BMWi VII B3

Bonn, 16. April 2008
Hausruf: 03018 615-4352

Nationale Datensicherheitspolitik für raumgestützte Erdfernerkundungssysteme

Hintergrundinformation zum
Satellitendatensicherheitsgesetzes SatDSiG
und zur Rechtsverordnung SatDSiV

Der Deutsche Bundestag hat am 20. September 2007 das Gesetz zum Schutz vor Gefährdungen der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG) verabschiedet.

Das Gesetz ist am 01. Dezember 2007 in Kraft getreten.

Hintergrund

Ziel des Gesetzes ist zum einen die Wahrung der sicherheits- und außenpolitischen Interessen der Bundesrepublik Deutschland beim Verbreiten und kommerziellen Vermarkten von satellitengestützt erzeugten Erdfernerkundungsdaten – insbesondere auch auf den internationalen Märkten. Zum anderen wird durch das Gesetz Rechtssicherheit für betroffene Unternehmen geschaffen und die Besetzung der neuen Geschäftsfelder für die sich entwickelnden Unternehmen im Satellitendatenvertrieb - und damit auch für die wachsende Geodatenindustrie - kalkulierbar gemacht. Damit wird eine wichtige Voraussetzung dafür geschaffen, dass die deutschen Unternehmen Satellitenanwendungen in wirtschaftlich tragfähige Geschäftsmodelle umsetzen und neue Absatzmärkte erschließen können.

Zur Erreichung dieses Zieles wurde der Gesetzentwurf in enger Abstimmung mit den betroffenen Ministerien (insbesondere AA, BMI, BMVg, BMJ, BMF, BMELV, BMVBS, BMU, BMBF), dem BKAmt sowie den betroffenen Behörden (BND, BKA, BSI, AGeoBw) und Bundesbeauftragten entwickelt. Zusätzlich wurde bereits in frühen Phasen der Konzeption Kontakt mit den unmittelbar und mittelbar betroffenen Unternehmen sowie den betroffenen Verbänden aufgenommen.

. . .

Erforderlichkeit gesetzgeberischen Handelns

Das SatDSiG wurde erforderlich, weil in Deutschland sehr leistungsfähige Erdfernerkundungssatelliten mit dem Ziel einer gewerblichen weltweiten Vermarktung der Bilder/Daten realisiert werden. Mit dem Start des deutschen TerraSAR-X Satelliten (räumlich hochauflösender Radarsatellit mit Allwetter- sowie Tag/Nacht-Beobachtungsfähigkeit) im Juni 2007 hat Deutschland in Europa – und möglicherweise auch weltweit - eine Führungsrolle in der satellitengestützten Erdfernerkundung eingenommen und wird diese mit bevorstehenden Starts der Satellitenflotte RapidEye (Flotte kleiner optischer Satelliten zur multispektralen Beobachtung mit hoher zeitlicher Wiederholrate, Start Frühjahr 2008) und den sich bereits in fortgeschrittenen Projektphasen befindlichen noch leistungsfähigeren Systemen der nächsten Generation TanDEM-X (Interferometrisches Radarsatellitensystem mit drei-dimensionaler Beobachtungsfähigkeit, Start 2009) und EnMAP (hyperspektraler optischer Satellit, Start 2011) ausbauen.

Die entstehenden Erdfernerkundungsdaten stehen zur zivilen weltweiten Vermarktung zur Verfügung und haben insbesondere bei Satelliten wie TerraSAR-X oder TanDEM-X eine Qualität, welche bis in der Vergangenheit nur von klassifizierten militärischen bzw. nachrichtendienstlichen Satelliten erzeugt werden konnte und ausschließlich in diesem eng begrenzten Umfeld genutzt wurde.

Das Verbreiten dieser hochwertigen Erdfernerkundungsdaten kann außen- oder sicherheitspolitische Interessen gefährden: so etwa bei Satellitenaufnahmen von Gebieten, in denen sich die Bundeswehr im Auslandseinsatz befindet, oder von Gebieten, in denen sich große Flüchtlingsströme aufhalten. Selbst ohne eine unmittelbare Sicherheitsgefährdung können Wirkungen von Waffen oder politische Drohungen durch solche Erdfernerkundungsdaten erheblich verstärkt werden.

Ein unkontrolliertes Verbreiten solcher Daten aus Deutschland oder von deutschen Erdfernerkundungssystemen liefe auch dem Friedensgebot des Grundgesetzes zuwider. Das gilt nicht nur für die Nutzung der Daten in zwischenstaatlichen Konflikten, sondern auch durch nichtstaatliche Akteure bei Gewaltanwendung unterhalb einer kriegerischen Auseinandersetzung, beispielsweise in ethnischen Konflikten, bei bürgerkriegsähnlichen Unruhen oder terroristischen Akten. Politisch kann die Bundesrepublik Deutschland hierdurch auch Vorwürfen ausgesetzt sein, dass militärisch verwendbare Daten von deutschen Erdfernerkundungssystemen infolge fehlender Kontrolle an Dritte gelangen und hierdurch zur Gefährdung für andere Staaten werden.

Eine Gefährdung der sicherheits- und außenpolitischen Interessen der Bundesrepublik

. . .

kann dabei nicht nur durch eine besonders hohe geometrische Auflösung sondern beispielsweise auch durch andere technischen Merkmale oder durch die besondere Aktualität der Erdfernerkundungsdaten entstehen.

Daten von hochwertigen raumgestützten Erdfernerkundungssystemen sind daher nicht mit frei zugänglichen Daten, wie sie beispielsweise im Internet angeboten werden, zu vergleichen. Daraus ergibt sich einerseits der hohe kommerzielle Wert dieser Satellitendaten und andererseits die in betroffenen Staaten wie USA, Kanada, Frankreich oder Indien ebenfalls erkannte Notwendigkeit zur staatlichen Regulierung beim Verbreiten solcher Daten.

Aus außenpolitischer Sicht ist die nationale gesetzliche Regelung wichtig, um die Zusammenarbeit der Länder mit hoch entwickelten Erdfernerkundungssystemen vorantreiben zu können. Praktisch alle leistungsfähigen Satellitensysteme (auch die erwähnten deutschen Vorhaben) sind beispielsweise auf Exportgenehmigungen einzelner US-Bauteile angewiesen. Die USA fordern in diesen Fällen verbindliche nationale Regelungen, die die Sicherheitsinteressen bezüglich der Daten berücksichtigen. Eine gesetzliche Regelung ermöglicht an dieser Stelle die Berücksichtigung der amerikanischen Anforderungen und bietet zugleich die Chance, auf diesem Feld eigenständige Lösungen zu verfolgen, mit denen deutsche Unternehmen weltweit operieren können.

Von besonderer Bedeutung ist dafür, dass das SatDSiG ein schnelles und dennoch effizientes Verfahren zum Verbreiten von Erdfernerkundungsdaten vorsieht, in dem die betroffenen Unternehmen selbst anhand eines Prüfverfahrens mit klaren Kriterien feststellen, ob das Verbreiten der Daten an einen Kunden möglicherweise kritisch ist.

Internationale Rechtslage

In den USA gibt es eine entsprechend formalisierte nationale Datensicherheitspolitik seit 1992 und in Kanada seit Ende 2005. Die kanadische Regelung wurde auf Grundlage eines amerikanisch-kanadischen Regierungsabkommens erstellt und lehnt sich an die amerikanischen Regelungen an.

In Frankreich ist Ende April 2007 der Entwurf eines Gesetzes zur Regelung von Weltraumaktivitäten veröffentlicht worden, der auch Regelungen bezüglich der Verwendung von Erdfernerkundungsdaten enthält und in dessen Kurzbegründung auf das deutsche SatDSiG verwiesen wird. Seit Kurzem bestehen auch Regelungen in Indien und in Japan wird ein Gesetzentwurf vorbereitet.

Das weitgehende Fehlen entsprechender Regelungen in anderen Ländern begründet sich in der noch geringen Zahl von Staaten, die über derart leistungsfähige

. . .

Erdfernerkundungssatelliten verfügen. Insbesondere in Europa nimmt Deutschland technisch und mit seinen Überlegungen zu einer nationalen Datensicherheitspolitik und deren Umsetzung SatDSiG eine Vorreiterrolle ein und könnte so auch einen wesentlichen Beitrag zu der Gestaltung der in Zukunft vermutlich auch auf EU-Ebene und im ESA-Rahmen erforderlichen Regelungen leisten.

Zentrale Aspekte des SatDSiG

Grundgedanke des Gesetzes ist es, einerseits nur im Sinne des SatDSiG „hochwertige“ raumgestützte Erdfernerkundungssysteme zu erfassen und andererseits ein klar definiertes und transparentes Verfahren zum Verbreiten von Daten dieser Systeme zu etablieren.

Es fallen daher weder Luftbilder noch Daten von Navigationssatellitensystemen wie GPS oder dem zukünftigen europäischen Galileo in den Anwendungsbereich des Gesetzes. Militärische und nachrichtendienstliche Erdfernerkundungssysteme sind ausdrücklich aus dem Anwendungsbereich ausgenommen.

Die Hochwertigkeit eines Erdfernerkundungssystems im Sinne des SatDSiG ergibt sich aus dessen Potential, Daten mit besonders hohem Informationsgehalt zu erzeugen. In die Beurteilung fließen u.a. die geometrische Auflösung, die spektrale Abdeckung, die Zahl der Spektralkanäle und die spektrale Auflösung mit ein. Eine Rolle können auch die radiometrische und zeitliche Auflösung spielen; bei Mikrowellen- oder Radarsensoren zusätzlich Polarisationsmerkmale und Phasengeschichte.

Kern des SatDSiG ist die Etablierung eines Kontrollverfahrens zum Verbreiten von Satellitendaten/-bilder solcher hochwertiger Erdfernerkundungssysteme. Ziel ist es Schaden für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker und die auswärtigen Beziehungen der Bundesrepublik Deutschland zu vermeiden. Das SatDSiG definiert dabei das Verbreiten als jede Form des erstmaligen Inverkehrbringens oder Zugänglichmachens der Daten für Dritte, unabhängig davon, ob es sich um eine gewerbliche oder wissenschaftliche Nutzung handelt. Infolgedessen sind die primären Datenvertreiber wie beispielsweise das Unternehmen Infoterra oder das Deutsche Fernerkundungsdatenzentrum (DFD, Einrichtung des DLR) betroffen – in der Regel jedoch nicht die typischen Fernerkundungs-Dienstleister, Datenveredler (Value-Adding-Unternehmen) oder Datenweiterverkäufer.

Das Kontrollverfahren ist zweistufig. Zunächst erfolgt durch den Datenvertreiber („Datenanbieter“ im Sprachgebrauch des SatDSiG) für jede individuelle Datenanfrage eines Kunden die sogenannte Sensitivitätsprüfung. Die Sensitivitätsprüfung ist ein

. . .

formalisiertes und standardisiertes Prüfverfahren mit fest vorgegebenen Kriterien und ist ein wesentlicher Mechanismus des SatDSiG. Stellt der Datenanbieter dabei fest, dass die Anfrage nicht sensitiv ist, kann er die Daten ausliefern. Stellt er dagegen die Sensitivität einer Anfrage fest, kann er entweder die Auslieferung unterlassen oder eine behördliche Prüfung und Erlaubnis beantragen.

In die Sensitivitätsprüfung fließen technische Daten der verwendeten Sensorbetriebsmodi (z.B. geometrische Auflösung des konkreten Datensatzes, beobachteter Spektral-/Frequenzbereich, Zahl der Spektralkanäle etc.), der durch die verwendete Verarbeitung erzielte Informationsgehalt der Daten (Spezifikation des Datenproduktes), das mit den Daten dargestellte Zielgebiet, der Zeitpunkt der Erzeugung der Daten und der Zeitraum zwischen der Erzeugung der Daten und der Bedienung der Anfrage (Zeitverzögerung zwischen Aufnahme der Daten und Lieferung an den Kunden), die Person des Anfragenden/Bestellers sowie die Bodensegmente, an welche die Daten gesendet werden sollen, ein.

Wesentlich für die praktische Anwendung ist, dass den betroffenen Unternehmen die Sensitivitätsprüfung als durch eine Verordnung fest vorgegebenes, automatisierbares Prüfverfahren übertragen wird, was insbesondere für den kommerziellen Datenvertrieb eine hohe Transparenz, Berechenbarkeit und Schnelligkeit des Prüfungsvorgangs garantiert und gleichzeitig den Verwaltungsaufwand für behördliche Prüfungen gering hält.

Dieses im SatDSiG realisierte zweistufige Verfahren aus der Kombination von Sensitivitätsprüfung als fest vorgegebene und standardisierte Vorprüfung mit einer gegebenenfalls erforderlichen behördlichen Einzelfallentscheidung ermöglicht es, kritische Fälle bereits beim Datenanbieter zuverlässig zu identifizieren und dann gegebenenfalls in einem normalen Verwaltungsverfahren durch die zuständige Behörde zu entscheiden. Gleichzeitig kann aus den bisherigen Erfahrungen erwartet werden, dass je nach Kundenstruktur und spezifischen Interessen der Kunden der weit überwiegenden Teil der Anfragen nicht sensitiv ist und daher ohne unmittelbare Einschaltung einer Behörde vom Datenanbieter bedient werden kann.

So werden die außen- und sicherheitspolitischen Interessen Deutschlands mit einem möglichst geringen Eingriff gewahrt und zugleich für den Datenanbieter ein hohes Maß an Rechtssicherheit geschaffen.

Um einen sicheren Umgang mit den Daten (Erzeugung, Übermittlung, Verarbeitung, Verbreiten, Archivierung) zu gewährleisten, müssen gewisse Anforderungen an den Betrieb der Satelliten, den Betreiber und den Datenanbieter gestellt werden. Hierzu sind eine Genehmigung zum Betrieb hochwertiger Erdfernerkundungssysteme sowie eine Zulassung für die Datenanbieter erforderlich.

Anlage

Überblick über das „Gesetz zum Schutz vor Gefährdungen der Sicherheit durch das Verbreiten von raumgestützten Erdfernerkundungsdaten“ (Satellitendatensicherheitsgesetz - SatDSiG)

Das Satellitendatensicherheitsgesetz gewährleistet, dass die durch Erdbeobachtungssatelliten („Erdfernerkundungssystemen“ im Sprachgebrauch des SatDSiG) modernster Bauart inzwischen auch kommerziell verfügbaren Erdfernerkundungsdaten nicht die sicherheits- und außenpolitischen Interessen der Bundesrepublik gefährden. Zugleich dient es der Rechtssicherheit für die betroffenen Unternehmen und fördert die wirtschaftliche Entwicklung im Bereich des Geoinformationsmarktes. Das SatDSiG ist 01. Dezember 2007 in Kraft getreten.

Die entsprechend der Verordnungsermächtigung im SatDSiG erforderliche ergänzende Rechtsverordnung SatDSiV wurde im Einvernehmen mit AA, BMI und BMVg am 05. April 2008 in Kraft gesetzt. SatDSiV legt einerseits die Kriterien und Grenzwerte zur Bestimmung der Hochwertigkeit eines Erdfernerkundungssystems sowie andererseits das Verfahren und die Parameter für die zum Verbreiten der Daten erforderliche Sensitivitätsprüfung fest.

Während das Gesetz die Rahmenbedingungen, Anforderungen und Verfahren für die Betreiber der betroffenen Satelliten und Datenanbieter sowie allgemeinen Eigenschaften von Erdfernerkundungssystemen und der damit erzeugten Daten festlegt, ermöglicht die Festlegung der eher technischen Kriterien und Grenzwerte in einer Verordnung eine Anpassung an die zukünftige technische Entwicklung und an Veränderungen der sicherheits- und außenpolitischen Gefahren. SatDSiV legt gemäß der Verordnungsermächtigung im SatDSiG (i) die Kriterien und Grenzwerte zur Bestimmung der Hochwertigkeit eines Erdfernerkundungssystems sowie (ii) das Verfahren, die Kriterien und Grenzwerte für die zum Verbreiten der Daten erforderliche Sensitivitätsprüfung fest.

Die Regelungen stehen beim Bundesgesetblatt, Teil I auch auf elektronischem Weg zur Verfügung:
SatDSiG: http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s2590.pdf
SatDSiV: http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s0508.pdf

Kernpunkte des Gesetzes

Das Satellitendatensicherheitsgesetz findet Anwendung auf den Betrieb „hochwertiger“, nicht-militärischer Erdfernerkundungssatelliten und auf das Verbreiten der damit erzeugten Daten bzw. der daraus ableitbaren Datenprodukte/Bilder. Die Hochwertigkeit im Sinne des SatDSiG ergibt sich aus den technischen Eigenschaften des Systems, die eine sicherheitsrelevante Nutzung erlauben können. Eine Vielzahl bestehender und zukünftiger Systeme wird jedoch wegen Fehlens solcher technischer Fähigkeiten nicht vom SatDSiG erfasst werden.
Zentrales Element der gesetzlichen Regelung ist das Verfahren der Sensitivitätsprüfung durch den Datenanbieter nach § 17. Dabei prüft der Datenanbieter durch Anwendung eines in der SatDSiV vorgegebenen Verfahrens, ob das Verbreiten der Daten eine mögliche Sicherheitsgefährdung zur Folge haben kann; ist dies der Fall, so wird eine behördliche Einzelfallprüfung erforderlich. Die streng formalisierte Sensitivitätsprüfung dient dazu, in einem ersten Prüfungsschritt unbedenkliche Datenanfragen zu ermitteln. Indem diese Prüfung vom

. . .

Datenanbieter selbst durchgeführt werden kann, belastet sie den Datenanbieter nur gering und ermöglicht täglich eine Vielzahl von Datenverbreitungsvorgängen ohne behördliche Prüfung. Wegen der eindeutigen Vorgaben zu Verfahren, Kriterien und Grenzwerten, ohne die Möglichkeit eines Beurteilungsspielraums für den Datenanbieter und mit der Ermächtigung für behördliche Kontrollen werden zugleich die außen- und sicherheitspolitischen Interessen Deutschland wirksam geschützt.
Daneben wird eine Genehmigungspflicht für den Satellitenbetreiber und eine Zulassungspflicht für den Datenanbieter eingeführt, um zu gewährleisten, dass die gesetzlichen Sicherheitsanforderungen eingehalten werden, und um der zuständigen Behörde im Vorfeld ein eingehende Prüfung zu ermöglichen.

Inhalt der Regelungen

Schutzgüter

Schutzgüter des Gesetzes sind die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker und die auswärtigen Beziehung der Bundesrepublik Deutschland. Dieser Schutz verläuft parallel zum Außenwirtschaftsrecht. Eine Bezugnahme auf die Schutzgüter findet sich in den §§ 2 Abs. 2, 10 Abs. 1 u. 2, 17 Abs. 2, 19 Abs. 2, 27 und 29 Abs. 1.

Anwendungsbereich

Der Anwendungsbereich (§ 1) wurde weit gezogen, um keine Lücken oder Umgehungsmöglichkeiten zu lassen. Erfasst werden alle deutschen Staatsangehörigen und Organisationen deutschen Rechts. Zusätzlich sind solche ausländischen Betriebe erfasst, die entweder ihren Hauptsitz im Bundesgebiet haben oder tatsächlich hier die maßgebliche Kontrolle über ihr Unternehmen ausüben. Damit sind alle Betriebe erfasst, gegenüber denen eine wirksame Durchsetzung des Gesetzes möglich ist.
Nicht in den Anwendungsbereich fallen militärische und nachrichtendienstliche Satelliten. Denn deren Daten werden von der staatlichen Stelle, die den Satelliten betreibt, in geeigneter Weise geheim gehalten. Zudem sind oder können solche Systeme ausgenommen werden, die einer in Hinblick auf die Schutzgüter vergleichbaren ausländischen Sicherheitsregelung unterworfen sind.
Da ausschließlich raumgestützte Erdfernerkundungssysteme in den Anwendungsbereich fallen, werden Kommunikations- oder Navigationssatelliten ebenso wenig erfasst wie die Erzeugung und das Verbreiten luftgestützter Erdfernerkundungsdaten.

Genehmigung des Satellitenbetriebs

Ist ein raumgestütztes Erdfernerkundungssystem (üblicherweise ein Satellit mit Erdfernerkundungssensor) als hochwertig anzusehen, so bedarf derjenige, der es betreibt einer behördlichen Genehmigung, § 3. Die Kriterien, aus denen sich die Hochwertigkeit des Erdfernerkundungssystems ergibt, sind u.a. die räumliche Auflösung, die spektrale Abdeckung sowie die spektrale und zeitliche Auflösung, § 2 Abs. 2. Sie werden in der Rechtsverordnung SartDSiV ausgefüllt.
Für die Betreibergenehmigung gelten nach § 4 Sicherheitsanforderungen, sowohl für die

. . .

verantwortlichen Personen, als auch für den Betrieb. Neben der Zuverlässigkeit des Betreibers müssen Personen, die Zugang zu den wesentlichen Betriebsanlagen haben, eine einfache Sicherheitsüberprüfung im Sinne des Sicherheitsüberprüfungsgesetzes besitzen. Die Betriebsräume müssen hinreichend gegen ein unbefugtes Eindringen gesichert sein und die Kommandierung des Satelliten muss mittels einer harten Verschlüsselung gesichert sein. Dabei kommen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüfte Verfahren zum Einsatz.
Weiterhin treffen den Betreiber Dokumentations- und Auskunftspflichten, damit die zuständige Behörde jederzeit in der Lage ist, sich ein Bild von den Aktivitäten des Betreibers zu machen, §§ 5 - 7. Darüber hinaus wird die Behörde zu Betriebsbesichtigungen ermächtigt, damit sie sich vor Ort vom vorschriftsmäßigen Verhalten des Betreibers überzeugen kann, § 8. Eine Generalklausel berechtigt die zuständige Behörde dazu, die erforderlichen Maßnahmen zu treffen, um einen rechtmäßigen Betrieb herzustellen oder den Betrieb zu untersagen, § 9.

Verbreiten von Erdfernerkundungsdaten

Wer Daten eines hochwertigen Erdfernerkundungssystems verbreiten möchte, bedarf einer Zulassung. Die Anforderungen, die das Gesetz an den Zulassungsinhaber stellt, sind dabei mit denen vergleichbar, die in § 4 an den Betreiber gestellt werden, § 12.
Der Datenanbieter (Zulassungsinhaber) darf in der Folge Daten eines hochwertigen Erdfernerkundungssystems nur dann verbreiten, wenn hierdurch die außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland nicht gefährdet werden.
In dem typischen Fall der Datenanfrage eines Kunden auf Lieferung von Daten wird dies durch ein zweistufiges Verfahren der Kontrolle realisiert. Hintergrund hierfür ist, dass bei der zu erwartenden hohen Zahl der Datenanfragen (derzeit wird von etwa 100 zu prüfenden Kundenanfragen pro Tag ausgegangen) eine behördliche Kontrolle einer jeden Kundenanfrage nicht praktikabel wäre. Denn der Aufwand und die dafür benötigte Zeit wären zu groß. Mangelnde Effizienz und eine Behinderung der Kommerzialisierung wären die Folge. Die zwei Stufen der Prüfung sehen folgendermaßen aus:
Die erste Stufe ist eine „Sensitivitätsprüfung“ konkreter Datenanfragen, welche der Datenanbieter nach dem in der SatDSiV vorgegebenen formalisierten Verfahren und mit klar definierten Kriterien (ohne Beurteilungsspielraum) durchführt, § 17. Die Prüfung erfolgt im Hinblick auf die Möglichkeit einer Sicherheitsgefährdung. In die Kriterien der Sensitivitätsprüfung fließen technische Parameter und u.a. Angaben über das beobachtetes Zielgebiet, die Person des Bestellers, das Bestimmungsland für die Datenprodukte und den Zeitabstand zwischen Aufzeichnung und Bedienung der Datenanfrage ein. Obwohl sich die Prüfung auf das Verbreiten eines konkreten Satellitenbildes bzw. Satellitendatensatzes bezieht, wird der eigentliche Inhalt der Daten selbst nicht geprüft, sondern nur die sogenannten Metadaten. Die Metadaten erlauben eine abstrakte Beschreibung des konkreten Datensatzes und eine Prüfung der Zulässigkeit der Weitergabe dieses Datensatzes bereits vor der Beobachtung des Zielgebiets durch den Satelliten. Zudem muss der Datenanbieter niemals einen Datensatz der Behörde offen legen.
Ergibt die Prüfung, dass die konkrete Datenanfrage als nicht sensitiv eingestuft wird, kann der Datenanbieter ohne weitere behördliche Prüfung die angefragten Datenprodukte liefern oder gegebenenfalls den Download der Daten zu einer Bodenstation des Kunden veranlassen.
Erst wenn der Datenanbieter bei dieser Prüfung eine besondere Sensitivität einer Kundenanfrage feststellt, ist ihm eine Bedienung der Kundenanfrage zunächst verboten. Er kann jedoch als zweite Stufe eine behördliche Prüfung beantragen, falls er die Anfrage dennoch bedienen möchte, § 19. Die Behörde prüft dann im Einzelfall, ob die Kundenanfrage geeignet ist, die Sicherheit zu gefährden. Wenn eine Gefährdung ausgeschlossen ist, wird dem Datenanbieter die

. . .

Erlaubnis erteilt, die Anfrage zu bedienen. Mögliches Prüfungsergebnis kann auch sein, dass eine Gefährdung ausgeschlossen ist, wenn die Datenanfrage geringfügig verändert wird, z.B. verringerte Auflösung, Zeitverzögerung, verringerte Verarbeitungsqualität der Daten oder Auslassen bestimmter Zielgebiete. In diesem Fall gewährt die Behörde eine Erlaubnis unter Auflagen. Wenn schließlich trotz möglicher Auflagen eine Gefährdung gegeben ist, bleibt dem Anbieter die Bedienung der Datenanfrage untersagt. Um den kommerziellen Betrieb dabei nicht mehr als nötig zu beeinträchtigen, wird die Behörde angehalten, den Antrag innerhalb einer kurzen Frist (max. ein Monat) bescheiden.

Gesellschaftsrechtliche Beschränkungen für Betreiber

Um Sicherheitsrisiken auszuschließen, die entstehen könnten, wenn ausländische Staatsangehörige eine Betreibergesellschaft oder Anteile an ihr, oder den Satelliten oder andere Teile des Erdfernerkundungssystems erwerben, werden diese Vorgänge durch § 10 mit einer Melde- bzw. Erlaubnispflicht beschränkt. Denn Ausländer können sich einfacher der Kontrolle, dem Zugriff und gegebenenfalls der Strafverfolgung entziehen.
Zudem stellt § 10 die Übernahme eines Erdfernerkundungssystems oder Teilen eines solchen unter einen Erlaubnisvorbehalt. Dies ist erforderlich, da bspw. der Übertragung eines im Orbit befindlichen Erdfernerkundungssatelliten andernfalls ohne weiteres erfolgen könnte. Weder wäre ein Verbreiten von Daten gegeben, welche nach dem SatDSiG geprüft werden könnte, noch wäre ein Exporttatbestand gegeben, welcher nach der EG Dual Use Verordnung geprüft werden könnte.

Vorrangige Bedienung von Anfragen der Bundesrepublik

Das Gesetz beinhaltet die Verpflichtung für den Betreiber und den Datenanbieter, Datenanfragen der Bundesrepublik in Ausnahmefällen zeitlich vorrangig zu behandeln. Als solche Ausnahmefälle werden der NATO-Bündnisfall, der Verteidigung- oder Spannungsfall und der Notstand angesehen. Ferner greift dieses Vorrecht auch zum Schutz von im Ausland eingesetzten militärischen oder zivilen Kräften der Bundesrepublik Deutschland, § 21. Dadurch wird gewährleistet, dass in diesen besonderen Fällen eine wichtige Datenanfrage in jedem Fall auch kurzfristig ausgeführt wird.
Um den Eingriff in die Rechte der betroffenen Datenanbieter bzw. Betreiber gering zu halten und um das Ziel einer Kommerzialisierung der Erdfernerkundung nicht zu gefährden, ist die Zahl dieser Ausnahmetatbestände sehr beschränkt. Relevant wird § 21 auch nur dann, wenn zusätzlich zur Datenanfrage der Bundesrepublik eine konkurrierende Datenanfrage eines anderen Kunden vorliegt und so ein Konflikt um die Ressourcen des Satelliten entsteht, also der Datenanbieter sich in diesen Fällen auch aus technischen Gründen nur für eine der Anfragen entscheiden kann.

Bußgeld- und Strafvorschriften

Es sind eine Reihe von Ordnungswidrigkeits- und Straftatbeständen in den Entwurf aufgenommen worden, §§ 28, 29. Auf diese Weise soll die Einhaltung dieses Gesetzes sichergestellt werden. Sie richten sich an den Betreiber und den Anbieter.

Zuständige Behörde

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) in Eschborn ist mit Ausnahme der Zuständigkeit für die Sicherheitsüberprüfungen und der Kontrolle des Unternehmenserwerbs als zuständige Behörde benannt und mit dem Verwaltungsvollzug des Gesetzes beauftragt. Zu den Aufgaben gehören insbesondere die Genehmigung zum Betrieb hochwertiger Erdfernerkundungssysteme, einschließlich der Aufsicht des Betreibers, die Erlaubnis zur Übertragung des Erdfernerkundungssystems nach § 10 Abs. 2, die Zulassung der Datenanbieter, einschließlich der Aufsichtsaufgaben (§§ 11, 12, 13 – 16); die Erlaubnis zur Bedienung sensitiver Anfragen nach § 19 und die Sammelerlaubnis zum Verbreiten nach § 20

Die Aufgaben der Erteilung der Erlaubnis für den Erwerb von Unternehmen (§ 10 Abs. 1) und die Prüfungsverfahren nach dem Sicherheitsüberprüfungsgesetz (SÜG) für Teile des Personals von Betreiber und Anbieter als Voraussetzung für eine Betreibergenehmigung und Anbieterzulassung sind beim BMWi angesiedelt.

Des Weiteren sind die Sicherheitsverfahren des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Rahmen der Betreibergenehmigung und der Anbieterzulassung zu berücksichtigen.