European Earth Observation Data Policy

Meeting Various Goals by Multiple and Diverse Actors: A Herculean Task?

Irmgard Marboe[*]

Abstract

The European Union has recently engaged in formulating political and legal principles, which should be guiding the European activities in the area of Earth observation data collected by satellites, in particular in the framework of the Copernicus programme. The focus of this program is the development of the necessary infrastructure and the generation and use of the acquired data. The European Union is especially interested in the use of Earth observation data for disaster and crisis management, land and sea monitoring, and the monitoring of the atmosphere. In addition, the generation and use of security related data is also envisaged. In this context, the European Union, due to its nature as a regional supranational organization, is confronted with particular challenges as it has to take into consideration the respective activities and competences of its member States as well as of its most important international partner in this endeavour, the European Space Agency (ESA). Over the past months, the European Union and ESA have been developing institutional mechanisms and procedures to provide the necessary framework for negotiation and decision-making in the area of Earth observation data policy. The most recent legal and political instruments as well as some further proposals will be presented and analysed in this paper.

An important characteristic of the European data policy is that, on the one hand, it propagates the concept of an "open data-policy" (see already the Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 about the re-use of public sector information) but that, on the other, it is also committed to the protection of several other rights and principles, such as the right to private life, the protection of personal data and of intellectual property, the freedom of arts and science, entrepreneurial freedom as well as national security interests. It is therefore of interest to have a closer look at the respective documents and proposals in order to find out how the balance between a "full and open access" to data policy and the protection of other rights and principles is supposed to be achieved.

* Univ. Prof., University of Vienna, Austria, irmgard.marboe@univie.ac.at.

I. Introduction

A discussion of European Earth observation data policy needs to start with a definition of what "European" actually means.[1] On the European continent, several actors are carrying out Earth observation activities and several layers of law and policy come into play. The most prominent actor is the European Union (EU) with its 28 member States and 500 million inhabitants. In the area of space activities, however, the EU is relatively new, and it is the European Space Agency (ESA), founded in 1975, that has been the gravitational centre of European space cooperation in the past decades. The two have joined their efforts for a major endeavour in the field of Earth observation, the Copernicus programme.[2] However, individual European States also continue to carry out national Earth observation activities on the basis of national laws and policies. The European Commission has launched an attempt to harmonize these national data policies in order to create a "European" data policy also outside the Copernicus programme. Finally, there is still another European organization which determines the legal framework of European governmental and private activities, namely the Council of Europe. With its focus on human rights, democracy and the rule of law and its role as the guardian of the European Convention of Human Rights, it gives important guidelines for data policies and laws in its 47 member States. As will be seen, this interaction of diverse actors and diverse policies and laws does not render the identification of a "European" data policy easy.[3] Yet, important developments have taken place recently which will shape the European regulatory framework for the access and use of Earth observation data in the near future. It is therefore important to analyse and discuss them in a timely manner to raise awareness of possible contradictions or lacunae.

1 Similarly Frans von der Dunk, 'European Satellite Earth Observation: Law, Regulations, Policies, Projects, and Programs' in 42 Creighton Law Review (2008-2009) 397-445, 397; See also idem, 'Earth Observation Data Policy in Europe – an Inventory of Legal Aspects and Legal Issues', in: Ray Harris (ed), *Earth Observation Data Policy and Europe* (Balkema Publishers, Lisse 2002) 19-28, 19.

2 Copernicus, previously Global Monitoring for Environment and Security (GMES) collects data from multiple sources to provide users with information related to environmental and security issues. See //www.copernicus.eu/.

3 See also the insightful article by Frans von der Dunk, 'Europe and the "Resolution Revolution": "European" Legal Approaches to Privacy and Their Relevance for Space Remote Sensing Activities', in 34 Annals of Air and Space Law (2009) 809-844.

II. The Copernicus Programme

The current legal framework of the Copernicus Programme is constituted mainly by a EU Regulation of 2014 (hereinafter Copernicus Regulation)[4] and a EU Commission Delegated Regulation of 2013 (hereinafter Commission Delegated Act).[5] Copernicus is a civil, user driven programme under civil control, building on the existing national and European capacities.[6] It shall contribute to monitoring the Earth to support the protection of the environment and the efforts of civil protection and civil security,[7] maximising socio-economic benefits,[8] and fostering the development of a competitive European space industry.[9]

The Copernicus Space Component Data Access (CSCDA) provides comprehendsive and coordinated access to Earth observation data products from multiple satellites for Copernicus data users across Europe.[10] It manages the coordinated production of Data Sets: multi-mission coherent data collection pre-defined according to specific user needs in terms of data type and mode of operation.[11] The key component is the Coordinated Data Access System (CDS) ensuring Data Set construction and dissemination.[12]

The Copernicus data and information policy is contained in Chapter IV of the Copernicus Regulation.[13] The promotion of the use and sharing of Copernicus data and Copernicus information is one of its principal objectives.[14] Dedicated mission data and Copernicus information shall be made available through Copernicus dissemination platforms "on a full, open and free-of-charge basis."[15] However, in addition to pre-defined technical conditions,

---

4 Regulation (EU) No 377/2014 of the European Parliament and the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, OJ L122/44 of 24 April 2010.

5 Commission Delegated Regulation (EU) No 1159/2013 of 12 July 2013, OJ L309/1 of 19 November 2013.

6 Article 2 Copernicus Regulation.

7 Article 4 (a) Copernicus Regulation.

8 Article 4 (b) Copernicus Regulation.

9 Article 4 (c) Copernicus Regulation.

10 See https://copernicusdata.esa.int/web/cscda/ data-offer. For previous developments See Ray Harris and Richard Browning, *Global Monitoring. The Challenges of Access to Data* (UCL Press, London 2005), 115-124.

11 ESA, 'Copernicus Space Component Data Access Architecture', 27 May 2014, Vienna, Austria. See https://www.ffg.at/sites/default/files/esa_csc_data_access_architecture.pdf.

12 See www.esa.int/Our_Activities/Observing _the_Earth/Copernicus/Coordinated_ data_access_system.

13 Chapter IV, Articles 23 to 25 Copernicus Regulation.

14 Article 23 (1) (a) Copernicus Regulation.

15 Article 23 (2) Copernicus Regulation. This is in line with the main trend in Earth observation data policy for some years. See Ray Harris, 'Main Trends in Earth Observation Data Policy', in Ray Harris (ed), *Earth Observation Data Policy and Europe* (Balkema Publishers, Lisse 2002) 9-16.

there are also other important limitations. These include (a) licensing conditions for third party data and information, (b) formats, characteristics and dissemination means, and (c) security interests and external relations of the EU or its member States.[16]

The latter two limitations pose, of course, a major problem and raise the question of how to balance the claim to "full and open" access to data with the protection of security interests and external relations of the Union or its member States. As is well known, the member States retain "the sole responsibility" for national security under the distribution of competences between the EU and its member States.[17] With regard to their "external relations", the member States also maintain their freedom of action and sovereignty. Some of them are members of NATO, others are not,[18] and some are permanently neutral.[19] It follows that the "security interests and external relations" of the member States are very diverse so that the implementation of this limitation in practice will be a major challenge.

Furthermore, the EU's "security interests and external relations" can only be defined under the Common Foreign and Security Policy (CFSP) which is subject to specific rules and procedures.[20] In this area, as is also well known, the European Council and the Council must act unanimously.[21] The adoption of legislative acts is excluded, and the Court of Justice of the European Union does not have jurisdiction. It follows that the definition of the EU's "security interests and external relations" will also represent a major challenge. As unanimity in this regard is neither easy nor frequent, a preliminary assessment may be that this limitation on the "full and open" access to data will not be very relevant in practice.

By contrast, the limitation for "security interests and external relations" of the individual member States will remain relevant. The Copernicus legal framework has introduced specific procedures to cope with the expected divergent views and sensitivities.

III. The Copernicus Committee

Under the Copernicus Regulation, it is the role of the European Commission to assess the necessary security measures to avoid any risks or threats for the

16 Article 23 (2) (a) to (c) Copernicus Regulation.
17 Article 4 (2) Treaty on European Union.
18 Six EU member States are not members of NATO: Austria, Cyprus, Finland, Malta and Sweden.
19 Austria, Finland and Sweden.
20 See Title V, Chapter 2 of the Treaty on European Union on "Specific Provisions on the Common Foreign and Security Policy", Articles 23 to 25.
21 Article 24 (1) Treaty on European Union.

interest or security of the EU or its member States.[22] On this basis, it shall establish the necessary security-related technical specifications for Copernicus by means of implementing acts. Where EU classified information is generated or handled within Copernicus, all participants ensure a degree of protection equivalent to the rules set out for classified information.[23]

In the procedure of safeguarding security interests, the Commission shall be assisted by a committee, the "Copernicus Committee".[24] This Committee shall meet in specific configurations with regards to security aspects ("Security Board").[25] Its rules of procedure are contained in a Regulation of 2011 which provides mechanisms for control by member States of the Commission's exercise of implementing powers.[26]

The Committee consists of representatives of all member States and is chaired by a representative of the Commission.[27] The chair shall "endeavour to find solutions which command the widest possible support within the committee".[28] If there is persistent disagreement, the Committee can also decide by a vote. Two different voting procedures are available, namely (1) the Advisory procedure, and (2) the Examination procedure. In the Advisory procedure, the Committee may take a vote by simple majority.[29] The Commission then decides "taking the utmost account of the conclusions drawn from the discussion".[30] In the Examination procedure,[31] the Committee shall deliver its opinion by a weighted majority as established for Council decisions.[32] This generally requires the so-called "double majority" of 55% of member States representing 65% of the EU population. In case of a positive decision, the Commission shall adopt the implementing act; in case of a negative decision it shall not adopt it.

---

22 Article 25 (1) Copernicus Regulation.
23 See the Annex to the Decision of the Commission 2001/844/EC on Commission Provisions on Security, OJ L 317/2, and the Council Decision on the security rules for protecting EU classified information 2013/488/EU, including Annexes OJ L 274/1.
24 Article 30 (1) Copernicus Regulation.
25 Article 30 (2) Copernicus Regulation.
26 Regulation (EU) No 182/2011 of the European Parliament and of the Council laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L55/13 of 28 February 2011 (hereinafter Implementing Powers Regulation).
27 Article 3 (2) Implementing Powers Regulation.
28 Article 3 (4) Implementing Powers Regulation.
29 Article 4 (1) Implementing Powers Regulation.
30 Article 4 (2) Implementing Powers Regulation.
31 Article 5 Implementing Powers Regulation.
32 Article 16 (4) and (6) of the Treaty on European Union and, where applicable, Article 238 (3) TFEU.

The control mechanism includes also an appeals mechanism. Where applicable, referral to an appeal committee is possible which decides by a weighted majority and shall deliver its opinion within two months of the date of referral.[33]
The installation of a Copernicus Committee can be regarded as a valuable tool for solving disagreements and balancing the "full and open access" to data policy with "security interests and external relations" of the EU member States. However, it remains to be seen whether the decision-making within the Copernicus Committee can be organized and structured in a way that allows responding quickly enough to claims for security sensitive data. Furthermore, the decision making by a majority vote is in contrast to the rule that in sensitive areas of national security and external relations the States remain solely responsible.
The option of majority voting could represent a problem for States participating in the Copernicus programme that are not represented, i.e. the non-EU members Switzerland and Norway. This is one of the aspects in the complex relationship between EU and ESA in the Copernicus Programme.

IV. Sentinel Data Policy

Sentinel satellites are developed and launched by ESA under the Copernicus Space Component (CSC) programme. Sentinel-1A was launched on 3 April 2014, and Sentinel-2A on 23 June 2015.[34]
On 24 September 2013, the ESA Earth Observation Programme Board approved the "Copernicus Sentinel Data Policy" (hereinafter Sentinel Data Policy).[35] It establishes the policy governing the provision of Sentinel data.[36] It covers the Sentinel 1 to 5 missions, the Sentinel-5 Precursor mission and Jason-CS missions developed by ESA under the CSC programme. The Sentinel Data Policy describes itself as a part of the overall Copernicus Data and Information Policy under EU responsibility.[37] As such, it also aims at "promoting the use and sharing of information and data" and "full and open access to information produced by Copernicus services and data collected through Copernicus infrastructure."[38]
Limitations to "full and open access" should be possible subject to "relevant international agreements, security restrictions and licensing conditions,

33 Article 3 (7) Implementing Powers Regulation.
34 See a short description of the "new family of missions called Sentinels specifically for the operational needs of the Copernicus Programme" at www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Overview4.
35 ESA Earth Observation Board, Copernicus Sentinel Data Policy, ESA/PB-EO(2013)30, rev. 1, 2 October 2013.
36 *Ibid.*, 3.
37 Ibid.
38 Ibid.

including registration and acceptance of user license".[39] The Sentinel Data Policy is only a short document and not very specific in how the different goals should be balanced. Yes, it enlists a number of instruments which are supposed to provide the respective legal and programmatic framework, amongst which are the relevant EU Copernicus legal instruments, the agreement with the EU on the Implementation of the Space Component of Copernicus[40] and the UN Remote Sensing Principles.[41] It does not address the fact that not all ESA members are EU-members and therefore not involved in the decision making process in the Copernicus data policy within the EU and its implementation. Yet, as the spatial resolution of the Sentinel satellites is rather low, i.e. so far not higher than 5x5 meters, security concerns might not have been a major concern of the ESA Earth Observation Programme Board.

V. EU Commission Delegated Act

The EU Commission, by contrast, has addressed the security concerns and sensitivity criteria which need to be balanced against the "full and open access" to some detail in its Delegated Act of 2013.[42] While the latter still remains the general principle and guideline, reference is also made to "conflicting rights" which need also to be taken into account. The EU Commission makes clear that the Copernicus data and information policy should be consistent with other relevant EU policies, instruments and actions, most importantly INSPIRE,[43] the policy on the re-use of public sector information[44] and the "Digital Agenda for Europe".[45]

Then, it elaborates on the more concrete conditions concerning use. Reiterating that users shall have free, full and open access to Copernicus dedicated data and service information,[46] it explains that free access shall be given to

39 Ibid.

40 Agreement on the Implementation of the Space Component of GMES concluded on 28 February 2008 and amended on 28 January 2009 and on 15 June 2011, ESA/LEG/382.

41 "Principles Relating to Remote Sensing of the Earth from Outer Space", adopted by the UN General Assembly in its Resolution 41/65 of 3 December 1986.

42 See above, fn 5. Yet, according to Article 13, the specific rules on "sensitivity criteria" are only applicable to space based observation systems meeting at least one of the characteristics listed in the Annex of the Delegated Act. The Annex explains that the system must be technically capable of generating data of a geometric resolution of 2.5 metres or less in a least one horizontal direction, or other high resolution data.

43 Directive 2007/2/EC of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

44 Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information, reinforced by Commission Decision 2011/833/EU of 12 December 2011.

45 European Commission, 'A Digital Agenda for Europe', COM(2010) 245 final/2 of 26 August 2010.

46 Article 3 Commission Delegated Act.

Copernicus dedicated data and service information made available through dissemination platforms under pre-defined technical conditions.[47]
Access to Copernicus dedicated data and service information shall be given for the purpose of the following use in so far as it is lawful: (a) reproduction; (b) distribution; (c) communication to the public; (d) adaptation, modification and combination with other data and information; (e) any combination of points (a) to (d).[48] Copernicus dedicated data and service information may be used worldwide without limitations in time.[49]
Four levels of registration of users should be provided as regards the access to data and information:
(a) Discovery and view services[50] should be provided without registration;
(b) a light form of registration should be required as regards download services;[51]
(c) an intermediate level of registration should allow the reservation of access to certain groups of users;
(d) a strict registration procedure should be used to address the need to restrict access for security reasons requiring the unequivocal identification of the user.[52]

With respect to "conflicting rights", the Commission shall take the necessary measures where the open dissemination of data or information conflicts with "international agreements" or the "protection of intellectual property rights", or would in a disproportionate manner affect the "rights and principles enshrined in the Charter of Fundamental Rights of the EU, such as the right for private life or the protection of personal data".[53]
This shows that the Commission is well aware of the need to find a balance between the "full and open access" to data policy and other legitimate rights and interest. Some of those which could be especially relevant will be highlighted in the following.

VI. Relevant International Agreements

The "international agreements" mentioned in the Commission Delegated Act include in particular obligations under international treaties forming a common defence organisation.[54] Many of the EU members are members of NATO which is a military alliance based on the right to collective self-defence under

47 Article 4 Commission Delegated Act.
48 Article 7 (1) Commission Delegated Act.
49 Article 7 (2) Commission Delegated Act.
50 Within the meaning of Article 11(1)(a) and (b) of Directive 2007/2/EC.
51 Within the meaning of Article 11(1)(c) of Directive 2007/2/EC.
52 Preambular paragraph 17 Commission Delegated Act.
53 Article 11 Commission Delegated Act.
54 See Preambular paragraph 13 Commission Delegated Act.

Article 51 of the UN-Charter. The most important norm of the founding treaty, the Washington Treaty of 1949, is Article 5 according to which "[t]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[55]

This obligation of mutual assistance in case of an armed attack triggers a lot of other obligations in terms of cooperation, coordination and preparation in security related matters. Certainly not all information that is gathered in the area of Earth observation, including by satellites, can be shared with other States or the general public. While, so far the Copernicus Space Component (CSC), mainly represented by the Sentinel satellites, is not considered to be security sensitive,[56] information from other Copernicus contributing missions and, in particular, the combination of data from various sources may create security relevant information.

Other international agreements relevant in the area of Earth observation are treaties establishing the rights and obligations of States in times of war and armed conflict. For example, the Hague Convention respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land[57] determines specific obligations of neutral powers not to support belligerents in case of war. Otherwise, they lose their status as neutral power and can be legitimately attacked by the opposing belligerent. The obligations include the prohibition to erect and use "wireless telegraphy stations" on the territory of a neutral power.[58] Even if, in 1907, the use of satellites and ground stations was not envisaged, it is not too far-reaching to interpret this prohibition as being applicable also to new technology with similar functions – namely the wireless sending and receiving of information.

A neutral power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.[59] However, every measure of restriction or prohibition taken by a neutral power must be

55 Article 5 Treaty of Washington, 4 April 1949, 34 UNTS 243.
56 See already *supra*, fn 42.
57 Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907, 205 Consolidated Treaty Series 299 (hereinafter Hague Convention V).
58 Article 3 Hague Convention V.
59 Article 8 Hague Convention V.

impartially applied by it to all of the belligerent parties.[60] A neutral power must see the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.[61]
These obligations are not incumbent only on permanently neutral States, as Austria, Finland, Sweden and Switzerland, but on all States that do not want to become engaged in a specific international armed conflict. In the process of granting access to and allowing the use of Earth observation data, these obligations therefore need to be kept in mind.

VII. Human Rights

The EU Commission Delegated Act identifies as "conflicting rights" also the "rights and principles enshrined in the Charter of Fundamental Rights of the EU, such as the right for private life or the protection of personal data".[62]
The "the right for private life or the protection of personal data" is specifically highlighted as it needs particular attention in the context of "full and open access" to data.
Article 7 on the "Respect for private and family life" of the EU Charter of Fundamental Rights provides that "[e]veryone has the right to respect for his or her private and family life, home and communications."[63] Article 8 on the "Protection of personal data" declares that "[e]veryone has the right to the protection of personal data concerning him or her."[64] Personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[65] In order to ensure that this right is implemented in the member States, "[c]ompliance with these rules shall be subject to control by an independent authority."[66]
The judicial control of the implementtation of the EU Charter of Fundamental Rights is not entirely settled yet. The Court of Justice of the European Union, as EU organ, adjudicates on the EU's acts. As regards the implementation at the member State level, all of the EU member States are also members of the Council of Europe and have ratified the European Convention on Human

60 Article 9 Hague Convention V.
61 Article 9 Hague Convention V.
62 Article 11 Commission Delegated Act.
63 Atricle 7 Charter of Fundamental Rights oft he European Union, as adapted and entered into force with the Treaty of Lisbon, OJ C 326/391 of 26 October 2012 (hereinafter EU Charter of Fundamental Rights).
64 Article 8 (1) EU Charter of Fundamental Rights.
65 Article 8 (2) EU Charter of Fundamental Rights.
66 Article 8 (3) EU Charter of Fundamental Rights.

Rights.[67] Many of them have incorporated the Convention in their national constitutions. Judicial control of its implementation is provided by established jurisprudence of the European Court of Human Rights. In order to ensure a common understanding and level of human rights protection in Europe, the European Union shall accede to the European Convention on Human Rights according to the Treaty of Lisbon.[68] However, so far this accession has not taken place.

In the current situation, EU member States are primarily bound by their human rights obligations under the European Convention on Human Rights.[69] The Convention also contains a "Right to respect for private and family life".[70] While the substance of this right is similar to that of Article 8 of the EU Charter of Fundamental Rights, namely that "[t]here shall be no interference by a public authority with the exercise of this right", there are also differences. Notable is the explicit possibility to limit this right by law, if this "is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[71]

The jurisprudence of the European Court of Human Rights informs States how their obligations under this right have to be interpreted. It makes clear that Article 8 covers the physical and psychological integrity of a person and embraces aspects of an individual's physical and social identity, such as, for example, gender identification, name and sexual orientation and sexual life.[72] It also protects the right to personal development. The notion of personal autonomy is an important principle underlying the interpretation of the guarantees of Article 8. Protection is particularly warranted against attacks on honour and reputation, manipulation and misuse of personal information.[73]

The obligations of States encompass the duty not to interfere with personal privacy ("to respect") and to take positive measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves ("to protect"). They also protect juridical persons from undue interference.[74]

---

67 Convention for the Protection of Human Human Rights and Fundamental Freedoms, Rome, 4 November 1950 (ECHR).

68 Article 6 (2) of the Treaty on European Union.

69 Irmgard Marboe, 'Human Rights Considerations for Space Activities', in: Stephan Hobe and Steven Freeland (eds), *In Heaven as on Earth? The Interaction of Public International Law on the Legal Regulation of Outer Space* (2013) 135, 144 f.

70 Article 8 (1) ECHR.

71 Article 8 (2) ECHR.

72 von Hannover v. Germany (2004); Anastasios Reklos v. Greece (2009).

73 See also Lauren H. Rakower, 'Zooming In. On Google Street View and the Global Right to Privacy', in: 37 Brooklyn Journal of International Law (2011) 317-347.

74 Colas Est v. France (2002).

The Court highlighted that increased vigilance in protecting private life was necessary to contend with new communication technologies which make it possible to store and reproduce personal data.[75] Exceptions are allowed under the conditions of Article 8 (2)[76] and in times of war or other public emergency threatening the life of the nation under Article 15 (1) ECHR.[77]

It follows from the above that national measures on privacy and data protection can be different from country to country. These differences can be an obstacle to the free movement of goods and services in the internal market,[78] as it is envisaged within the EU.[79] Harmonisation of national measures would grant a better level playing field for companies operating in the EU. The EU has therefore issued a Data Protection Directive[80] that identifies principles on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The ways and means of implementing the Directive are left to the member States, but the common goals contained therein must be fulfilled.

Under the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes, be adequate, relevant and not excessive in relation to the purposes. They must be accurate and, when necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate or incomplete data are erased or rectified. The data must be stored for no longer than necessary for the purposes, except for historical, statistical or scientific use, against appropriate safeguards.[81] Furthermore, they may be processed only if the data subject has given his/her consent, if this is necessary for the performance of a contract or a legal obligation or to protect the vital interests of the data subject. Another reason may also be the performance of a task carried out in the public interest or in the exercise of official authority.[82]

Another Directive, the E-Privacy-Directive, provides for the harmonisation of national provisions concerning the processing of personal data and the

75 von Hannover v. Germany (2004), para. 70.

76 See above, text at fn 70.

77 Article 15 (1) ECMR reads: "In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law."

78 Frans von der Dunk, above fn 3, 824.

79 According to Article 3 (3) TEU, the objective of the EU is, amongst others, to "establish an internal market".

80 Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995, OJ of 23 November 1995, L281/31-50.

81 Article 6 (1) Data Protection Directive.

82 Article 7 Data Protection Directive.

protection of privacy in the electronic communication sector.[83] According to this Directive, member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. They must guarantee that subscribers are informed of the data which are being collected and that location data may only be processed when they are made anonymous, or with the consent of the users or subscribers. Users or subscribers must be informed, prior to obtaining their consent, of the type of location data, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing value added service. Furthermore, users or subscribers must have the possibility to withdraw their consent for the processing of location data at any time.[84]

The question, of course, arises of how these rules and principles can be brought in line with a "full and open access" to data policy. In particular in view of the fact that Earth observation data are collected in a general and automated way, generally without the consent of the sensed subjects. They are used for a large variety and not only for specific purposes. Large quantum is collected and processed which has become known under the term "Big Data".[85]

As regards Copernicus data and information, the EU does not provide any express or implied warranty as regards quality and suitability for any purpose.[86] Data and information are stored for long periods, for historic, statistical, scientific, and other purposes.

There is, so far, no real guidance how these privacy concerns will be handled with be the respective EU organs. It is only clear that privacy issues become increasingly relevant with the improvement of spatial resolution of Earth observation data.[87]

VIII. National Data Policies and Their Attempted Harmonization

In recent years, national data policies have been developed to address the increasing commercialization of space activities.[88] Earth observation is not any longer a purely governmental activity but more frequently also carried out by the private sector. With improving technical performance and increasing capabilities, the resolution of the images is improving, raising concerns to national security.

---

83 Directive 2002/58/EC of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the electronic sector, amended by Directive 2009/136/EC, OJ of 31 July 2002, L201/37-47.

84 Article 12 E-Privacy-Directive.

85 See, for example, Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. A revolution that will transform how we live, work, and think* (Houghton, Mifflin, Harcourt Publishing, New York 2013).

86 Article 9 Commission Delegated Act.

87 Frans von der Dunk, 'The Resolution Revolution'.

88 See Raymond Harris, *Earth Observation Data Policy* (Wiley & Sons, Chichester 1997) 39 ff.

The most notable example of a very detailed national law on Earth observation data is the German 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 2007. The Act applies to the operation of high-grade Earth remote sensing systems for which licenses must be obtained from the government.
The licenses depend on a sensitivity check to assess the possibility of harm being caused to the vital security interests of Germany, to the peaceful coexistence of nations or to Germany's foreign relations, including obligations assumed under international agreements.
In view of this new development, the European Commission sees the need to provide guidelines to EU member States who also consider enacting such a law. In order to prevent further distortions of the internal market, it prepared a proposal for a Directive on the dissemination of Earth observation satellite data for commercial purposes.[89] The purpose of the directive is to establish a comprehensive regulatory framework to improve legal coherence and foster the emergence of a European market for space products and services concerning the production and dissemination of high resolution satellite data for commercial purposes. The proposal is currently under discussion by the EU Parliament and the Council. There exists some scepticism, whether such harmonization is warranted and useful at this point. Furthermore, there is a concern about the costs caused by such a directive, including administrative costs.[90] Future discussions will show whether the need for such a directive is perceived by the member States.

IX. Conclusion

The ambitious activities in the area of Earth observation in Europe are challenges not only in the technical but also in the legal and policy sphere. Several actors can be identified that influence the development of Earth observation data policy on the European continent. This leads to the conclusion that up to now, there is not one "European" policy on Earth observation data. What can be observed so far, are the legal and policy parameters in which the joint EU-ESA programme Copernicus is going to operate. But even in this limited context, many questions still remain open. How the different challenges will be met within the given framework described above will also form the shape of the European data policy in the future and help to answer some of the questions raised in this article in the years to come.

---

89 European Commission, 'Proposal for a directive on the dissemination of Earth observation satellite data for commercial purposes', COM(2014) 344 final of 17 June 2014.

90 Council of the EU, 'Proposal for a directive on the dissemination of Earth observation satellite data for commercial purposes – Guidance for further work', 2014/0176 (COD) of 20 March 2015.