 34 Abs. 7 BDSG jedoch, wenn der Betroffene – wie im vorliegenden Fall – nach § 33 Abs. 2 Nr. 5 BDSG nicht zu benachrichtigen ist.[293]

Recht auf Berichtigung, Löschung[294] und Sperrung[295] von Daten

Der Betroffene kann gem. § 35 BDSG weiterhin verlangen, dass seine Daten berichtigt, gelöscht oder gesperrt werden.[296] Die Berichtigungspflicht folgt aus § 35 Abs. 1 S. 1 und betrifft ausschließlich unrichtige Daten.

Nach § 35 Abs. 2 S. 2 Nr. 3 BDSG sind die zu eigenen Zwecken verarbeiteten personenbezogenen Daten zu löschen, sobald sie nicht mehr zur Zweckerreichung benötigt werden. Da es dem DLR-RY grds. nicht auf die Merkmale angekommen ist, aus denen sich der Personenbezug ergab,[297] war von einer Pflicht zur Löschung auszugehen.

An die Stelle einer Löschung kann gem. § 35 Abs. 3 BDSG eine Sperrung treten, soweit „Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden“ (Nr. 2) oder „eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist“ (Nr. 3). Eine Pflicht zur Sperrung nach § 35 Abs. 3 Nr. 1 BDSG kommt dagegen nur in Betracht, wenn der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten entgegenstehen. Ein gesetzliches Verbot der Löschung hätte sich bspw. aus § 35 Abs. 4 BDSG ergeben können, wonach Daten zu sperren sind, „soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.“ In diesem Fall würde zugleich § 35 Abs. 3 Nr. 2 zum Tragen kommen, da die Löschung insofern die schutzwürdigen Interessen auf Überprüfung der Richtigkeit der Daten beeinträchtigen dürfte.

---

[293] S. o.

[294] Vgl. zum Begriff der Datenlöschung § 3 Nr. 5 BDSG.

[295] Vgl. zum Begriff des Sperrens von Daten § 3 Nr. 4 BDSG.

[296] Da die Vorschrift direkt auf personenbezogene Daten abstellt, besteht eine solche Pflicht nicht, sofern die Informationen bereits anonymisiert sind, s. o.

[297] S. o.

§ 35 Abs. 7 BDSG legt fest, dass die Stellen, denen die Daten zur Speicherung übermittelt wurden, von einer Berichtigung unrichtiger Daten, Sperrung bestrittener Daten und der Löschung bzw. Sperrung wegen Unzulässigkeit der Speicherung zu benachrichtigen sind.[298]

Gesperrte Daten dürfen außer in den Fällen des § 35 Abs. 8 BDSG allerdings nur übermittelt werden, wenn der Betroffene zuvor eingewilligt hat.

2.2.9 EU Datenschutz-Grundverordnung

Für die Zukunft ist ferner die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung (DS-GVO))[299] zu beachten Das Europäische Parlament hat der Verordnung am 12. März 2014 zugestimmt;[300] sie wurde am 27. April 2016 erlassen und beansprucht ab dem 25. Mai 2018 in den Mitgliedstaaten Geltung. Aus der Rechtsnatur der Verordnung heraus folgt, dass sie in allen ihren Teilen verbindlich ist und unmittelbar in jedem Mitgliedstaat gilt, vgl. Art. 288 Abs. 2 AEUV. Das bedeutet, dass die Mitgliedstaaten ihre datenschutzrechtlichen Regelungen an die Vorgaben der Verordnung anzupassen haben.

2.2.9.1 Sachlicher Anwendungsbereich – personenbezogene Daten

Zunächst war zu klären, ob die DS-GVO anwendbar ist. Aus Art. 2 Abs. 1 DS-GVO ergibt sich insofern, dass die Verordnung u. a. für die automatisierte Verarbeitung personenbezogener Daten gilt. Der sachliche Anwendungsbereich der DS-GVO ist daher eröffnet, sofern es sich bei den AIS-Daten um personenbezogene Daten handelt. Dies ist der Fall.[301] Die DS-GVO findet damit Anwendung.

2.2.9.2 Zu beachtende Grundsätze für die Verarbeitung personenbezogener Daten

Obschon die Projektlaufzeit endete, bevor die DS-GVO in den Mitgliedstaaten Geltung beanspruchen konnte, war zu überprüfen, inwieweit diese ggf. bei einer späteren Datenverarbeitung – etwa im Rahmen einer Verlängerung des Projekts – zu beachten wäre. Insofern musste besonderes Augenmerk auf die Grundsätze des Art. 5 DS-GVO gelegt werden, aus denen sich folgende Prinzipien ergeben:

---

[298] Eine Ausnahme dazu ergibt sich aus § 35 Abs. 4a BDSG.

[299] VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

[300] Vgl. *Philipp*, Otmar, EuZW 2014, Datenschutz: Annahme der Datenschutz-Grundverordnung, 283.

[301] S. o. unter Punkt II. 2.2.8.

- Rechtmäßigkeit, Verarbeitung und Transparenz, Art. 5 Abs. 1 lit. a) DS-GVO
- Zweckbindung, Art. 5 Abs. 1 lit. b) DS-GVO
- Datenminimierung, Art. 5 Abs. 1 lit. c) DS-GVO
- Richtigkeit, Art. 5 Abs. 1 lit. d) DS-GVO
- Speicherbegrenzung, Art. 5 Abs. 1 lit. e) DS-GVO
- Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit. f) DS-GVO
- Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO

Rechtmäßigkeit der Datenverarbeitung

Von Belang war dabei v.a. die Frage nach der Rechtmäßigkeit der Datenverarbeitung. Wann diese gegeben ist, ergibt sich aus Art. 6 Abs. 1 DS-GVO, wobei für eine AIS-Datenverarbeitung im hier interessierenden Bereich Buchstabe f) einschlägig sein könnte. Dann müsste die Verarbeitung „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, dürften nicht überwiegen“. Das bedeutet, dass eine Interessenabwägung zu erfolgen hat. Insofern konnte vollumfänglich auf die entsprechenden Ausführungen zum BDSG verwiesen werden,[302] sodass grds. von der Rechtmäßigkeit ausgegangen werden konnte.

In diesem Kontext war allerdings ebenfalls der Frage nachzugehen, wie es sich verhalten würde, wenn die personenbezogenen Daten, deren Erhebung ausschließlich zweckgebunden erfolgen durfte, zu anderen als den ursprünglichen Zwecken weiterverarbeitet werden. Das war deshalb von Belang, weil die AIS-Daten im Projekt EMSec zunächst allein aus Forschungsgründen erhoben, später allerdings in ein Echtzeitlagebild integriert und mit weiteren Daten verknüpft wurden, womit die Erhöhung der maritimen Sicherheit bezweckt war. Hier wurden also durchaus verschiedene Zwecke verfolgt. Insofern war Art. 6 Abs. 4 DS-GVO zu beachten, wonach die Weiterverarbeitung mit den ursprünglichen Zwecken vereinbar sein muss. Dabei berücksichtigt der Verantwortliche u. a. „jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung“, vgl. Art. 6 Abs. 4 lit. a) DS-GVO. Da die Forschung EMSecs in dem Bestreben erfolgte, die Sicherheit im maritimen Bereich zu erhöhen, bestünde eine hinreichende Verbindung zwischen den beiden Zwecken und die Weiterverarbeitung wäre folglich mit den ursprünglichen Zwecken vereinbar. Eine

[302] S. o. unter Punkt II. 2.2.8.

gesonderte Rechtsgrundlage für die Weiterverarbeitung der Daten wäre in einem solchen Fall dann nicht erforderlich.[303]

2.2.9.3 Rechte der Betroffenen

Doch auch in diesem Fall der rechtmäßigen Datenverarbeitung gibt die DS-GVO der betroffenen Person eine Reihe von Rechten an die Hand, die sich aus den Art. 12 ff. DS-GVO ergeben.

Informationspflicht

Beispielsweise trifft den Verantwortlichen grds. eine Informationspflicht, wenn die personenbezogenen Daten – wie hier – nicht bei der betroffenen Person erhoben wurden, Art. 14 Abs. 1 DS-GVO. Diese Pflicht bezieht sich u. a. auf die Nennung des Namens und der Kontaktdaten des Verantwortlichen (lit. a)) oder die Zwecke und die Rechtsgrundlage der Datenverarbeitung (lit.c)). Zusätzlich zu übermittelnde Informationen ergeben sich aus Abs. 2. Allerding sind in Abs. 5 Ausnahmen zu den vorgenannten Pflichten vorgesehen; dies betrifft bspw. Fallgestaltungen, in denen sich die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (lit. b)). Bei der Ermittlung, ob mit der Information des Betroffenen ein unverhältnismäßiger Aufwand verbunden ist, sind die o.g. - im Rahmen der Untersuchung zum BDSG aufgeführten - Maßstäbe[304] anzulegen. Dergestalt würde auch in diesem Fall der Ausnahmetatbestand des Art. 14 Abs. 5 lit. b) DS-GVO greifen, weil die Information aller betroffenen Schiffscrews praktisch unmöglich wäre.[305]

2.2.9.4 Weitere Rechte des Betroffenen

Als weitere Rechte des Betroffenen ergeben sich

- das Recht auf Berichtigung unrichtiger personenbezogener Daten, Art. 16 DS-GVO,
- das Recht auf Löschung, zB, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, Art. 17 Abs. 1 lit. a) DS-GVO,
- das Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO,
- das Recht auf Datenübertragbarkeit, Art. 20 DS-GVO,

[303] Vgl. EG 50 DS-GVO.

[304] S. o. unter Punkt II. 2.2.8.

[305] S. o. unter Punkt II. 2.2.8.

- ein Widerspruchsrecht, Art. 21 DS-GVO.

2.2.9.5 Pflichten des Verantwortlichen

Zudem treffen den Verantwortlichen allgemeine Pflichten im Zusammenhang mit der Datenverarbeitung.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung

Nach Art. 24 Abs. 1 S. 1 DS-GVO setzt er bspw. „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“. Konkretisiert wird dies in Art. 25 DS-GVO, wonach Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewähren ist. Als Beispiel für geeignete technische und organisatorische Maßnahmen wird dabei die Pseudonymisierung genannt, Art. 25 Abs. 1 DS-GVO. Unter dem Begriff der Pseudonymisierung ist dabei „die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Die weitere Verwendbarkeit der im Projekt EMSec gesammelten personenbezogenen Daten war nicht ersichtlich, weil es tatsächlich allein auf die Position des Schiffes ankam und es dergestalt keine Rolle spielte, welche Personen sich an Bord befinden. Insofern wäre es möglich und würde auch dem Grundsatz der Datenminimierung entsprechen, dass die Daten nach ihrer Erhebung pseudonymisiert werden.

Weitere technische und organisatorische Maßnahmen zum Schutz der gesammelten Daten benennt Art. 32 Abs. 1 DS-GVO. Dies sind

- die Verschlüsselung personenbezogener Daten, (lit. a)),
- die Fähigkeit, die Vertraulichkeit und Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, ((lit. b)),
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, (lit.c)), sowie

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, (lit. d)).

Verzeichnis von Verarbeitungstätigkeiten

Überdies hat der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, welches verschiedene näher bezeichnete Angaben zu der Datenverarbeitung enthält, Art. 30 Abs. 1 DS-GVO. Abs. 5 sieht allerdings Ausnahmen für den Fall vor, dass es sich um ein Unternehmen oder eine Einrichtung handelt, die weniger als 250 Beschäftigte hat; dies jedoch nur insoweit, als mit der Verarbeitung keine Risiken für die Rechte und Freiheiten der betroffenen Personen einhergehen. Solche Risiken waren im Projekt EMSec nicht ersichtlich und sind auch für Folgeprojekte dieser Art nicht zu befürchten, da es sich bei den AIS-Daten um keine besonders sensiblen Informationen handelt und die Rechte und Freiheiten der Betroffenen mit hinreichenden Datenschutzvorkehrungen wie der Pseudonymisierung gewahrt werden können.

Meldepflicht

Nach Art. 33 DS-GVO besteht ferner die Pflicht des Verantwortlichen, unverzüglich eine entsprechende Meldung an die Aufsichtsbehörde herauszugeben, wenn es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist. Diese Pflicht besteht dann nicht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Sollten die entsprechenden Datenschutzvorkehrungen getroffen werden, ist ein solches Risiko nicht anzunehmen (s. o.).

Benachrichtigungspflicht

Für den Fall, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, sieht die DS-GVO in Art. 34 Abs. 1 weiterhin die Pflicht des Verantwortlichen vor, die betroffene Person unverzüglich darüber zu benachrichtigen. Ein erhöhtes Risiko ist hier jedoch nicht ersichtlich (s. o.), sodass die Benachrichtigungspflicht entfällt.

Datenschutzfolgenabschätzung

Ein neues Instrument, das mit der DS-GVO eingeführt wird, ist die sog. Datenschutz-Folgenabschätzung, mit der ein Verantwortlicher abschätzt, welche Folgen die vorgesehene Datenverarbeitung für den Schutz personenbezogener Daten hat. Einer solchen Folgenabschätzung bedarf es wiederum nur, wenn die Verarbeitung voraussichtlich ein

hohes Risiko für die Rechte und Freiheiten natürlicher Personen in sich birgt, was hier indes nicht angenommen werden kann.

2.2.9.6 Weitere Vorschriften

Weitere Vorschriften betreffen bspw. die Benennung eines Datenschutzbeauftragten (Art. 37 DS-GVO), neuartige Zertifizierungsverfahren (Art. 42 DS-GVO), allgemeine Grundsätze der Datenübermittlung (Art. 44 ff. DS-GVO) oder auch Regelungen zur Aufsichtsbehörde (Art. 51 ff. DS-GVO).

2.2.9.7 Zwischenergebnis

Die DS-GVO stellt ähnliche Voraussetzungen für die Datenverarbeitung wie das BDSG auf, sodass eine entsprechende Verarbeitung der AIS-Daten auch künftig rechtmäßig erfolgen dürfte. Hinsichtlich der Weiterverarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwecken lockert die DS-GVO das bisher geltende nationale Datenschutzrecht allerdings dahingehend auf, dass keine gesonderte Rechtsgrundlage erforderlich ist, sofern beide Zwecke miteinander vereinbar sind. Darüber hinaus führt sie weitere Instrumente für den Datenschutz ein wie die Datenschutz-Folgenabschätzung. Voraussetzung für den Einsatz dieser Mittel ist jedoch zumeist das Bestehen eines erhöhten Risikos für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Person.

2.2.9.8 Fazit

Die Untersuchung hat aufgezeigt, dass sich aus mehreren Gesetzeswerken Vorschriften für den Umgang mit AIS-Daten ergeben. Aufgrund der Einhaltung dieser Vorgaben stand und steht der Datenverarbeitung zu den Zwecken des Verbundvorhabens sowie etwaiger Folgeprojekte nichts entgegen.

3. Wichtigste Positionen des zahlenmäßigen Nachweises

Zu den wichtigsten Positionen des zahlenmäßigen Nachweises gehört v. a. die Beschäftigung von wissenschaftlichem Personal. Mit den Arbeiten der Arbeitspakete sowie mit Verwaltungsaufgaben, die sich während der Projektlaufzeit ergaben, war eine wissenschaftliche Mitarbeiterin dauerhaft betraut. Unterstützung erhielt sie dabei von weiteren wissenschaftlichen Mitarbeitern und studentischen Hilfskräften; dies insbesondere, was Literaturbeschaffungs- und Kopierarbeiten betraf. Teile des Arbeitspakets Nr. 3300 wurden dabei von den letztgenannten Mitarbeitern übernommen.

Eine weitere wesentliche Position des zahlenmäßigen Nachweises ist in der Literaturbeschaffung zu sehen. Für die Erstellung der Gutachten und hier v. a. des Datenschutzkatalogs war es notwendig, aktuelle Fachliteratur, welche sich nicht im Bestand der Bibliothek des Ostseeinstituts für Seerecht, Umweltrecht und Infrastrukturrecht befand, anzuschaffen.

Zuletzt waren zahlreiche Dienstreisen erforderlich, um Verpflichtungen ggü. dem Projektgeber zu entsprechen, die erzielten Ergebnisse zu präsentieren und sich fachlich auf einschlägigen Veranstaltungen weiterzubilden.

4. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Hinsichtlich des Arbeitspakets Nr. 3300 konnten vielfältige datenschutzrechtliche Fragestellungen aufgezeigt werden. Insbesondere ergaben sich einige Problemfelder, auf die näher eingegangen werden musste. Fraglich war z. B., ob es sich bei den AIS-Daten um personenbezogene oder zumindest -beziehbare Daten handelt und das BDSG somit Anwendung finden konnte. Sodann musste hinterfragt werden, ob die zahlreichen Vorschriften des Gesetzes von den Projektpartnern eingehalten wurden bzw. werden konnten. Besonderes Augenmerk war darauf zu legen, dass es sich um eine AIS-Datenerhebung resp. -verarbeitung handelte, die zu Forschungszwecken erfolgte, sodass die entsprechenden Normen heranzuziehen waren. Hinsichtlich der Kombination „Erhebung bzw. Verarbeitung von AIS-Daten zu Forschungszwecken) konnte nur marginal auf bestehendes Material zurückgegriffen werden. Das Gutachten wird insofern für weitere Arbeiten, welche AIS-daten zum Gegenstand haben, verwertbar sein. Ein weiterer Themenschwerpunkt, für den im Grunde gleiches gilt, betraf die verständliche Aufbereitung der Vorgaben des SatDsiG, für die zu einem wesentlichen Teil ausschließlich auf die Gesetzesmaterialien zurückgegriffen werden konnte. Aus alledem ergibt sich die Notwendigkeit und Angemessenheit der geleisteten Arbeiten.

5. Darstellung des voraussichtlichen Nutzens

Die Forschungsergebnisse zielten darauf ab, Rechtssicherheit für die Forscher und die Endnutzer zu schaffen, insbesondere was datenschutzrechtliche Vorgaben betrifft. Dementsprechend wurde ein umfassender Datenschutzkatalog erstellt, mit dem bestimmte Fragestellungen der Projektpartner beantwortet wurden. Auch für zukünftige Forschungsvorhaben, die sich mit der Erhebung und Verarbeitung von AIS-Daten befassen, kann auf jenes Dokument zurückgegriffen werden, sodass die jeweiligen Stellen mit der Gewissheit forschen, sich in einem rechtlich abgesicherten Bereich zu bewegen, sofern sie die Maßgaben der einschlägigen Gesetze einhalten. Mit der Bearbeitung des Datenschutzkatalogs konnte ferner erreicht werden, das bisher eher stiefmütterlich behandelte Thema der rechtlichen Besonderheiten von AIS-Daten der öffentlichen Diskussion zuzuführen und das Bewusstsein für damit im Zusammenhang stehende Problemstellungen zu fördern. So wurde das Thema auf zahlreichen – auch internationalen –

Plattformen diskutiert und wird ein Workshop eigens zu diesem Gegenstand abgehalten.[306] Die Diskussion könnte dazu führen, dass notwendige Rechtsgrundlagen geschaffen werden wie dies etwa bereits im Bereich von Inland-AIS durch Änderungen des Binnenschifffahrtsaufgabengesetzes geplant ist.[307]

6. Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

Wie gesehen, behandelten die im Projekt bearbeiteten Arbeitspakete Themenschwerpunkte, für die nur wenig verwertbares Material bestand. Demzufolge ist davon auszugehen, dass die wissenschaftliche Diskussion darüber mit den geleisteten Arbeiten erst angestoßen wurde/wird. Während der Projektlaufzeit waren nach Einschätzung des Antragstellers somit auch keine Fortschritte auf dem Gebiet des Teilvorhabens bei anderen Stellen zu verzeichnen.

7. Erfolgte und geplante Veröffentlichungen der Ergebnisse

C. *Reuker*, Combating Piracy – Legal and technical solutions, in: P. Chaumette (Hrsg.), Maritime areas: control and prevention of illegal traffics at sea – Espaces marins: surveillance et prévention des trafics illicites en mer, S. 221-232

C. *Wegener* (nunmehr *Reuker*), Globale Maritime Sicherheitsstrategie der EU: Lageerfassung, Überwachung und Informationsaustausch im maritimen Bereich, Vortrag zum Deutschen Luft- und Raumfahrtkongress 2015, abrufbar unter http://www.dglr.de/publikationen/2015/370282.pdf

C. *Wegener* (nunmehr *Reuker*)/J. *Martens*, Rechtlicher Rahmen für die AIS-Datenerhebung zu Forschungszwecken durch nicht-öffentliche Stellen, Poster für den Deutschen Luft- und Raumfahrtkongress 2015, abrufbar unter http://www.dglr.de/publikationen/2015/370295.pdf

C. *Reuker*, Optimierung maritimer Sicherheit durch Vorsorge - raumbezogenes Risikomanagement, Dissertation, Einreichung in Vorbereitung

Geplant ist überdies die Veröffentlichung der Ergebnisse des am 20. Juni 2017 stattfindenden Workshops „AIS-Daten“ in einem eigenen Tagungsband des Ostseeinstituts für Seerecht, Umweltrecht und Infrastrukturrecht

[306] AIS-Workshop des Ostseeinstituts für Seerecht, Umweltrecht und Infrastrukturrecht der Universität Rostock am 20. Juni 2017.

[307] Siehe dazu den Gesetzentwurf der Bundesregierung, Drs. 18/10818.

Berichtsblatt

1. ISBN oder ISSN Geplant	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schussbericht
3. Titel Schlussbericht für das BMBF-Verbundprojekt „Echtzeitdienste für die Maritime Sicherheit – Security (EMSec)“ - Begleitforschung für die maritime Sicherheit/Rechtliche Aspekte	
4. Autor(en) [Name(n), Vorname(n)] Reuker, Caroline	5. Abschlussdatum des Vorhabens Dezember 2016
	6. Veröffentlichungsdatum Geplant
	7. Form der Publikation Buch
8. Durchführende Institution(en) (Name, Adresse) Ostseeinstitut für Seerecht, Umweltrecht und Infrastrukturrecht der Universität Rostock, Richard-Wagner-Straße 31, 18119 Rostock-Warnemünde	9. Ber. Nr. Durchführende Institution -
	10. Förderkennzeichen 13N12751
	11. Seitenzahl 154
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 831
	14. Tabellen 0
	15. Abbildungen 0
16. Zusätzliche Angaben -	
17. Vorgelegt bei (Titel, Ort, Datum) -	

18. Kurzfassung

<u>Datenschutzkatalog</u> (Arbeitspaket 3300)

1. Derzeitiger Stand
Den rechtlichen Rahmen für den Umgang mit AIS-Daten bilden das SatDsiG, das GeoZG, das UIG, das IFG, das BSIG, das TMG, das TKG, das BDSG und die EU-Datenschutzgrundverordnung.

2. Begründung/Zielsetzung der Untersuchung
Das Forschungsvorhaben EMSec zielte darauf ab, maritimen Risiken und Gefahren mithilfe von verständlich aufbereiteten Informationen und Lagebildern aus verschiedenen Quellen (Satelliten, Flugdienste) frühzeitiger begegnen zu können. Um die entsprechenden Möglichkeiten erforschen zu können, war für die Projektpartner der Umgang mit AIS-Daten essentiell. Dergestalt war es Aufgabe der rechtlichen Begleitforschung, die übrigen - technisch geprägten – Teilvorhaben in rechtlicher Hinsicht abzusichern und einen umfassenden Datenschutzkatalog zu erstellen.

3. Methode
Zunächst war dafür der Datenkontakt der einzelnen Projektpartner untereinander darzustellen. Im Abschluss daran wurden die Gesetze ermittelt und ausgewertet, die diesbezüglich zum Einsatz gelangen könnten.

4. Ergebnis
Im Ergebnis waren v. a. das SatDSiG und das BDSG mit ihren jeweiligen Vorgaben zu beachten, da es sich bei den AIS-Daten um personenbezogene bzw. -beziehbare Geodaten handelt. Der persönliche Anwendungsbereich des GeoZG war hingegen nicht eröffnet und es bestand auch kein Zugangsanspruch zu den im Projekt erhobenen Daten nach dem UIG und dem IFG. Überdies war weder der persönliche noch der sachliche Anwendungsbereich des BSIG eröffnet. Auch den datenschutzrechtlichen Vorgaben des TMG war nicht weiter nachzugehen, weil sie ausschließlich für das spätere Anbieter-Nutzer-Verhältnis zwischen Betreiber und Endanwender gelten. Es ergaben sich aus dem TMG indes Informationspflichten, die zu beachten waren. Die datenschutzrechtlichen Vorschriften des TKG mussten ebenfalls nicht berücksichtigt werden, da insofern ein öffentlich zugänglicher Informationsdienst vorausgesetzt wurde, den das Vorhaben EMSec jedoch nicht zum Gegenstand hatte.

5. Schlussfolgerungen/Anwendungsmöglichkeiten
Die Auswertung der datenschutzrechtlichen Rahmenbedingungen hat ergeben, dass die Durchführung des Forschungsvorhabens aus rechtlicher Sicht nicht beanstandet werden konnte, soweit die entsprechenden Vorgaben von den Projektpartnern eingehalten wurden.

19. Schlagwörter
Datenschutzkatalog, SatDSiG, GeoZG, UIG, IFG, BSIG, TMG, TKG, BDSG, EU-DSGVO, Personenbezogene Daten, AIS-Daten, Geodaten, Grundsatz der Direkterhebung, Datenerhebung zu Forschungszwecken, Daten aus allgemein zugänglichen Quellen

20. Verlag	21. Preis
geplant	geplant

Document Control Sheet

1. ISBN or ISSN planned	2. type of document (e.g. report, publication) Final report

3. title

Final report for the joint BMBF project „Echtzeitdienste für die Maritime Sicherheit – Security (EMSec)“ -
Accompanying research regarding maritime security/legal aspects

4. author(s) (family name, first name(s))	5. end of project December 2016
Reuker, Caroline	6. publication date planned
	7. form of publication Book
8. performing organization(s) (name, address)	9. originator’s report no. -
Ostseeinstitut für Seerecht, Umweltrecht und Infrastrukturrecht, University of Rostock, Richard-Wagner-Straße 31, 18119 Rostock-Warnemünde	10. reference no. 13N12751
	11. no. of pages 154
12. sponsoring agency (name, address)	13. no. of references 831
Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. no. of tables 0
	15. no. of figures 0

16. supplementary notes
-

17. presented at (title, place, date)
-

18. abstract

<u>Catalogue for data protection</u> (work package no. 3300)

1. Current state of science and technology
The legal framework for the dealing with AIS-data consists of the SatDsiG, the GeoZG, the UIG, the IFG, the BSIG, the TMG, the TKG, the BDSG and the General Data Protection Regulation oft he European Union.

2. Aim of the research
The joint BMBF project „EMSec“ aimed to tackle maritime risks and dangers at an earlier stage. This should be realised by creating comprehensibly prepared information and situation pictures from various sources (satellites, air services). In order to be able to explore the corresponding possibilities, the handling of AIS data was essential for the project partners. It was thus the task of the legal accompanying research to point out the relevant regulations.

3. Method
First of all the data contact of the partners was tob e presented. Then the relevant regulations were identified and evaluated.

4. Result
As a result, especially the SatDSiG and the BDSG were applicable because AIS-Data are personal data as well as geodata.

5. Conclusions
The evaluation of the data protection framework has shown, that the research of the remaining project partners could not be objected.

19. keywords
data protection, SatDSiG, GeoZG, UIG, IFG, BSIG, TMG, TKG, BDSG, General Data Protection Regulation oft he European Union, personal data, AIS-data, geodata

20. publisher planned	21. price planned