the selected data, or for other purposes, the distinction between primary data and processed data, as defined by UNGA Resolution 41/65, is very close to the distinction between jurisdiction under article VIII of the Outer Space Treaty and jurisdiction under article VI of the Outer Space Treaty. Indeed, considering primary data, it is remarkable that the definition does not include their *reception* on Earth. Only the transmission or the delivery is taken into account. This allows considering the production of primary data under the exclusive jurisdiction of the registering State according to article VIII of the Outer Space Treaty. With the production of processed data, it seems logical to consider that phase from the moment of the reception, on the ground, of the primary data until their transformation into a next level's product. This, of course, raises other questions about the line between space activities and non-space activities, and the actual scope of article VI of the Outer Space Treaty: must Google Earth be considered a potential source of a State's international responsibility under that provision?

These considerations lead to the conclusion that the registration of earth observation satellites by intergovernmental organizations might end up in some legal void when it comes to fulfilling the commitments under other provisions of the Outer Space Treaty. The wrongful or criminal use of *PROBA* or of the data it generates could definitely make Belgium and ESA internationally responsible, not only according to article VI of the Outer Space Treaty, but also according to general international law. The elaboration of an appropriate legal framework regulating earth observation activities would be difficult in such a context, since only the national jurisdiction on the satellite can effectively ensure the application of national law to it.

CURRENT STATUS AND RECENT DEVELOPMENTS IN GERMAN REMOTE SENSING LAW

Dr. Bernhard Schmidt-Tedd & Max Kroymann[*]

ABSTRACT

On December 1, 2007, the German Act on Satellite Data Security (Satellitendatensicherheitsgesetz – SatDSiG)[1] came into force. The purpose of the Act is, firstly, to safeguard the security and foreign-policy interests of the Federal Republic of Germany in connection with the dissemination and commercial marketing of satellite-generated earth remote sensing data especially on international markets. Secondly, the Act will create legal certainty for affected companies and enable emerging companies involved in satellite data marketing to determine the operating terms and calculate the risks in new business areas.[2] This paper provides an introduction to the policy background and to the Act as well as a survey of the practical requirements and Germany's first experiences in its administrative implementation.

PART I: POLICY AND CONTEXT OF THE REMOTE SENSING LEGISLATION

A. Development Trend / Background

The need for national space legislation has been under discussion in Germany for several years. The reason for this is the increasing number of space activities operated by the private sector. The Act to give Protection against the Security Risk to

---

[*] Please insert short (up to 5 sentences) bio.

[1] The unofficial English translation of the SatDSiG is appended to this paper in the Annex. The German text is also available at http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s2590.pdf.

[2] Drucksache des Bundestages, BT-Drs. 16/4763, p. 1, available at http://dip.bundestag.de/extrakt /16/019/16019379.htm.

the Federal Republic of Germany by the Dissemination of High-Grade Earth Remote Sensing Data, also known by its abbreviated name, the Satellite Data Security Act (SatDSiG), now regulates one area of application of space activities. This legislative initiative is closely linked with the first large-scale Public-Private-Partnership (PPP) projects in the field of earth remote sensing, in particular, in the field of radar observation.

Germany was first faced with the issue of the security relevance of radar data while participating in the bilateral Shuttle Radar Topography Mission (SRTM) Project with the United States in 2000. At that time, first considerations of a data policy were formulated between the Ministry that was then competent (Federal Ministry of Education and Research – BMBF) and the German Aerospace Center (DLR). Initially a system with a unique non-transferable license for the data in question (digital elevation models) was opted for. This enabled the DLR image archive (DFD) to have an oversight on all users, since these were not allowed to further distribute the data without authorization. The system was found to be incompatible with large-scale commercial dissemination as it had been envisaged when preparing the *TerraSAR-X* case.

Telecommunications were the first space application to be completely privatized. In contrast to telecommunications, observation of the Earth is commercially viable only to a limited extent. The funding of operative systems still relies mainly on public demand. Earlier attempts to achieve complete privatization failed.[3] Nevertheless, the aims to exploit the commercial potential of this application and thereby ease the financial burdens on public budgets remain.[4] In Europe, France was the first country to gradually undertake privatization with Spot Image, and with simultaneous linkage to the French national space

---

[3] Project 2001 – Legal Framework for Commercial Remote Sensing Activities Workshop, Toulouse, France (Oct. 28, 1998).

[4] Annie Martin-Moreno, *La Privatisation et la Commercialisation appliquées à l´observation de la Terre*, *in* LAURENCE RAVILLON, DROIT DES ACTIVITES SPATIALES 231 (CNRS, Dijon, France, 2004); L. Dufresne, *Le système de distribution français*, *in* S. COURTEIX, DROIT TELEDETECTION ET ENVIRONNEMENT 149 (SIDSE, Antony, France 1994).

agency Centre National d'Etudes Spatiales (CNES).[5] CNES, as grantor of the license, undertakes the security-relevant aspects of monitoring these activities in an informal manner, i.e. without a specific legal instrument in the form of a law or decree. The general competences of CNES are listed in the Act of 1961 establishing the French Space Agency.[6] It was clear, for the German legal position, that the national provisions on export control provide no legal basis for administrative intervention in the free dissemination of satellite data under existing law. Indeed, the provisions strictly apply to items listed in the applicable regulation, and only concern technology, know-how and material. Earth remote sensing data are not included in the listed items and do not constitute "technology," "know-how," or "material."

There is also no general space act in Germany that could provide a legal basis for administrative regulations (license obligations). On the other hand, it was obvious to the persons involved in the preparation of the *TerraSAR-X* Public-Private-Partnership (PPP) project that there was a need for action. For this reason, the objective was to create a concept that would both support the independent industrial commercialization of Earth observation data whilst adequately accommodating vital security interests.

B. PPP Projects as Triggers

Preparations for the SatDSiG took place during the implementation of the *TerraSAR-X* project. To better understand the SatDSiG, several characteristics of the implementation of this first PPP in the field of Earth remote sensing will be considered.

---

[5] Pierre-Marie Adrien, *A US-dilemma – Satellite Remote Sensing Privatization*, *in* II (1) SPACE POL'Y 93 (1986); S. Reif, B. Schmidt-Tedd, & K. Wannenmacher, *Report of the `Project 2001´ Working Group on Privatisation*, *in* `PROJECT 2001´- LEGAL FRAMEWORK FOR THE COMMERCIAL USE OF OUTER SPACE 458 (K.-H Bockstiegel ed., Böckstiegel, Cologne 2002).

[6] Loi No. 61-1382 du instituant le Centre National d´Etudes Spatiales (Dec. 19, 1961), analysed in Tedd B. Schmidt, *Staatliches Engagement bei partiell marktfähigen Raumfahrtanwendungen und die Verankerung des öffentlichen Interesses bei kommerziellen Raumfahrtanwendungen*, *in* LIBER AMICORUM KARL-HEINZ BÖCKSTIEGEL 424, 430 (M. Benkö & W. Kröll,Ed., Cologne 2001).

The *TerraSAR-X*-PPP project is based on investment jointly by the public sector (Federal space budget / DLR Space Agency / DLR Research & Development) and the private sector (EADS-Astrium / Infoterra). Even though there is joint investment in the project, the goals pursued (scientific / commercial) are different. There can be no talk of a common enterprise. DLR retains ownership of the satellite. All data obtained are first received by the DFD of DLR. The industrial partner receives a copy of the data, which means that ultimately both parties have a complete set of data in their archives. Contrary to a common misconception, the data are not split between the DLR and industry; instead each partner has a complete set of all data. The only distinction concerns the different rights that the DLR has on the data, as opposed to those of the industry. While DLR holds the exclusive rights to scientific use Infoterra, as an offshoot of EADS-Astrium, holds the exclusive commercialization rights. "Commercial use" includes both the data request of the private as well as of the public sectors. The public funds for *TerraSAR-X* originate from the research and space budgets. Other ministries, who are potential users of the data, had no intention to participate in the investment. The defense and security sectors deliberately decided against any share in investment and reserved the right to purchase data as required on completion of the system. Consequently, data requests of the public sector are part of the commercial business model. Only the scientific use of the data is excluded. This impacts some provisions of the SatDSiG. Even if the security authorities are mere "customers", and not investors, they must obviously be granted priority in ordering and tasking in times of crises. SatDSiG provides for such events. This means that Infoterra must also be prepared for such a situation within the framework of its commercialization concept. In principle, the *TerraSAR-X*-PPP distinguishes between only two categories, i.e. either scientific or commercial use. Also, data required for preventive environmental measures are regarded as user requirements and, therefore, constitute commercial use. Administrations and organizations acting in the public interest should also allocate regular budgets for recurring data requirements. Subsequent investments can only be financed in the long term through the sale of data. In the *Ter-*

raSAR-X-PPP, EADS-Astrium specifically undertook the obligation to finance the successor satellite *TerraSAR-X 2* from its own funds, respectively from revenues generated by the *TerraSAR-X* business case.

For the sake of completeness, it is necessary to add that, in the wake of the 2005 tsunami disaster and the development of the International Charter on Space and Major Disasters (Charter), to which DLR has also acceded, EADS-Astrium has agreed to make data available outside the normal dissemination channels in urgent crises situations. This adds to DLR's potential as a public entity and member of the Charter.

As a result, it can be said that the *TerraSAR-X*-PPP assumes the creation of a proper market for Earth observation data, which is used by public authorities, including defense, domestic security and public services. A system that would prevent the data provider from accessing sensitive data from the outset would therefore not be suitable.

It must also be clearly noted at this point that, based on the underlying legal principles, even data generated using public funds are legally protected. There is no concept under which data funded by public money should be public property *per se* with the result that anyone should have free access to these data. Throughout the entire project-development and preparation phases, great care was taken to prevent this from happening also by means of indirect influences. The extent to which public organizations provide data free of charge or at preferential rates to scientific organizations, for the public benefit or in general is logically a second independent step in the decision-making process.[7] European regulations on the free exchange of data between administrations[8] do not apply to the present PPP

[7] For basic information about data pricing policy, *see* RAY HARRIS, EARTH OBSERVATION DATA POLICY AND EUROPE 100 (West-Sussex, Great Britain 1997).

[8] *E.g.*, Directive 2003/4/EC of the European Parliament and of the Council of January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, O.J. (L 41/26)(EU); *see* Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 established an Infrastructure for Spatial Information in the European Community (INSPIRE), at Preamble (9): "This directive should not affect the existence or ownership of public authorities' intellectual property rights."; and Preamble (23): The mechanisms for sharing spatial data sets and services between government and other public administrations…should take into account the need to protect

case. Each PPP partner has the right to decide on its own data within the framework of the division of rights (scientific or commercial).

C. Basic Concepts and Policy

Prior to the commencement of its legislation process, Germany took decisions that also reflected the existing situation in Canada. When developing its own *Radarsat-2*, Canada had undertaken, in an intergovernmental agreement with the United States in June 2000, to adopt a security check comparable with the United States' standards. The Bill C-25: Act governing the operation of remote sensing space systems, which followed at the end of 2005, implements the provisions of the agreement in the domestic law system with effect towards non-governmental operators and data providers. Germany could have taken this easier course of action but this would have considerably reduced the ability to allow for German national particularities.

The first of these particularities is that the underlying economic conditions in Germany are entirely different. In the United States, the public sector's demand for data is very high, so that genuine private data requests can be considered merely as a small part of the whole. If the State buys all the data of a data provider at once for security reasons during a crisis situation, this may interfere with the operation of the market but it certainly will not have the same repercussions as in a country with a relatively low public demand and a market primarily for commercial data.

Further particularities include, in some cases, significant differences in the conception of the applicable national legal

---

the financial viability of public authorities, in particular those that have a duty to raise revenue."

Art. 1(2) "INSPIRE shall build upon infrastructures for spatial information established and operated by the Member States."

Art. 2(2) "This Directive does not affect the existence or ownership of public authorities' intellectual property rights."

Art. 4(5) "In case of spatial data sets…in respect of which a third party holds intellectual property rights, the public authority may take action under this Directive only with the consent of that third party."

framework. This is true of the concept of a "public good" in the case of data funded with public money, largely entrenched in the United States' legal system. Differences also exist in export-control regulations, which have similar importance for the security check in the case of sensitive Earth remote sensing data. United States' law gives exporters trading privileges and not trading rights.[9] The German law on Foreign Trade and Payments (AWG) is based on the principle of freedom of foreign trade. Approvals for legal transactions, for which a license is required (export list), must be granted if the competent authorities consider that the objectives of the Act are not endangered or only insignificantly so (§ 3.1.1 AWG).

As a result, Germany decided in favor of the more complicated method of drafting its own statute, which not only satisfies national requirements but also the legitimate expectations of international partners. Given the requirements of constitutional law, it was also clear that a purely administrative or informal rule without legal foundation could not be considered.

The following elements were taken into account during the legislation process of the SatDSiG:

- Prevention of an obvious gap between export-control provisions and loopholes in the regulation of security-relevant data.
- Basic principles of the freedom of trade on the one hand, and comprehensible, transparent decisions in case of necessary restrictions on a legal basis on the other hand.
- Support of the development of an autonomous commercial Earth observation data market for private and public users (outside scientific purposes).
- The legal protection of the data of Earth remote sensing PPP Projects, regardless of whether they are publicly or privately funded.

---

[9] Jürgen Cloppenburg, *Jüngste Entwicklungen im U.S.-amerikanischen Außenwirtschaftsrecht – Die Regulierung von Hochtechnologie-Exporten und ihr Einfluss auf die betroffenen Wirtschaftszweige am Beispiel der amerikanischen Satellitenindustrie* [New Export Regulations with Regard to High Technology and their Impact on the Satellite Industry in the US], 4 ZLW 510, 514 (2001).

- A security check that does not prevent fast data dissemination and based, if possible, on an automated control procedure.
- Flexible adaptation to changing external conditions through separation into general rules in the statute and adaptable, practice-oriented rules in the implementing regulation.

D. Conformity with U.N. Space Law

According to Article VI (2nd sentence) 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (Outer Space Treaty), "activities of non-governmental entities in outer space … shall require authorization and continuing supervision by the appropriate State Party to the Treaty." This refers primarily to the operation of the remote sensing satellite but also to the conformity of the private space-system operator with international law, in particular international space law.

More explicitly concerned with remote sensing is the United Nations General Assembly Resolution 41/65 on "Principles Relating to Remote Sensing of the Earth from Outer Space,"[10] adopted on December 3, 1986.

Although the Resolution of the General Assembly as a catalogue of principles is not internationally binding, it ended years of discussion with consensus between the States. It is therefore the guiding principle for the practice of Earth remote sensing and was, accordingly, considered in the preparation of SatDSiG and in the development of the *TerraSAR-X*-PPP concept. The core principle is the confirmation of the "open-sky policy", in return of which, Principle XII of the 1986 Remote Sensing Principles states: "As soon as the primary data and the processed data concerning the territory under its jurisdiction are produced, the sensed State shall have access to them on a non-discriminatory basis and on reasonable cost terms."

---

[10] *See* THE UN PRINCIPLES RELATING TO REMOTE SENSING OF THE EARTH FROM SPACE: A LEGISLATIVE HISTORY (Joanne Irene Gabrynowicz, ed., Mississippi 2002).

In theory, it could be asked whether restrictions on the dissemination of data for security-relevant reasons affect this principle. However, Principle III provides limitations to remote sensing activities: "Remote sensing activities shall be conducted in accordance with international law, including the Charter of the United Nations." The criteria of Section 19 (2) SatDSiG (Permit) – "if the dissemination of data in the individual case does not harm the vital security interests of the Federal Republic of Germany, does not disturb the peaceful coexistence of nations and does not substantially impair the foreign relations of the Federal Republic of Germany" – is fully in line with the inherent limits of remote sensing and the rights resulting therefrom.

The provisions of the *TerraSAR-X*-PPP and SatDSiG, favorable to commercial dissemination, create *de facto* a wide database accessible to all third persons on a non-discriminatory basis. Without a sensitivity check, such open dissemination would not be feasible. A totally uncontrolled commercial dissemination of Earth remote sensing data would also not be in conformity with Article VI of the Outer Space Treaty.

Moreover, when implementing the *Terra-SAR-X*-PPP, care was taken to ensure that no areas are intentionally "blacked out" from the available data map i.e. it is impossible for a customer to prevent a third person from accessing data about a specific region. This limitation of contractual freedom in the dissemination of commercial data is the specific result of the observation of remote sensing principles.

PART II: SATELLITE DATA SECURITY ACT

A. Background – Legislative Process

1. Technical Development Particularly in Germany

Over the last few years, great advances were achieved in the technical capabilities of remote sensing sensors and significant progress was made in satellite design. As a result, there was great improvement in space-borne remote sensing data and data products. At the same time, the fields of application of the data, the data products, and the geographical information ac-

quired with the data became broader and the instruments to manage and to distribute this information advanced to a similar extent. The quality and the availability of geographical information increased enormously.

With the launch of the German *TerraSAR-X* satellite (up to 1 meter spatial resolution radar satellite with all-weather and day/night observation capabilities; launched June 15, 2007) and the *RapidEye* satellite constellation (multispectral optical observation with a high revisit frequency; launch scheduled for the first half of 2008), Germany will assume an important role in Europe in the field of satellite-based earth remote sensing. This position will be further expanded with even more capable next-generation systems that are already in advanced project phases: *TanDEM-X* (interferometric radar satellite system with three-dimensional observation capabilities; launch in 2009) and *EnMAP* (hyperspectral optical imaging satellite; to be launched in 2011). This progress in remote sensing technologies will be used for a broad distribution of such data for commercial and scientific purposes.

2. Need for Legislative Action

The quality of the acquired space-borne remote sensing data is such that, until recently, it could only have been produced by classified military and intelligence-service satellites and used exclusively in that closely defined environment. As a broad distribution of such data for commercial and scientific purposes is intended, the accessibility of the data is essential. Therefore a secrecy scheme, as it is applies to military remote sensing systems, would be disadvantageous.

Whereas the greater part of the information acquired with a high-resolution remote sensing system is obviously not associated with any risk, some of this information may nevertheless be detrimental to national security or the foreign-policy interests of States.[11] So it is not primarily the data that endanger national security and foreign policy interests, but rather the

[11] Volker Liebig & Kai-Uwe Schrogl, SPACE APPLICATIONS AND POLICIES FOR THE NEW CENTURY 132 (Frankfurt 2000).

combination of the information about a certain area obtained by a certain person and the timing of dissemination. This means, for example, that nothing within Google Earth is detrimental to national security interests, even though the database is accessible to everyone and some data are of very high resolution. However, the information in this database was gathered months and years ago.

Thus, it is necessary to distinguish between the minor portion of the data potentially detrimental to national security or to foreign-policy interests and the remainder, which can be distributed or commercialized without risk. The German Act on Satellite Data Security provides a system to achieve this distinction. Therefore the Act closes the gap in the legislative framework because, unlike the export of the corresponding satellites or related technologies, there are no rules governing the distribution or transfer of satellite data or images and export-control regulations make no provision for such data products.

Giving transparency and certainty to companies, the Act aims to enable German operators to translate satellite applications into commercially viable business models and enter new sales markets.

The German government established a policy to safeguard national security and foreign-policy interests in the dissemination of high-resolution satellite data in 2004/05. Based thereon, the Federal Ministry of Education and Research presented a first draft bill in mid 2005. During the period of consultation with other ministries – in particular the Ministry of Defense, the Ministry of Foreign Affairs and the Ministry of the Interior - the German government was reorganized. Therefore this legislation was assigned to the Ministry of Economics and Technology, which introduced a final draft in the cabinet of ministers in January 2007.

B. Contents of the Act

The Act introduces regulations for the operation of a remote sensing system, for the data provider and the dissemination of the remote sensing data. The Act is intended firstly to cover "high-grade" space-based earth remote sensing systems and to

establish a clearly defined and transparent procedure for the dissemination of earth remote sensing data. "High-grade" Earth remote sensing systems within the meaning of the Act are systems capable of acquiring data of particularly high information content. The criteria assessed to determine whether systems have such capabilities include spatial resolution, spectral coverage, the number of spectral channels, and spectral resolution. Other factors that may play a role in the case of microwave and/or radar sensors are radiometric and temporal resolution, polarization features and phase history.

The backbone of the Act is the establishment of a control procedure for the dissemination of satellite data/images from such high-grade earth remote sensing systems. The Act therefore defines dissemination as bringing data into circulation or making data accessible to third parties. It consequently pertains to primary data providers such as the Infoterra company or the German Remote Sensing Data Center (one of the DLR's cluster institutes), but generally not to typical remote sensing service providers, value-adding firms, or data resellers.

The primary data provider is obliged to review requests for data transactions on a case-by-case basis. This sensitivity check is a key mechanism of the Act. If the data provider finds that the request is sensitive, the case must then be examined by government authorities, which then decide whether to issue or deny authorization.

1. Dissemination of the Data

The essential element of the Act is a two-phase procedure: the sensitivity check undertaken by the data provider and the granting of the permit by the responsible authority. The reason is that the anticipated large number of data requests would make it infeasible for the authorities to review each request; the effort required and the time needed would be excessive and it could result in a lack of efficiency and an impairment of commercialization. The two phases of the review may be described as follows:

The first phase is the sensitivity check of specific data requests that the data provider carries out in accordance with set

procedure and clearly defined criteria with no room for discretionary assessment (Section 17). The check is conducted to determine any potential endangerment of security. The criteria for the sensitivity check take account of the technical parameters and factors such as the observed target area, the customer requesting the data, the country of destination for the data products, and the length of time between data acquisition and the processing of the data request. Where the review classifies the specific data request as non-sensitive, the data provider can provide the requested data products without additional consideration by the responsible authority (Federal Office of Economics and Export Control - BAFA[12]) or allow the download of the data to a receiving station of the customer.

Only where the data provider's check classifies the customer data request as sensitive is the provider initially prohibited from complying with the customer's request. The data provider may, however, apply for consideration by the Federal Office in a second-phase review if it nevertheless wishes to comply with the request (Section 19). The Federal Office then conducts a case-specific review to determine whether the customer request would endanger the security of the Federal Republic. If the risk is ruled out, a permit is issued for the data provider to comply with the request. Another possible result of the review is to rule out a risk if the data request is altered slightly, for example, lowered resolution, time delay, reduced processing quality of the data, or the omission of certain target areas. In such cases, the authorities issue conditional authorizations. If a risk is ultimately sustained despite potential conditions, compliance with the data request remains prohibited. To impair commercial transactions no more than necessary, the Federal Office is required by law to decide on requests within a short period of time (maximum one month).

2. Licensing of Remote Sensing Systems

If a space-based Earth remote sensing system (normally a satellite with Earth remote sensing sensor) is considered to be a

[12] Abbreviation of "Bundesamt für Wirtschaft und Ausfuhrkontrolle."

high-grade system, Section 3 of the Act requires the operator to obtain a license from the Federal Office of Economics and Export Control (BAFA). The criteria determining the high-content nature of the Earth remote sensing system are listed in Section 2(2), inter alia, as the system's capabilities for spatial resolution, spectral coverage, and spectral and temporal resolution. These aspects are defined more precisely in a statutory ordinance.

Pursuant to Section 4, security requirements must be met both by the responsible persons and by the enterprise in order to obtain a license for operations. In addition to the operator, the persons who have access to the essential operational elements of the system must be considered reliable. To allow a better assessment of reliability, a basic security check is carried out in accordance with the Security Clearance Check Act (SÜG). The operational premises must be adequately secured to prevent unauthorized entry and the transmission of commands to the satellite must be safeguarded by means of strong encryption. In this connection, procedures certified by the BSI[13] are used.

In addition, the operators are subject to detailed documentation and information obligations, allowing the responsible government authorities at all times to form a picture of the activities of the operator (Sections 5 - 7). In addition, the government authorities are authorized, as is usual in commercial law, to inspect operators' premises and convince themselves on-site that operators are conducting themselves in accordance with the regulation (Section 8). A general clause entitles the responsible government authorities to take such measures as are necessary to ensure lawful operations or to prohibit operations (Section 9).

3. Licensing of the Data Provider

Those wishing to disseminate the data of a high-grade Earth remote sensing system must obtain a license. The requirements imposed on the licensee by the Act are comparable

[13] BSI is the abbreviation of "Bundesamt für Sicherheit in der Informationstechnik“ (Federal Office for Information Security).

to those imposed on the operator in Section 4 (Section 12), see above point 2.

4. Scope of Application

The scope of application (Section 1) has been extensively defined in order to avoid gaps or possibilities of circumvention. At the same time, it has been limited closely by technical characteristics and thus produces accurate effects. The Act covers all German citizens and organizations under German law. It also covers those foreign enterprises either domiciled in or essentially exercising effective control over their operations within Germany's Territory. That means that all enterprises are covered for which the Act can be effectively enforced.

The scope of application is also restricted to high-grade remote sensing systems. These are systems, which are technically able to generate data, which may be detrimental to national security or to foreign-policy interests. The criteria therefore are given in the Act (Section 2) (spatial resolution, spectral coverage, number of spectral channels etc.) while the precise limits of these criteria are given in the statutory ordinance.

Military and intelligence-service satellites do not fall within the scope of application of the Act; their data are appropriately kept secret by the government authorities, which operate the satellites. Moreover, such systems are or may be exempted if they are subject to comparable foreign-security arrangements with respect to protected property.

Since the scope of application of the Act specifically targets space-based earth remote sensing systems, it has no effect on communications and navigation satellites, on applications for use in conjunction with earth remote sensing data, or on the acquisition and distribution of air-based earth remote sensing data.

5. Other Regulations

With regard to the protection of high-ranking interests of the government, the Act will reserve a right of prior tasking for governmental purposes as well as a right of prior dissemination

of data to the government. These governmental rights will be restricted to rare cases of national crisis.

To insure that no risks arise when foreign nationals acquire an operating company or shareholdings in an operating company, or the earth remote sensing system, such transactions are restricted by Section 10 by imposition of a reporting and licensing requirement. Foreigners can more easily avoid supervision, access, and possibly criminal prosecution. Finally, a number of definitions of administrative and criminal offences have been included in the Act (Sections 28 and 29). This has been done to insure observance of the Act. They are aimed at satellite operators and data providers.

C. Implementation and Experiences

1. Practical Implementation

The most relevant aspect of the practical implementation of the Act is the definition of the criteria to identify the high-grade earth remote sensing system and the criteria for the sensitivity check, both given in the statutory ordinance. As the statutory ordinance has not come into force yet, the criteria have not yet been precisely determined at the present time. Nevertheless, it is possible to outline the basic principles.

The criteria used to identify the high-grade system will be spatial resolution in conjunction with the technique used by the remote sensing sensor to generate the data. The remote sensing sensors are classified into different types: optical sensors, radar sensors, infrared sensors, and multi-/hyperspectral sensors. To be regarded as a high-grade system, a multi-/hyperspectral sensor needs the least spatial resolution and an optical sensor needs the highest spatial resolution of the types. The spatial resolution of radar and infrared sensors lies between the extremes. As the criteria are determined with regard to the international situation and the availability of remote sensing data, remote sensing systems with capabilities like *Radarsat-1*, *Spot 5* or *Landsat* would probably not be classified as high-grade, whereas capabilities of systems like *Radarsat-2*, *Quickbird* or *Ikonos* would probably be classified as high-grade.

The criteria for the sensitivity check - observed target area, spatial resolution, the customer requesting the data, the country of destination for the data products, and the length of time between data acquisition and the processing of the data request – will be implemented in a listing system. As a result, data requests of NATO member states will not be sensitive in most instances. As regards target area, very high resolution data of some regions will be excluded for almost all customers, for example, regions with military-operation zones. Technical parameters like spatial resolution will be defined with regard to the definition of the high-grade remote sensing systems. Transactions of data capable of being generated by a non high-grade system will not be sensitive.

If the data provider's check classifies the customer data request as sensitive, the transaction is not prohibited, but the provider must apply for a permit from the Federal Office of Economics and Export Control.

2. Administrative Experience

The German radar satellite *TerraSAR-X* is the first space object affected by the Act. From the time of the satellite's launch in June 2007, the satellite operations and the generation and dissemination of the data were governed by a contractual regime between the German Ministry of Economics and Technology and the German Aerospace Center (DLR) as satellite operator/data provider and Infoterra as data provider. The contractual regime was designed as an analog to the Act to safeguard the security and foreign-policy interests during the commissioning of the satellite and to reduce the complexity of the period of transition, when the Act comes into force. Due to the contractual regime, administrative experience is based on more than 2000 sensitive data requests. Taking account of the fact that the *TerraSAR-X* satellite became ready for operation in 2008, the number of data requests is relatively high. Moreover, about 99 percent of the applications for permits could be granted. These statistics indicate, firstly, the high demand for *TerraSAR-X* data and, secondly, that the criteria of the sensitivity check in the contractual regime were possibly having too restricting of an

effect. However, this effect was anticipated somehow, because the satellite was commissioned at the same time as the implementation of its regulatory framework with a rather large safety margin. The experience gathered will be applied when determining the criteria of the sensitivity check in the forthcoming statutory ordinance, so that the criteria support the dissemination of data.

2590 Federal Gazette (BGBl.) Year 2007 Part I No. 58, issued in Bonn on 28 November 2007

Act to give Protection against the Security Risk to the Federal Republic of Germany by the Dissemination of High-Grade Earth Remote Sensing Data (Satellite Data Security Act — SatDSiG)

of November 23, 2007

Unofficial Translation

The Federal Parliament (Bundestag) has passed the following Act:

Outline of contents

Part 1
Scope of Application

Section 1

Scope of Application

(1) This Act applies

1. to the operation of high-grade earth remote sensing systems

a) by German nationals or by legal persons or associations of persons under German law,

b) by foreign legal persons or foreign associations of persons with their head office within the territory of the Federal Republic of Germany, or

c) if inalterable sequences of instructions to command the orbital system are transmitted from within the territory of the Federal Republic of Germany;

2. to the handling of data generated by a high-grade earth remote sensing system as described in Number 1 until the moment of their dissemination

a) by German nationals or by legal persons or associations of persons under German law,

b) by foreign legal persons or foreign associations of persons with their head office within the territory of the Federal Republic of Germany, or

c) where the data are disseminated from within the territory of the Federal Republic of Germany.

(2) This Act does not apply to the operation of high-grade earth remote sensing systems by a State agency with military or intelligence duties, provided that the possibility of unauthorized third parties gaining knowledge of the generated data is excluded. This Act may not be applied to the operation of a high-grade earth remote sensing system that is permitted under the applicable law of another Member State of the European Union and the latter is comparable to

the provisions and to the protected interests of this Act. The responsible authority may waive the application of the Act if the legal provisions of a third country satisfy the requirements of Sentence 2 and if there is an international treaty between the third country and the Federal Republic of Germany which affirms the comparability of the provisions and protected interests.

Section 2

Definitions

(1) For the purposes of this Act

1. The "Operator" is the person who has the control of the earth remote sensing system under his own responsibility;

2. "Data" are signals from one or more sensor(s) of an orbital or transport system and all products derived from the same, regardless of their degree of processing and their type of storage or representation; a unit of data for the purpose of Section 27 is each individual detail;

3. The "Data Provider" is any person who disseminates data generated by a high-grade earth remote sensing system;

4. A "high-grade earth remote sensing system" is a space-based transport or orbital system, including the ground segment, by means of which data about the earth are generated, where its sensor is itself/sensors are themselves technically capable either alone or in combination with one or more other sensors of generating data with a particularly high information content within the meaning of Para (2);

5. A "sensor" is a part of a space-based earth remote sensing system, which records electromagnetic waves of all spectral ranges or gravimetric fields;

6. "Dissemination" means bringing data into circulation or making data accessible to third parties.

(2) The Federal Ministry of Economics and Technology shall determine by statutory ordinance without the consent of the

Federal Council the conditions under which data have particularly high information content. The information content shall thereby be determined according to

1. geometric resolution,

2. spectral coverage,

3. the number of spectral channels and the spectral resolution,

4. the radiometric resolution and

5. the temporal resolution.

The information content of microwave sensors or radar sensors shall also be determined according to

1. the polarization characteristics and

2. the phase history.

The provisions consider the possible effects of disseminating data with particularly high information content on the vital security interests of the Federal Republic of Germany, the peaceful co-existence of nations and the foreign relations of the Federal Republic of Germany.

Part 2

Operation of a high-grade earth remote sensing system

Section 3

Operator license

(1) The operation of a high-grade earth remote sensing system requires an operator license.

(2) Subsequent alterations of the operator license are permitted if this is necessary to ensure that the requirements for the operator license are adhered in the event of subsequent occurrences or an amended legal provision.

(3) This does not affect the requirements made by other statutes on the operation of a high-grade earth remote sensing

system. The operator license is granted without prejudice to the private rights of third parties.

(4) If a space-based earth remote sensing system is not high-grade, the responsible authority shall affirm the same on application by the operator. If the need for an operator license is subsequently dispensed with by amendment of the provisions of Section 2(2), the operator license is extinguished.

Section 4

Operator license requirements

(1) Operator license shall be granted if

1. the operator of the high-grade earth remote sensing system possesses the requisite degree of reliability,

2. the sequences of instructions to

a) command the orbital or transport system,

b) control of the sensor(s),

c) control of the transmission of data by the orbital or transport system to a ground segment of the Operator or to a person admitted under Section 11 and

d) control of the dissemination of data directly by the orbital or transport system

are produced within the Federal Republic of Germany and protected against alteration by third parties by means of a method tested and declared suitable by the Federal Office for Information Security (BSI),

3. the transmission of the data by the orbital or transport system to a ground segment of the operator or to a person admitted under Section 11, the transmission of data between various locations of the ground segment of the operator, and transmission of the data by the operator to a person admitted under Section 11, are protected from becoming known to unauthorized third parties by means of a method tested and declared suitable by the Federal Office

for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI), and

4. the operator has taken technical and organizational measures preventing unauthorized persons from gaining access to the command installations of the high-grade earth remote sensing system and to the installations for receiving, processing and storing the data and entry to the control rooms used for the same.

(2) The operator shall arrange for persons having access to the command installations of a high-grade earth remote sensing system or to the installations for receiving, processing and storing the data of such systems to undergo a simple security check in conformity with the Security Check Clearance Act (Sicherheitsüberprüfungsgesetz - SÜG) which is performed by the responsible authority.

Section 5

Obligation of documentation

The operator of a high-grade earth remote sensing system is obliged to record

1. the sequences of instructions to command the orbital or transport system,

2. the sequences of instructions to control the sensor(s),

3. details of encryption processes, codes used and code management and

4. the time and path of the command sequences.

The records under Para. (1) shall be filed for at least five years after execution of the relevant command sequence and be made available for inspection by the relevant authority.

Section 6

Obligation of notification

(1) The operator of a high-grade earth remote sensing system shall notify the responsible authority in writing without delay of

1. Changes in facts which it is obliged to notify to the commercial register (Handelsregister) or register of associations (Vereinsregister), and

a) if the operator is organized under the legal form of a partnership, changes in the articles of partnership or

b) if the operator is organized in the legal form of a limited-liability company (GmbH), changes in the persons of the corporate members or in the extent of their participation,

2. Actual indications that a third party is transmitting or attempting to transmit the sequences of instructions to command the orbital or transport system, to control the sensor(s) or to control the transmission of data from the orbital or transport system, and

3. any changes made to the measures taken under Section 4 (1) No. 4.

(2) The operator of a high-grade earth remote sensing system shall notify the responsible authority without delay in writing of the persons admissible under Section 11 to whom he transmits data.

Section 7

Obligation to provide information

(1) The operator of a high-grade earth remote sensing system shall provide the responsible authority with information on demand and submit documents, if this is required to monitor adherence to this Act and the statutory ordinances passed under this Act.

(2) Persons obliged to provide information may refuse to answer any questions if the answers would expose those persons or relatives of those persons as defined in Section 383(1) Nos. 1 to 3 German Code of Civil Procedure (Zivilprozessordnung - ZPO) to the risk of criminal prosecution or to proceedings under the statute on administrative offenses (Gesetz über Ordnungswidrigkeiten - OWiG).

Section 8

Rights of entry and examination

The officers of the responsible authority are authorized to gain entry to the business and operating premises of the Operator of a high-grade earth remote sensing system during normal business and operating hours and to undertake the examinations required in performance of their duties; Sections 196, 197 (1) Sentences 1 and 2 and (2), Section 198, Section 199(2) and Sections 200 to 202 German Tax Code (Abgabenordnung - AO) apply mutatis mutandis.

Section 9

Measures of the responsible authorities

(1) The responsible authority can take measures that are necessary towards the operator of a high-grade earth remote sensing system in the individual case to ensure the due performance of the operator's obligations.

(2) The responsible authority can, in particular

1. temporarily prohibit the transmission of data to a ground segment or to a person admitted under Section 11 or

2. order that operation be transferred wholly or in part to a special commissioner.

(3) The operator of the high-grade earth remote sensing system pays the costs incurred for the appointment of the special commissioner including the compensation payable to the same. The responsible authority determines the amount of compensation.

Section 10

Acquisition of enterprises and participating interests in enterprises; business takeovers

(1) The acquisition of an enterprise that operates a high-grade earth remote sensing system or the acquisition of a direct or indirect participating interest in such an enterprise by

1. foreign nationals or by legal persons or associations of persons under foreign law, or

2. legal persons or associations of persons under German law in which foreign nationals or legal persons or associations of persons under foreign law hold at least 25 per cent of the voting rights

shall be notified to the responsible authority by the buyer without delay. This does not apply if, after acquiring the share, the buyer's direct or indirect share of voting rights in the relevant enterprise does not attain the level of 25 per cent. When calculating the buyer's share of voting rights, the shares of other enterprises held in the enterprise to be acquired shall be attributed to the buyer if the buyer holds at least 25 per cent or more of the voting rights in these other enterprises. The responsible authority can prohibit the acquisition within one month of receiving the complete documents governing the sale, if this is necessary to safeguard the vital security interests of the Federal Republic of Germany.

(2) The complete or partial takeover of the operation of a high-grade earth remote sensing system or parts thereof requires a permit if the takeover dispenses with the need for an operator license under Section 3(1). The acquirer shall apply for the granting of the permit. The permit shall be granted if the further operation of the high-grade earth remote sensing system or of parts of the high-grade earth remote sensing system does not endanger the vital security interests of the Federal Republic of Germany.

Part 3
Dissemination of data

Chapter 1
General requirements

Section 11

Dissemination license

(1) A data provider wishing to disseminate data requires a dissemination license.

(2) Subsequent alterations of the dissemination license are permitted if this is required in order to ensure that the requirements for the dissemination license are adhered to in the event of subsequent occurrences or an amended legal provision.

Section 12

Dissemination license requirements

(1) The dissemination license shall be granted if

1. the data provider possesses the requisite degree of reliability,

2. the data provider has taken technical and organizational measures preventing unauthorized persons from gaining access to the installations for receiving, processing or storing the data of a high-grade earth remote sensing system or entry to the control rooms used for the same.

3. The transmission of the data between various locations of the ground segment of the data provider and the transmission of the data to a different data provider are protected from becoming known to unauthorized third parties by means of a method tested and declared suitable by the Federal Office for Information Security (BSI) and

4. the dissemination of the data generated by a high-grade earth remote sensing system is guaranteed to be secure according to the state of the art.

(2) The data provider shall arrange for persons having access to the command installations of a high-grade earth remote sensing system or to the installations for receiving, processing and storing the data of such systems to undergo a simple security check in conformity with the Security Clearance Check Act (Sicherheitsüberprüfungsgesetz - SÜG) undertaken by the responsible authority.

Section 13

Obligation of notification

The data provider shall notify the responsible authority without delay in writing

1. of changes in facts which it is obliged to notify to the commercial register (Handelsregister) or register of associations (Vereinsregister), and

a) if the data provider is organized under the legal form of a partnership, any changes in the articles of partnership or

b) if the data provider is organized in the legal form of a limited-liability company (GmbH), changes in the persons of the corporate members or in the extent of their participation,

2. of any changes made to the measures taken under Section 12 (1) No. 2 and

3. of any actual indications that the security of data generated using a high-grade earth remote sensing system is not maintained.

Section 14

Obligation to provide information

(1) The data provider shall provide the responsible authority with information on demand and submit documents if this is required for monitoring adherence to this Act and the statutory ordinances passed under this Act.

(2) The data provider may refuse to answer any questions if the answers would expose that person or a relative of that person as defined in Section 383(1) Nos. 1 to 3 of the German Code of Civil Procedure (ZPO) to criminal prosecution or to proceedings under the statute on administrative offenses.

Section 15

Rights of entry and inspection

The officers of the responsible authority are authorized to gain entry to the business and operating premises of the data provider during normal operating and business hours and to undertake the examinations required in performance of their duties; Section 196, Section 197(1) Sentence 1 and 2 and (2), Section 198, Section 199(2) and Section 200 to Section 202 of the German Tax Code (Abgabenordnung - AO) apply mutatis mutandis.

Section 16

Measures of the responsible authorities

The responsible authority can order the data provider in the individual case to take the measures required for due performance of the data provider's duties. It may, in particular,

1. require the dissemination of the data to be adapted to the state of the art, or

2. temporarily prohibit the dissemination of data.

Chapter 2

Process of data dissemination

Section 17

Sensitivity check

(1) The data provider who wishes to comply with a request for the dissemination of data of a high-grade earth remote sensing system shall examine the request for its sensitivity as defined in the statutory ordinance under Para. (3).

(2) A request is sensitive if

1. the information content of the data obtained as a result of the sensor-operating mode used and form of processing used,

2. the target area represented by the data,

3. the time of generation of the data and the period of time between generation of the data and compliance with the request and

4. the ground segments to which the data are to be transmitted,

when viewed as a whole, reveal the possibility of harm being caused to the vital security interests of the Federal Republic of Germany, to the peaceful co-existence of nations or to the foreign relations of the Federal Republic of Germany. The view as a whole according to Sentence 1 takes account of the personal characteristics of the requesting party and should take account of the persons who prospectively come into contact with the data as provided for in the request, including their usual places of residence. The data provider shall check the identity of the requesting party in suitable manner and require the names of the persons who prospectively come into contact with the data as provided for in the request, including their usual places of residence.

(3) The Federal Ministry of Economics and Technology shall, by agreement with the Federal Ministry of Defense, the Foreign Office and the Federal Ministry of the Interior, determine provisions in a statutory ordinance without the consent of the Federal Council regarding the conditions under Para (2) in which there is

a possibility of harm being caused to the aforementioned interests requiring protection. It also takes account of the decisions of the authorities concerned, regarding the security requirements that have to be updated at regular intervals, the obligations assumed and agreements entered into by the Federal Republic of Germany with the Member States of the European Union, the parties to the North Atlantic Treaty of April 4, 1949 (federal gazette BGBl. 1955 II p. 289) as amended by the Protocol of October 17, 1951 (federal gazette BGBl. 1955 II p. 293) and Australia, Japan, New Zealand and Switzerland, the state of the art with regard to the generation of data with particularly high information content, the existing rules under which the requesting party could further transmit the data and the availability of comparable data on international markets. It is necessary to define in the statutory ordinance the procedure according to which the view as a whole required by Para (2). Sentences 1 and 2 is to take place. The statutory ordinance shall not give the Data Provider any scope for own discretion as to whether a request is sensitive. The Data Provider may be notified of forthcoming amendments of the statutory ordinance. The Federal Ministry of Economics and Technology can, by agreement with the Federal Ministry of Defense and the Foreign Office, transfer the authority wholly or partly to the Federal Office of Economics and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle - BAFA) by statutory ordinance without the consent of the Federal Council.

Section 18

Obligation of documentation

(1) The data provider is obliged to record all requests for the dissemination of data of a high-grade earth remote sensing system. This covers

1. the actual request including the persons who prospectively come into contact with the data as provided for in the request and their usual places of residence,

2. checking the identity of the requesting party,

3. the procedure and the results of the check of the sensitivity of the request under Section 17 (1) in conjunction with the provisions of a legal ordinance under Section 17 (3),

4. the data-generation order placed with the Operator of the high-grade earth remote sensing system,

5. the receiving logs of ground segments,

6. the details of encryption processes, codes used and code management,

7. the reports of the processing sequences of the ground segment,

8. the meta data of the data, in particular, target area, time of generation of the data, sensor operating mode and data-processing parameters,

9. the transfer logs or delivery notes including delivery confirmations with regard to compliance with the request and

10. the invoices.

Sentences 1 and 2 Nos. 4 to 10 apply mutatis mutandis if data are disseminated without a request. If a request for the dissemination of data of a high-grade earth remote sensing system is executed out of an archive, a reference to the other logs and documentation suffices for the logging and documentation purposes of Sentence 2 Nos. 4 and 5.

(2) The records under Para (1) shall be filed for at least five years after generation of the relevant data and be held available for inspection by the responsible authority.

(3) The data provider is obliged to have ready similar products and documentation of third-party ground segments, which he has used in complying with the request for dissemina-

tion of data of a high-grade earth remote sensing system. Para (2) applies mutatis mutandis.

(4) The data provider shall notify the requesting party of the storage of the data and the possibility of inspection by the authorities.

Section 19

Permit

(1) If a data provider wishes to comply with a sensitive request, he requires a permit. This also applies in the event that he wishes to disseminate data of a high-grade earth remote sensing system without a request.

(2) The permit of Para (1) shall be granted if the dissemination of data in the individual case does not harm the vital security interests of the Federal Republic of Germany, does not disturb the peaceful co-existence of nations and does not substantially impair the foreign relations of the Federal Republic of Germany.

(3) The responsible authority should decide on the application for the permit within one month of its receipt at the latest.

(4) The permit is granted without prejudice to the private rights of third parties.

Section 20

Collective permit

The responsible authority may grant a collective permit if the data provider wishes

1. to make representations of data with strongly reduced information content or meta data available to anyone or

2. to comply with sensitive requests made by the same person for an indefinite number of quantities of data of a high-grade earth remote sensing system.

The collective permit is granted subject to the conditions of Section 19(2) and may only be granted if a right of revocation is reserved. A collective permit as per Sentence 1 No. 1 shall determine the maximum information content that the data may have. A collective permit under Sentence 1 No. 2 may only be granted for a specific period, which should not exceed three years.

Part 4

Priority compliance with requests from the Federal Republic of Germany

Section 21

Obligations of the Data Provider

The data provider is obliged to give priority to complying with requests for the dissemination of data from the Federal Republic of Germany, represented by the Federal Chancellery, over all other requests, in the following cases:

1. in the event of the casus foederis in accordance with Article 5 of the North Atlantic Treaty of April 4, 1949 (federal gazette BGBl. 1955 II p. 289) as amended by the Protocol of October 17, 1951 (federal gazette BGBl. 1955 II p. 293),

2. in case of defense as per Article 115 letters a to German Basic Law (GG),

3. if the requirements for the internal state of emergency as per Article 91 Basic Law are satisfied,

4. in the event of tension as per Article 80a of the Basic Law or

5. if there is a current danger to military or civil forces of the Federal Republic of Germany deployed in a foreign country or to employees of the diplomatic service employed at German foreign embassies, who are working to counter a concrete impairment to the external security of the Federal Republic of Germany.

Section 22

Obligations of the Operator

The operator of a high-grade earth remote sensing system is obliged, in the events of Section 21, to give priority treatment to orders for the generation of data for the Federal Republic of Germany over all other orders for the generation of data. Without prejudice to Sentence 1, the request for earth remote sensing from the Federal Republic of Germany, represented by the Federal Chancellery, should be made to a data provider. If the request is nevertheless made to the operator of a high-grade earth remote sensing system, the operator does not require any license under Section 11 for the dissemination of these data.

Section 23

Remuneration

(1) Without prejudice to the obligations arising under this Part, remuneration may be required for the generation of data under Section 22 and for compliance with the request under Section 21. The remuneration should correspond to the relevant average market price.

(2) All further claims against the Federal Republic of Germany are excluded.

Part 5

Implementing regulations

Section 24

Responsibility

(1) The responsible authority under this Act, subject to Paras 2 and 3, is the Federal Office of Economics and Export Control (BAFA).

(2) Responsible for performing a security check under Section 4 (2) and Section 12 (2) is the Federal Ministry of Economics and Technology.

(3) A notification under Section 10 (1) Sentence 1 is made to the Federal Ministry of Economics and Technology. The Federal Ministry of Economics and Technology, by agreement with the Foreign Office and the Federal Ministry of Defense, is responsible for prohibiting the acquisition of enterprises or shares in enterprises under Section 10 (1) Sentence 4.

Section 25

Procedure

(1) An operator license under Section 3(1), a dissemination license under Section 11(1) and a permit under Section 10(2) Sentence 1, Section 19(1) Sentences 1 and 2 and under Section 20 Sentence 1 each require submission of a written application. A notification under Section 10(1) Sentence 1 shall be made in writing. An application or a notification shall be accompanied by the documents required to examine the conditions for granting the application.

(2) The Federal Office for Information Security (BSI) shall be consulted at an early stage to determine the suitability of a method under Section 4(1) Nos. 2 and 3 and Section 12(1) No. 3. The BSI provides the applicant with documents on the contents and procedure of the examination.

(3) Orders issued by an administrative authority under this Act shall be issued and served in writing.

Section 26

Fees and expenses

The responsible authorities charge fees and expenses for official acts under this Act. The Federal Ministry of Economics and Technology is empowered to determine in a statutory ordinance without the consent of the Federal Council the fee headings, fee amounts and the expenses to be refunded and to provide for fixed rates or outline rates. The fee rates shall be set in such a way as to cover the costs associated with the official acts.

The significance, economic value or other utility value of the official act to the beneficiary will be given due consideration.

Section 27

Transmission of personal data, operating and business secrets

(1) The responsible authority can transmit personal data which have become known to it in the performance of its duties under this Act to other authorities if it believes that the knowledge of such personal data is required

1. to avert an endangerment to the vital security interests of the Federal Republic of Germany or to prevent a disturbance of the peaceful coexistence of nations or a substantial disturbance of the foreign relations of the Federal Republic of Germany or

2. to prevent or to prosecute criminal offenses.

Transmission under Sentence 1 No. 2 is permitted only if there is actual cause to assume that criminal offenses have been committed or will be committed in the future. Furthermore, the responsible authority may transmit these personal data to the federal intelligence agency (BND) if the requirements of Section 8(3) of the BND statute (BND-Gesetz) are met. The third party to whom the personal data are to be transmitted may only use these data for the purpose for which they have been transmitted.

In criminal proceedings for a breach of this Act, courts and public prosecutors may transmit personal data to the highest federal authorities only if this is required to avert an endangerment to the vital security interests of the Federal Republic of Germany or to prevent a disturbance of the peaceful coexistence of nations or a substantial impairment of the foreign relations of the Federal Republic of Germany. The personal data obtained under Sentence 1 may only be used for the purposes specified therein. The third party to whom the personal data are transmitted may only further transmit the same to a public authority not specified in Sentence 1 if the interest in the use of the per-

sonal data transmitted considerably outweighs the interest in secrecy of the person affected and the investigative purpose of the criminal proceedings cannot be endangered.

(2) Business and operating secrets are deemed equivalent to personal data.

Part 6

Administrative-fine provisions, penal provisions

Section 28

Administrative offenses

(1) A person commits an administrative offense if that person willfully or recklessly

1.operates a high-grade earth remote sensing system under Section 3(1) without an Operator license,

2.in breach of Section 10(1) Sentence 1 fails to make a notification or fails to make such notification on time or in full or correctly under Section 10(1) Sentence 1 or acts in breach of an enforceable order under Section 10(1) Sentence 4

3.without a permit

a) takes over the operation of a high-grade earth remote sensing system or parts of such a system under Section 10(2) Sentence 1,

b) complies with a sensitive request under Section 19(1) Sentence 1 or

c) disseminates data under Section 19(1) Sentence 2 without a request,

4. breaches an enforceable order under Section 9(1), (2) or Section 16.

5. disseminates data under Section 11(1) without a Dissemination license,

6. in breach of Section 17(1) in conjunction with the provisions of a statutory ordinance based on Section 17(3) fails

to examine the sensitivity of a request for the dissemination of data of a high-grade earth remote sensing system, fails to do so correctly or in full or to do so in the prescribed manner,

7. in breach of Section 5(1) or Section 18(1) Sentences 1 and 2, fails to make a record, fails to do so correctly or in full or fails to file the record or fails to do so for at least five years under Section 5(2) or Section 18(2) or

8. in breach of Section 18(3) fails to hold ready the logs and documentation specified therein.

(2) A person commits an administrative offense if

1. in breach of Section 6(1) Sentence 13 that person fails to report a crime, fails to do so correctly or in full or on time or

2. in breach of Section 7(1) or Section 14(1) fails to provide information, fails to do so correctly or in full or on time.

(3) An administrative offense as defined in Para. (1), Nos. 1 to 5 is punishable by a fine of up to five hundred thousand euros; in Para. (1), Nos. 6 to 8 by a fine of up to fifty thousand euros and in Para (2) by a fine of up to twenty-five thousand euros.

Section 29

Criminal offenses

(1) Liable to punishment of a term of imprisonment of up to five years or a fine is a person who commits a deliberate act specified in Section 28(1) Nos. 1 to 6 that is capable of substantially endangering

1. the vital security interests of the Federal Republic of Germany,

2. the peaceful co-existence of nations or

3. the foreign relations of the Federal Republic of Germany.

(2) The attempt is punishable.

Section 30

Offenses committed in foreign countries by German citizens

Section 29 applies independently of the law of the place of the crime, also in foreign countries, if the offender was a German citizen at the time of the offense.

Section 31

Criminal proceedings and administrative-fine proceedings

(1) Where a local court (Amtsgericht) has material jurisdiction for criminal offenses under Section 29, the local court in whose district the Regional Court (Landgericht) has its seat has local jurisdiction.

(2) Section 49(2), Section 63(2) and (3) Sentence 1 and Section 76(1) and (4) Act on Administrative Offenses (OWiG) apply mutatis mutandis in criminal proceedings and in court proceedings with regard to the participation of the administrative authorities in the proceedings of the public prosecutor.

Part 7
Transitional and final provisions

Section 32

Amendment of the Federal Constitutional Protection Act (Bundesverfassungsschutzgesetz - BVerfSchG)

Section 3(2) Federal Constitutional Protection Act (BVerfSchG) of December 20, 1990 (federal gazette BGBl. I p. 2954, 2970), most recently amended by Article 6(1) of the Act of August 19, 2007 (federal gazette BGBl. I p. 1970), is amended as follows:

1. In Sentence 1, the full stop after No. 3 shall be replaced by a comma and the following No. 4 shall be appended:

" 4. in the examination of persons in other cases determined by statute."

2. In Sentence 2, the indication "Nos. 1 and 2" is replaced by the indication "Nos. 1, 2 and 4".

Section 33

Amendment of the Security Clearance Check Act (Sicherheitsüberprüfungsgesetz - SÜG)

The Security Check Act of April 20, 1994 (federal gazette BGBl. I p. 867), most recently amended by Article 10 (5) of the Act of January 5, 2007 (federal gazette BGBl. I p. 2), is amended as follows:

1. In Section 1(2), the full stop after No.3 shall be replaced by a comma and the following No. 4 is appended:

"4. is subject to a security check under other provisions, insofar as reference is made to this statute."

2. In Section 3(2) Sentence 1, the indication "under Section 3(2) No. 1" shall be replaced by the indication "under Section 3(2) Nos. 1, 2 and 4".

3. In Section 24, the phrase "to be entrusted with a security-sensitive activity at a non-state organization under Section 1(4)" shall be is replaced by the phrase "to be entrusted with a security-sensitive activity at a non-state organization under Section 1(2) No. 4 or Section 1(4)".

Section 34

Transitional rule

(1) The operation of a high-grade earth remote sensing system prevailing at the time that this Act comes into force is deemed to have an operator license until a final and non-appealable decision is given on the application for an operator license if such application is made within three months of this Act coming into force.