

# Data protection and space: What challenges will the General Data Protection Regulation face when dealing with space-based data?

Received: 11th December, 2020



## Shakila Bu-Pasha

Postdoctoral Researcher at the Faculty of Law, University of Helsinki, Finland

Shakila Bu-Pasha is doing her postdoctoral research at the Faculty of Law, University of Helsinki, Finland. Her work covers interdisciplinary research in communication law and data protection law with keen focus on location data, personal data protection and privacy under EU law. She completed her doctoral study with the same university in December 2018. She received her second Master of Laws degree in Law and Information Society in August 2015 from the Faculty of Law, University of Turku, Finland. Before that, Shakila completed her Bachelor of Laws and first Master of Laws degrees in the Faculty of Law, University of Dhaka, Bangladesh.

PL 4 (Yliopistonkatu 3), 00014, Helsinki, Finland  
Tel: +358 50 531 1633; E-mail: shakila.bu-pasha@helsinki.fi



## Heidi Kuusniemi

Professor and Director of Digital Economy, University of Vaasa, Finland

Heidi Kuusniemi is a professor in computer science and director of the multidisciplinary research platform Digital Economy at the University of Vaasa in Finland. She is also a part-time research professor in satellite navigation at the Finnish Geospatial Research Institute of the National Land Survey of Finland. She has an MSc (Tech) degree (with distinction) from 2002 and a DSc (Tech) degree from 2005 in information technology, respectively, from Tampere University of Technology, Finland. Part of her doctoral research in 2003–2004 on navigation reliability was conducted at the Department of Geomatics Engineering, University of Calgary, Canada. In 2017, she was a visiting scholar at Stanford University's GPS Laboratory. She has worked in research and development within positioning technologies for over 18 years. She is also an adjunct professor in satellite navigation and positioning technologies at Tampere University and Aalto University in Finland. She serves as a member of the council of natural sciences and technology at the Academy of Finland and in the scientific advisory committee for global navigation satellite system (GNSS) (GSAC) at the European Space Agency. Her research interests include GNSS reliability, GNSS interference detection and mitigation, self-contained sensors, indoor positioning, internet of things, new space and the role of geospatial data and its privacy in the digital economy.

Digital Economy, University of Vaasa, Yliopistonranta 10, FI-65200 Vaasa, Finland  
Tel: +358 29 449 8504; E-mail: heidi.kuusniemi@univaasa.fi

**Abstract** Recently, space or satellite technology, as well as space data applications, is developing rapidly, resulting in a variety of uses. At the same time, related legal issues raise questions about how they can be handled efficiently. In addition to pointing out the importance of managing satellite activities in a legally sound environment, this paper explains the relevance of the General Data Protection Regulation and the challenges it will face in handling space-based data, as well as in managing threats to privacy and personal data regarding the outer space context.

**KEYWORDS:** satellite, GDPR, personal data, space-based data, privacy, technology

## INTRODUCTION

Space and the related satellite technology have created immense potential to facilitate human civilisation with various services. This sector plays important roles, ranging from accelerating faster communication systems to fostering the digital economy, and it contains more potential to contribute immensely to smart technological networks.<sup>1</sup> The new space economy<sup>2</sup> refers to business characterised by new commercial actors and business models and the utilisation of small satellites to provide services, space-based data and applications.

For the purpose of this paper, there are two aspects related in the context of space and space-based data. The first aspect regards regulation and control of satellite ownership, licensing, technical requirements, limitations and responsibilities.<sup>3</sup> The second aspect is the protection of personal data and privacy in relation to space-based data. Many latest technologies are used to generate satellite industry and data, including remote sensing, internet of things (IoT), 5G and so on.

Space-based arrangements, especially with the ever-widening use of technologies — such as the IoT, global navigation satellite systems (GNSSs), high-resolution remote sensing and future radio communication, such as 5G networks — are technically able to deduce accurate information, including much personal data, from the interconnected smart devices and sensors, which can cause threats to personal data and privacy. Legal issues and regulation, including the protection of personal and location data related to space-based big data, are key enablers for a viable and sustainable new space economy in the era of digital infrastructures being expanded to space.

The use of remote-sensing technology, as well as satellite connectivity, is generating and distributing huge amounts of data, which have developed into ‘space big data’. This variety of data may apparently seem unconnected, but in combination with other factors, it can produce accurate user

information.<sup>4</sup> The Infrastructure for Spatial Information in the European Community Directive<sup>5</sup> that entered into force in May 2007 covers spatial data and data services that are mainly limited to environmental issues, and it is therefore not widely applicable to data protection aspects.

The prime European Union (EU) law in the field of personal data protection and privacy is the General Data Protection Regulation (GDPR), which also has international application in certain circumstances. It is important to note that the GDPR does not contain a separate provision on outer space or space data perspectives, but many provisions of the GDPR can be interpreted by relating them to the space data context. Therefore, it is relevant to question whether the scope of the GDPR was intended to include space-based data. And if GDPR applies to data connected to space, is it a necessity to have a separate law regulating space big data? This paper provides a brief outlook on space-based data as well as explains what challenges the GDPR will face in handling such data and how GDPR provisions could or could not be applied regarding the outer space context or space big data. It also asks what would be the appropriate solution if the GDPR does not apply.

## AN OUTLOOK ON SPACE-BASED DATA

Space-based data typically encompasses data from meteorology, telecommunications, earth observation and navigation satellites. This means that the data sources and types of data vary widely, ranging from images to radio signals in different frequencies. Remote-sensing data types can include, for example, aerial optical images, thermal imagery, hyperspectral imagery, radio detection and ranging (RADAR) data or light detection and ranging (LIDAR) data. Space-based data is increasingly also open data<sup>6</sup>, predominantly from the large governmental space-based infrastructures,

referred as ‘old space’ for short. These include, for example, data sources such as the EU Copernicus Earth Observation Sentinel satellites, the US Geological Survey’s Landsat remote-sensing satellites, GNSS satellites — such as GPS, Galileo, Glonass and BeiDou — and meteorological satellites contributing to the World Meteorological Organisation’s Global Observing System, to name but a few. Space-based data offerings and access are currently undergoing a revolution due to the introduction of small, commercially available satellite infrastructures that are able to provide connectivity, remote sensing, positioning, and timing data and services much more affordably than ever before. Operators and data providers will be various commercial entities, thereby democratising the access to space and thus ultimately the earth-bound data provided by these space-based sensors. While the economic impacts of the commercial space industry<sup>7</sup> and data provision are evidently broad, this brings pressure to have globally coherent and transparent data privacy policies in relation to the various space-based data.

Many companies are operating hundreds of satellites including earth observation technologies. High-resolution imagers are revolving around the earth, which are able to point any place on the earth, and thus, it involves questions about location privacy.<sup>8</sup>

### **THE RELEVANCE OF THE GENERAL DATA PROTECTION REGULATION**

A country may have ownership in the airspace up to 160 km above the ground, although this height is not unanimously agreed internationally. But normally, satellites orbit in higher space, and therefore, those are not included by the national airspace.<sup>9</sup> In the confusion regarding whether the provision on extraterritorial application of the GDPR will apply in case of communications and data transmissions

via satellite, it can be said that, even though government satellites and remote sensing are involved, if personal data of EU citizens are concerned, and data is processed on the earth, the GDPR should apply, except some exceptions.

The GDPR becomes relevant with regard to satellite services and data in relation to television broadcasting, telecommunications and location-based services when the service providers and companies collect and process personal data as data processors and controllers.<sup>10</sup> Several provisions of the GDPR relate to the context of personal data processing in a space data platform, including the general principles of data processing, the rights of data subjects, the obligations of data controllers and processors (including the security of personal data), cross-border issues and the transfer of personal data, data protection by design and by default, and so on. The controllers are required to follow lawfulness of processing as described in Article 6. At the same time, informing data subjects about personal data processing, obtaining their consent, applying anonymisation and pseudonymisation, charging fines for infringements of GDPR provisions and other related requirements under the GDPR apply.

These aspects in general, with regard to personal data processing, however, have been featured in various research already. Therefore, instead of only discussing the connections between the GDPR and space data, this paper explores the reality related to satellite and space data and how effective the GDPR provisions are in handling space big data.

It is also important to determine whether a satellite operator is acting as a data controller or a processor because processors have different obligations to controllers. In some instances, satellite operators do not have a direct connection with data subjects, and they process data on behalf of the controller. According to Article 4(2) of the GDPR, the term ‘processing’

includes diverse meanings, for example, the ‘collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’ of personal data (here, via satellite). Therefore, drawing a contract between data controller and processor as per Article 28(3) of the GDPR is an important step for mentioning the processor’s main obligations in processing personal data.<sup>11</sup>

### **CHALLENGES AND EXCEPTIONS UNDER THE GENERAL DATA PROTECTION REGULATION**

In many cases, satellites in the EU region are run by EU institutions, and processing personal data by EU institutions is normally not governed by GDPR provisions. As an example, the Copernicus programme, previously known as the Global Monitoring of Environment and Security (GMES), is an earth observation programme in the EU for satellite remote sensing which generates and uses huge amounts of data.<sup>12</sup> The European Commission coordinates and manages the programme in partnership with EU member states, the European Space Agency (ESA) and other EU agencies.<sup>13</sup> The ESA coordinates the technical sides of the Copernicus initiative. Thus, EU institutions operate as the key entities for the functioning of the Copernicus programme.<sup>14</sup> In such instances, Regulation (EC) No. 45/2001 of the European Parliament used to apply.<sup>15</sup> A new regulation (Regulation [EU] 2018/1725),<sup>16</sup> however, has been introduced to replace Regulation (EC) No. 45/2001 in order to cope with GDPR requirements as well as to fulfil the current EU data protection legal framework.<sup>17</sup> Although this different regulation governs personal data protection aspects for EU institutions, it is important to note that Regulation (EU) 2018/1725 provides

rules for EU institutions in line with the GDPR standards.<sup>18</sup> For example, Article 5 of Regulation (EU) 2018/1725 reflects the conditions for the lawfulness of personal data processing as articulated in Article 6 of the GDPR, which states that only on some specific and lawful grounds can EU institutions, bodies and agencies process personal data.<sup>19</sup>

While the GDPR applies to the EU region, which consists of 27 member states, European satellite activities are not confined to the EU. European cooperation in space is targeted towards the member states of the Council of Europe. Institutions — for example, the European Commission or the European GNSS Agency — are not subject to the GDPR.<sup>20</sup>

The ESA is a very relevant institute which is not limited to the EU region; rather, it is considered as a global, transnational organisation. Except for some exceptions, the scope of the GDPR does not normally cover such international organisations. It is good, however, that the ESA’s internal personal data protection policy reflects the wording of the GDPR relating to the processing and protection of personal data.<sup>21</sup>

Regarding the exception mentioned earlier, according to Article 3 and Recital 23 of the GDPR, the provisions of the GDPR apply to both EU and non-EU companies (here, satellite operators) if they offer goods or services in the EU or to data subjects in the EU. Thus, the GDPR permits extraterritorial application in certain circumstances.<sup>22</sup> But such an ‘offering of goods or services’ requirement may not always match the space context. Most satellite activities, as well as remote-sensing activities, have a global effect.<sup>23</sup> As outer space indicates a common area with no boundary, space objects and satellite services, and the derived applications, are universal in nature. The existence of multiple satellites in space requires secure coordination among different networks to avoid possible conflicts. Therefore,

international dialogues and the enactment of applicable, binding international legal instruments are very important.<sup>24</sup>

Satellites are often operated by a public authority or state. It is relevant to mention that in certain circumstances the state or public authorities can enjoy some exceptions to the GDPR provisions where the general restrictions of that regulation will not apply.

It is alleged that there is a lack of transparency and openness in regard to the general public about the collection, sale and processing of data through satellite systems. Perhaps because of the military involvement and defence perspectives regarding satellite activities, some restrictions are maintained.<sup>25</sup> Governments across the world restrict satellite data as per their policies.<sup>26</sup> Uncontrolled access to satellite data can even threaten national security. National security is such a sensitive ground that different laws, including the GDPR, permit exceptions to general rights when there is the possibility of threats to national security. If transparency and openness, however, does not threaten national security, then it is the citizen's right to know more about the satellite data that she or he is being subjected to, or more specifically, the satellite data that are collected about herself or himself.<sup>27</sup> In particular, if someone's personal data is collected via satellite technologies, she or he should be informed about that. No more data should be collected than that which was initially intended to be shared.<sup>28</sup>

In the context of national security, if states assign security-related tasks to corporate or private entities which, at the same time, conduct the processing of personal data for civilian purposes, in such circumstances, determining the scope of the GDPR in regard to those entities may become challenging.<sup>29</sup>

Simultaneously, confusion arises about the circumstances in which open and free access to space data should be allowed. It

has also been highlighted that there needs to be a balance between the legal issues of the private ownership of data and information, and public interests when remote sensing or localisation is concerned.<sup>30,31</sup> There are two prevalent and apparently differing approaches in this context: while the European community considers the protection of personal data and privacy a fundamental human right, it also promotes business convenience with the free flow of data and open data platforms. Therefore, balancing these two approaches efficiently is very important in order to mitigate potential conflicts.<sup>32</sup> Open access to public digital data is always encouraged in order to benefit from such data, spur on new, innovative business opportunities and impact on society. The same approach to space-based data is also developing.<sup>33</sup> But protection of personal data and privacy must be guaranteed while making open any space data.<sup>34</sup> In this context, the instruction of Recital 4 of the GDPR can be considered; the recital communicates that 'the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.

## CONCLUSION

Technologies are constantly advancing, and space technologies are thereby growing fast and at an increasing pace. Space has become an essential part of our daily lives — data communications solutions, transport, weather forecasting, as well as agriculture and forestry are highly dependent on the space-based data resources offered by satellites. 'New space' offers the possibility of using satellite platforms for new, economically driven activities as it is orders of magnitude less costly than before because of advances in technologies, standardisation procedures and decreases



in launch costs. Due to the relatively low resolution of satellite imagery so far, not many privacy issues have been raised up to this point. Forecasts show that space-based data developments, however, are moving towards higher and higher resolutions, as are the obtainable localisation accuracies with GNSS, which explains why data privacy will become more and more important with space data. Although the GDPR provisions were intended to deal with the personal data protection issues that appeared with the rapid expansion of modern technologies, in certain circumstances its provisions may seem difficult to suit for handling satellite and space-based data. Because of its distinctive nature, introducing a new legal framework with a worldwide effect in order to secure the proper use of space-based data is a demand that needs to be met soon. Considering the link to national security and personal data protection with the satellite data, as well as the involvement of technical and legal speciality, a transparent and interdisciplinary regulatory framework would be effective in handling such data.<sup>35</sup> The enactment of such a regulatory framework will help to create a secured and steady environment for generating and using space-based data to its maximum potential. Also, the concerned law should efficiently balance privacy against the open data platform<sup>36</sup>, and this can be a topic for future research.

## ACKNOWLEDGMENT

The work is supported jointly by the Olga and Kaarle Oskari Laitinen foundation grant and the EU Interreg Botnia-Atlantica funded project KvarkenSpaceEconomy (www.kvarkenspacecenter.org).

## References

1. Wheeler, J. and Puschman, N. (2018) 'On the EU's space program and new EU agency for space proposal', available at: [http://interactive.satellitoday.com/via/july-2018/on-the-eus-space-program-and-](http://interactive.satellitoday.com/via/july-2018/on-the-eus-space-program-and-new-eu-agency-for-space-proposal/)
2. Pomeroy, C. et al. (2019) 'Fund me to the moon: Crowdfunding and the new space economy', *Space Policy*, Vol. 47, pp. 44–50, available at: <https://doi.org/10.1016/j.spacepol.2018.05.005> (accessed 30th May, 2020).
3. McKenna, A. T. et al. (2019) 'The role of satellites and smart devices: Data surprises and security, privacy, and regulatory challenges', *Penn State Law Review*, Vol. 123, p. 625.
4. Stefoudi, D. (2017) 'Space big data: Big data troubles in the final frontier', available at: <https://leidenlawblog.nl/articles/space-big-data-big-data-troubles-in-the-final-frontier> (accessed 22th March, 2020).
5. Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), available at: <https://eur-lex.europa.eu/eli/dir/2007/2/oj> (accessed 22 March, 2020).
6. Harris, R. and Baumann, I. (2015) 'Open data policies and satellite Earth observation', *Space Policy*, Vol. 32, pp. 44–53, available at: <https://doi.org/10.1016/j.spacepol.2015.01.001> (accessed 30th May, 2020).
7. George, K. W. (2019) 'The economic impacts of the commercial space industry', *Space Policy*, Vol. 47, pp. 181–186, available at: <https://doi.org/10.1016/j.spacepol.2018.12.003> (accessed 30th May, 2020).
8. Amos, J. 'Planet's satellites aim for still sharper view of Earth', available at: <https://www.bbc.com/news/science-environment-52980330> (accessed 20th November, 2020).
9. DataRep. 'Danger! GDPR ... In Space!', available at: <https://www.datarep.com/blog/2017/11/26/danger-gdpr-in-space/> (accessed 20th November, 2020).
10. Harebottle, A. (2018) 'GDPR is here but, what does it really mean for satellite?', available at: <https://www.satellitoday.com/business/2018/05/30/gdpr-is-here-but-what-does-it-really-mean-for-satellite/> (accessed 30th May, 2020).
11. Cocco, M. and Mendonca, H. C. (2018) 'GDPR for satellite operators: What you need to know', available at: <https://www.satellitoday.com/business/2018/06/19/gdpr-for-satellite-operators-what-you-need-to-know/> (accessed 30th May, 2020).
12. NEXTSPACE-SC5 (Final Report) (2019) 'Study on the Copernicus data policy post-2020', available at: [https://www.copernicus.eu/sites/default/files/2019-04/Study-on-the-Copernicus-data-policy-2019\\_0.pdf](https://www.copernicus.eu/sites/default/files/2019-04/Study-on-the-Copernicus-data-policy-2019_0.pdf), (accessed 30th May 2020).
13. Copernicus.eu. (2018) 'What is Copernicus?', available at: <https://web.archive.org/web/20181103182626/http://www.copernicus.eu/main/overview> (accessed 30th May, 2020).
14. Von der Dunk, F.G. (2009) 'Europe and the "resolution revolution": "European" legal approaches to privacy and their relevance for space remote sensing activities', *Space, Cyber, and Telecommunications*

- Law Program Faculty Publications*, pp. 810–844, available at: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1034&context=spacelaw> (accessed 30th May, 2020).
15. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001.
  16. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC Text with EEA relevance, OJ L 295.
  17. Balboni, P. (2018) 'Welcoming regulation (EU) 2018/1725 and new data protection rules for EU Institutions', available at: <https://www.paolobalboni.eu/index.php/2018/12/14/welcoming-regulation-eu-2018-1725-and-new-data-protection-rules-for-eu-institutions/> (accessed 30th May, 2020).
  18. European Data Protection Supervisor (2018) 'EDPS welcomes adoption of new data protection rules for EU institutions', available at [https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-welcomes-adoption-newdata-protection-rules\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-welcomes-adoption-newdata-protection-rules_en) (accessed 30th May, 2020).
  19. Bu-Pasha, S. (2019) 'Legal challenges with regard to open data in the EU and Finland', *Viestintäoikeuden vuosikirja 2018* (Yearbook of Communication Law 2018).
  20. Harebottle, ref 10. above.
  21. *Ibid.*
  22. Bu-Pasha, S. (2017) 'Cross-border issues under EU data protection law with regards to personal data protection', *Information & Communications Technology Law*, Vol. 26, No. 3, pp. 213–228, available at: <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740> (accessed 30th May, 2020).
  23. Von der Dunk, ref 14. above.
  24. Bu-Pasha, S. (2018) 'Vulnerabilities in localization with regard to GNSS and harmful radio interference: International and EU law aspects', *IEEE Access*, Vol. 6, pp. 8332–8339, available at: <https://helda.helsinki.fi/bitstream/handle/10138/299343/08289432.pdf?sequence=1> (accessed 30th May, 2020).
  25. Stefoudi, ref 4. above.
  26. Scoles, S. (2018) 'How the government controls sensitive satellite data', available at: <https://www.wired.com/story/how-the-government-controls-sensitive-satellite-data/> (accessed 30th May, 2020).
  27. Swayne, M. (2019) 'Researchers detail privacy-related legal, ethical challenges with satellite data', 12th July, available at: <https://phys.org/news/2019-07-privacy-related-legal-ethical-satellite.html> (accessed 30th May, 2020).
  28. Stefoudi, ref 4. above.
  29. Cocco and Mendonca, ref 11. above.
  30. Smith, L. J. and Doldirina, C. (2016) 'Remote sensing: A case for moving space data towards the public good', *Space Policy*, Vol. 37, No. 3, pp. 162–170, available at: <https://doi.org/10.1016/j.spacepol.2016.11.006> (accessed 30th May, 2020).
  31. Leppälä, L. (2018) 'Understanding the current trends in mobile crowdsensing: A business model perspective', Case MyGeoTrust, M.Sc. Thesis, Aalto University, available at: <https://aaltodoc.aalto.fi/handle/123456789/30685> (accessed 30th May, 2020).
  32. Von der Dunk, ref 14. above.
  33. Harris and Baumann, ref 6. above.
  34. Bu-Pasha, ref 19. above.
  35. McKenna, ref 3. above, p. 657.
  36. Stefoudi, ref 4. above.