PERSONAL DATA PROTECTION, FREQUENCY REGULATION AND COMPETITION LAW IN THE CONTEXT OF SMART CITY INFRASTRUCTURE

*Anette Alén-Savikko, Shakila Bu-Pasha, Heidi Himmanen, Päivi Korpisaari, Sara Lehtilä & Juha Vesala**

Introduction

This article considers the legal aspects to be taken into consideration when creating a smart city ecosystem.[1] The focus of this paper is on current legal regulation and interpretation of personal data protection, regulation of frequencies, together with competition and procurement law in a smart city context. The current legal situation will be analyzed by benchmarking the smart city data platform regulatory environment and identifying the regulatory bottlenecks when creating data based services for people in a smart city. This article relates to a larger project, *Neutral Host Pilot,* which consists of twenty-six stakeholders (mostly business companies) and funded by Business Finland. The aim of the project is to develop technical solutions for a smart pole-based

* Anette Alén-Savikko LL. D. is the main author of the network and spectrum regulation part, Shakila Bu-Pasha LL. D. is the main author of the personal data protection and privacy part, and Juha Vesala LL. D. is the main author of the competition law and public procurement part. In addition, Heidi Himmanen, D.Sc. (Tech), Professor Päivi Korpisaari and Sara Lehtilä LL.M. contributed to the article. The authors express their warm thanks to research assistant, law student Oona Ojajärvi and Päivi Karkkola, Annina Lehtonen and Henriikka Rosti, who are officials of Finnish Transport and Communications Agency (Traficom), for their help when writing the state-of-the-art report.

[1] This article is a modified version of a state-of-the-art report written for the Neutral Host Pilot project, which is funded by Business Finland. More information on this project is available here: https://www.luxturrim5g.com/new-blog/2019/11/4/nokia-driven-luxturrim5g-smart-city-ecosystem-extending (accessed 27 March 2020).

5G infrastructure, and to create business and service innovations and an open access ecosystem for digital services. Those services may relate, for example, to navigation, information sharing, advertizing, security, weather monitoring and smart lighting. (LuxTurrim5G, 2017.)

There is no legal definition of the concept of 'smart city'. However, in practical terms a smart city is built on smart uses of information technology – for example, software systems, server infrastructure, network infrastructure, and client devices. A city that monitors and integrates the conditions of all of its critical infrastructures can help city residents and the city administration. Connected components might, for example, involve the city administration, education, healthcare, public safety, real estate, transportation, and utilities. (Washburn et al, 2010.) A smart city can better optimize its resources, plan preventive maintenance, and monitor security aspects. It can also provide citizens with better services. (Hall, 2000.)

The starting point in our project is that, in order to improve the quality of living this way, smart cities need a digital service infrastructure based on small cell 5G radio frequency technology and higher frequencies. This is because the capacity of mobile networks will be far too insufficient due to the increased number of users and new digital services. (LuxTurrim5G, 2017.) As part of this project we also aim to create a platform that uses high-speed city networks, where a wide variety of data can be used in a reliable and secure way for development of digital services. This data platform is here termed Neutral Host. (LuxTurrim5G, 2019.)

As using the Internet of Things (IoT) and 5G technology will be inseparable in a digital smart city ecosystem, it is apprehended that privacy and the protection of personal data will be at risk in 5G network-based platforms because of interconnected smart sensors and devices. Enhanced 5G services support network-based positioning capabilities in a more accurate way than before. Such a high resolution in locating the user and their personal data can trigger enormous benefits for network operators and their end users, but at the same time creating important privacy concerns from users' point of view. There is also a risk of hacker attacks against databases and malicious or erroneous data inputs. (Lohan et al, 2018, pp. 281–320.) This explains why research is needed concerning threats to personal privacy and personal data protection in the context of the smart city.

In addition, network and radio spectrum regulation is explored because it is important to establish possible ways to use frequencies in the context of the smart city and Neutral Host platform. Attention has also been paid to competition law, because data sharing and platforms need to be designed in a way that does not include agreements restricting competition or, if Neutral Host were to become dominant in some markets (for example, as data supplier in an area), does not lead to foreclosure of competitors or impose unjustified restraints on customers or suppliers. Moreover, certain aspects of procurement law are discussed here.

In this article we will focus on the following aspects that are relevant in the context of the digital smart city:

1. Personal data protection and privacy
2. Network and spectrum regulation
3. Competition law
4. Public procurement legislation.

1 Personal data protection and privacy

1.1 General remarks

Personal data protection and privacy are major concerns when planning and implementing smart city services. Personal privacy of individuals may be threatened and at risk in a variety of ways in a digital smart city platform. However, following legal mandates and properly fulfilling legal requirements can mitigate these concerns.

At present, the most important and comprehensive data protection law in the EU addressing protection of personal data is the General Data Protection Regulation (GDPR)[2] which deals with personal data protection concerns exposed via modern technological developments.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, OJ L 119, 4 May 2016, pp. 1–88.

The scope of material[3] and territorial[4] application is wide, as is also the concept of personal data.

To start with, it is important to discuss some terminology and provisions under the GDPR in the smart city context. For example, Article 4(1) of the GDPR defines the concept of personal data:

> "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Recital 26 mentions that

> "[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (...). To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

The CJEU has interpreted the concept of personal data widely. For example, in *Breyer*, the Court stated that a dynamic IP address

---

[3] As a main rule, GDPR "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"; see more closely GRPR Art. 2.

[4] See GDPR Art. 3:

"1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

can constitute personal data if the service provider has the legal means enabling it to identify the data subject with additional data which the internet service provider has about that person. (*Patrick Breyer v. Bundesrepublik Deutschland*, 2016.) In *Breyer* the CJEU applied the Data Protection Directive (DPD),[5] but the line of interpretation regarding the concept of personal data is still valid. So, too, is the Court's practice relating to the concept of controller.

Article 9 (1) of the GDPR states,

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

Processing of such data requires special protection under the GDPR.

According to Article 4 (7),

> "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

The CJEU has also interpreted the concept of controller widely. For example in *Jehovan todistajat* the Court concluded that a religious community, such as the Jehovah's Witnesses, was a controller, jointly with its members who were engaged in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching (*Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta*, 2018.) In *Wirtschaftsakademie* the Court stated that the administrator of a fan page on Facebook was a joint controller jointly responsible with Facebook for processing the data of visitors to the page, when Facebook was – by means of cookies – collecting and

[5] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, pp. 31–50.

then processing the personal data of visitors. (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, 2018.) As a result, processing of personal data carried out in the context of such activity had to respect the rules of EU law on protection of personal data.

Article 4 (8) in turn defines that the concept of 'processor' "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

EU Member States are under obligation to enact national data protection laws fulfilling the requirements of the GDPR in order to secure the rights of data subjects. Both the GDPR and national laws bind different entities which can collect and process individuals' personal data. To illustrate, technology companies or different digital service providers as data controllers have to comply with privacy laws at certain levels by ensuring certain proper features. They have to follow legal requirements in drafting their terms and conditions, privacy policies, and end-user license agreements in order to protect the data privacy of smart device users.

Legal issues that have to be resolved when developing the digital smart city include, for example, general principles of data processing, lawful grounds for processing, rights of data subjects, and obligations of data controllers and processors. Those who use smart city services enjoy some control over their personal data. For example, when processing is based on consent, service providers should avoid drafting long, one-sided policy statements and default settings in order to meet the requirements of EU data protection law as well as to establish a fair, transparent and accountable data protection and data processing system. At the same time, companies and organizations can process personal data when operating a smart city platform if there is a legal basis for processing and if the requirements of the GDPR are fulfilled.

Articles 16–22 of the GDPR describe different rights of data subjects which need to be fulfilled. These rights include, for example, "the right to be forgotten" under Article 17 of the GDPR, which in the EU implies that a data subject has the right to require the controller to remove their personal data when such data "are no longer necessary in relation to the purposes for which they were collected or otherwise processed".

The integrity and confidentiality of personal data is mentioned in Article 5 (f) of the GDPR as one of the basic principles for processing

personal data. Article 32 requires data controllers and processors to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". In the context of the smart city it is also important to explore the existence of such "high risk" to personal data that – according to Article 35 – requires a Data Protection Impact Assessment (DPIA), which can be called "a process for building and demonstrating compliance". (Article 29 Working Party, 2017.) This is a new requirement that reflects the principle of privacy by design. Article 35 requires data controllers to carry out a DPIA if new technologies and data processing operations are "likely to result in a high risk to the rights and freedoms of natural persons". According to WP29, such a high risk is involved, for example, with "a systematic monitoring of a publicly accessible area on a large scale". (Article 29 Working Party, 2017, p. 8.) Non-compliance with the GDPR can lead to fines imposed by the competent supervisory authority.

1.2 Identifiable information, anonymization and pseudonymization

Anonymization and pseudonymization can be applied to protect privacy and personal data. These two methods, though interconnected, are different and require different techniques in relation to protection of personal data. The relevance of identifiable information is evident in the definition of personal data in Article 4(1) of the GDPR as already mentioned.

The name, address, phone number, personal picture, account information, social security number are amongst others considered as direct identifiers; on the other hand, information which can lead to reaching direct identifiers, for example, job designation, work location and salary, information on particular health syndromes and so on are indirect identifiers. According to the US National Institute of Standards and Technology, "De-identification is a tool that organizations can use to remove personal information from data that they collect, use, archive, and share with other organizations." (Garfinkel, 2015.)

The main purpose of anonymization is to prevent irreversible identification. True and effective anonymization should ensure two criteria: it has to be irreversible and, after applying anonymization, it is not possible to identify an individual. In short, in anonymized data

identifiable elements no longer exist and re-identification is not possible. After ensuring effective anonymization, data ceases to be personal data. (Bu-Pasha, 2018.)

The GDPR does not define anonymization, although Recital 26 provides a conceptual definition:

> "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

Effective anonymization not only mitigates risks to personal data but also promotes opportunities to benefit from an open data platform. However, ensuring true anonymization is very difficult.

In pseudonymization, identifiable elements are replaced by pseudonyms or values in pseudonymized data with which data subjects cannot be directly identified, but identifiable data are reversible. The GDPR introduces "pseudonymisation" with a legal basis, as Article 4 (5) states that

> "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

This means that, with the use of additional information, re-identification is possible in pseudonymized data. Article 25 (1) of the GDPR describes pseudonymization as an "appropriate technical and organisational measure" for implementing data protection principles.

According to Recital 26, pseudonymized personal data are considered identifiable information if they could be attributed to a specific natural person in association with some additional information. The controller should single out all the means which could reasonably be used to directly or indirectly identify a natural person. Objective factors – for example the required time and costs of identification, and the current available technology and technological developments – should

be taken into account to determine the identifying means. Because the concept of personal data in the GDPR refers to an identified or identifiable person, pseudonymized data is personal data.

1.3 Consent and other legal grounds for processing

If processing of data is based on consent, the GDPR requires data controllers to obtain the data subject's explicit and freely given consent when processing their personal data. According to Article 6(1)(a) of the GDPR, processing of personal data is lawful when "the data subject has given consent to the processing of his or her personal data for one or more specific purposes". Article 7 sets some conditions for consent: indeed, an important task for smart city initiators is to take those conditions into account when processing users' personal data.

When data processing is based on the data subject's consent, the controller has to be able to demonstrate consent [Article 7(1)]. According to Article 7(2), if consent relates to a written declaration, "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".

The data subject should be able to express their genuine or voluntary choice for freely consenting to processing of personal data (Recital 42). The text of Recital 32 can be a good guideline for obtaining data subjects' consent:

> "[c]onsent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent…"

In a smart city context, consent can be a basis for processing – for example, when a data subject downloads an app, which collects and uses their personal data in order to provide smart city services. But it

may not always be an appropriate basis when data are collected from bus terminals, streets, and other public places.

Other legal grounds for processing personal data include performance of a contract, compliance with legal obligations by the controller, protecting the data subject's or some other natural person's vital interests, for the purposes of the public interest or a controller's or a third party's legitimate interest.

In a smart city context, a legal obligation or public interest are common grounds for processing personal data by the city. Legitimate interest, in turn, is a common ground for processing for private purposes.

According to Article 6 (1)(e) of the GDPR, processing is lawful if it "is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". Both public and private sectors can be entitled to rely on this ground in appropriate situations or in exercising public authority. The basis for processing must be laid down by European Union law or Member State law to which the controller is subject. The reason for regulation can relate for example to national security, crime prevention, safeguarding public health, social security, maintaining safety and quality of services and devices and so on.

According to Section 4 of the Finnish Personal Data Act (1050/2018, Tietosuojalaki) personal data may be processed in accordance with Article 6 (1)(e) if:

> "1) the data describe the position of a person, their duties or performance of those duties in a public sector entity, business and industry, activities of civil society organizations, or other corresponding activities, in so far as the objective of processing is of public interest and processing is proportionate to the legitimate aim pursued;
> 2) processing is proportionate and necessary for performance of a task carried out in the public interest by an authority;
> 3) processing is necessary for scientific or historical research or statistical purposes and is proportionate to the aim of public interest pursued; or
> 4) processing research material and cultural heritage material containing personal data and processing personal data included in their metadata for archiving purposes is necessary and proportionate to the aim of public interest pursued and to the rights of the data subject."[6]

[6] Unofficial translation by the Ministry of Justice.

The controller's or a third party's legitimate interest is another lawful ground for processing personal data unless overridden by other interests and the fundamental rights of data subjects [Article 6 (1)(f), Recital 47]. Many business entities being data controllers like to adopt the legitimate interest ground as a comparatively convenient option. According to Article 6 (1) subparagraph 2 it will not apply to processing carried out by public authorities in the performance of their tasks.

Recital 47 of the GDPR expresses direct marketing as a possible legitimate interest: "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". Debate surrounds the scope of several interpretations in defining legitimate interest. (Kamara and de Hert, 2018.) It is also important to bear in mind the accountability principle in Articles 5 (2) and 24 (1) of the GDPR. According to this principle, the controller is responsible for demonstrating that processing is lawful – and must be able to do so.

1.4 Extra-territorial aspects

Worldwide, many companies, organizations and research institutions are experimenting on the smart city concept. In maintaining coordination with other smart cities as well as in running and spreading business platforms, data may be transferred from one region to another.

Moreover, we need to consider the possibility of processing data outside the EU. Article 3 (2) of the GDPR states:

> "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

This provision ensures protection of personal data with extra-territorial effect. On the other hand, business activities among different regions of the world can benefit from such simplified legal provision.

As for personal data transfers outside the EU, if the European Commission decides that, for example, a third country or an international organization, offers an adequate level of data protection, transfer

of personal data can take place without the need to obtain specific authorization [Article 45 (1)(3), Recital 103 GDPR].

1.5 Principles relating to processing of personal data

Article 5 describes principles relating to processing of personal data which data controllers need to consider in implementing a smart city. These principles include lawfulness, fairness, and transparency in processing personal data [Article 5 (1)(a)]. According to the 'purpose limitation' principle, personal data can be "collected for specified, explicit and legitimate purposes": this prohibits further processing in a manner incompatible with the original purpose [Article 5 (1)(b)].

According to Article 6 (4), if processing is not based on consent or law,

> "the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
> (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
> (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
> (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
> (d) the possible consequences of the intended further processing for data subjects;
> (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

The 'data minimization' principle requires that collected data shall be "adequate, relevant and limited" and necessary to achieve the original purpose [Article 5 (1)(c)]. Such data must no longer be stored after fulfilling the purpose [the 'storage limitation' principle, Article 5 (1)(e)].

In addition, the collected data must be accurate [the 'accuracy' principle, Article 5 (1)(d)], and the controller must maintain security and protection of personal data under the 'integrity and confidentiality' principle.

The 'accountability' principle requires that the controller be responsible for demonstrating compliance with the above principles.

1.6 The rights of data subjects under the GDPR

The GDPR promotes data subjects' control over their personal data and thereby confirms certain rights for them. In implementing a smart city ecosystem, companies and organizations as data controllers must consider those rights while processing personal data.

The European Data Strategy ensures individuals' right to their own data. This reflects the recent MyData concept by "giving users rights, tools and skills to stay in full control of their data". (European Commission, 2020.) In the long run, this aspect is likely to be relevant in the smart city context as well. Accordingly, MyData models should be considered when thinking about the Neutral Host Pilot data platform as one possible business model. In short, the MyData model improves the right to self-determination by empowering individuals in terms of exercising control over their personal data.

According to the GDPR, data subjects have the right under Article 21 to object to the processing of their personal data in relation to their particular situations even if processing is conducted on the grounds of public interest [under Article 6 (1)(e)] or legitimate interest [under Article 6 (1)(f)]. They also have the right to object to processing carried out for direct marketing purposes. They can object to processing of personal data for scientific, historical research or statistical purposes if that is not justified on the ground of public interest.

As per Article 15 of the GDPR and Article 8 (2) of the EU Charter of Fundamental Rights, a data subject has the right to access personal data on him or her in order to ascertain relevant information regarding the processing of their personal data. The GDPR confers on data subjects the right to immediate rectification of inaccurate and incomplete personal information (Article 16), prompt erasure of unnecessary information (Article 17) and restriction of invalid processing (Article 18). Even after giving consent, a data subject can withdraw it in a simple way at any time under Article 7 (3).

Controllers are required to inform data subjects about their identity and contact information, the purpose(s) of processing, how long

the personal data would be stored, and other related information as per Articles 13 and 14. Informing data subjects about the location of data collection and the reason for it is important for maintaining transparency. In a smart city context, fulfilling these obligations is highly important in order to maintain citizens' trust in the system. Transparency must be assigned special importance when processing of personal data is not based on consent and the data subject may not even be able to prevent processing of their personal data. This is why special attention has to be paid to how and when citizens are informed of the processing of their data.

1.7 Controller, joint controller and processor

As mentioned in Article 4 (7) of the GDPR, controllers can process data alone or jointly. In relation to smart city platforms, controllers will jointly conduct data processing operations. Article 26 (1) states: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation."

As per the requirement of Article 35 (1) of the GDPR, smart city implementing authorities as data controllers have to carry out a data protection impact assessment if data processing operations – especially using new technologies – have a likelihood of resulting in high risk to the rights and freedoms of data subjects. It would be useful if the responsibilities of joint controllers were described in the DPIA. Controllers also need to implement proper technical and organizational measures for ensuring security of processing as prescribed in Article 32 (1).

In addition, there might be app developers and other entities that will process personal data on behalf of the data controller and act as data processors. Their duties should also be defined in running a smart city.

Without endangering personal data or by adopting adequate measures to protect personal data, the ecosystem can explore the opportunity to promote open data platforms by balancing with personal data protection and privacy. In doing so, data controllers need to be very careful and take into account the lawfulness of processing under Article 6 of the GDPR.

1.8 Summary

The use of modern technologies in developing smart city ecosystems involves issues related to privacy and personal data protection. In order to mitigate the risk to protection of personal and location data in a smart city platform, data controllers and processors need to follow the provisions of the GDPR. By following lawful procedures, maintaining principles of processing personal data and safeguarding data subjects' rights under the GDPR, organizations can conduct processing operations fairly in a smart city ecosystem. At the same time, data controllers must take into account the necessity of ensuring proper anonymization and pseudonymization of personal data in an efficient way.

2 Network and spectrum regulation

Exploring network and radio spectrum regulation in relation to running networks in a smart city ecosystem and recognizing the possible ways to use frequencies is important for the Neutral Host. The spectrum for electronic communication services is harmonized at a European level to enable common markets and use of the same user equipment within the EU. Indeed, global harmonization has been possible in some bands. The frequency bands identified for 5G in Europe are 700 MHz, 3,5 GHz and 26 GHz. The World Radio Conference in November 2019 further identified other high bands to be investigated for 5G in the future.

Finland has allocated more spectrum – relative to the population – to public mobile telecommunications networks than other European countries, in total about 1200 MHz. The following spectrum bands have been awarded to mobile operators in Finland: 450 MHz, 700 MHz, 800 MHz, 900 MHz, 1.8 GHz, 2.1 GHz, 2.6 GHz and 3.5 GHz. Three telecom operators have nationwide coverage. The bold spectrum policy together with functioning competition between operators is seen as one of the success factors for Finland, which is a top country in mobile broadband worldwide.

Applicable laws regarding the network and spectrum regulation are the national Act on Electronic Communication Services[7] (ECSA)

[7] Act on Electronic Communication Services (917/2014).

and provisions of the European Electronic Communications Code.[8] The Decree of the Council of State on the use of radio frequencies and frequency plan[9] is also relevant in defining and deciding the factors relating to radio and public mobile (GSM, 5G etc.) network frequencies, spectrum band, licensing, and the like. It is still important to notice the ongoing reform of ECSA and the allocation of a new frequency band – 26 GHz – the impact of which on the Neutral Host will be crucial. The final implications of these amendments can only be seen later in 2020.

2.1 National network and radio spectrum regulation: Act on Electronic Communications Services

2.1.1 Application

The ECSA applies to many activities in the field of electronic communications. For their part, teleoperators (section 3, paragraph 27) are those engaged in *public telecommunications services*, in other words, companies that provide network or communication services to an unrestricted circle of users: "telecommunications operator means a network operator or a communications service operator offering services to a set of users that is not subject to any prior restriction, i.e. provides public telecommunications services".[10] If and when Neutral Host aims to operate locally, catering for an unlimited amount of people, it will be regarded as a teleoperator under the ECSA. Moreover, there are other relevant definitions in ECSA: "network service means a service which telecommunications operator (network operator) provides comprising a communications network in its ownership or for other reasons in its possession for the purposes of transmitting or distributing messages" (section 3, paragraph 34), while "communications service means a ser-

[8] Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), OJ L 321, 17 December 2018, pp. 36–214.

[9] Decree of the Council of State on the use of radio frequencies and frequency plan (1246/2014).

[10] Unofficial translation of the Information Society Code (917/2014) translated by the Ministry of Transport and Communications. Available at: https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf (accessed 10 April 2020).

vice consisting either completely or primarily of transmitting messages in a communications network, and of transfer and transmission service in a mass communications network" (section 3, paragraph 37).[11]

The relevant factors are thus whether the circle of users is unrestricted and in which phase(s) the service provider is involved in transmitting messages. (See also Traficom, 2019.)

2.1.2 Spectrum for mobile telecommunications and licensing procedure

Prior to operating in the field of telecommunications, the teleoperator is required to follow a specific procedure defined in the Act. The teleoperator must notify the Finnish Transport and Communications Agency (Traficom) (section 4). To operate in the public network, a license is needed "to provide a network service that uses radio frequencies in a digital terrestrial mass communications network or in a mobile network practising public telecommunications" (network license; section 6)[12].

The Government grants network licenses (section 8). At the national level, network licenses are granted either via a comparative procedure – the so-called 'beauty competition' (section 10) – or by auction (section 11). Since 2009, the auction process has been the main procedure in use for new mobile frequencies. Licenses are granted for a fixed term, with a possible covenant which includes, for example, the geographic area of function and an obligation to prevent interference on the frequency band (section 16). The given range for teleoperators on the market is normally nationwide. An operator which has been granted a network license at auction can lease the right to use its frequencies (section 20). Leasing out the right to use frequencies requires governmental approval.

Besides public networks, the Act also regulates private radio networks. Private networks are used in business and professional communications, for example, in industry, public utilities (energy and water supply), transport and traffic control, and by the authorities. A radio license "is required for the possession and use of radio transmitters" (section 39), and the licensing authority is Traficom (section 40). Radio

[11] Id.

[12] Id.

licenses are granted to private radio networks on the basis of case-by-case frequency planning. The license and frequencies are granted for a specific geographical area, such as a harbor or factory, based on the customer`s needs. On the other hand, private 4G networks have been built by telecom operators in ports and similar environments using the spectrum of commercial operators. The first dedicated 4G/5G spectrum in Finland will be 2300–2320 MHz. The first radio licenses in this band are planned to be granted after summer 2020.

A need to lighten the licensing process has been identified in Finland so as to enable 5G development and to promote possible demand for new types of operator models. (Finnish Communications Regulatory Authority, 2016.) There is a draft government proposal concerning overall ECSA reform, which should enter into force during the autumn of 2020, including provisions about license requirements. The reform is based mainly on the European Communications Code but also includes national proposals for amendments to the licensing process.[13]

As for frequency bands already allocated for public mobile communication services[14] in Finland, these are shared among the major operators on the market, namely DNA, Elisa and Telia. (Ministry of Transport and Communications, 2018.) It should be noted that the frequencies allocated already enable many of the activities pursued within the Neutral Host concept. The new frequency band, 26 GHz, one of three bands identified for 5G at EU level, covers 24.25–27.5 GHz. It will be allocated during 2020. Band 25.1–27.5 GHz will be auctioned for national use as three 800 MHz frequency blocks. The proposed starting price at auction would be EUR 7 million for each 800 MHz frequency blocks.

The lower part of the frequency spectrum, 24.25–25.1 GHz, i.e. 850 MHz, would be excluded from the auction. This spectrum would be reserved for local networks. In the future, local networks could be constructed in ports/harbors and industrial facilities, for example, and companies could use them for remote control, robotization and sensor data collection among other things. The way in which this frequency

[13] See the draft Government proposal, available at: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=36773abd-fb0b-4593-a36a-0d843e1af094&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744 (accessed 25 February 2020).

[14] The official term for public mobile communication services is “Terrestrial systems capable of providing electronic communications services”.

band will be allocated has not yet been decided at the government level so regulatory amendments are still open with the new frequency band.[15]

However, taking into account 5G networks multiple use-cases, the 26 GHz frequency band is not the only way for Neutral Host to operate while lower frequencies are also applicable to smart city needs. Based on the current legal framework and with these frequencies, Neutral Host could already operate in co-operation with frequency holders (for example, by contracting on access and to the extent this is successful). Within the current regulatory framework, the only long-term solutions are either to have an own network license (if possible for new non-allocated frequencies) or to gain a right of access from current license holders (for allocated frequencies). Ways to cooperate are many in terms of benefits for both parties. (Ahokangas et al, 2018.)

2.1.3 Obligations and rights of the teleoperator

Regardless of whether the operator works in cooperation or alone, the law imposes some obligations for telecompanies engaged in public telecommunications activities. These obligations need to be taken into account when constructing the Neutral Host. In general, an activity might be free of charge or commercial by nature. Thus, a non-profit entity, such as a city, might also fall under the scope of provisions addressing a telecompany. (See also Traficom, 2019.) Obligations are many (chapters 7–10 and 34) and they might target an activity as a whole or parts of it. The main obligations, alongside notification and licensing, are the following:

- paying a fee
- ensuring technical functionality and data security
- providing assistance for authorities in emergency situations[16]
- ensuring consumer protection and other end user rights and catering for basic services
- safeguarding confidentiality of communications

[15] See the Government Project (LVM045:00/2019), available at: https://valtioneuvosto.fi/hanke?tunnus=LVM045:00/2019 (accessed 25 February 2020).

[16] See e.g. section 280 ECSA on the obligation of a telecommunications operator to transmit a targeted message from the authorities.

– promoting competition
– complying with regulation of the use of radio frequencies. (See also Traficom, 2019.)

The teleoperator will be monitored by Traficom (sections 302–304). An annual information society fee must be paid to Traficom (section 289). Moreover, Traficom conducts market analyses and renders decisions on significant market power. Thereby obligations are imposed to secure competition in the market. These can include, for example, an obligation to grant rights of access, interconnection obligations, or non-discrimination obligations (sections 52–54, 56–57, 60–64, and 68). According to section 55 ECSA, Traficom may impose obligations to relinquish access rights (section 57) or an interconnection obligation (section 62) as well as other obligations related thereto (sections 67−69, 72, and 74) also based on reasons other than significant market power.

When contracting with consumers, chapter 15 ECSA applies. The law also imposes obligations to the teleoperator regarding data security and confidentiality (chapters 17–19, section 197 and chapters 32, 33 and 40). In addition, chapters 24 and 26 include regulation on marketing. Chapters 29 and 30 ECSA also impose some general quality requirements, for instance, regarding the network and transmitters (e.g. avoiding interference with others or society in general).

For its part, net neutrality (section 110) also comes into question when tele companies are operating in a 5G network. This means that teleoperators have to treat all internet traffic equally and enable users' right to an open internet. Net neutrality is ensured by Regulation (EU) 2015/2120.[17] Traficom may provide further regulation (section 110), while it is also obligated to cooperate with EU authorities in other telecommunications issues (section 308).

Besides obligations, teleoperators also have some rights concerning the construction of infrastructure for their network. In specific cir-

[17] Regulation (EU) 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26 November 2015, pp. 1–18.

cumstances, a teleoperator is allowed to place equipment, including a telecoms cable, a base station or a radio mast, on third party land or building on certain conditions (section 229). If placement is not agreed with the owner, the municipal supervisory authority decides on the matter [section 229 (3), section 233]. Contracts regarding such equipment are also binding in relation to any new owner or holder of a building or property [section 229 (4)]. If no agreement is reached with the owner, the teleoperator must draft a plan and inform all stakeholders, while the municipal authority may base its decision on this plan (sections 230–233). Teleoperators may also take other measures on third party land or building related to the construction plan (for example, remove vegetation, maintenance) if they are necessary for the placement of equipment (section 236). Resulting from the overall reform of the ECSA, some rights regarding construction of infrastructure may become wider, especially concerning the right to place small-area wireless 5G access points.

2.1.4 Ongoing legislative reform

In the context of implementing the new EU provisions (European Electronic Communications Code) amendments have been proposed to the ECSA and related acts in Finland. To begin with, the reform responds to the need to lighten the licensing process. It is proposed that the government-granted network license would not be needed in small-scale public telecommunications services in the case of local activities in a geographically restricted area which is indicated for such use by government decree.[18] Operating in this area would be covered by a radio license. Besides, amendments are also directed to the terms and use of a network license, aiming inter alia to support the common and efficient use of frequencies and investments in the network infrastructure. Proposals concern for example the duration of license, transfer of license and leasing the right to use a license.[19]

Amendments have also been proposed regarding provisions on access and interconnection (see Chapter II European Electronic Communications Code). Amendments include some new obligations to inter-

[18] See section 6 ECSA in the draft Government proposal.

[19] See sections 16, 17 a–b, 18 and 20 ECSA in the draft Government proposal.

connect and to relinquish the right to access concerning both companies with significant market power and based on other grounds.[20] Moreover, the European Electronic Communications Code includes new provisions for companies with significant market power (Chapters III–IV) in areas such as migration from so-called legacy infrastructure[21] as well as co-investments[22] which are being implemented. The draft Government proposal also includes amendments to chapter 28 of the ECSA regarding placement of equipment by telecom operators. Moreover, alongside amendments to the ECSA, amendments to the Land Use and Building Act[23] (LUBA) have been proposed in order to facilitate the construction of a 5G network.[24] Article 57 of the European Electronic Communications Code includes provisions on the deployment and operation of small-area wireless access points as follows:

> "1. Competent authorities shall not unduly restrict the deployment of small-area wireless access points. Member States shall seek to ensure that any rules governing the deployment of small-area wireless access points are nationally consistent. Such rules shall be published in advance of their application.

---

[20] See sections 55 a–e and 56 ECSA in the draft Government proposal.

[21] See section 81 c ECSA in the draft Government proposal; Art. 81 (1) of the European Electronic Communications Code: "Undertakings which have been designated as having significant market power in one or several relevant markets in accordance with Article 67 shall notify the national regulatory authority in advance and in a timely manner when they plan to decommission or replace with a new infrastructure parts of the network, including legacy infrastructure necessary to operate a copper network, which are subject to obligations pursuant to Articles 68 to 80."

[22] See sections 81 a–b ECSA in the draft Government proposal; Art. 76 (1) of the European Electronic Communications Code: "Undertakings which have been designated as having significant market power in one or several relevant markets in accordance with Article 67 may offer commitments, in accordance with the procedure set out in Article 79 and subject to the second subparagraph of this paragraph, to open the deployment of a new very high capacity network that consists of optical fiber elements up to the end-user premises or base station to co-investment, for example by offering co-ownership or long-term risk sharing through co-financing or through purchase agreements giving rise to specific rights of a structural character by other providers of electronic communications networks or services." See also Recitals 198–201.

[23] Land Use and Building Act (132/1999).

[24] See the draft Government proposal.

In particular, competent authorities shall not subject the deployment of small-area wireless access points complying with the characteristics laid down pursuant to paragraph 2 to any individual town planning permit or other individual prior permits.

By way of derogation from the second subparagraph of this paragraph, competent authorities may require permits for the deployment of small-area wireless access points on buildings or sites of architectural, historical or natural value protected in accordance with national law or where necessary for public safety reasons. Article 7 of Directive 2014/61/EU shall apply to the granting of those permits.

(…)

5. Without prejudice to any commercial agreements, the deployment of small-area wireless access points shall not be subject to any fees or charges going beyond the administrative charges in accordance with Article 16."

Related amendments proposed in Finland concern chapter 28 ECSA and section 161 LUBA. If the provisions enter into force, communal authorities would not be allowed to restrict – nor could they require a prior permit for deployment of – small-area wireless access points. Moreover, access to the physical infrastructure (for example, light poles, traffic lights) controlled by public authorities should be allowed for operators to arrange placement of such access points.[25]

The proposed section 55 c ECSA would allow Traficom to impose obligations (based on other grounds than significant market power) regarding the sharing of (passive) infrastructure which is used for provision of wireless electronic communications services or contracting on localized roaming. Obligations may be imposed if they are directly necessary for local (radio frequency-based) service provision and if other companies cannot gain access to comparable infrastructure on fair and reasonable terms. Imposing such obligations would be restricted to situations where there are insurmountable hindrances to market-based deployment resulting in end-users having limited opportunities to access the network or use services.[26]

However, this legislative reform is still ongoing and final amendments are expected to enter into force later in 2020. Therefore, the effect of the proposal on Neutral Host can only be estimated. Despite any direct effect, there is a move towards principles such as non-dis-

[25] Id.

[26] Id.

crimination and co-operation among telecompanies, which might affect Neutral Host more indirectly.

2.1.5 Summary

In general, it is already possible to execute Neutral Host as a concept, that is, even with current (already allocated) frequencies and operators as well as in the current regulatory framework. This would mean a need to cooperate with existing teleoperators (who hold relevant frequencies) and obtain a contract covering the relevant frequencies. Even then, Neutral Host could fall under the scope of legal obligations when regarded as a telecompany providing public telecommunications services.

With regard to relevant frequencies that remain unallocated (26 GHz), the means of allocating them will be crucial. It remains to be seen how they are allocated. Additionally, the influence of overall ECSA reform – for example, on the licensing process – remains to be seen. Many open questions remain: whether there is a chance to participate in an auction of new nation-wide frequencies (and a government-granted network license would be needed for operation), and whether in the future a radio license would cover local activities in the case of geographically restricted and small-scale public telecommunication services. The procedure might become lighter in the future, but on the other hand the applicability of the obligations of a telecompany remains to be seen.

3 Competition law

The national Finnish Competition Act[27] (FCA) and EU competition law apply to Neutral Host and organizations participating in its activities. Competition (antitrust) law prohibits 1) agreements and other forms of cooperation that restrict competition and 2) abuse of a dominant position. Breaches of these rules may result in administrative remedies (e.g. fines and orders) resulting from investigations by competition authorities (the European Commission or national competition authorities). Courts and arbitrators can also apply competition law

[27] Competition Act (948/2011).

and impose remedies for competition law infringements (for example, compensation by way of damages, invalidation of agreements). There can also be other legal consequences (including criminal liability in some countries) and non-legal consequences (such as costs, publicity) for competition law infringements.

Additionally, Finnish and EU competition law requires that 3) certain transactions, including permanent joint ventures be notified in advance to competition authorities (the European Commission or national authorities) and may not be implemented unless the authorities clear the transaction. Below the key rules are outlined and their applicability to Neutral Host discussed.

3.1 Finnish and EU competition law

3.1.1 Antitrust prohibitions

Section 5 FCA and Article 101(1) of the Treaty on the Functioning of the European Union (TFEU)[28] prohibit agreements and other forms of cooperation between undertakings that restrict competition in a market.[29] Prohibited practices cover contracts, concerted practices and decisions by associations of undertakings which appreciably prevent, restrict or distort competition. Parties to a restrictive practice can, however, justify the practice by establishing that it improves the production of goods or promotes technical progress, allows consumers a fair share of the resulting benefit and does not allow the undertakings in question to eliminate competition in the market (section 6 FCA and Article 101(3) TFEU).

Additional rules apply to undertakings that are in a dominant position in a relevant market. Acquiring a dominant position is not prohibited but abuse of that position is (section 7 FCA and Article 102 TFEU). Abuse can comprise, for example, 1) exclusion of rivals from the market, 2) exploitation of customers or suppliers, or 3) discrimina-

[28] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26 October 2012, pp. 47–390.

[29] The TFEU prohibitions only apply when there may be an effect on trade between EU Member States but since that threshold is relatively easily reached, the rules will often apply in addition to the national, such as Finnish, competition rules.

tion between customers. A dominant position generally requires a relatively high market share (for example, a market share over 50% supports a presumption of dominance) and barriers to entry or expansion.

The Finnish Competition and Consumer Authority (FCCA) has jurisdiction to investigate suspected infringements of these prohibitions in Finnish and EU competition law (sections 5 and 7 FCA and Articles 101 and 102 TFEU), to impose certain remedies (such as prohibitions) and to propose fines for infringements before the Market Court. Additionally, the European Commission enforces Article 101 and 102 TFEU throughout the EU and national competition authorities in other EU Member States can enforce EU and their own national competition rules. National rules are typically similar to EU rules, but in national law they may be stricter particularly as regards unilateral practices.

3.1.2 Merger control

Merger control rules apply to so-called "concentrations", which entail acquisition of control, acquisition of the entire business operation of an undertaking or part thereof, a merger and creation of a joint venture which is to perform all the functions of an autonomous economic unit on a lasting basis (section 21). If the combined turnover of the parties to the concentration exceeds certain thresholds, it must be notified to the FCCA (sections 23 and 24) or the European Commission. If an authority concludes that the concentration would significantly impede effective competition in a relevant market, particularly due to creating or strengthening a dominant position, the concentration can be prohibited or conditions can be imposed on its implementation. (sections 25–27).

3.1.3 Other relevant rules

Relevant sector-specific rules also apply to undertakings. In particular, the Act on Electronic Communications Services complements the general competition rules. In particular, the Act can impose duties on providers of certain telecommunications services that have significant market power. They can, for example, be required to allow other telecompanies to use its network or infrastructure (sections 56, 61, 63, and 67 of the Act on Electronic Communications Services).

The Finnish Competition and Consumer Authority secures the balance between the business activities of the private and public sectors (chapter 4a), referred to as "competition neutrality". The aim of these rules is in particular to ensure that public actors do not prevent or distort competition in the market area. These rules may particularly apply if public sector organizations become involved in the market.

3.2 Implications of competition law on the practices of Neutral Host operator

Neutral Host and participating undertakings are generally required to evaluate their compliance with Finnish and EU competition law by themselves; no advance clearance by competition authorities is generally possible. Undertakings must, in particular, avoid engaging in cooperation that restricts competition and, if dominant in any relevant market, refrain from practices that amount to abuse of that position. Moreover, transactions such as creation of a permanent joint venture may need to be notified to competition authorities (the European Commission or the Finnish and/or other national authorities) and cleared before it can be implemented. Since competition law limits the practices that can be adopted and establishes duties for undertakings to act in certain ways, competition law also affects which business strategies are attractive for Neutral Host.

3.2.1 Competition law analysis of Neutral Host practices

Assessing Neutral Host from the perspective of competition law requires examining all aspects of creating and operating it. Generally, competition law analysis considers:

1) The form and nature of the practice (mergers/acquisitions/JVs, agreements/cooperation, unilateral conduct)
2) Legal and economic context of the practice
    a. Economic: relevant market (rivals), market position of parties, customers, entry barriers
    b. Legal: legal rules affecting competition on the market
3) Effects on competition (reduction of rivalry, or other forms of acquiring, maintaining and exploiting market power)

4) Efficiencies and other justifications: benefits produced that compensate consumers for anti-competitive effects, necessity of anti-competitive practices, no elimination of competition

On some practices there is legislation and case law that sets standards and tests. However, this is not the case for most aspects of the Neutral Host. As regards particularly platforms and data, the legal approaches are still under development in the Member States and at the EU level. For this reason there is uncertainty over how competition authorities and courts would analyze these types of practices. However, authorities, legislators and courts are currently examining these issues, which may clarify the situation in some aspects relevant to Neutral Host in the future.

3.2.2 Potential competition law issues raised by Neutral Host

Although the state of the art does not provide standards or tests on Neutral Host practices, it is possible to identify potential competition law issues that Neutral Host might raise in light of the concerns competition generally pays attention to, which are horizontal collusion, vertical restraints, foreclosure of rivals, and exploitation of customers or suppliers.

Relevant aspects for Neutral Host are for example:

1) Formation of Neutral Host operators
   - Joint venture that requires merger notification to competition authorities.
   - Agreements and cooperation that may restrict competition.
2) Connectivity layer: network and facilities
   - Agreements/cooperation – particularly among actual or potential rivals:
     - Is cooperation among telecommunications likely to restrict competition?[30]

[30] In the future, these types of competition law issues may become more frequent. First, proposed amendments to network and frequency regulation in Finland would enable broader sharing than is currently the case. Second, greater network densification driven by 5G and also greater emphasis on cost management of small cell networks supports the need for sharing arrangements. (See Body of European Regulators for Electronic Communications, 2018a, p. 95 and Body of European

        - Can restrictive cooperation be justified on the grounds that it is ultimately pro-competitive and beneficial to consumers?
    - Direct or indirect duties to provide access to NH connectivity facilities to other firms?
3) Data platform: collection and use of data
    - Collection of data
        - Agreements between data collectors/holders and NH?
            - Horizontal aspects: e.g. restrictions between competing data collectors
            - Vertical issues: restrictions on data collectors or NH that restrict competition?
        - Abusive collection of data (e.g. without consent or under unfair terms)?
    - Use of collected data
        - Packaging of data: data pools, other bundles of data, separate data types?
            - Joint (collusive) selling of data?
            - Bundling: risks of excluding rival data providers?
        - Terms of supplying data to customers:
            - Pricing of data
            - Restrictions/conditions on using the data by customer

---

Regulators for Electronic Communications, 2018b, p. 3.) In Finland, The Finnish Competition and Consumer Authority (FCCA) has expressed concerns that a joint venture among DNA Oyj and Telia Finland Oyj with Suomen Yhteisverkko Oy, with the parties sharing a mobile network in Northern and Eastern Finland, would restrict competition in the mobile communications market. However, the FCCA accepted commitments offered by DNA and TeliaSonera to address the FCCA's concerns. The commitments include the parties offering virtual and service operators access to their national networks, renting out mast and equipment location sites to competitors and restricting information exchange within the sphere of the joint venture. (See the FCCA's decision in Finnish: Finnish Competition and Consumer Authority, 2015.) Also the European Commission has examined network sharing under antitrust rules (Article 101 TFEU) and recently preliminarily concluded that network sharing in the Czech Republic restricts competition. (See European Commission, 2019.)

        - Use of data
        - Disclosure of data
        - Other conditions: e.g. duty to provide own data to NH?
    - Sharing data within NH (founders/partners) and through NH (to customers):
        - Risks of collusion among those having access to data that can be used to coordinate conduct among rivals
        - Abusive use of data (e.g. to exclude rivals)
  - Direct or indirect duty to allow data collectors' access to NH or customers' access to data collected?
4) Marketplace: rules applicable to those willing to provide their products via NH market place
  - Rules for operating on the marketplace set by NH
    - Pricing related rules
    - Requirements, conditions and limitations applying to products offered in the marketplace
  - Direct or indirect duty to allow access to firms seeking to offer their products in the marketplace?

These potential concerns have to be taken into consideration when the rules and practices of Neutral Host are planned and built. Consideration also depends on the market position of the parties, the position of their competitors, customers and suppliers, as well as the effects of the practices on competition and consumers. An issue that also needs to be further examined is the implications of the network and spectrum regulation, including conditions set in spectrum licenses, as these may affect the competition law treatment of sharing and renting spectrum as well as sharing infrastructure.

3.3 Summary

Finnish and EU competition law prohibit all forms of cooperation that restrict competition and practices that constitute abuse of a dominant position. Since the formation and operation of Neutral Host involves cooperation and agreements with various undertakings, it is import-

ant to ensure that the agreements and their specific conditions do not reduce rivalry or can be justified by efficiency benefits (such as cost efficiencies). For example, if Neutral Host activities involve firms that otherwise would have competed (for network access, data, services, and so on), competition between them could be restricted and the parties to the activity must justify it. More permanent structures for cooperation may also require notification to competition authorities under merger control rules. Data sharing and platforms need to be designed in a way that does not include agreements restricting competition or, if Neutral Host were to become dominant in some market (such as data supplier in an area), does not lead to foreclosure of competitors or impose unjustified restraints on customers or suppliers.

4 Public procurement legislation

The aim of public procurement legislation is to ensure cost and quality efficiency in the use of public funds as well to maintain competition in the market by providing equal opportunities to provide goods and services. To achieve this, procurements have to be tendered under certain circumstances. The obligation to arrange competitive tendering depends principally on the organization (procurer) as well as the value and type of procurement.

4.1 Act on Public Procurement and Concession Contracts

Finnish national legislation on public procurement[31] will be applied and the competitive tender procedure needs to be arranged when 1) the contracting entity is one of those mentioned in the Act and it arranges procurement outside of its organization and 2) the value of the procurement exceeds the national threshold values defined in section 25 (60,000–500,000 euros depending on the type of procurement).[32]

---

[31] Act on Public Procurement and Concession Contracts (1397/2016).

[32] Sections 27 and 28 define how to calculate the estimated procurement value. Dividing or combining procurement artificially in order to evade application of the law (section 31) is prohibited.

Contracting entities subject to the duties under section 5 are:

"1) authorities of central and local government and joint municipal authorities;
2) the Evangelical-Lutheran and Orthodox churches of Finland and their parishes and other authorities;
3) state commercial institutions;
4) institutions of a public law character;[33]
5) any party conducting a procurement when it has secured support in doing so from a contracting entity referred to in paragraphs 1–4 amounting to more than half of the value of the procurement."[34]

The competitive tender procedure needs to comply with certain requirements set in legislation. These include, for example, notifications and set timelines for the call for tenders, competency requirements when selecting the service provider and the requirement that the whole procurement process is fulfilled in accordance with the principles of equality and non-discrimination (section 3, chapters 6–11 and chapter 14). As a rule the most economically advantageous tender has to be selected (section 93).

Purchasing bodies can choose among certain procedures and contract types (chapter 5). One method of executing public works or service procurement is to use concession contracts. A concession contract denotes an agreement concluded for financial consideration, whereby the contracting entity assigns – to the supplier – performance of public works, or the provision and administration of services, and the associated operational risk. The consideration for the assignment consists either solely in the right to exploit the works or services, or in that right together with the payment.[35]

---

[33] Institutions of a public law character referred to in paragraph 4 are defined as "a legal person expressly established to satisfy public interest needs that are not of an industrial or commercial nature and: 1) are mainly financed by a contracting entity referred to in paragraphs 1–4; 2) are managed under the regulatory control of a contracting entity referred to in paragraphs 1–4; or 3) of whose administrative, managerial or regulatory organs a contracting entity referred to in paragraphs 1–4 appoints more than half of the members".

[34] Unofficial translation by the Ministry of Economic Affairs and Employment.

[35] Chapter 13 regulates concession contracts. The national threshold value for

Generally, all medium and high value contracts must be awarded through competitive procedures. However, there are some exclusions from and exceptions to this. These include, for example, procurements "whose principal purpose is to enable the contracting entity to make public communications networks available or to maintain them or to provide the public with one or more electronic communication services". (section 8 paragraph 1) and procurements concerning research and development services defined in schedule A (section 9 paragraph 13). Additionally, in some circumstances – when purchasing real estate or where there is only one possible supplier – competitive tendering is not required (section 9 paragraph 1, section 40).

4.2 Directive 2014/24/EU on Public Procurement

The EU Directive on Public Procurement[36] requires that if the value of the procurement exceeds the threshold values defined in the directive (2020 threshold values lie between 139,000–5,350,000 euros)[37] somewhat stricter requirements as to the competitive tender procedure have to be taken into account[38] and the competitive tender has to be arranged EU-wide. In EU-wide competitive tenders, providers from any Member States which fulfil certain requirements can participate in the call for tenders and are eligible to be chosen as a provider of a service or goods.

The primary organs for reviewing the procedure are the courts or independent review bodies based in the EU country where the tender

concession contracts is 500,000 euros (section 25). EU regulation will be applied if the value of a concession contract is over 5 million euros (Directive 2014/23/EU of the European Parliament and of the Council on the award of concession contracts, OJ L 94, 28 March 2014, pp. 1–64, Article 8).

[36] Directive 2014/24/EU of the European Parliament and of the Council on public procurement and repealing Directive 2004/18/EC, OJ L 94, 28 March 2014, pp. 65–242.

[37] Article 4. The values are reviewed every two years.

[38] Articles 23, 27–31, 42, 50, 51, 59, 61. Stricter requirements include required notifications, longer set periods for tenders and the use of common EU standards and forms as well as more detailed competency criteria for the selected tender. The EU has created, e.g., a common public procurement vocabulary (CPV-codes) which needs to be used when specifying procurement types.

was published. These processes need to comply with certain requirements. For procurements whose value exceeds the EU threshold limits, the European Commission has jurisdiction to intervene in unlawful acts among Member States.[39]

4.3 Summary and implications of public procurement law for Neutral Host

Public procurement rules in Finland and throughout the EU require certain organizations to arrange their procurements through a tendering process. From the perspective of the NH project, public procurement rules raise two particular questions: 1) whether Neutral Host is required to arrange competitive tendering of its procurements or 2) whether another entity that purchases goods or services from Neutral Host has to do so and what implications this has for Neutral Host.

As to the first question, when structuring the Neutral Host it is relevant to establish whether Neutral Host could be regarded as a contracting entity. This mainly comes into question if a public entity (e.g. city) occupies a central role in Neutral Host activities. With regard to the second question, a strategic consideration is that entities purchasing goods and services from Neutral Host may need to arrange procurement procedures required by law. As the applicability of public procurement rules to the customers of Neutral Host depends on the value and object of procurement by the procurer, it is relevant what the object of procurement is, whether goods and services of Neutral Host are acquired as separate components or as one package and what their value is deemed to be. An issue requiring further analysis is to what extent the exceptions applying to "electronic communications services" (section 8 paragraph 1 of the Finnish Act on Public Procurement and Concession Contracts; Article 8 of Directive 2014/24/EU) cover products offered by Neutral Host.

---

[39] Council Directive 89/665/EEC on the coordination of the laws, regulations and administrative provisions relating to the application of review procedures to the award of public supply and public works contracts, OJ L 395, 30 December 1989, pp. 33–35.

5 Concluding remarks

Neutral Host, as an operating model for a digital smart city ecosystem, may open many unforeseen business possibilities that can benefit both citizens and the government. In any case, many legal aspects need to be taken into account when developing the Neutral Host business model. Legal requirements and obligations must be fulfilled, for example, when collecting and using (processing) personal data, operating in a network with the possible new operator model and producing services and applications for the data platform's marketplace. Neutral Host also needs to be organized and operated in a way that meets the requirements of competition law, which in some situations may require notification of planned joint ventures to the competition authorities.

In addition, when evaluating whether digital smart city ecosystems' functions are compliant with the law, it has to be noted that the regulatory environment is new and the legal approaches and praxis are constantly developing. This is why exhaustive answers to all the upcoming questions can be challenging to give. To provide a more precise analysis of the legal framework for Neutral Host, for example, the actors and functions in the ecosystem need to be further clarified. However, as the purpose of regulation is also to enable the development of future smart cities, there is also a need to adjust or lighten certain regulatory procedures and practices that are no longer applicable in the 5G era. The need to update regulation is already recognized at the EU level, as well as in Finland, where ongoing reform of network and spectrum regulation implicates the trend. In the context of digital smart cities, where many new legal concerns will arise in the future, legislators and regulators need to achieve a balance between responsibilities and restrictions and rights and reliefs.

However, the Neutral Host as a concept could already be executed under the current regulatory framework. Current legislation provides a frame where the 5G ecosystem can operate ensuring that, inter alia, the privacy and data protection of citizens is secured, that market balance and fair competition remain and that the elements needed for the digital smart city's function are shared and used fairly and effectively. Looking into the future, the ongoing reforms and proposed amendments can be relevant for the Neutral Host, but their final influence can only be estimated later. Meanwhile, Neutral Host

can be further developed by following existing legal mandates and legal requirements.

References

Ahokangas, P., Matinmikko-Blue, M., Yrjölä, S., Seppänen, V., Hämmäinen, H., Jurva, R. and Latva-aho, M. (2018). Business Models for Local 5G Micro Operators. In *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)* 1 January. Available at: https://research.aalto.fi/files/31560142/ELEC_Hammainen_IEEE_DySPAN_Business_models_for_local_5G_operators_camera_ready.pdf (accessed 25 February 2020).

Article 29 Working Party (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017.* Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (accessed 20 April 2020).

Body of European Regulators for Electronic Communications (2018a). *Study implications of 5G Deployment on Future Business Models. A Report by DotEcon Ltd and Axon Partners Group. 14 March 2018.* Available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8008-study-on-implications-of-5g-deployment-on-future-business-models (accessed 20 April 2020).

Body of European Regulators for Electronic Communications (2018b). *Report on infrastructure sharing. A Report by BEREC. 14 June 2018*. Available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8164-berec-report-on-infrastructure-sharing (accessed 20 April 2020).

Breyer, P. v. Bundesrepublik Deutschland (2016) Case C-582/14. ECLI:EU:C:2016:779.

Bu-Pasha, S. (2018). *Location Data, Personal Data Protection and Privacy in Mobile Device Usage: An EU Law Perspective*. Doctoral dissertation, University of Helsinki.

European Commission. (2020). *European Data Strategy, 20 February 2020.* Available at: https://ec.europa.eu/eip/ageing/news/european-data-strategy_en (accessed 13 March 2020).

European Commission. (2019). *Antitrust: Commission sends Statement of Objections to O2 CZ, CETIN and T-Mobile CZ for their network sharing agreement. Press release, 7 August 2019.* Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5110 (accessed 19 March 2020).

Finnish Communications Regulatory Authority. (2016). *Viestintäviraston TAE 2017*, Available at: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-78656.pdf (accessed 25 February 2020).

Finnish Competition and Consumer Authority. (2015). *Decision dnro 438/14.00.00/2014, 5 November 2015*. Available at: https://www.kkv.fi/

globalassets/kkv-suomi/ratkaisut-aloitteet-lausunnot/ratkaisut/kilpailuasiat/2015/kielto--sitoumus--ja-toimitusvelvoiteratkaisut/r-2014-00-0438.pdf (accessed 19 March 2020).

Garfinkel, S.L. (2015). *De-Identification of Personal Information.* National Institute of Standards and Technology Internal Report 8053. U.S. Department of Commerce. Available at: http://dx.doi.org/10.6028/NIST.IR.8053 (accessed 25 February 2020).

Hall, R.E. (2000). The vision of a smart city. In *Proceedings of the 2nd International Life Extension Technology Workshop.* Paris, France. September 28. Available at: https://webcache.googleusercontent.com/search?q=cache:oygpf30o6rgJ:https://www.osti.gov/servlets/purl/773961/+&cd=1&hl=fi&ct=clnk&gl=fi (accessed 28 March 2020).

Kamara, I. and De Hert, P. (2018). *Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach*. *Brussels Privacy Hub Working Paper, Vol. 4, N° 12.*

Lohan, E.S., Alén-Savikko, A., Chen, L., Järvinen, K., Leppäkoski, H., Kuusniemi, H. and Korpisaari, P. (2018). '5G Positioning: Security and Privacy Aspects' in Liyanage, M., Ahmad, I., Abro, A.B., Gurtov, A. and Ylianttila, M. (eds), *A Comprehensive Guide to 5G Security*. Wiley, pp. 281–320.

LuxTurrim5G. (2019). *Nokia Driven LuxTurrim5G Smart City Ecosystem Extending* [Online]. Available at: https://www.luxturrim5g.com/newblog/2019/11/4/nokia-driven-luxturrim5g-smart-city-ecosystem-extending (accessed 3 April 2020).

LuxTurrim5G. (2017). *Project Summary* [Online]. Available at: https://www.luxturrim5g.com/project-summary (accessed 3 April 2020).

Ministry of Transport and Communications. (2018). *Valtioneuvosto myönsi 5G-verkkotoimiluvat* [Online]. Available at: https://www.lvm.fi/-/valtioneuvosto-myonsi-5g-verkkotoimiluvat-987074 (accessed 25 February 2020).

Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta (2018) Case C-25/17. ECLI:EU:C:2018:551.

Traficom. (2019). *Mikä on teletoimintaa?* [Online]. Available at: https://www.traficom.fi/fi/viestinta/viestintaverkot/mika-teletoimintaa (accessed 25 February 2020).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (2018) Case C-210/16. ECLI:EU:C:2018:388.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R.A., Hayes, N.M. and Nelson L.E. (2010). *Helping CIOs Understand "Smart City" Initiatives: defining the smart city, its drivers, and the role of the CIO.* Cambridge: Forrester Research, Inc. Available at: http://goo.gl/4XHk0F (accessed 9 April 2020).