Federal Ministry
of Economics
and Technology

Federal Ministry of Economics and Technology • D-53107 Bonn • Germany

SWITCHBOARD +49 228 99615 0
FAX +49 228 99615 4436
INTERNET www.bmwi.de

PREPARED BY Wolfgang Schneider
TEL +49 228 99615 4352
FAX +49 228 99615 8-4352
E-MAIL Wolfgang.Schneider@bmwi.bund.de
FILE NO. VII B3 -

DATE Bonn, 15. April 2008

SUBJECT

National Data Security Policy for Space-Based Earth Remote Sensing Systems

Background Information for the Act on
Satellite Data Security (Satellitendatensicherheitsgesetz - SatDSiG)

The Bundestag passed the Act to Safeguard the Security Interests of the Federal Republic of Germany from Endangerment by the Distribution of High-Grade Earth Remote Sensing Data" *(Satellitendatensicherheitsgesetz - SatDSiG)*

The law became effective on 01 December 2007.

Background

The purpose of the Act is, on the one hand, to safeguard the security and foreign policy interests of the Federal Republic of Germany in connection with the distribution and commercial marketing of satellite-acquired earth remote sensing data especially on international markets. On the other hand, the Act will create legal certainty for affected companies and make the terms of operating in the new business areas calculable for the developing companies involved in satellite data marketing - thus also for the

STREET ADDRESS Villemombler Straße 76, 53123 Bonn
BUS LINES 632, 634, 635, 638, 639, 843

expanding geo-data industry. It will therefore fulfil an important condition, enabling German companies to translate satellite applications into commercially viable business models and enter new sales markets.

To meet these needs, the bill was developed in close cooperation with the responsible ministries (above all the Foreign Office; the Federal Ministry of the Interior; Federal Ministry of Defence; Federal Ministry of Justice; Federal Ministry of Food, Agriculture, and Consumer Protection; Federal Ministry of Transport, Building, and Urban Affairs; Federal Ministry for the Environment, Nature Conservation, and Nuclear Safety; Federal Ministry of Education and Research), the Federal Chancellery, and the relevant agencies (Federal Intelligence Service; Federal Criminal Police Office; German Information Security Agency, Geo-Information Office of Germany's Federal Armed Forces) and federal commissioners. Since the very early phases of planning the legislation, a dialogue has also been conducted with companies that it directly and indirectly affects, and with the associations affected by it.

The Need for Legislative Action

The Act on Satellite Data Security is needed to provide legal certainty, establish binding rules, and ensure enforcement; it is also necessary in the interest of sending a foreign policy signal and furnishing legal foundations for the issues addressed.

The *SatDSiG* became necessary since highly capable space-based earth remote sensing satellites are constructed in Germany with the intention of the worldwide commercial marketing of the acquired images/data. With the launch of the German TerraSAR-X satellite (high resolution space radar satellite with all-weather and day/night observation capabilities) in June 2007, Germany had assumed a strong role in Europe in the field of satellite-based earth remote sensing and will further expand this position with the upcoming launch of the RapidEye satellite constellation (constellation of small optical satellites for multispectral observation with a high revisit frequency; launch scheduled for mid 2008) and the 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; launching in 2011).
The generated earth remote sensing data are made available for worldwide civilian commercialization. They are now of a quality – in particular with satellites such as TerraSAR-X or TanDEM-X – which was previously produced only by classified military and intelligence service satellites and used exclusively in that closely defined environment.

The distribution of these high-value or high-grade earth remote sensing data may endanger foreign or security policy interests, for instance the distribution of satellite images of areas in which the Bundeswehr (German Armed Forces) is deployed on assignments abroad or of areas in which massive refugee flows are concentrated. Weapon capabilities and political threats can be considerably reinforced by such earth remote sensing data even where security interests are not directly endangered.

An uncontrolled distribution of such data from Germany transmitted by German earth remote sensing data systems would also contravene the commitment to the maintenance of peace enshrined in the German Basic Law. This applies not only to the use of these data in transnational conflicts but also to their use by non-governmental actors to exert violence below the threshold of armed conflict, such as ethnic strife, civil unrest or terrorist acts.
Politically, the Federal Republic of Germany may perhaps be reproached that, due to a lack of control, data usable for military purposes provided by German earth remote sensing data systems could fall into the hands of third parties and thus turn into a threat for other states.
In this regard, an endangerment of the Federal Republic's security-policy and foreign-policy interests can derive not only from an extremely high geometrical resolution but, for example, from other technical features or the particularly up-to-date status of the earth remote sensing data.

High-grade earth remote sensing data are therefore not to be compared with the freely accessible data offered on the Internet. This, on the one hand, explains the high commercial value of these satellite data and, on the other hand, was the reason why the

countries affected, such as the US, Canada, France and India have also recognized the need for governmental regulation of the distribution of such data.

From a foreign-policy perspective, the national legislative framework is important to foster cooperation between countries with advanced earth remote sensing systems. Nearly all capable satellite systems (including the planned German systems mentioned above) depend on export licenses for various US components. In these cases, the United States calls for binding national rules that take account of security interests in connection with the data. A legislative framework allows to take into account the US requirements while at the same time offering the opportunity to pursue independent solutions in this field which enable German enterprises to operate at a worldwide level.

In this context, it is of particular importance that the Act on Satellite Data Security foresees a fast, yet efficient, procedure for distributing earth remote sensing data, which allows the companies concerned to determine themselves, based on a review procedure with clearly defined criteria, whether the distribution of data to a customer might be of a sensitive nature.

International Legal Situation

Appropriate formalized national data security policies have been in effect in the United States since 1992 and in Canada since the end of 2005. The Canadian approach is based on a government agreement between the US and Canada and is law largely based on the US approach. In late April 2007, France announced a draft bill governing space activities which also contains provisions on the use of earth remote sensing data and which makes reference to the German Act on Satellite Data Security in its brief explanatory memorandum. Recently, such legislation has also been introduced in India and a bill is being drafted in Japan.

The far-reaching lack of relevant legal provisions in other countries is the result of the still low number of countries having such capable earth remote sensing satellites. Above all in Europe, Germany is a pioneer in terms of the technical achievements and its thoughts on a national data security policy and their implementation in the SatDSiG; it

could thereby also make an important contribution to shaping similar provisions presumably also needed at EU level and in the framework of ESA.

Central Aspects of the SatDSiG

The main idea underlying the Act is, on the one hand, to cover only "high-grade" space-based earth remote sensing systems while, on the other hand, to establish a clearly defined and transparent procedure for distributing data of these systems.

Consequently, neither aerial photographs nor data from navigation satellite systems such as GPS or the future European Galileo fall within the area of application of the Act. Military and intelligence services' earth remote sensing systems are explicitly excluded from the area of application.

The high-grade nature of an earth remote sensing system within the meaning of the SatDSiG derives from the respective system's capacity for acquiring data of particularly high information content. The criteria that are assessed to determine whether systems have such capacities include spatial resolution, spectral coverage, the number of spectral channels, and the spectral resolution. Other factors that may play a role are radiometric and temporal resolution; polarization features and phase history are additional factors in the case of microwave and/or radar sensors.

The backbone of the SatDSiG is the establishment of a control procedure for distributing satellite data/images from such high-grade earth remote sensing systems. It is designed to prevent harm to the security interests of the Federal Republic, the peaceful coexistence of peoples and the Federal Republic’s external relations. The SatDSiG defines every form of first-time marketing or disclosure of data to third parties, whether for commercial or scientific use, as data distribution. The draft Act consequently pertains to primary data distributors such as the Infoterra company or the German Remote Sensing Data Center (one of the DLR's cluster institutes), but generally not to the typical remote sensing service providers, value-adding firms, or data resellers.

The control procedure is designed as a two-layered approach. Initially, the primary data supplier (*"Datenanbieter"* within the meaning of the SatDSiG) carries out a so-called **sensitivity check** of requests for data transactions on a case-by-case basis. The sensitivity check is a key mechanism of the SatDSiG. If the data supplier finds that the request is not sensitive, he may deliver the requested data. If he finds, however, that a request is sensitive, he may deny delivering the data or request a **review and authorization by a government authority**.

Elements that are examined as part of the sensitivity check include technical data of the sensor operation modes that are used to acquire the specific data set (e.g. spatial resolution, observed spectral/frequency range, number of spectral channels, etc.), the information content of the data retained by the type of processing used (specification of the data product), the target area surveyed by the data, the time of data acquisition, and the time lag between data acquisition and supply to the customer, the individual making the request or submitting the order, and the ground segments to which the data are to be transmitted.

Of key importance in practice is the fact that the relevant companies are given the responsibility for the sensitivity check as a clearly defined procedure that is stipulated by an ordinance (SatDSiV), and which can be automated. This guarantees good transparency, certainty of planning, and speedy implementation of the procedure, particularly for commercial data-distribution, and it confines to a necessary minimum the administrative effort required for government review.

This two-layered approach set forth in the SatDSiG, combining a sensitivity check as a fixed and standardized initial check, where appropriate with a case-by-case decision by a government authority, allows reliable identification of critical cases whilst still at the data supplier level and then, if necessary, a final decision by a competent authority in a normal administrative procedure. Based on the experience so far, it can however be expected that, depending on the customer structure and the customers' specific fields of interest, the bulk of the requests will be non-sensitive and can therefore be complied with by the data supplier without directly involving an authority.

In this way, Germany's foreign and security policy interests are safeguarded with minimum intervention. Such an approach also offers the data supplier a high degree of legal certainty.

To guarantee the secure handling of data (acquisition, transmission, processing, distribution, archiving), certain requirements have been set for satellite operation and must be met by satellite operators and data suppliers. In order to fulfil these requirements, a license must be obtained for the operation of high-grade earth remote sensing systems, and a license is required for data suppliers.

Appendix

Some Aspects outlining the "Act to Safeguard the Security Interests of the Federal Republic of Germany from Endangerment by the Distribution of Space-Based Earth Remote Sensing Data" *(Satellitendatensicherheitsgesetz - SatDSiG)*

The Satellite Data Security Act will guarantee that the earth remote sensing data that are now also commercially available from state-of-the-art earth remote sensing satellites do not endanger the security and foreign policy interests of the Federal Republic of Germany. At the same time, the Act will additionally provide legal certainty for the involved companies and foster the commercial development of the market for geo-information.

The Act has been published in the Bundesgesetzblatt, Jahrgang 2007, Teil I, Nr. 58, page 2590ff, 28. November 2007.

Details on the definition of high-grade earth remote sensing satellites as well as the procedures and threshold values for the sensitivity check can be found in the statutory ordinance “Verordnung zum Satellitendatensicherheitsgesetz (Satellitendatensicherheitsverordnung – SatDSiV)”, published in the Bundesgesetzblatt, Jahrgang 2008, Teil I, Nr. 12, page 489ff, 04. April 2008.

German versions can be downloaded from:
SatDSiG: http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s2590.pdf
SatDSiV: http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s0508.pdf

Main Elements of the Act

The area of application of the Satellite Data Security Act is the operation of "high-grade" non-military earth remote sensing satellites and the distribution of the acquired data and derived data products/images. The high-grade nature as defined by the SatDSiG derives from the system's technical features, which can make it capable of security-relevant use. A number of existing and future systems, however, are not covered by the SatDSiG since they lack such technical capabilities.
A key element of the legislation is the procedure by which the data supplier carries out a sensitivity review or sensitivity check under Section 17. Based on a fixed procedure, the data supplier considers whether the distribution of the data could potentially endanger security; where this is seen as a legitimate concern, a review of the individual case by government authorities is then required. The purpose of the strictly formalized sensitivity check is, in a first review step, to identify unobjectionable requests for data (it is likely that these account for the overwhelming majority of requests). Since the review is carried out by the data supplier itself, the data supplier takes on only a slight burden and numerous data distribution requests can be handled on a daily basis without necessitating a review by government authorities. Germany's foreign and security policy interests are effectively protected since the parameters set forth for the procedure and criteria are explicit and do not give the data supplier the possibility of discretionary evaluation and since government authorities are empowered to exercise a control function.
In addition, a licensing obligation is introduced for the satellite operator, as well as a licensing requirement for the data supplier to ensure that the security demands required by law are met and to make possible a detailed advance review by the responsible authorities.

 The details of the procedure are defined in the statutory ordinance “Verordnung zum Satellitendatensicherheitsgesetz (Satellitendatensicherheitsverordnung – SatDSiV)“.

Contents of the Rules

Protected property
Protected property under the Act comprises the essential security interests of the Federal Republic of Germany, the peaceful co-existence of peoples, and the foreign relations of the Federal Republic of Germany. This protection runs parallel to that found in external economic policy. References to the protected property may be found in Sections 2(2), 10(1 and 2), 17(2), 19(2), 27, and 29(1).

Area of application
The area of application (Section 1) has been extensively defined in order to avoid gaps or possibilities of circumvention. The Act covers all German citizens and organizations under German law. It also covers those foreign enterprises that are either domiciled in or essentially exercise effective control over their operations in Germany's Federal Area. That means that all enterprises are covered for which the Act can be effectively enforced.
Military and intelligence service satellites do not fall within the area of application of the Act. For their data are appropriately kept secret by the government authorities that 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 area 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.

Licensing of satellite operations
If a space-based earth remote sensing system (normally a satellite with earth remote sensing sensor) is considered to be a high-grade system, Section 3 of the Act requires the operator to obtain a license from the government authorities. The criteria determining the high-grade nature of the earth remote sensing system are listed in Section 2(2) as, among others, the system's capabilities for spatial resolution, spectral coverage, and spectral and temporal resolution. These aspects are defined more precisely in a statutory ordinance (SatDSiV).
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’s reliability, the persons who have access to the essential operational elements of the system must possess a security clearance in accordance with the Security Clearance Act (*Sicherheitsüberprüfungsgesetz*). The operational premises must be adequately secured to prevent unauthorized entry and the transmission of commands to the satellite must be secured by means of strong encryption. In this connection, procedures verified by the BSI (German Information Security Agency) 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). Furthermore, the government authorities are authorized 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).

Distribution of earth remote sensing data
Those wishing to distribute 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 to those imposed on the operator in Section 4 (Section 12).
The primary data supplier (licensee) may then distribute data from a high-grade earth remote sensing system only where such distribution does not compromise the foreign and security policy interests of the Federal Republic of Germany.
In the typical case of a customer's request for the provision of data, a two-layered approach is conducted. The background is that, with the anticipated large number of data requests (roughly 100 customer requests are currently made are every day), it would be unfeasible for the government authorities to review each request. For the effort required and the time needed would be excessive; the result would be a lack of efficiency and an impairment of commercialization.
The two layers of the review may be described as follows:
The first phase is a "sensitivity check" of specific data requests that the data supplier carries out in accordance with set procedure and clearly defined criteria with no room for discretionary assessment (Section 17). The review is conducted to determine any potential endangerment of security. The criteria for the sensitivity check takes 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. Even though the sensitivity check refers to the distribution of a specific satellite image and/or satellite data set, the actual content of the data is not checked but only the so-called meta data. The meta data make possible an abstract description of the specific data set and a review of whether the transfer of this data set is admissible before the observation of the target area by the satellite. In addition, the data supplier is never required to disclose a data set to the authority.
Where the review classifies the specific data request as non-sensitive, the data supplier can provide the requested data products without additional consideration by the government authorities or occasion the download of the data to a receiving station of the customer.
Only where the data supplier's review classifies the customer data request as sensitive is the supplier initially prohibited from complying with the customer's request. The data supplier may, however, apply for consideration by the government authorities in a second phase review if it nevertheless wishes to comply with the request (Section 19). The authorities then conduct a case-specific review to determine if the customer request would endanger the security of the Federal Republic. If the endangerment is ruled out, permission is issued for the data supplier to comply with the request. A possible result of the review could also be to rule out endangerment if the data request is altered slightly, for example, less resolution, time delay, reduced processing quality of the data, or the omission of certain target areas. In such cases, the authorities issue conditional authorization. If an endangerment ultimately remains sustained despite potential conditions, compliance with the data request remains prohibited. To impair commercial transactions no more than necessary, the authorities should decide requests within a short period of time (a maximum one month is proposed).

Restrictive regulations under company law concerning operators
To insure that no risks to security arise when foreign nationals acquire an operating company or stakes in an operating company, or in a satellite or other parts of the earth remote sensing systems, such transactions are restricted by Section 10 by imposition of a reporting and licensing

requirement. For foreigners can more easily avoid supervision, access, and possibly criminal prosecution.
In addition, Section 10 makes the acquisition of an earth remote sensing system or of parts of such a system subject to authorization. This is necessary as otherwise the transfer of an earth remote sensing satellite in orbit, for example, could easily be effected. Neither would this constitute a distribution of data which could be reviewed under the SatDSiG nor would it be deemed an export which could be reviewed under the EC Dual Use Regulation.

Priority treatment for data requests by the Federal Republic
The Act contains the obligation for the satellite operator and data supplier in exceptional cases to give data requests by the Federal Republic priority chronological treatment before those of others. A NATO contingency situation and states of defense, tension, and emergency are viewed such exceptional cases. Furthermore, this right of priority also applies in the interest of protecting the military and civil forces of the Federal Republic of Germany employed abroad (Section 21). This guarantees that important data requests in these special cases are treated at short notice.
To keep at a minimum the intervention in the rights of the affected data suppliers and satellite operators, and to avoid endangering the goal of a commercialization of earth remote sensing activities, the number of cases whose features may be considered exceptional is very restricted. Section 21 becomes relevant only where, in addition to the data request by the Federal Republic, a competing data request has been placed by another customer, thus creating a conflict over the satellite's resources, with the result that the data supplier, for technical reasons, can only decide in favor of one of the requests.

Administrative fines and criminal provisions
A number of definitions of administrative and criminal offenses have been included into the Bill (Sections 28 and 29). This has been done to ensure observance of the Act. They are directed at satellite operators and data suppliers.

Competent Authority

The Federal Office of Economics and Export Control (BAFA) in Eschborn has been assigned the competent authority entrusted with the administrative enforcement of the Act, not including the competence for security checks and the control of acquisitions. Its responsibilities include, in particular, granting licenses for the operation of high-grade earth remote sensing systems including supervision of the operator, granting of permission to transfer the earth remote sensing system in accordance with Section 10 (2), granting licenses for data suppliers including the supervisory functions (Sections 11, 12, 13 – 16); the authorization to handle sensitive requests pursuant to Section 19 and the collective authorization for the distribution of data pursuant to Section 20.
It is in the competence of the Federal Ministry of Economics and Technology to authorize the acquisition of companies (Section 10 (1)) and the review procedures under the Security Clearance Act for parts of the operator and supplier staff as a prerequisite for obtaining supplier and operator licenses. Further to this, the security procedures of the German Information Security Agency (BSI) must be taken into account in connection with the operator and supplier licenses.