Privacy Law Issues Raised by Developing Satellite Usage

From a European Legal Perspective

*Laura Keogh**

1. Introduction

Many current business models are founded and function on this idea of gathering data, but they often do not realise that certain data may be considered personal data for the purposes of EU law. Furthermore, even by simply collecting personal data, EU data protection law comes into play. Personal data has been dubbed the "new oil" and the big data enterprise is set to create billions of euros each year.

When one considers potential space technological developments, much of it may fall under European Union (EU) data protection law obligations. For example, the space belt idea to have a whole separate internet network in space, or the forth coming internet of things, which will see increased use of GPS functionalities and remote sensing. Not to mention future planned space missions and explorations will be gathering more and more data about astronauts and their counterparts. EU data protection law will need to be considered. While a satellite launched from EU territory is obliged to comply with EU data protection law, those satellites outside the EU will have the same obligation if they happen to be monitoring the EU and collecting data that will come within the scope of the definition of personal data. While much of this data may be aggregated and for statistical purposes, the statistical exemption under EU law is not in any way absolute.

The interaction between international law and privacy shall first be outlined, followed by the applicability of the General Data Protection Regulation (GDPR)[1] and consequences of GDPR application. It shall be concluded that

* MHL-Law Rechtsanwaltsgesellschaft mbH.

1 European Union (EU) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation/GDPR)

with the latest developments in space, there should be awareness over whether any aspect of the activities may fall within the GDPR.

2. International space law and privacy

While the GDPR focuses on the right to privacy of the individual, international space law has discussed the right to privacy of the state, particularly arising out of remote sensing.

2.1 1986 Resolution

In the past countries were concerned about surveillance via remote sensing of their territories by foreign countries without consent. The UN discussions that took place within the 1970's and 1980's showed that there was international concern for the privacy of states within outer space. Thus, in 1986 the UN published Resolution 41/65, 3 December 1986, Principles Relation to Remote Sensing of the Earth from Outer Space, which gained unanimous approval.[2] Privacy was a large discussion within the talks. However, regarding the legality of remote sensing, there was no conclusion and it was left vague because each country had a fundamental different understanding of privacy.[3] The 1986 Resolution simply reinforced provisions of the already established international space treaties; however, it was put in the context of remote sensing and privacy.

Principle 4 of the 1986 Resolution stated that remote sensing shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State.[4] This enforced the due regard principle within Article IX of the Outer Space Treaty,[5] which creates an obligation on states to have "due regard to the corresponding interests of all other State Parties to the Treaty." There is no agreed upon definition of what "due regard" means, but at a basic level it means taking precautionary action in light of known information that may negatively affect states.[6] Thus, it may be an argument for satellite entities to comply with the law of the State that is being sensed.

Principle 12 of the 1986 Resolution stated that a sensed state should have access to the data gathered. This reinforced the duty to inform within Article XI of the Outer Space Treaty. This article requires State Parties to the Treaty who are conducting activities in outer space to inform the Secretary General

2 Principles relating to remote sensing of the Earth from space, Resolution adopted by the General Assembly on 3 December 1986, A/RES/41/65

3 Draft Principles adopted by the Legal Sub-Committee, 13 June 1986, 25 ILM 1334; Lyall and Larson, Space Law (Ashgate, 2009), 411

4 Reflected in Principle 9, 1978 Draft Principles

5 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force Jan. 27, 1967, 610 U.N.T.S. 205 (Outer Space Treaty)

6 ICJ *Corfu Channel* Case

of the UN, and the public: "to the greatest extent feasible and practicable, of the nature conduct, locations and results of such activities." Thus, via this, individuals should be in a position to be informed of when the territory in which they are situated is being sensed.
While the principles from the Outer Space Treaty and 1986 Resolution may be enforced via states, the issue with international law is that it lacks mechanisms for efficient enforceability. Furthermore, by its nature, individuals may not rely on it.

2.2 GDPR

The GDPR enables similar principles, of due regard and the duty to inform, to be enforced via the individual. This is what makes the GDPR important. The core principles of the GDPR are transparency and necessity, which mirror the due regard and the obligation to inform principles well. Transparency means that there must be complete clarity on what personal data is being gathered, on who is processing the personal data and what is being done with the data. Necessity means that only data that is necessary (for a legal purpose) may be collected, processed and retained.
Thus, while international space law may not effectively protect individual's privacy, the GDPR may be used. The GDPR provides rights that the individual may enforce as against any entity that falls within the applicability of the GDPR.[7]

3. The applicability of the GDPR

The GDPR is applicable where (1) personal data is (2) processed (3) within the scope of the GDPR.[8]

3.1 Personal Data

Personal data means "any information relating to an identified or identifiable natural person", called a data subject.[9] The key words are "relating to"; thus, as long as one piece of information is capable of being attributed to an individual, that is personal data. This can include everything from an identification number to location data.[10] It is not limited to obvious personal data, such as names and addresses. For example, if a remote sensing or other satellite is tracking a ship; personal data will be indirectly gathered. This is because, while the purpose of the processing is to track the ship, it will indirectly reveal location information on all employees on that ship. Data is considered personal data even when it is in an indirect manner. As long as it

7 For full details see Keogh, Data Protection Compliance (Clarus Press, 2019)
8 For full details see Keogh, Data Protection Compliance (Clarus Press, 2019)
9 Article 4(1) GDPR
10 Recital 26 GDPR, Recital 30 GDPR and Article 4(1) GDPR

is possible to combine data sets to reveal a piece of information about an identifiable person, it is personal data.

3.2 Processed

The concept of "processing" within the GDPR means "any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means…"[11] This includes even simply the collection of personal data. Thus, once personal data is even collected, processing occurs.

3.3 Scope of GDPR

There are three situations where personal data being processed will fall within the scope of the GDPR:[12]

3.3.1 EU entity

Where the processing of personal data is carried out by an entity within the EU, even if the processing may not actually take place within the EU. For examples, if an Irish company is selling goods or performing a service for the US market, the GDPR must still be complied with as the company is based within the EU.

3.3.2 Non-EU entity

Where personal data of data subject's within the EU is processed by an entity not within the EU, the GDPR is applicable if the processing relates (1) to the offering of goods or services to individuals within the EU or (2) monitoring of the behaviour of people within the EU. Thus, non- EU entities can be caught by the GDPR.

3.3.3 Public international law

Where processing of personal data takes place by an entity in a place where EU law applies by virtue of public international law. For example, while national laws do not apply beyond the delimitation of outer space,[13] a launching state's laws do apply to a nation's space objects.[14] For a State to be a launching State it has to either launch the space object, procure the launch, or be a State from whose territory or facility a space object is launched.[15]

11 Article 4(2) GDPR
12 Article 3 GDPR
13 Article 1-3 Outer Space Treaty
14 Article 8 Outer Space Treaty
15 Article 1(c) Convention on International Liability for Damage Caused by Space Objects, entered into force Oct. 9, 1973, 24 U.S.T. 2389, 961 U.N.T.S. 187 (Liability Convention); Article I Convention on Registration of Objects Launched into Outer Space, entered into force Sept. 15, 1976, 28 U.S.T. 695, 1023 U.N.T.S. 15 (Registration Convention)

Thus, any space object launched by an EU member state must abide by the GDPR in its activities.

3.4 Exceptions

The main exemption is that of annonymisation,[16] meaning that it is no longer possible to link a piece of information with a specific individual. However, if something is only pseudonymised (ie where information is separated from the identifiable piece of information) it still falls within the scope of the GDPR.[17] Thus, if the data is anonymised, statistical information does not fall within the GDPR. However, there is much research into whether any data may be truly annonymised; due to current technological developments and the vast amount of data available, nearly all pieces of information can be linked back to one single individual.[18] Furthermore, processing for statistical purposes or scientific research purposes, among others, is not an exemption to the GDPR; but Member States may provide for certain derogations in which the obligations under the GDPR are reduced.[19]

4. Consequences of GDPR application

Where the GDPR is applicable, this means that companies must ensure they are compliant with the law as fines can reach up to €20 million or 4% of world annual turnover. [20] As stated above, if the GDPR is applicable to a processing operation, the entity must comply with the obligations and principles within the GDPR.[21] Transparency and necessity were already mentioned as two such obligations, which resonate will with the 1986 Resolution. Another major obligation is that of security i.e. there must be appropriate security at all stages of the processing operation. Very specific obligations are contained within the GDPR that lie beyond the scope of this paper. In particular there are obligations for entities that need to transfer data to other entities or outside of the EU; there must be a data processing agreement with every entity to whom personal data is transferred; and where any personal data is transferred outside of the EU - the requisite legal formalities must be in place.

16 Sentence 5, Recital 26 GDPR
17 Article 4(5) GDPR
18 For example see Yves-Alexandre de Montjoye, Unique in the shopping mall: On the reidentifiability of credit card metadata (30 Jan 2015, Science, Vol. 347, Issue 6221, pp. 536-539)
19 Recital 159, 161 GDPR (scientific); Recital 162, 163 GDPR (statistical); Article 89 GDPR
20 Article 83 GDPR
21 For full details see Keogh, Data Protection Compliance (Clarus Press, 2019)

4.1 Potential relevance for space entities

Integrated GPS applications can collect personal data if it is capable of being linked to an individual. As referred to above, even systems that track trucks or ships may indirectly collect personal data as it would be possible to link that location data with employees on those vessels. The current challenge that may be equally applicable to the space sector is how to implement the GDPR for the exchange of data within the internet of things sphere, i.e. exchange of data between "things", without the intervention of a network operator,[22] i.e. between automated cars.

Furthermore, personal data is capable of being caught by all types of remote sensing, including imagery, with better resolution being sold each year. DigitalGlobe asserts that it can capture licence plates. Satellite imagery is viewed as a legitimate competitor to aerial imagery. Personal data can simply be the fact that a data subject visibly has certain machinery on their land, etc.

The GDPR is also a consideration if storage centres are to be in space, or if data is to be transferred in space. For example via plans of companies such as Space Belt whose intention is to have a secure transfer of data within space, what they call a "separate secure internet". There are plans for space assets to facilitate a 5G network arising from international entities, such as the ESA's "Satellite for 5G" initiative. Vodafone has committed to building a 4G network on the moon. Many of these innovations that space offer shall require the consideration of the GDPR and the related obligations that it brings. Consideration is required for how space entities may fulfil such obligations.

5. Conclusions

It is the hope of the author that the reader acknowledges from this paper a very simple notion: even space entities may gather personal data. It is simple but one that practitioners must bear in mind; the future of space will increasingly rely on data and the transfer of data as a source for research and also for revenue. Thus, such entities must be aware of whether the GDPR becomes applicable in order to avoid fines and related liabilities. There must be consideration on how such entities may fulfil any arising GDPR obligations.

22 See interesting discussion of this issue within Article 29 Working Party Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)