Public Procurement and Vendor Lock-in within the Area of Data Migration

Ex Post Measures from Selected Legal Regimes of Direct Applicability and Their Effectiveness in Achieving Data Migration

JAN SVOBODA

GRC Security Engineer at SUSE

Ph.D. Candidate at the Institute of Law and Technology, Faculty of Law,

Masaryk University

jan.svoboda@mail.muni.cz

ABSTRACT

This article is devoted to analyzing the extent to which the existing instruments from directly applicable EU legislation within the fields of free flow of non-personal data, personal data protection, and competition law are effective in addressing vendor lock-in in public procurement within the area of data migration. Although there are ways to reduce the risk of occurrence of vendor lock-in, this problem still arises. Therefore, it is appropriate to examine *ex post* measures to address it. The article aims, in particular, to fill the gap in the literature in a way that can be used in practice (especially in the practice of the contracting authorities) and to add something new to the current state of the art by focusing on measures and legislation not having public procurement as their main

DOI: 10.54103/milanlawreview/18741

MILAN LAW REVIEW, Vol. 3, No. 1, 2022
ISSN 2724 - 3273

regulatory subject. The three chosen regimes of general and direct applicability ensure that the lessons learned can also be applied to the very narrow context of data migration issues. The article uses practical examples to illustrate effectiveness and is written such that future research may use the observations made herein as a basis when assessing the need for the amendment of existing legislation.

Keywords: public procurement; vendor lock-in; data migration.

This paper has been subjected to double-blind peer review

Public Procurement and Vendor Lock-in within the Area of Data Migration

1. Introduction

As it accounts for over 14% of the European Union's GDP, public procurement represents a significant part of the European Union's economy.[1] Regulation in this area pursues several goals.[2] One of these goals is the promotion of efficiency in public spending.[3] This aim is expressly stated in Recital 2 of Directive 2014/24/EU and Recital 4 of Directive 2014/25/EU, and is thus mentioned in both directives which currently regulate the field of public procurement in the European Union.[4] Efficiency in public spending can be understood as a relationship between output and input – contracting authorities should be aiming to spend only the amount of resources necessary (input-efficiency) to achieve the required aims: to obtain goods, works, or services of an adequate quality and quantity (output-efficiency).[5] However, various phenomena represent

[1] European Commission, 'Single Market Scoreboard: Performance per policy area: Public Procurement', accessed 29 November 2020

[2] Marta Andhov, (Née Andrecka), 'Contracting Authorities and Strategic Goals of Public Procurement – A Relationship Defined by Discretion?' in Sanja Bogojević, Xavier Groussot and Jörgen Hettne (eds), *Discretion in EU Public Procurement Law* (Hart Publishing 2018) 121

[3] ibid

[4] European Commission, 'Environment: EU Public Procurement Directives', accessed 29 November 2020

[5] See Santiago Herrera and Abdoulaye Ouedraogo, 'Efficiency of Public Spending in Education, Health, and Infrastructure – An International Benchmarking Exercise' (Word Bank Group 2018) 2, accessed 4 January 2021

a threat to attaining this goal.[6] One of them, as will be explained below, is vendor lock-in.

Generally speaking, vendor lock-in adversely affects the public procurement environment and the management of sources by contracting authorities. It manifests itself as a contracting authority's dependence on the contractor.[7] This means that the contracting authority is reliant on a sole vendor who is the only vendor with the capability to provide with the required goods, works, or services. As a result, the buying choices of the contracting authority are tied.[8] Whereby, competition is reduced and the contracting authority is likely to be forced to spend more resources or gain inputs of lower quality or quantity than in a competitive situation.

There are several possible causes for vendor lock-in. One of them is a monopoly, which can occur both on the market for the original solution and the market for subsequently developed solutions – the aftermarket. Another reason for this dependence, occurring mainly on the aftermarket, may be that the original vendor holds specific contractual rights, intellectual property rights, know-how, or specific technology (needed to deploy a follow-up solution).[9] For instance, the company responsible for public transport in Prague, together with the city of Prague, purchased an IT solution known as "Open Card", which was essentially a piece of transport service software (check-in system) using chip cards.[10] However, the contracting authorities failed, among other things, to secure for themselves the option to edit the data on the chip cards (and to further develop the system without the original contractor). Thus they became dependent on the original contractor in relation to any possible adjustments.[11]

The importance of addressing the problem is illustrated by a 2015 survey, according to which 42% of respondents across the EU found themselves in some form of ICT[12] vendor lock-in.[13] Based on this survey, it is fair to say that the

[6] Another threat to goals of public procurement can be for example corruption. See for example: Steven Kelman, 'Goals, Constraints, and the Design of a Public Procurement System' in *The Costs of Different Goals of Public Procurement* (Konkurrensverket 2012) 13-14, accessed 4 January 2021

[7] Rajiv C. Shah, Jay P. Kesan and Andrew C. Kennis, 'Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience' (2007) Illinois Public Law Research Paper No. 07-13, 7, accessed 5 September 2020

[8] ibid

[9] ibid, 3-7

[10] The Supreme Administrative Court (of the Czech Republic) 1 As 256/2015-95 (2016)

[11] ibid

[12] Information and communication technologies

[13] European Commission, 'Study on best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in' (2016), accessed 5 September 2020

ICT sector is vulnerable to this kind of dependence. The percentage given above may have decreased since the time of the survey, but the reduction is unlikely to be significant, seeing as only partial steps have been taken at the EU level to prevent vendor lock-in. Moreover, none of these steps are part of the legislation that governs public procurement as its main regulatory subject,[14] i.e., the given rules do not apply to public procurement as a whole, but only to a specific kind of public procurement dealing with a subject matter governed by specific legislation, such as data processing. One step we can mention in this respect is the adoption of Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union ("RFFFND").[15]

Within the broader problem of vendor lock-in in the area of public procurement, this article will be focused specifically on issues relating to data migration. This problem may occur, in particular, where the contractor is a data processor[16] acting on behalf of the contracting authority (a data controller)[17] and the contractor is not obliged to transfer the data processed on behalf of the contracting authority back to that authority or to a new contractor (a new processor) appointed by the contracting authority. Alternatively, this problem also occurs, for example, if the contracting authority is contractually forbidden to process the data or if the contractor is not obliged to transfer these data in a format required for further processing. This means that the contracting authority is not able to process "its" data without the involvement of the original contractor, or else must bear high switching costs to collect the data once again, to convert the data to the required format or to purchase additional solutions enabling the contracting authority to work with the given format. Consequently, this kind of vendor lock-in constitutes a problem for the data portability of data processed on behalf of the contracting authority.

[14] Another attempt to address ICT third-party dependencies, this time in the field of financial sector, has manifested itself in the proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (see for example Recital 28 or Article 25 (2) of this regulation). As this proposal is still in its nascent stages, it will not be discussed further in these pages.

[15] This regulation is analysed in more detail in chapter 1 of this article.

[16] Nevertheless, data migration may be relevant also in the relationship between two data controllers or joint controllers (recipients in general), because the transfer of data may occur also between these entities.

[17] Justice Opara-Martins, Reza Sahandi and Feng Tian, 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective' (2016) 5 J Cloud Comp, accessed 5 September 2020

Although there are ways to reduce the risk of occurrence of vendor lock-in,[18] such as the adequate design of subject-matter and conditions of a contract, selection criteria, contract-award criteria, etc., the problem can still arise. Contracting authorities may in theory negotiate broad contractual rights (including data portability rights) in order to prevent this problem. However, negotiating such broad rights (without further consideration) likely results in a higher price for the offered solution. If these rights are conceived too broadly (and the contracting authority then does not exercise them), the process will not be in compliance with the efficiency principle within the meaning of Recital 2 of Directive 2014/24/EU and Recital 4 of Directive 2014/25/EU.[19] It is therefore understandable that in certain cases, the contracting authority does not consider the future need for data portability and does not reserve adequate data portability rights. Likewise, it may fail to secure these rights due to administrative or legal error. In situations such as these, *ex post* measures should be used.

If vendor lock-in occurs (or seems to have occurred) and the relevant dependence manifests itself, the bargaining power of the contractor increases. In such a case, the bargaining power of the contractor is much higher than that of the contracting authority, and this seriously threatens the efficiency of public spending. The person responsible for choosing the particular procedure and its legality is, of course, the contracting authority.[20] However, depending on the factual circumstances (such as the impossibility to choose another vendor without incurring high switching costs), the contracting authority may be "forced" by the contractor to use the negotiated procedure without prior publication (and thus to "exclude competition") and to award to the original contractor additional

[18] See an article written by former vice-chair of the Czech Office for the Protection of Competition: Josef Chýle, 'Jaké otázky si klást v IT veřejných zakázkách před zahájením migrace dat a problematika vendor lock-in' (2017) Informační list 2017 - Zakázkové právo v oblasti ICT a další aktuální témata, 19ff, accessed 29 November 2020.

[19] While I have not found any actual instances where the relevant authorities in the EU challenged excessive portability rights, it should be emphasized that stipulating overly broad rights (for instance) is not the proper way of preventing vendor lock-in. The contracting authority cannot simply purchase something which it does not need (without a proper previous assessment of its needs and potential risks). Police forces (at least in the EU) do not purchase Lamborghinis "just in case" they need to drive 300 km/h. It would not be proportionate to their actual or likely needs. The same applies to data migration processes. The contracting authority simply cannot apply all possible *ex ante* measures to prevent vendor lock-in – it should strive to find the right balance depending on the given situation.

[20] See for example Recitals 69 and 71 of Directive 2014/24/EU.

contracts based on terms *de facto* defined by this contractor.[21] The contractor's approach is logical, as it is mainly motivated by its own (future) profits. In such situations, the contracting authority should take a look into the *ex post* measures available under the applicable law to reduce possible costs (of various kinds) while resolving the issue. While no assumptions should be made as to the true motivations of the contracting authority, in the aforementioned Open Card case, the contracting authorities were compelled, as a consequence of the vendor lock-in, to use the negotiated procedure without prior publication even though the required conditions for such procedure were not met (i.e., the procedure was used unlawfully). As a consequence, the contracting authorities were fined.[22]

The rules governing public procurement as a primary regulatory subject (Directive 2014/24/EU, Directive 2014/25/EU, and the respective national acts implementing these directives) in principle allow only two ways how to address vendor lock-in which has already manifested itself (for example due to inappropriate conduct of the contracting authority in the past, or due to an unexpected event). The first one is using the above-mentioned negotiated procedure without prior publication; the second one is to repurchase the entire solution which is the subject of the vendor lock-in – this time under more favorable conditions. Generally speaking, neither option can actually be considered to be efficient.[23] Later in this article, we shall use these options as a benchmark to determine whether alternative *ex post* measures may be more effective in addressing vendor lock-in.

As outlined above, using the negotiated procedure without prior publication can result in a higher price than the price offered in a competitive market. In the course of repurchasing, the contracting authority is required to pay for a similar solution twice (i.e., for the original one and then for a new one). At this point, one should stress that even a mere 1% efficiency gain could result in 20 billion EUR savings per year.[24] Therefore, it is appropriate to look at how the given vendor lock-in within the area of data migration could be addressed by using other legal fields – regimes of general applicability. These regimes could be used to find solutions that would remove the need for any bargaining with the current contractor, as the contractor would be obliged to migrate the data.

---

[21] One of the fundamental aspects of the negotiated procedure without prior publication is the inherent restriction of competition. See David Dvořák and others, *Zákon o zadávání veřejných zakázek: Komentář* (CH Beck 2017) 338.

[22] The Supreme Administrative Court (of the Czech Republic) 1 As 256/2015-95 (2016)

[23] Jan Svoboda, 'Veřejné zakázky v oblasti ICT a problém závislosti zadavatele' (2019) 10(19) Revue pro právo a technologie 135, accessed 14 November 2020

[24] European Commission, 'Internal Market, Industry, Entrepreneurship and SMEs: Public Procurement', accessed 29 November 2020

As regards the state of the art, only a limited number of publications dealing with vendor lock-in in public procurement are available.[25] In addition, most of the publications addressing data portability mention this phenomenon only marginally (if at all)[26] and are often focused primarily on *ex ante* measures.[27] I am not aware of any publication, whether in English, Czech or Slovak, which would primarily be devoted to the possibilities of addressing vendor lock-in within the area of data migration by contracting authorities, especially not from the perspectives of *ex post* measures stated in legal regimes of general applicability. I would like to fill this gap in the literature in a way that can be used in practice (especially in the practice of the contracting authorities) and to add something new to the current state of the art by focusing on *ex post* measures and legislation that do not have public procurement as their main regulatory subject. Nevertheless, valuable sources addressing the problem of data portability do exist.

The first group of information sources relates to non-personal data. In this regard, it is necessary to mention the RFFFND, which aims to provide a framework to reduce certain vendor lock-in practices.[28] The regulation mainly ensures the free movement of non-personal data across borders within the EU. Based on Article 6 of the RFFFND, the development of self-regulatory codes of conduct at the Union level shall be encouraged and facilitated by the European Commission. These standards should be based on several principles, including the principle of interoperability. Thus, information on the state of the art,[29] including secondary sources, regarding the development of these codes of contact[30] is without doubt also beneficial for the analysis. The importance of data portability can also be seen in the European Commission's current approach that proposes measures to boost data sharing.[31]

The second group of sources consists of (but is not limited to) academic papers and other professional literature dealing with the instruments relating to

[25] See for example: Bianca Sjoerdstra, 'Dealing with Vendor Lock-in' (University of Twente 2016), accessed 5 September 2020.

[26] See for example: Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' (2012) 16, accessed 5 September 2020.

[27] Josef Chýle, 'Jaké otázky si klást v IT veřejných zakázkách před zahájením migrace dat a problematika vendor lock-in' in 'Informační list 2017 - Zakázkové právo v oblasti ICT a další aktuální témata' (Úřad pro ochranu hospodářské soutěže 2017), accessed 29 November 2020

[28] See Recitals 2, 6, and 31 of the RFFFND.

[29] SWIPO, 'SWIPO codes published', accessed 29 November 2020

[30] See for example: Petr Mišúr, 'Evropský parlament schválil nařízení o volném pohybu neosobních údajů v EU' (CH Beck 2018) 11-12 Obchodněprávní revue.

[31] European Commission, 'Commission proposes measures to boost data sharing and support European date spaces' (2020), accessed 29 November 2020

data portability as stated in Regulation (EU) 2016/679 ("GDPR"), also in connection with other regimes,[32] and the respective guidelines of the relevant authorities.[33]

Data portability is also a topic in another regime of direct applicability – namely, competition law.[34] In the area of competition law, a number of cases are dealing with abuse of a dominant position. Some of them relate directly to the refusal to provide certain information.[35] Such cases may be valuable sources to be applied in the area of public procurement as well.

Against the backdrop of the above, the present paper seeks to analyze to what extent the existing instruments from directly applicable EU legislation within the field of free flow of non-personal data, personal data protection, and competition law are effective in addressing vendor lock-in in public procurement within the area of data migration (as compared to the options provided by public procurement law – to use a negotiated procedure without prior publication, or to repurchase the entire solution). These three regimes are not the only ones through which the problem of data portability may be addressed (consider, for instance consumer protection law[36]), but they are the most relevant, as they are designed to regulate the processing of data or to prevent the abuse of a dominant position. Moreover, directly applicable legislation, as it generally needs no further transposition and implementation, allows for a more uniform regulation.[37]

---

[32] Janis Wong and Tristan Henderson. 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR' (2019) 9 3 International Data Privacy Law, accessed on 26 April 2021; Stephanie Elfering, 'Unlocking the Right to Data Portability – An Analysis of the Interface with the Sui Generis Database Right' (2019) 38 Munich Intellectual Property Law Center - MIPLC Studies, accessed 29 November 2020

[33] See in particular: Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (2017), accessed 29 November 2020.

[34] Carolina Banda, 'Enforcing Data Portability in the Context of EU Competition Law and the GDPR' (2017) MIPLC Master Thesis Series (2016/17), accessed 29 November 2020

[35] Case 238/87 *AB Volvo v Erik Veng (UK) Ltd.* [1988] ECR 6211, Joined cases C-241/91 P and C-242/91 *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities* [1995] ECR II575, Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG.* [1998] ECR I-7817, Case C-481/01 *IMS Health GmbH & Co OHG v. NDC Health GmbH & Co KG* [2004] ECR I-5039, Case T-201/04 Microsoft Corp. v Commission of the European Communities [2007] ECR II-3601

[36] In the Czech Republic, in some situations, vendor lock-in in the area of data migration can be addressed also on the basis of Section 6a (2) and (3), 15 of Act No. 181/2014 Coll. or Section 9e of Act No. 365/2000 Coll.

[37] Which is not to deny the possibility that there may be gaps in this legislation.

Consequently, the findings of the research reported herein can be used by contracting authorities across the EU. At the same time, the three chosen regimes of general and direct applicability ensure that the lessons drawn can also be applied within the very narrow context of data migration issues in public procurement. The observations can also be used in future research as the basis for assessing the need for amendment (if any) of EU legislation (including Directives) or of the national laws.

The main research question to be answered in this article is:

- *To what extent are existing instruments from directly applicable EU legislation within the field of free flow of non-personal data, personal data protection, and competition law effective in addressing vendor lock-in in public procurement within the area of data migration?*

To answer the above question to an adequate level of detail and in a comprehensible manner, I have divided it into the following three sub-questions:

- *To what extent are existing instruments from directly applicable EU legislation within the field of free flow of non-personal data effective in addressing vendor lock-in in public procurement within the area of data migration?*
- *To what extent are existing instruments from directly applicable EU legislation within the field of personal data protection effective in addressing vendor lock-in in public procurement within the area of data migration?*
- *To what extent are existing instruments from directly applicable EU legislation within the field of competition law effective in addressing vendor lock-in in public procurement within the area of data migration?*

In answering these sub-questions, the effectiveness "as such" will firstly be assessed, followed by an assessment of the extent of this effectiveness. An existing instrument (i.e., the possibilities introduced by the current legislation to address the given problem) will be, for the purpose of this article, deemed as effective if it provides the basis to achieve data migration even though there is no comprehensive contractual basis. However, the respective instrument will be deemed effective only if it provides at the same time for a solution that exceeds the benchmark based on the two possible solutions to address the problem of vendor lock-in under public procurement law, which has been described above. Then, the extent of effectiveness will be assessed as the set of situations to which these instruments apply (whereas this paper will generally describe the limitations of

the solution if it cannot be used in every case of vendor lock-in in public procurement within the area of data migration).

The aim of this article is not to describe the various types of vendor lock-in or analyze *ex ante* measures or how to find the proper balance between a high risk of occurrence of vendor lock-in and overly broad (and thus costly) contractual rights of the contracting authority. Also, the article does not analyze *ex post* measures addressing data portability issues in public procurement within any other field than the three fields mentioned in the main research question.

This article is based primarily on doctrinal legal research of statutory legislation, academic literature, guidelines, and other soft law of the relevant authorities and case law. Some of the sources may have originated in national legislation, or in legislation that is no longer in force. Such sources will be used only if the information provided therein is also relevant to the currently applicable EU legislation.

Following this introduction (Chapter 1), the article is structured into three main chapters (Chapters 2-4), one dedicated to each of the sub-questions, and a conclusion (Chapter 5). In Chapter 2, the possibilities to address vendor lock-in within the data migration area based on the RFFFND will be analyzed, particularly based on codes of conduct within the meaning of Article 6 of that Regulation.

Chapter 3 will be devoted to the analysis of two legal instruments governing personal data portability. The first is the obligatory written agreement on personal data processing, which shall be concluded between a controller and a processor within the meaning of Article 28 (3) of the GDPR. The second one is the data portability right stated in Article 20 of the GDPR. In particular, we shall analyze whether and how data controllers can use the data portability right (which really is a right of data subjects)[38] in order to address the data portability issues and to what extent this instrument can be used by contracting authorities.

Chapter 4 analyzes whether and under what circumstances conduct causing vendor lock-in (or taking advantage of vendor lock-in) may qualify as an abuse of a dominant position and therefore as a breach of Article 102 of the Treaty on the Functioning of the European Union ("TFEU").

The findings will be then summed up in Chapter 5.

Having now reached the conclusion of the introductory chapter, and before we dive into the analytical chapters laid out above, let's first have a look at a model case designed to illustrate the effectiveness of the current approaches in practice; this model case should increase the accessibility of the material presented further below in this article.

[38] According to Article 4 (1) of the GDPR, the data subject is an identified or identifiable natural person to whom the personal data relates.

Model case

A hypothetical EU member state (let it be called "Portain") is obliged under its national law to ensure the possibility of traveling across all regions by train. This national law, in particular, designates routes whose operation must be ensured by the government. Portain has decided to outsource the operation of trains on these routes to an external railway company. There is only one railway company in Portain which is able to operate the trains on all of the mandatory routes. This company is called Furious But Not Fast ("FBNF") and has operated these routes since 1999. The existing contractual relationship between Portain and FBNF will last until 1 December 2021. For the period thereafter, a new contract will have to be concluded.

In 2015, Portain decided to provide travelers with the option to buy train tickets online, including tickets that are valid for 24 months and registered via the personal account of the traveler. Thus, it was agreed with FBNF that FBNF would develop and operate a new complex IT system administrating the necessary data. FBNF holds the property rights to the IT system and the data is processed by FBNF on behalf of Portain. Both the IT system and the data are stored in cloud servers located in another EU member state. The agreement between Portain and FBNF sets out only the categories of data to be processed by FBNF (including the data on customers and their currently valid tickets and statistical data on the occupancy of individual routes), terms of remuneration and basic security requirements. Both personal and non-personal data are processed in the IT system. A data processing agreement has also been concluded, in accordance with Article 28 of the GDPR. Under the GDPR, a controller and a processor are obliged to conclude this agreement[39] (in writing)[40] if the processor processes personal data on behalf of the controller (and if the processing is not based on another act of the Union).[41] The duration of this data processing agreement is dependent on the duration of the main agreement. Portain has no complex, contractually stipulated, exit strategy in relation to data migration. In other words, none of the aforementioned agreements (and no other relevant agreement) contain any provision about what happens with the data when the main agreement expires (going beyond the mandatory provisions stipulated in Article 28 (3) of the GDPR).

In December 2020, Portain announced its plan to offer the operation of the trains on each mandatory operated route as a separate contract within separate public procurement procedures. Portain has several regional railway companies but none of them has the capacity to operate more than 8 % of the routes in Portain. FBNF announced that it will not allow the other railway companies to use the IT system and, more importantly, the data it contains. Based on this announcement, Portain decides to explore the necessary legal steps to gain complete control over

[39] Mandatory stipulations of this agreement are prescribed by Article 28 (3) of the GDPR.

[40] Article 28 (9) of the GDPR

[41] Article 28 (3) of the GDPR

key data so that it will be able to provide the data to the companies that will operate the mandatory routes in the future.

2. Vendor lock-in in the area of non-personal data

A data portability problem, including vendor lock-in in public procurement within the area of data migration, generally arises because the contracting authority (or another party) simply cannot request the contractor to "return" the data *ex lege*. This kind of problem is not generally expected with tangible goods, as it is clear who is the owner of the object in question. Thus, there is usually no problem to determine, in the absence of any other legal title (such as a rental agreement), the person who may *ex lege* request the possessor of the tangible good to return it to them. Thus, the concept of *data ownership* could potentially resolve the problem of vendor lock-in.

Indeed, from time to time, the concept of data ownership is being discussed and promoted.[42] Some professionals even note (maybe incidentally) that data (with no further specification) can actually be owned under the currently applicable legislation.[43] Nevertheless, the majority of scholars are of the opinion that data generally[44] should not and, most importantly, cannot be owned because of its specific nature.[45] This majority, to which I happen to belong myself, argues that it

[42] Nadezdha Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?' (2017) Tilburg Law School Legal Studies Research Paper Series.
No. 21/2017, accessed on 2 February 2021, Jeffrey Ritter and Anna Mayer, 'Regulating data as property, a new construct for moving forward' (2018) Duke Law & Technology Review, 1 16, 277, accessed 2 February 2021

[43] Petr Vévoda, 'Data obsažená v IT systémech, jejich vlastnictví a zakázkové právo' (2017) Zakázkové právo v oblasti ICT a další aktuální témata - Informační list 1 17, accessed 5 February 2021

[44] The flow of data can of course be limited by contractual or technical restrictions. Information derived from data can be also subject to copyright and the data itself may be subject to other kinds of intellectual property, but all these constructs should be regarded as an exemption from the default status of freely flowing data. Cf. Herbert Zech, 'A legal framework for a data economy in the European Digital Single Market: rights to use data' (2016) 11 6 Journal of Intellectual Property Law & Practice 460-470, accessed on 19 April 2021

[45] This specific nature, and the reasons supporting the claim against the possibility of ownership, are well described by Dan Sventesson and Radim Polčák in their book "Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law". See also Jakub Míšek, *Moderní regulatorní metody ochrany osobních údajů* (Masarykova univerzita 2020) 38, or, in relation to information, Jean Nicolas Druey, 'Information Cannot Be Owned: There is More a Difference than Many Think' (2004) Harvard Law School Public Law Research Paper Series, Research Paper no 96, 6-7.

is more suitable to set out rights and duties in relation to data processing activities. This approach, which can, among other aspects, allow several persons to exercise their rights to the same data at the same time, is in line with the data processing-oriented approach taken by the lawmaker in RFFFND (and in the GDPR[46]).[47, 48] This regulatory approach will be, for the purpose of this and the following chapter, deemed reasonable. Thus, the analysis will focus on the possibilities to address vendor lock-in within the area of data migration in public procurement by means provided for in this regulatory framework targeting the processing activities.

In this chapter, particular attention will be paid to the currently applicable RFFFND. It is the main regulation related specifically to the processing of non-personal data. The first subchapter will analyze the framework for free flow of non-personal data established by RFFFND, and the possibilities (and related effectiveness) of using the instruments introduced by this regulation as *ex post* measures to address vendor lock-in in public procurement within the area of data migration. The second subchapter is devoted to assessing the effectiveness and its extent, as well as to proposals *de lege ferenda*.

2.1. The RFFFND, self-regulation, and codes of conduct

The RFFFND has been introduced as a reaction to two negative phenomena which have made their presence felt in the EU. These two phenomena hamper the effectiveness and efficiency of data processing and the development of the data economy. They also result in insufficient competition between cloud service providers.[49] The first one is represented by requirements under national law concerning data localization practices; the second one is the vendor lock-in.[50] Thus, the RFFFND establishes the principle of free movement of non-personal data across EU member states,[51] according to which member states are generally not allowed to establish national laws which would limit data transfer within the EU (unless where justified on the grounds of public security, taking into account the proportionality principle).[52] This principle has already been established, in relation to the flow of personal data, in the GDPR.[53]

[46] Jakub Míšek, *Moderní regulatorní metody ochrany osobních údajů* (Masarykova univerzita 2020) 38

[47] Article 2 of the RFFFND

[48] Article 2 of the GDPR, see also Jakub Míšek, *Moderní regulatorní metody ochrany osobních údajů* (Masarykova univerzita 2020) 38

[49] Recital 6 of the RFFFND

[50] Recital 2 of the RFFFND

[51] Recital 10 of the RFFFND

[52] Article 4 (1) of the RFFFND

[53] Article 1 (3) of the GDPR

The RFFFND also represents a reaction to situations in which the users of data processing services are prevented, by legal, contractual, or technical means, from migrating their data from one vendor to another or to their own systems – that is, a reaction to vendor lock-in within the area of data migration.[54]

According to the explanatory memorandum,[55] the RFFFND seeks, among other things, to improve the mobility of non-personal data and to make it easier for professional users of data storage or other processing services to switch between providers and to port data. The general policy then is to achieve a more competitive and integrated internal market.[56]

The RFFFND seeks to protect all users, i.e., to protect the interests of both natural and legal persons.[57] Having said that, it does not state a framework for the free flow of *every* type of data, but only of non-personal data. Thus, the framework is not *ex lege* applicable to processing activities relating to personal data.

With regard to the fact that the RFFFND has been introduced to address vendor lock-in, it may be presumed that it provides the user, including the professional user, with the means to achieve data migration. However, this is not entirely true. The RFFFND does not provide the user (or the professional user) with any specific right to address vendor lock-in which can be exercised solely based on this Regulation. Nevertheless, in its Article 6, it states that the European Commission shall encourage self-regulatory activities (of service providers)[58] in the form of codes of conduct.

The self-regulatory framework has been chosen in order to comply with the proportionality principle as set out in Article 5 of the Treaty on European Union ("TEU"), according to which the introduced legal framework should not go beyond what is necessary.[59] This is at the same time an opportunity for the industry to develop solutions to address vendor lock-in itself. Until today, no official assessment of the efficiency of this self-regulatory framework established based on the RFFFND has been published. However, the European Commission is planning to review the implementation of the codes of conduct regularly.[60] If the industry

[54] Recital 5 of the RFFFND

[55] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union' (2017), accessed on 20 April 2021

[56] ibid

[57] See Article 5 (7) of the RFFFND

[58] Article 6 (3) of the RFFFND

[59] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Framework for the free flow of non-personal data in the European Union' (2017), accessed on 20 April 2021

[60] Europa Nu, 'A Framework for the free flow of non-personal data in the EU' (2018), accessed on 20 April 2021

develops no adequate solution, the European lawmaker could intervene and adopt additional measures, including legally binding *ex lege* obligations.[61] Encouragement and facilitation of the development of codes of conduct should be motivated by the aim to contribute to a competitive data economy.[62] The aspects that codes of conduct should cover are stated in Article 6 (1) of the RFFFND.[63]

The RFFFND does not state any duty of the contractors to bind themselves by such codes of conduct. The codes of conduct are voluntary. This is also why the RFFFND does not state any sanctions or remedial measures in this regard.

As of today, two codes of conduct have been introduced. Both of them have been developed by the SWIPO (switching and porting) Codes of Conduct Working Group. This group is one of the two digital single market cloud stakeholder groups; it finalized its codes in May 2020.[64] SWIPO currently has 26 members (mainly from the private sector), including AWS, Google, Microsoft, and SAP.[65] It is questionable whether other "smaller" stakeholders can effectively address their needs using the wording of the codes of conduct. Even more questionable is whether these stakeholders can have real incentive to address, within the codes of conduct, also the specific needs of contracting authorities as entities from the public sector.

The developed codes of conduct are the Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS)

---

[61] ibid

[62] Article 6 (1) of the RFFFND

[63] The codes of conduct should cover at least the following aspects:

"(a) best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;

(b) minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;

(c) approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;

(d) communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders."

[64] European Commission, 'DSM cloud stakeholder working groups on cloud switching and cloud security certification', accessed 5 February 2021

[65] SWIPO, 'About SWIPO', accessed 21 April 2021

Cloud services ("Code of Conduct for IaaS") and the Code of Conduct Switching and Portability of data related to Software as a Service (SaaS) ("Code of Conduct for SaaS"). These two codes of conduct should be subject to a governance agreement enforced by an independent legal entity: SWIPO AISBL. The European Commission should evaluate these codes and their impact before the end of 2022.[66]

Both codes introduce several duties of the contractor in the area of transparency. For example, according to Section 5.1 of the Code of Conduct for IaaS, an infrastructure cloud service provider is obliged to provide its customer in particular with up-front information on the processes and the applicable policies relevant to data portability. For instance, an infrastructure service provider should inform its customer on: *"[a]vailable porting methods and formats, including available protections and known restrictions and technical limitations"* and *"[c]harges and terms associated with porting"*. Similar requirements on transparency, concerning cloud service providers, can also be found in the Code of Conduct for SaaS.[67] These requirements are of course best considered to be *ex ante* measures, as they enable contracting authorities and other users to assess the risks and costs associated with potential data migration.

In Section 5.2, the Code of Conduct for IaaS lists the portability requirements for cloud services, e.g., that the infrastructure service provider should provide support to facilitate interoperability.[68] This section also expressly mentions the requirement to use a structured, commonly used, and machine-readable format. Moreover, it also covers the main scenarios of data migration and states, in relatively great detail, the minimum standards to which the infrastructure service provider should adhere (including a standard of cooperation). The relationship between portability and interoperability is best described by saying that data portability serves the data transfer itself, while interoperability ensures the possibility of subsequent processing of the data in the new environment.[69] Again, similar requirements can be found also in the Code of Conduct for SaaS.[70] However, the Code of Conduct for SaaS does not expressly stipulate the requirement to use structured, commonly used, and machine-readable format.

Both codes state that they do not replace a contract between the service provider and the customer.[71] Non-compliance with the code can be subject to civil

[66] European Commission, 'DSM cloud stakeholder working groups on cloud switching and cloud security certification', accessed 5 February 2021

[67] See for example Section 3.1.4 of the Code of Conduct for SaaS.

[68] See Section 5.2 DP02 of the Code of Conduct for IaaS.

[69] Section 1.3 of the Code of Conduct for IaaS

[70] See Section 3.2.9 et seq. of the Code of Conduct for SaaS.

[71] Section 1.4 and 3.3 of the Code of Conduct for IaaS, section 3.1.5 of the Code of Conduct for SaaS

proceedings based on a breach of the governance agreement between the service provider and SWIPO AISBL.

2.2. Effectiveness of the instruments from directly applicable EU legislation within the field of free flow of non-personal data

The impact of the RFFFND on addressing vendor lock-in cannot be predicted in this article because the RFFFND provides us with no normative certainty as it is based on self-regulation. Analyzing the probability of success of this solution is an economic rather than a legal question. The statement that the RFFFND counters vendor lock-in practices, provided in the Guidance on the Regulation on a framework for the free flow of non-personal data in the EU, must be taken with a pinch of salt. At a later point, the same document proclaims that the RFFFND provides incentives for the industry to promote the possibility of switching of service providers and data migration; this statement is much more precise.[72]

The RFFFND was written and adopted based on several public consultations.[73] During the public consultations, 56.8% of the respondents from the group of small and medium-sized enterprises answered that they ran into trouble when they attempted to change service providers. This percentage is even higher than the overall percentage of 42% for the occurrence of ICT vendor lock-in across the EU in the study mentioned in Chapter 1 of this article.

As for the potential of the RFFFND, it is fair to say that thanks to the RFFFND, vendor lock-in is expressly mentioned in directly applicable regulation of significant importance. This promotes awareness of the vendor lock-in problem in the area of data migration and may increase the number of situations in which users and professional users will require vendors to provide them with effective anti-vendor lock-in solutions.

Moreover, taking into account the possibility of rising pressure from the industry (as the problem of vendor lock-in will become more known and maybe also more urgent), as well as the possibility that the European lawmaker introduces stricter measures in the future, the potential of the framework introduced by the RFFFND becomes even more significant. This is also borne out by the following facts: Firstly, the RFFFND governs, as expressly acknowledged in Recital 17 of the Regulation, *all* types of IT systems as well as *all* schemes for the provision of the services related to data processing. Therefore, it has the potential to affect a vast spectrum of data processing activities. Secondly, self-regulation allows the stakeholders to use the market's innovation potential and the

[72] See European Commission, 'Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', accessed 5 February 2021

[73] Petr Mišúr, 'Evropský parlament schválil nařízení o volném pohybu neosobních údajů v EU' (CH Beck 2018) 11-12 Obchodněprávní revue 333-342

experience and knowledge of service providers and professional users.[74] Applying these in codes of conduct can facilitate the right balance between the needs of users and the business practices of service providers.

As described above, adherence to the codes of conduct is voluntary, and the codes of conduct do not replace contracts between the service provider and the customer. In other words, if the contracting authority plans to rely on these codes of conduct, it generally needs to incorporate their terms and conditions in the agreement (for example, by reference) so that it can easily invoke these rules within civil proceedings in which it may be one of the involved parties.[75] Some national laws may consider non-compliance with the code of conduct also to constitute a breach of contract (or similar act), seeing as it is being taken into account during the conclusion of the agreement and, what is more, it can be understood as a public promise.[76] This is supported by the fact that the requirements stated in the codes shall apply at all times, as stated in these documents.[77] Nevertheless, this article is focused on EU law and thus will not analyze those instruments of national laws any further.

As mentioned in the previous subchapter, the codes of conduct introduce a number of requirements to achieve data portability, address the main scenarios in great detail and increase transparency. Thus, if the contractor adheres to one of these codes and at the same time the contracting authority links the code to the respective agreement (or otherwise ensures that the code is contractually binding), the code of conduct can be used as an effective tool to achieve data migration under transparent terms and conditions known before the conclusion of the contractual relationship for the original solution (to which the data migration is a follow-up service).

Returning now to the model case presented earlier, it is fair to say that, thanks to the rules introduced by the RFFFND, no requirements for localization practices should generally be introduced by national law which FBNF could use as an argument for not transferring the data to Portain. The data are currently stored in the cloud located in another member state, and there is no legal ground of this member state to limit the transfer to Portain (as the data does not relate

[74] This approach is also appropriate from the point of view of competition law. Thanks to self-regulation, the industry may come up with its own solutions. This creates incentives for innovation, which in turn may promote consumer welfare.

[75] According to the Code of Conduct for IaaS, the agreement shall determine the terms under which the data migration and switching of the cloud service is delivered. See Section 6.1 of the Code of Conduct for IaaS.

[76] See for example Section 1728 et seq. and Section 1733 of the Czech Civil Code: Act No. 89/2012 Coll.

[77] Section 6.1 of the Code of Conduct for IaaS and section 3.1.5 of the Code of Conduct for SaaS

to the public security of that member state). However, the RFFFND does not directly provide for any right of the contracting authority which could then be used to achieve data migration. As FBNF does not adhere to any of the codes of conduct, the contracting authority cannot rely on them. Thus, the only legal instrument in the area of free flow of non-personal data which the contracting authority can use as an *ex post* measure is the conclusion of an adequate agreement addressing this problem. Considering the announcement made by FBNF, it is unlikely that FBNF would enter into such an agreement.

In relation to codes of conduct, this article has identified several cases in which codes of conduct can serve as a ground to achieve data migration, and in which it is not necessary to use the negotiated procedure without prior publication or to repurchase the entire solution that is currently the subject of the vendor lock-in. Therefore, codes of conduct can be considered effective instruments; however, as we shall see, their reach is limited.

One may conclude that the existing instruments from directly applicable EU legislation can be effective provided that they are actually implemented by the industry. At this moment in time, the codes of conduct govern only cloud services. Thus, more codes have to be developed also to address other services relating to the processing of non-personal data. However, the main limitation is that the RFFFND does not introduce any right of the contracting authority which could be used as an *ex post* measure to address vendor lock-in *ex lege*. Thus, this framework (applicable only to non-personal data) is only effective if the contractor adheres to the respective code of conduct. If and to the extent that the industry does not voluntarily use these codes of conduct, additional measures should be introduced by the European lawmaker to increase the effectiveness of the RFFFND (and of the framework created by it).

In case self-regulation will be found insufficient, the effectiveness of the RFFFND in the area of free flow of non-personal data can be increased by amending it in such a way that processors of non-personal data shall have the duty (*qua* analogy to the right to data portability under Article 20 of the GDPR) to provide the controller (the user) with the data in a structured, commonly used and machine-readable format. This can be achieved, for example, by transforming the mandatory provisions of voluntary codes of conduct set out in Article 6 (1) of the RFFFND into mandatory requirements that are directly applicable based on the RFFFND without the need for additional steps to make these requirements binding for the processor of non-personal data. Moreover, the European lawmaker could introduce a rule to the effect that every code of conduct, once approved by the European Commission (or other authority), is binding *ex lege*. These approaches would ensure the user's legal and factual control over the data in a normative way.

3. Vendor lock-in in the area of personal data migration

The main legislation governing the processing and protection of personal data is the GDPR. This piece of legislation governing the processing of personal

data mainly focuses on protecting data subjects and their rights[78] (with a few exemptions)[79]. Thus, it protects mainly the interests of natural persons.[80] The GDPR governs only processing activities relating to personal data,[81] not to data in general. Therefore, it cannot be used to address vendor lock-in within the area of data migration in every case, but only within the specific area directly related to personal data.

The GDPR does not create any pathway to ownership of personal data.[82, 83] Instead, it lays down other rights of natural persons – data subjects[84] and governs data processing activities,[85] including the obligations relating to these activities.[86, 87]

The GDPR has been adopted based on Article 16 of the TFEU.[88] Article 16 aims at protecting individuals with regard to the processing of personal data (and to ensure the free movement of personal data within the EU – a so-called "double purpose"[89]). The main aim of the GDPR is to protect natural persons to whom the personal data relates – data subjects. This derives, for example, from Recitals 1 and 2 of the GDPR. It is also expressly stated in Article 1 of the GDPR. This means – and this fact should be highlighted – that the GDPR is not designed to protect legal persons or even specifically contracting authorities (and to address their problems in the area of vendor lock-in). However, the GDPR does provide data controllers (including contracting authorities) with certain rights. As stated in Recital 4 of the GDPR, the right to data protection *"(…) must be considered in relation to its function*

[78] See for example Recitals 1 and 2 of the GDPR.

[79] See Article 28 of the GDPR. While this article aims to empower the controller with rights against the processor, these rights are in fact designed to protect the interests of the data subjects.

[80] Article 4 (1) of the GDPR

[81] Article 1 of the GDPR

[82] See Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds) *Reinventing data protection?* (Springer 2009) 3-4.

[83] In relation to the right to data portability, see Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data portability and data control: Lessons for an emerging concept in EU law' (2018) 19 6 German Law Journal 1368, accessed 29 November 2020

[84] See Chapter III of the GDPR

[85] See Article 1 of the GDPR

[86] See for example Chapters II and IV of the GDPR

[87] As explained in the previous chapter, this fact should not not be understood as a limitation to the GDPR.

[88] Preamble to the GDPR

[89] Hielke Hijmans, 'Article 1 Subject-matter and objectives' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford 2020) 54

in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." In relation to this Recital, the GDPR states the legal grounds on which other entities (other than the data subjects) – controllers – can process personal data.[90] Nevertheless, these grounds are still formulated in a way that the main aim of the GDPR – to protect data subjects – is apparent. Specifically, the controller can process personal data only if the data subject has given consent or if the processing is necessary for one of the activities stated in Article 6 (1) letters b)-f) (and if at the same time other prescribed conditions are met).

Highlighting the chief objective of the GDPR in this article is not self-serving: In taking into account this chief objective, one may conclude that even if the GDPR introduces certain instruments which can be used to address vendor lock-in of the controller – the contracting authority, it still does so to protect the data subject, not the controller (though the possibility to use the given instrument by the controller in its favor can be a secondary outcome of the aim to protect the data subject). This knowledge will help us interpret some of the rules laid down in the GDPR and assess the possibilities for amending the GDPR.

The rules from the area of personal data migration which can be potentially used to address vendor lock-in (as will be analyzed below) include the duties related to the data processing agreement between the controller and the processor[91] and the right to data portability.[92]

These two instruments can help the controller achieve an adequate level of control over the data. This control is essential to achieve various aims relating to data processing.

If the data processing is based on consent – as per Article 6 (1) letter a) of the GDPR, it is likely that the data subject gives the consent to receive some advantage in return. In case the controller cannot control the data, granting this advantage may be in jeopardy. Similarly, if the data processing is necessary for the performance of a contract – as per Article 6 (1) letter b) of the GDPR, the data subject may be expected to have an interest in the performance of the contract. If the controller is unable to control the data, this might cause problems during the performance of the contract which, again, may adversely affect the data subject. Article 6 (1) letter d) of the GDPR in fact explicitly states that the protection of the vital interests of the data subject (or of another natural person) forms part of the legal ground to process personal data. Therefore, it will be generally in the interest of the data subject that the controller can actually control the data, especially if the data are processed based on Article 6 (1) letters a), b) or d) of the GDPR. This kind of reasoning could also apply to other legal grounds. After all, the controller is obliged to protect data against unauthorized or unlawful processing and against

[90] Article 6 of the GDPR

[91] See Article 28 of the GDPR

[92] Article 20 of the GDPR

accidental loss,[93] destruction, or damage.[94] To do so, an adequate level of control is required. It is also in line with the broad concept of the controller[95] aiming to ensure effective and complete protection of the people concerned, as stated in the Google Spain and Google[96] or Jehovah's Witnesses[97] judgments.

To sum up the previous paragraph, the control over the data exercised by the controllers can be beneficial for data subjects for two reasons in particular. Firstly, this control is often essential to achieve the aim of data processing (or related aims), which can be beneficial for the data subjects (e.g., to buy and verify online train tickets). Secondly, control is vital to ensure an adequate level of data protection.

Both aforementioned instruments will be analyzed in this chapter (each in a separate subchapter). In each of these subchapters, these instruments will be applied to solve the problem set out in the model case. Moreover, solutions *de lege ferenda* will be proposed. Based on the analysis, the extent to which the existing instruments under directly applicable EU legislation within the field of personal data protection are effective in addressing vendor lock-in in public procurement within the area of data migration will be evaluated. The effectiveness (and its extent) will be evaluated in the fourth subchapter.

There exists also a third instrument that could potentially be used in addressing vendor lock-in – the corrective powers of the data processing authorities. However, these powers can be used in this way only if the respective member state determines, in accordance with Article 58 (6) of the GDPR, that the data protection authority has additional corrective powers which can be used in this way. Given that this is an issue of national law, it will not be further discussed in this article.

3.1. Data processing agreement

According to Article 28 (3) of the GDPR, the controller and the processor shall conclude a data processing agreement (unless their relationship is governed

[93] It should be emphasized, also with regards to the aforementioned principles, that loss of (or loss of control over) personal data can be regarded as an undesirable phenomenon (see Recital No. 85 of the preamble to the GDPR) and should thus be avoided.

[94] Article 5 (1) letter f) of the GDPR. Office for Personal Data Protection (of the Czech Republic) Instruction No. UOOU-08449/16

[95] See Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018] para 27.

[96] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] para 34

[97] Case C-25/17 Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta [2014] para 66

by another legal act under EU or member state law). This agreement shall be in writing[98] and include several mandatory stipulations.[99] One of these stipulations may be used to address vendor lock-in.

A mandatory provision on which the controller may to a certain extent rely is stated in Article 28 (3) (g) of the GDPR, which provides that the data processing agreement shall include a stipulation to the effect that the processor is obliged, at the choice of the controller, to delete or return all personal data to the controller after the end of the provision of services relating to personal data processing. At the same time, the processor shall delete all existing copies unless required otherwise by applicable law. However, this provision may not be sufficient to achieve personal data migration in the required quality and time for two particular reasons.

The first reason is that the parties to the agreement are not obliged to agree on the format in which the personal data should be migrated. The problem here lies in the quality. The controller may receive the personal data in a format which it is unable to process or requires additional investments to be processed. Such investments may be necessary, for example, to convert the personal data, to purchase additional software to process the data in the relevant format or to train staff administering the data processing activities.

The relationship between the controller and the processor is generally a business-to-business relationship because the processor processes personal data on behalf of the controller. Thus, one could argue that some responsibility to further define the terms and conditions of the contract lies with the contractual parties.

Jenna Lindqvist notes that the legislation paradoxically focuses on controllers even though, in practice, the contractual terms of data processing agreements are often imposed by the processor on the client – the controller.[100] In any case, the regulation of personal data processing activities is based mainly on the controller's liability.[101] Thus, it would not be conceptually correct to make this kind of exemption. Indeed, it can be, in some cases, complicated for the controller to negotiate adequate terms to achieve data migration in the required quality (and also within the adequate timeframe). But putting the processor into the position of the entity primarily responsible for the conclusion of the data processing agreement would only increase the power of the processor in this regard. Hence, it is a missed opportunity that the lawmaker, in preparing the GDPR, did not draft

[98] Article 28 (9) of the GDPR

[99] Article 28 (3) of the GDPR

[100] Jenna Lindqvist, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (2018) 1 26 International Journal of Law and Information Technology 54, accessed 1 January 2021

[101] Article 5 (2) of the GDPR

the provisions of Article 28 governing the conclusion of the data processing agreement by analogy to the provision on the right to data portability.[102] This would have made the regulation conceptually sound and would have ensured that the controller faces no problem negotiating the minimum standards for portability.

The second reason why it may not be possible to achieve personal data migration (and to address vendor lock-in in the area of personal data migration) merely by adopting the required wording in the data processing agreement is that the processor is obliged to migrate the personal data only if the provision of services relating to data processing is terminated. This means that the controller cannot simply request copies of the processed personal data continuously or in advance – prior to the termination of the provided services. This again, as outlined above, can also threaten the interests of data subjects because the data subject often provides its data to the controller so the controller can process it in order for the data subjects to receive some value/service in exchange for the data (for example, taking into account our model case, the opportunity to use an IT system to book train tickets online).

Can the data processing agreement be used as an instrument to address the model case? Portain determines the purposes and the means of the processing activity – it is a controller. FBNF processes personal data on behalf of Portain – it is a processor. These parties concluded a data processing agreement. This agreement states only the mandatory provisions pursuant to the GDPR. Thus, it can be used by Portain to achieve data migration, but only of personal data (not of all data) and only at the end of the provision of the services relating to the processing. The format of data is not specified. Therefore, Portain cannot be sure whether it will be able to process the data (or to process it without significant investment) after it has received the data from FBNF.

Several *de lege ferenda* proposals could be made. For instance, one may want to amend the GDPR so that the parties to the data processing agreement are required to contractually agree on the format of the personal data that becomes subject to personal data migration. Of course, this amendment is desirable only if it increases the protection of data subjects as well. Without this amendment, controllers are dependent on the ability to implement sufficient and well-balanced *ex ante* contractual measures to prevent vendor lock-in within the area of personal data migration. However, as is apparent from the aforementioned surveys, contracting authorities are not particular successful in this discipline. It can jeopardize their ability to actually control the data, which, as explained above, can also negatively affect the interests of data subjects. Thus, this amendment has the

[102] The provision on the right to data portability established in Article 20 of the GDPR states the obligation to share the personal data "in a structured, commonly used and machine-readable format". Concerning the ability to process migrated personal data, this (or similar) language would provide for a higher level of legal certainty and of control over the "controller's" personal data.

potential to increase the level of protection of data subjects and can be in line with the main objective of the GDPR. Alternatively, the same duty could be stated by national acts governing personal data processing (or processing of data in general). National laws may pursue objectives other than those of the GDPR.

Moreover, it is important to note that the main provision stating the duty to conclude the data processing agreement has one major shortcoming. It does not state the parties' obligations in case no data processing agreement is concluded (contrary to applicable law).[103]

Again, to promote legal certainty and the possibility of the controller to exercise its control over the processing activities, it would have been better to amend the GDPR in a way that the essential rights and obligations of each party were stated directly by the GDPR, not indirectly by the duty to conclude an agreement. The parties could then be entitled to contractually adjust, within the stated scope and prescribed way, these rights and duties to address their needs. Thus, the GDPR would ensure a minimum level of control over the processed personal data, which could be increased further by a mutual agreement between the controller and the processor. There is no reason to argue that this approach would not be in line with the proportionality principle as set out in Article 5 of the TEU, because the respective duty is already enshrined in the current wording of the GDPR, and the proposed amendment would just change the way it is stated and applied. Similarly to the proposals mentioned above relating solely to the provision of Article 28 (3) (g) of the GDPR, this proposal could also be implemented by regulating the discussed obligations of each party in national acts.

3.2. Right to data portability

The right to data portability was introduced based on various queries of data subjects who were unable to obtain their personal data.[104] This newly

[103] It is important to emphasize that the origination of the relationship between the controller and the processor is not dependent on the existence of a written agreement containing a list of mandatory stipulations. It is dependent solely on the factual circumstances under which the controller determines, in the main, the purposes and means of the processing of personal data (see Article 4 (7) of the GDPR) and under which the processor processes these personal data on behalf of the controller (see Article 4 (8) of the GDPR. A relationship between the controller and the processor may arise even if the mandatory stipulations are not agreed upon between the parties at all or are agreed only partially. In such a case, the parties can be fined by the competent data protection authority (see Article 83 of the GDPR), but the controller cannot rely on obligations on which the parties did not agree.

[104] European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM(2010) 609 final 7, accessed on 26 April 2021

established[105] right is now stated in Article 20 of the GDPR. Its main objective is to improve the data subject's control over personal data.[106] In addition, it has a secondary rationale – to avoid vendor lock-in of the data subject.[107] The right to data portability gives the data subject the power to request and receive personal data concerning them. The controller shall provide the data subject with the personal data in a structured, commonly used, and machine-readable format.[108] According to the Article 29 Data Protection Working Party ("WP29"), the formats may vary across sectors. However, formats that require costly licensing constraints should not be deemed as meeting the requirements mentioned above.[109]

This right can be exercised on the basis of the GDPR, i.e., no additional documents, such as a written agreement, are required. At the same time, the basic requirements on the format of the personal data are normatively stated, which prevents any omission of the parties in this regard. The GDPR does not impose an obligation to use one specific format. Even though the requirements set out in the GDPR do not ensure that the data subjects (or the controllers) will receive the data in their *preferred* format, it at least provides them with a relatively high level of certainty that they will be able to process the data without high switching costs. In spite of all this, the right to data portability has still several significant limitations.

The most significant limitation of this right when addressing vendor lock-in in the area of personal data migration is the fact that the right to data portability is a right of the *data subject*, rather than of the controller. It serves the data subject.[110] Therefore, it can be used by the contracting authority only indirectly.

The data subject can exercise its right in person or via an authorized representative, for example, an attorney-at-law or other person based on power of attorney. The British regulator, i.e., the Information Commissioner's Office, expressly mentions the possibility of using a power of attorney to request personal data and data portability in its organizational document.[111] Thus, the contracting

---

[105] Stephanie Elfering, 'Unlocking the Right to Data Portability – An Analysis of the Interface with the Sui Generis Database Right' (2019) 18 Munich Intellectual Property Law Center - MIPLC Studies, accessed 29 November 2020

[106] ibid

[107] ibid, 19

[108] Article 20 (1) of the GDPR

[109] Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (2017) 17, accessed on 1 January 2021

[110] See Janis Wong and Tristan Henderson. 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR' (2019) 9 3 International Data Privacy Law 177, accessed on 26 April 2021.

[111] Information Commissioner's Office, 'Requests for personal data (SARs) & Data Portability', accessed on 26 April 2020. Audi even provides the data subjects with a

authority could ask the data subject for authorization to exercise the right to data portability on their behalf (or for exercising this right in a certain way). However, it may be complicated to motivate the data subject to use their right in a way that allows the contracting authority to achieve personal data migration.[112]

Another significant limitation is that the data subject can only request personal data from the controller, not from the processor. There are situations in which one entity is the controller and at the same time the processor of the same personal data. The occurrence of these situations, however, cannot be controlled by the contracting authority. Thus, the contracting authority cannot rely on the presumption that its contractor is in the role of the controller *and* the processor of all relevant personal data. This situation is improbable as the definitions of these roles are different. According to the legal classification of its role under the GDPR, the controller is generally an independent entity. However, the processor is always, to a certain extent, dependent on the controller. The reason for this is that the processor processes personal data on behalf of the controller.[113] Thus, there cannot be a processor without a controller. It is the controller who generally solely or jointly with others determines the purposes and means of the processing activity.[114] Nevertheless, provided that the contractor is both in the position of the controller and the processor in relation to certain personal data, the contracting authority may motivate the data subject to use its right to data portability and help the contracting authority get access to these data in a structured, commonly used and machine-readable format by exercising its right.

If the contractor is only the processor of the personal data relevant to the contracting authority, the contracting authority may motivate the data subject to exercise its right to data portability (by means of a request to the contracting authority) in order to transfer the data to another controller cooperating with this contracting authority. Provided that the data processing agreement has been duly concluded, the processor is obliged to cooperate with the controller so that the controller can respond to the request of the data subject.[115] Even though the

template power of attorney to authorize a representative to exercise data subject rights, including the right to data portability. Audi, 'Power of attorney: Rights of data subjects', accessed on 26 April 2021

[112] Hence, the contracting authority needs, for example, to use media campaigns or similar instruments to explain to the data subject why they should ask one entity to transfer the data to another.

[113] Article 4 (8) of the GDPR

[114] See Article 4 (7) of the GDPR and Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] para 34

[115] Article 28 (3) (e) of the GDPR

GDPR stipulates this duty using rather vague terminology,[116] one may reasonably expect the processor to be obliged, taking into account the nature of the processing, to assist the controller during the request of the data subject to migrate the personal data in a structured, commonly used and machine-readable format. Therefore, it should assist the controller also in converting the personal data to the required format. This conclusion is logical, as it is often the processor who is better equipped to administrate the data subject's requests.[117]

Unfortunately, the list of limitations to the right to data portability which reduce its power to address vendor lock-in in the area of personal data migration is rather extensive. The data subject can request the personal data only if the data was provided to the controller by this data subject, not by any other person.[118] At the same time, the data subject has the right to receive this personal data only if the processing is based on the consent of the data subject or on a contract to which the data subject is a party (or on the steps requested by the data subject in order to enter the contract).[119] As examples for situations in which this right can be exercised, WP 29 in its Guidelines on the right to data portability mentions data processing in relation to purchasing a book from an online bookstore or listening to songs via a streaming platform.[120, 121] The data subject has this right also in case the processing is carried out based on automated means.[122]

As we have seen, Portain is not a data subject but a controller. Thus, it has no right to data portability. It can only motivate the data subject to exercise this right (either in person or via granting power of attorney to Portain to do so). In this case, the data is provided to the controller by the data subject while purchasing the train tickets online. This situation is analogous to those described as examples for the processing of personal data for the purpose of performance of a contract in the Guidelines on the right to data portability. Thus, it can be concluded that the processing is necessary for the performance of the contract between the data subject and Portain. It means that the data subject can use its right to data portability.

---

[116] Jenna Lindqvist, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (2018) 1 26 International Journal of Law and Information Technology 56, accessed 1 January 2021

[117] ibid

[118] Article 20 (1) of the GDPR

[119] Article 20 (1) (a) of the GDPR

[120] Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (2017) 8, accessed on 1 June 2021

[121] These examples are of the same nature as the online purchase of train tickets. Thus, this activity described in the model case should also be subject to the right to data portability.

[122] Article 20 (1) (b) of the GDPR

The data subjects can make requests only toward controllers, not to processors. As FBNF does not hold the position of the controller with respect to the relevant data, the request to port the data can be made only to Portain. Because of this, it makes (in this particular case) no sense to ask the data subject to grant power of attorney to Portain. Thus, the only possibility to benefit from this right by Portain is to motivate the data subject to request Portain to port personal data to newly appointed processor(s). In such a case, the processor (FBNF) is, if the data processing agreement is duly concluded, obliged to cooperate with the controller (Portain) so that the controller can respond to the data subject's request. This situation results from the fact that the definition of the controller does not include the actual ability/possibility of the controller to control the data. Therefore, it can be responsible for the request even though it is technically or otherwise dependent on other entities. However, it is evident that this theoretical possibility is so complicated that it would be onerous to apply it in practice (especially if the problem concerns a high number of data subjects).

The possibility to use this right to data portability by the contracting authority would be significantly increased if the GDPR were amended in such a way that the right to data portability would not only be enjoyed by data subjects towards the controller but also by the controller towards the processor. This kind of amendment would provide the controllers with the same level of control over the data processed by the processors as the proposal related to the amendment of the applicable law in the area governing the conclusion of the data processing agreement (as described in the previous subchapter). I have already noted that this would well be in line with the stated objectives of the GDPR, as increased control over personal data exercised by the controllers can be beneficial also to data subjects. Alternatively, this right of the controller could also be stipulated by national acts.

3.3. Effectiveness of the instruments from directly applicable EU legislation within the field of personal data protection

For each of the two instruments analyzed in this chapter – the data processing agreement and the right to data portability – we have identified cases in which they can be used to achieve data migration. In those cases, it is not necessary to use negotiated procedure without prior publication or to repurchase the entire solution which is currently the subject of the vendor lock-in. Therefore, the instruments can be deemed effective, though only to a limited extent. The first limitation common to both of them is that they can only be used to address vendor lock-in within the area of personal data migration (as opposed to data migration in general). The other limitations derive mainly from the principal objective of the GDPR, which is to protect data subjects, not contracting authorities in the role of the controller.

The data protection agreement, in order to be used as an effective instrument, has to be, first of all, duly concluded (thus, similarly to codes of

conduct described in the previous chapter, it is partially also an *ex ante* measure). In case it is duly concluded and meets only the minimum GDPR requirements, it provides the contracting authority with the possibility to request the personal data only if and to the extent that the provision of services relating to data processing is terminated. At the same time, however, it does not provide the contracting authority with legal certainty as to the format of the migrated personal data unless the format is explicitly specified in the agreement between the parties. Even though the contracting authority can rely on the data processing agreement only in specific situations, it is the more effective instrument (compared to the right to data portability), as the data migration can be requested directly by the contracting authority without the need for further support by a third party.

The right to data portability can be deemed as effective for the purpose of allowing contracting authorities to address vendor lock-in in the area of personal data migration to the extent that the respective data subjects are willing to support the contracting authority in this endeavor. The data subject can request the personal data only if it has been provided by them and if at the same time the processing is based on consent or on a contract or if the processing is carried out by automated means.[123] Moreover, it can be used only when the contractor is also a controller of the respective personal data or if the personal data should be migrated to another controller cooperating with the contracting authority. The limitations of these instruments mean that it will be rather complicated in practice for contracting authorities to use them.

This chapter has made several proposals to amend the currently applicable legislation. These amendments to the GDPR or national acts would undoubtedly lead to a reduction of the risk of occurrence of vendor lock-in in the area of personal data migration, as they would allow the contracting authority in the role of the controller to exercise control over the processed personal data even without a written data processing agreement or without the need of cooperation on the part of the data subjects. Nevertheless, it is necessary to note that it is unlikely that the European lawmaker will accept these amendments. Arguments could be made why these amendments are aligned with the objectives of the GDPR, and some of them have been presented above, but I have not found any significant concerns in the academic literature (or similar documents) arguing that the current wording of the relevant GDPR provisions causes serious problems to data subjects – and the protection of rights of data controllers is *not* the aim of the GDPR. Amendments could however be implemented on a national level, as national laws may pursue other goals.

4. Competition law and vendor lock-in within the area of data migration

Competition law addresses, as the main areas of regulation (and prevention) within its purview, i) cartels, collusion, and other anti-competitive

[123] Article 20 (1) of the GDPR

practices;[124] ii) abuse of a dominant position;[125] iii) concentrations and iv) state aid[126]. In the introduction to this article, I've noted that where vendor lock-in occurs or appears to occur, and the given dependence manifests itself, bargaining power increases – more specifically, it increases unilaterally for the benefit of the contractor. Therefore, the only area of competition law which potentially allows us to address the problems deriving from the bargaining power of the contractor is the area governing abuse of a dominant position. The question relevant for the application of competition law (particularly the restrictions preventing abuse of a dominant position) is then whether the bargaining power of the contractor reaches a level that amounts to a dominant position within the relevant market. In other words, competition law can be used to address data portability issues in public procurement only if the contractor holds a dominant position and if its activities qualify as an abuse of such a position.

The first subchapter will analyze whether the relationship between the contracting authority and the contractor resulting in the need for a follow-up contract between the same parties creates a specific, relatively niche, relevant market. As it will be explained, such a qualification would mean that the contractor likely holds a dominant position, which it could abuse. A dominant position can be, of course, achieved also on markets of a different structure (e.g., because of the network effect[127]). This, however, is not specific to the area of public procurement and thus will not be elaborated further in this article.

The second subchapter will be devoted to analyzing the possibilities for abuse of a dominant position in the field of data migration in public procurement. Then, competition law will be applied to the model case. The third subchapter will be focused on the assessment of the effectiveness and its extent.

4.1. Follow-up contract and the market definition

Market definition is a prerequisite for determining whether an undertaking holds a dominant position or not.[128] It allows a comparison of the market power of a selected undertaking to the market powers of the rest of the undertakings operating within the same relevant market. The relevant market is a combination of product and geographic markets. It comprises all interchangeable or substitutable products or services within the area in which the undertakings providing the given goods and services operate and in which the conditions for

[124] 101 TFEU

[125] 102 TFEU

[126] 107 TFEU

[127] Emanuela Arezzo and Gustavo Ghidini, 'On the Intersection of IPRS and Competition Law with Regard to Information Technology Markets' (2006) 7, accessed 30 April 2021

[128] Case T-321/05 *AstraZeneca AB and AstraZeneca plc vs European Commision* [2010] paras 165-166, 174, 181, 187

the competition can be deemed as sufficiently homogenous.[129] Simply put, the relevant market is a "place" in which the relevant offer meets the customer's demand.

If vendor lock-in occurs and the contracting authority needs to purchase a follow-up solution (e.g., to migrate the data), the contracting authority has, in general, two options, as described in the introduction of this article. The first one is to conclude a follow-up contract with the original contractor (usually based on the negotiated procedure without prior publication). The second one is to bear high switching costs (which in general also include the costs for repurchasing the original solution, e.g., for obtaining/producing the data). The fact that the switching costs are so significant that they dissuade the contracting authority from switching to a new contractor represents the very nature of vendor lock-in, as the purchase options of the contracting authority are now tied.[130] Purchase of potentially substitutable products or services, if there is such a theoretical possibility, would result in spending such high costs that these products or services cannot actually be regarded as substitutes. These products or services would not meet the requirements of a hypothetical monopolist test.[131] This test evaluates whether consumers would switch their purchases from a hypothetical monopolist if this monopolist increased competitive prices by 5-10% (a small but significant non-transitory increase in prices – also known as the SSNIP test).[132]

While the original public procurement procedure can take place within a competitive relevant market, in case vendor lock-in occurs, the follow-up public procedure takes place on the market legally, technically, or otherwise limited.[133]

It has for instance been determined that one can distinguish between the market(s) for the sale of motor vehicles and separate repair and maintenance

[129] European Commission, 'Commission notice on the definition of relevant market for the purposes of Community competition law 97/C 372/03' (1997) paras 7-9

[130] Rajiv C. Shah, Jay P. Kesan and Andrew C Kennis, 'Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience' (2007) Illinois Public Law Research Paper No. 07-13, 7, accessed 5 September 2020

[131] For more information on the market definition, see Louis Kaplow, 'Market Definition and the Merger Guidelines' (2011) The Harvard John M. Olin Discussion Paper Series, accessed on 20 April 2021.

[132] For more information on the SSNIP test, see Andrea Amelio and Daniel Donath, 'Market definition in recent EC merger investigations: The role of empirical analysis' (2009) Concurrences Revue des droit la concurrence, accessed 20 April 2021.

[133] For more information on the reasons for the occurrence of vendor lock-in, see Bianca Sjoerdstra, 'Dealing with Vendor Lock-in' (University of Twente 2016) 3-7, accessed 5 September 2020

markets (often separate for each brand of motor vehicles).[134] In relation to access to data produced by connected vehicles (which are needed for repair and maintenance), Giles Warrington argues that if customers are effectively locked-in to the original equipped manufacturer, each of these manufacturers is likely to have its own aftermarket.[135] An analogy can be drawn to other areas and thus it can be concluded that the market of the original goods and services and the market for the follow-up – complementary goods and services can be separated into two markets: "original market" and aftermarket. It does not mean that the relevant markets for the original solution and the follow-up solution are always separated.

Generally speaking, if the contracting authority gives relatively significant consideration to the possibility that a follow-up contract will be needed in the future, it is likely that there is a single market. The reasoning is that the original and follow-up solution may be regarded as a complex solution demanded by the contracting authority. However, it is unlikely that vendor lock-in occurs in such a case, as the situation is expected by the contracting authority and thus taken into account by establishing sufficient preventive *ex ante* measures.[136] On the other hand, if the purchase of the follow-up solution occurs in new, relatively unexpected circumstances, the markets should be regarded as separate – an aftermarket is created, as the original and the follow-up solution are not mutually substitutable; they are complementary.

The limitations on the aftermarket when vendor lock-in occurs may be of such extent that there is only one undertaking which is able to offer the required goods or services (i.e., for the purpose of this article, the service of data migration). In this way, the market for the follow-up solution can actually be subject to a monopoly of the original contractor in this specific relationship, usually deriving from the contracting authority's choice made in the past.

The above conclusion is supported by the fact that, in a case of vendor lock-in, the contractor can, while negotiating the terms of the follow-up contract, act from a position of economic strength and behave to an appreciable extent

---

[134] Frank Wijckmans and Filip Tuytschaever, *Vertical Agreements in EU Competition Law* paras 11.172-11.180

[135] Giles Warrington, 'Competition law, data sharing and connected vehicles aftermarkets' (Pinsent Masons 2020), accessed on 25 April 2021

[136] Moreover, some initiatives seek to also forbid the abuse of relevant market power. One of these initiatives has been recently introduced in Switzerland. If adopted also in the EU, these rules could serve to address abuse of a position based upon which other companies depend on a particular undertaking with respect to the supply of given products or services (if there is no sufficient and reasonable possibility to change the contractor). See Marcel Meinhardt,
Astrid Waser and Benoît Merkt, 'New Swiss unilateral conduct rules significantly broadened' (Lexology, 2021), accessed on 26 April 2021.

independently of its competitors and customers (i.e., contracting authorities). Therefore, this situation meets the definition of a dominant position stated by the European Court of Justice ("ECJ") in United Brands judgement.[137]

Albert Sánchez Graells, in his book "Public procurement and the competition rules", devotes a relatively large amount of attention to the dominant position of a buyer.[138] If the contracting authority is a dominant buyer, it can likely resolve the problem of vendor lock-in by using its bargaining power deriving from its position. Nevertheless, the dominant position, as it will be explained below, must not be abused.[139] However, Graells also acknowledges the fact that the abuse of a dominant position can occur on the contractor's side and can be used against the contracting authority.[140] Hence, he does not specify the reasons for the emergence of a dominant position. This fact also indirectly confirms that the grounds for a dominant position may vary. Even though this article is focused on *ex post* measures addressing the occurrence of vendor lock-in within the area of data migration in public procurement, the outcomes of this chapter may be often used also when addressing other situations of abuses of a dominant position, e.g., an abuse of a dominant position relating to refuse to provide certain IP rights or other goods and services (even in the private sector).

To conclude this subchapter, if the contracting authority decides to demand a solution which is a follow-up solution to the previously purchased goods and services and finds itself in some form of vendor lock-in, it is likely that the markets for the original and follow-up solutions should be deemed to be separate markets. In this situation, taking into account the nature of vendor lock-in, it is likely that the original contractor holds a dominant position on the aftermarket. The dominant position of the contractor can, of course, also occur under other circumstances. The question of whether and under what circumstances the use of the bargaining practices of the contractor (while the contracting authority demands data migration) can be qualified as an abuse of a dominant position will be answered in the following subchapter.

4.2. Abuse of a dominant position and its qualification

Data is, in general, non-rival. This means that the same data can be available to (and processed by) several persons. At the same time, the quantity of data is not affected. This is why some scholars state that access to data, or in

[137] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECR 207

[138] Albert Sánchez Graells, *Public Procurement and the EU Competition Rules* (Hart Publishing 2011) 34, 61-64, 196

[139] 102 TFEU

[140] Albert Sánchez Graells, *Public Procurement and the EU Competition Rules* (Hart Publishing 2011) 196

particular to personal data, is not relevant for assessing market power.[141] Nevertheless, the fact that data is non-rival does not automatically mean that it is easily accessible,[142] and thus, its value can lie in particular in the ability to access and process it. Thus, data can be a relevant factor to determine dominance.[143] A dominant position relating to data thus can be based solely on access or also on other circumstances, such as the ability to convert the data, use it within databases, compile it with other data sets, transfer or otherwise process it. Moreover, dominance can also be based on a combination of these factors with other circumstances, which are not directly related to data.[144] For example, the Czech Office for the Protection of Competition concluded in the CHAPS case[145] that a dominant undertaking cannot, without objective justification, refuse to provide its competitors (intending to introduce a product for which these data were indispensable) with transport timetables, as this conduct qualifies as an abuse of a dominant position.[146]

Under Article 102 of the TFEU, any abuse of a dominant position within the internal market or a substantial part of it is prohibited. Determining what kind of activities/relevant markets meets the condition of "occurrence within a substantial part of the internal market" exceeds the scope of this article and thus will not be further elaborated upon. Nevertheless, we may at least note that basic criteria can be found in the Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, which among other things, state: *"If the dominant position covers part of a Member State that constitutes a substantial part of the common market and the abuse makes it more difficult for competitors from other Member States to gain access to the market where the undertaking is dominant, trade between Member States must normally be considered capable of being appreciably affected."*[147] The guidelines expressly mention regions, ports, or airports as examples for what may constitute

[141] Marixenia Davilla, 'Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules' 8 (2017) *Journal of European Competition Law & Practice* 378

[142] Thorsten Mäger and Philipp Otto Neideck, 'European Union – Data-related Abuse of Dominance' in Claire Jeffs (ed), *E-Commerce Competition Enforcement Guide* (Global Competition Review 2018), accessed 30 April 2021

[143] ibid

[144] ibid

[145] Office for Personal Data Protection (of the Czech Republic) R12/2016/HS-01402/2018/310/HBt (2018)

[146] This decision was annulled by the Regional Court in Brno, but on strictly procedural grounds. The findings relating to substantive law are still relevant.

[147] Commission Notice – Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty [2004] OJ C101/81, para 97

a substantial part of the internal market.[148] Thus, where this article speaks of abuse of a dominant position, it is always presumed that the aforementioned condition is met. Moreover, even if this were not the case, the national completion law would still apply. As it is generally modeled on EU competition rules, similar concepts will apply also to "local" markets.[149]

Article 102 of the TFEU provides a non-exhaustive list of possible abuses of a dominant position. Concerning the nature of lock-in described above, three types of abuse may be of particular relevance: excessive pricing, unfair terms, and refusal to deal. These abuses can appear during the negotiation of the follow-up contract with the contractor which provided the original solution but are not limited to such cases. The given conduct is not forbidden only if the dominant undertaking demonstrates that it produces efficiencies that outweigh the negative effects (e.g. if it is objectively necessary to provide the given service, or it is a loss-minimizing reaction to competition from other undertakings).[150, 151]

4.2.1 Unfair conditions and excessive pricing

According to Article 102 a) of the TFEU, it is prohibited for a dominant undertaking to directly or indirectly impose unfair trading conditions or prices. Unfair conditions may serve as a ground to create vendor lock-in. Based on these trading conditions, the contracting authority can be prohibited from including some *ex post* measures within the contract or can be actually forced to include stipulations increasing the probability that vendor lock-in will actually occur. Thus, in this case, the contractor has the dominant position already in the market for the original solution and is able to use its bargaining position to adjust the terms (which are otherwise, by default, defined by the contracting authority) of the contract eventually resulting in vendor lock-in.[152]

Article 102 a) of the TFEU concerns those terms which an undertaking without dominance is not able to impose on its customers – but the dominant

[148] ibid, para 98

[149] See for example Section 10 et seq. of Czech Act No. 143/2001 Coll.

[150] European Commission, 'DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses' (2005) para 5.5

[151] A certain degree of lock-in may serve as an incentive to innovation. See Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335, 340, accessed 30 April 2021

[152] World Law Direct explicitly mentions vendor lock-in as prohibited anti-competitive behavior. See World Law Direct 'Prohibited Anti-Competitive Behavior', accessed 22 June 2021

undertaking is.[153] The test to assess whether the imposition of these kinds of terms qualifies as an abuse of dominant position or not was firstly established in BRT/SABAM[154]. It is focused on the criterion of necessity (the imposition of certain terms does not qualify as an abuse of a dominant position if it is absolutely necessary in relation to the subject matter of the contract). This test was later elaborated in GEMA II[155], Tetra Pak II[156] and AAMS[157]. In accordance with the later decisions, one needs to assess whether the term in question is reasonably necessary and, at a second stage, whether the term is reasonable taking into account also the legitimate interests of the dominant undertaking, other concerned parties, and especially customers.[158] This test was subsequently detailed in DSD.[159] According to this decision, it is necessary to establish whether the term is central to the subject matter of the contract and, at a second stage, to determine whether it is proportionate.

Thus, if the contractor is a dominant undertaking which imposes on the contracting authority terms resulting in vendor lock-in and these terms are not central to the subject matter of the contract (which is likely, as limitation of data migration is not usually essential in this regard) and at the same time proportionate, the contractor abuses its dominant position, which is forbidden. In such a case, the competition authority may initiate proceedings with FBNF, incl. the imposition of a fine up to 10% (or more if permitted under national law) of FBNF's worldwide turnover and call upon it to adjust the contentious terms.[160]

The problem of excessive pricing may arise because the contractor, motivated as it is by financial gain, will tend to charge the highest possible price for data migration when this service is demanded on the aftermarket. In case of vendor lock-in, it is fair to conclude, from the economic perspective, that this highest possible price is the one which does not exceed the amount of the potential switching costs of the contracting authority (or that at least does not exceed them by more than 5-10%, in accordance with the SSNIP test criteria). Otherwise, the

---

[153] Robert O'Donoghue and Jorge Padilla, *The Law and Economics of Article 102 TFEU* (3rd edn, Hart Publishing 2020) 1023

[154] Case 127/73 *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior* [1974] ECR 51

[155] *GEMA II* (Case IV/29.971) Commission Decision 82/204/EEC [1981] OJ *L94/12*

[156] Case C-333/94 P *Tetra Pak International SA v Commission of the European Communities* [1996] ECR I-5951

[157] Case T-139/98 *Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission of the European Communities* [2001] ECR II-3413

[158] Robert O'Donoghue and Jorge Padilla, *The Law and Economics of Article 102 TFEU* (3rd edn, Hart Publishing 2020) 1033-1037

[159] *DSD* (Case COMP D3/34493 — DSD) Commission Decision 2001/463/EEC [2001] OJ *L166*

[160] Article 15 of Directive (EU) 2019/1

contractor would be at risk that the contracting authority decides for another solution. This, of course, applies only if the contracting authority does not intend to purchase more follow-up solutions. If more follow-up solutions are planned/expected, additional aspects should be considered and calculated. It could be more economical to cover "one-time" switching costs to quit the vendor lock-in relationship for a more open one, as this decision can lead to savings in the future when follow-up solutions will be purchased on a competitive market with more undertakings being able to offer the solutions sought.

Does a contractor's tendency to set a high price for migrating the data because it is the only undertaking which can offer the demanded solution, qualify as excessive pricing? First of all, it is necessary to state that, in general, the threshold for intervening with excessive pricing is relatively high.[161] Moreover, it is not the objective of competition law to set specific price levels.[162] Therefore, the assessment has to be done on a case-by-case basis.

To assess whether the activity outlined above amounts to excessive pricing, the difference between the undertaking's (potential) costs and its income should be investigated. If suspicion of excessive pricing arises, the observations made in this step may lead to further investigation. As part of this investigation, the price level set by the contractor for the contracting authority can be compared to the price level on another comparable relevant market as a benchmark.[163] Finding comparable relevant markets when addressing the vendor lock-in problem should in general not be hard, as they can be markets with the same product or service (in our case, the service of data migration) in which competition is not restricted by the previous choice of the contracting authority. They are markets where the legal, technical or other restrictions resulting in vendor lock-in do not apply. The ECJ firstly introduced this two-stage test in the previously mentioned United Brands case.[164] However, it is necessary to note that a mere comparison may not be sufficient, as the different price levels can be caused by objective conditions applicable within the relevant market. Thus, it might also be necessary to take into account additional criteria.[165]

Three outcomes to this investigation are possible. Firstly, the investigation may reveal that the price level is comparable to the price level within similar (competitive) relevant markets. That would mean that even if vendor lock-in is

[161] 'Types of abuse of dominant position related to pricing' (Finnish Competition and Consumer Authority 2014), accessed on 27 April 2021

[162] ibid

[163] ibid

[164] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECR 207

[165] Case C-177/16 *Autortiesību un komunicēšanās konsultāciju aģentūra / Latvijas Autoru apvienība v Konkurences padome* (ECJ, 14 September 2017), paras 42-45

present (as the purchase choices of the contracting authority are tied), it does not (from this point of view) represent a problem. The follow-up contract can be still efficient; efficiency in public spending on data migration can be ensured.

Secondly, the investigation may show that the price level set by the contractor is higher compared to the similar (competitive) market, but not excessively so. This would be a problem, as the contracting authority is not able to ensure efficiency in public spending. However, competition law does not provide us with any *ex post* measure to address this situation.

The third possible outcome is that the investigation actually shows that the price level is excessive, which is forbidden. Under these circumstances, the competition authority may initiate proceedings with FBNF, including the imposition of a fine of up to 10% (or more if permitted under national law) of FBNF's worldwide turnover and call upon it to lower the price.[166]

Looking at the model case of Portain and FBNF, it becomes evident that some information in relation to FBNF's market share for operating the routes is available. However, as the problem here lies specifically within the area of data portability, this information will likely not be sufficient, as the relevant market for the data migration service and for the provision of data itself would be almost certainly considered as separated from the original one – as an aftermarket. It is fair to assume that the data will be so unique that there are no substitutes. This would mean that FBNF holds a monopoly and a dominant position (especially as the barriers to gaining data of this specific character are high).

We do not know whether the terms of development and administration of the IT system were subject to the parties' negotiations. If the terms were stated on a take-it-or-leave-it basis by Portain, FBNF certainly did not impose unfair conditions on Portain in this regard.

However, if FBNF used its dominant position on the original market in such a way that it did not allow Portain to implement *ex ante* measures to achieve data migration, this conduct might qualify as abuse of a dominant position. The conduct will be found abusive if the terms are not central to the subject matter of the contract (which is unlikely in this situation, as there is no objective justification to limit the data migration – other than to create a vendor lock-in affecting Portain) and at the same time proportionate. Such conduct is forbidden, and thus Portain can seek protection with the competition authority.

In considering the possibility that the conduct of FBNF falls within the definition of excessive pricing, it is necessary to note that FBNF does not aim to charge Portain excessive prices for the provision of the data to Portain or other competitors. It uses the control over this data as a bargaining strategy to be the only company operating all the mandatory routes in Portain in the future. This means that its activity cannot qualify as an abuse of a dominant position by excessive pricing.

[166] Article 15 of Directive (EU) 2019/1

4.2.2 Refusal to deal

The third type of abuse which might be relevant for the situation of vendor lock-in within the area of data migration is a refusal to deal.[167] A dominant undertaking can generally choose with whom (and on what terms) it conducts business. However, under exceptional circumstances, it cannot refuse to deal with other undertakings. The test to determine when the dominant undertaking is obliged to engage with the other party has been developed in case law, particularly in Magill[168], Bronner,[169] IMS Health,[170] and Microsoft[171]. The Microsoft case dealt with a situation in which Microsoft refused to provide Sun Microsystems with the necessary information to optimize software of Sun Microsystems to ensure interoperability with Microsoft's operating system software. As the core of this case lies in the provision of information, the test applicable there should also be sufficient to address the relatively similar problem of data migration.

According to the Microsoft ruling, for certain conduct (refusal to share certain information) to qualify as a refusal to deal and thus as an abuse of a dominant position, it has to meet the following criteria: i) the information has to be indispensable for competition, ii) refusal excludes effective competition on the secondary market, iii) the refusal prevents the emergence of a new product and iv) the refusal to provide the information (i.e., to license it) is not objectively justified. It should be noted that this case was based on the presumption that the information is protected by IP rights.[172] Lacking this kind of protection can result in a situation in which it may be easier for the competitor to attain knowledge of the information and so no intervention using competition law concepts is needed. On the other hand, such intervention of competition law may be even "easier", as there would be no risk of a conflict between the aims of IP rights protection and competition law. Moreover, the test applied in non-IP cases[173] does not contain the

[167] For more information on the refusal to deal see Liyang Hou, 'Refusal to Deal within EU Competition Law' (2010) SSRN Electronic Journal, accessed 30 April 2021.

[168] Joined cases C-241/91 P and C-242/91 *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities* [1995] ECR II-575

[169] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG.* [1998] ECR I-7791

[170] Case C-481/01 *IMS Health GmbH & Co OHG v. NDC Health GmbH & Co KG* [2004] ECR I-5039

[171] Case T-201/04 *Microsoft Corp. v Commission of the European Communities* [2007] ECR II-3601

[172] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG.* [1998] ECR I-7791

[173] ibid

criterion of prevention of the emergence of a new product. Thus, it might be even easier to conclude that certain conduct qualifies as an abuse of a dominant position also from this point of view.

In this part of the article, it is appropriate to take a closer look especially at the indispensability criterion, as its interpretation can be affected by the fact that the given problem relates to data processing. Indispensability can be defined as the lack of a realistic potential alternative. Indispensability is established if it is not economically viable to create a second product comparable to the relevant existing one.[174] There are cases in which the contractor collects the data for several years. It might be, for example, personal data of customers, logistic data, or data on production efficiency. In these cases, it is likely that the value of these data sets increases as more and more data is collected. If vendor lock-in in the area of data migration occurs, it is likely that it would not be economically viable to collect certain data sets once again. Moreover, often it will be almost impossible to collect the same (or comparable) data sets. Portain (more precisely, the new railway companies interested in operating the mandatory routes), for example, needs the data of users who have bought the tickets which are valid for 24 months and registered via a personal account of the traveler. The Czech Republic recently introduced the option to buy the mandatory highway stickers online. In this case, the Czech Republic (or a company administering this kind of service) needs exactly the data set enabling it to identify the cars allowed to use the highway. No other data set can replace it. Thus, it is possible to identify cases in which the data (which is subject to a data migration request/demand on a market where the contractor is a dominant undertaking) can be found indispensable. This was also the case of the already mentioned CHAPS decision.

Nevertheless, it should be noted that in this type of abuse, it is not the contracting authority who can claim the duty of the contractor to deal, but the potential direct competitors of the contractor. Firstly, the competitors are the undertakings that are mainly affected on the secondary market. Secondly, the contractor wishes to deal with the contracting authority (as this may lead to profit for the contractor). The problem is that the contractor does not wish to deal with its competitors, and so these competitors cannot offer their goods or services to the contracting authority. Thus, to rely on this limitation of abuse of a dominant position, the contractor's competitors have to be actually interested in receiving the data in question.

Applying the analysis above on the model case, we find that FBNF refuses to provide the data to other competitors. Thus, if the relevant test stated in the Microsoft judgement is met, the current approach of FBNF can qualify as a refusal to deal. This means that FBNF can be obliged to share the data with competitors.

[174] ibid, paras 45-46

4.3 Effectiveness of the instruments from directly applicable EU legislation within the field of competition law

To conclude this chapter, competition law can serve as a tool to address vendor lock-in in the area of data migration. Several scenarios in which competition law can intervene and be used as an *ex post* measure to address vendor lock-in within the area of data migration in public procurement have been described in this chapter. In these scenarios, competition law provides us with tools to achieve data migration in a way exceeding the efficiency benchmark stated above in the introduction to this article. Thus, Article 102 of the TFEU which forbids the abuse of a dominant position can be found effective for this purpose, though to a limited extent. Conduct relating to the vendor lock-in can, if the required tests are met, qualify in particular as the imposition of unfair terms, excessive pricing, or refusal to deal.

The limits of effectiveness result from the tests described above. Thus, competition law is effective in addressing vendor lock-in within the area of data migration in public procurement to the extent to which the contractor holds a dominant position and its activities qualify as an abuse of this position. Only a limited set of specific situations can be resolved based on competition law. On the other hand, when we compare these rules with rules governing personal data and non-personal data, we find that competition law has the advantage of applying to activities dealing with all types of data and information.

5. Conclusion

This article is devoted to an analysis of the extent to which the existing instruments from directly applicable EU legislation within the field of free flow of non-personal data, personal data protection, and competition law are effective in addressing vendor lock-in in public procurement within the area of data migration. The introduction to this article has described how the rules governing public procurement as their primary regulatory subject in principle allow one to address vendor lock-in which has already manifested itself, by use of the negotiated procedure without prior publication or by repurchasing the entire solution which is currently the subject of the vendor lock-in. As the article is focused on *ex post* measures, the existing instruments (i.e., the legal possibilities introduced by current legislation to address the given problem) have been deemed effective only insofar as they serve as a basis for successful data migration even in the absence of a comprehensive contractual arrangement between the parties, provided further that they are more effective than the benchmark represented by the possibilities given by public procurement law. The extent of the effectiveness has been assessed as the set of the situations (and its limitations) in which these instruments can be applied.

The first chapter is focused on the field of free flow of non-personal data. This chapter found that the RFFFND, while introduced as a reaction to vendor lock-in, creates no normative certainty because it states no direct obligations. The

RFFFND establishes a self-regulatory framework. Based on this framework, the European Commission shall encourage self-regulatory activities in the form of codes of conduct. As of today, two codes of conduct have been introduced: the Code of Conduct for IaaS and the Code of Conduct for SaaS. Both of them stipulate relatively extensive obligations of the providers in relation to portability requirements and transparency. The identified situations in which contracting authorities can rely on one of these codes are those in which a contracting authority aims to migrate non-personal data. For this to be possible in the first place, the provider must have agreed to adhere to one of these codes (and must be contractually or otherwise obliged to comply with the rules set out therein). Thus, while this framework has the potential to be effective in addressing vendor lock-in, it has some limitations.

As to the extent of the effectiveness of the codes of conduct based on the RFFFND, it is fair to say that they are only effective to achieve migration of non-personal data (as opposed to data in general). Moreover, these codes are not binding *ex lege* (and the RFFFND does not state any *ex lege* alternative to achieve data migration otherwise than based on these codes). Thus, these codes are effective only to the extent that the contractor adheres to them. Hence, these codes cannot qualify as pure *ex lege* measures – they partially qualify also as *ex ante* measures. As the European lawmaker has opted for a self-regulatory approach, the extent of the effectiveness will be big only if the industry broadly accepts the codes of conduct and if additional codes of conduct are introduced that will govern also other business relationships.

The second chapter is devoted to the field of personal data. In this chapter, two instruments have been identified as effective in achieving data migration: the data processing agreement and the right to data portability. The contracting authority can only rely on these instruments if it wishes to migrate *personal* data. A data processing agreement can obviously only be invoked if one was concluded in the first place. Thus, it is not a pure *ex post* measure. To rely on the right to data portability, the contracting authority needs cooperation from the data subjects because this right is a right of the data subject. It may therefore be complicated for the contracting authority to benefit from this right in practice. Thus, it is evident that even though these instruments can be effective in some situations as described above, the extent of their effectiveness is significantly limited (as these situations are very specific). Most of the limitations are caused by the fact that the GDPR, which is the regulation establishing these instruments, aims to protect data subjects, not contracting authorities in the role of controllers. Therefore, the possibility to use the given instrument by the contracting authority in its favor can only be a secondary outcome of the main objective of the GDPR – to protect the data subjects.

The third chapter addresses the topic of competition law, in particular its tools designed to restrict abuse of a dominant position. In this chapter, we found that demand for data migration in case a vendor lock-in has (at least seemingly)

occurred, likely meets an offer on the aftermarket on which the original contractor (for the solution to which the data migration relates) holds a dominant position. We then identified the three types of abuse of a dominant position which may be relevant in the area of data migration. These are, in turn, unfair conditions, excessive pricing, and refusal to deal. All these kinds of conduct are forbidden (unless they can be objectively justified in the individual case). In relation to each of them, the legal measures to prevent abuse of a dominant position can serve as grounds to achieve data migration and so they can be deemed effective in addressing data migration. They are effective to a limited extent, in that they presuppose that the contractor holds a dominant position and its conduct relating to data migration qualifies as an abuse of this position under the respective tests.

As for unfair conditions, one must assess in particular whether the respective term (which might cause vendor lock-in) is central to the subject matter of the contract and, in the second stage, to determine whether it is proportionate. If not, the dominant undertaking imposing this term generally abuses its dominant position. To assess whether certain activities amount to excessive pricing, the difference between the undertaking's (potential) costs and its income must be investigated. If this initial assessment raises suspicion of excessive pricing, further investigation is required. As part of this investigation, the price level set by the contractor for the contracting authority can be compared to the price level on another, comparable relevant market. For a certain kind of conduct to qualify as a refusal to deal in products protected by intellectual property rights, it must meet the following criteria: i) it has to be indispensable for competition, ii) the refusal excludes effective competition on the secondary market, iii) the refusal prevents the emergence of a new product and iv) the refusal to provide the product is not objectively justified. (The test applied in non-IP cases does not contain the criterion that refusal prevents the emergence of a new product.)

If one compares the current instruments in the field of competition law to those mentioned in previous chapters, one may conclude that their effectiveness is the highest as they apply *ex lege* (no further action, such as adopting certain standards by the industry, is needed); what is more, the contracting authority generally does not need any other party to initiate administrative proceedings to achieve data migration with the competition authority. Even so, if the given contractor does not comply with competition law, the competition authority or a court must first impose the relevant remedy before the contracting authority can access the data.

This article should have made it evident that existing instruments from directly applicable EU legislation within the field of free flow of non-personal data, personal data protection, and competition law can only be effective in specific situations when it comes to addressing vendor lock-in within the area of data migration. While the measures discussed in this article can be used in the practice of contracting authorities, they cannot be applied in every case in which vendor lock-in occurs.

Considering the model case used in this article, contracting authorities may use the information provided herein to control their data, for example, in the field of public transport. However, this article has shown that in order to have a legal framework which can be effective (without significant limitations) in addressing vendor lock-in, amendments to current legislation are needed. As the aim of this article was not to propose solutions *de lege ferenda*, the amendments have been proposed in a rather cursory manner. While this article can serve as a basis for such subsequent legislative changes, it will be necessary, as part of the preparatory steps, to precisely analyze how and at what level (whether on the EU or national level, general or sectoral) these amendments should be adopted (such that the amendments are effective and at the same time proportional).

I sincerely hope that this article will have made a worthwhile contribution, however modest and preliminary in scope, to reducing the phenomenon of vendor lock-in. At the same time, I would like to believe that it may also contribute to increasing efficiency in the area of public procurement.[175]

Bibliography

Amelio A and Donath D, 'Market definition in recent EC merger investigations: The role of empirical analysis' (2009) Concurrences Revue des droit la concurrence, accessed 20 April 2021

Andhov M, (Andrecka N), 'Contracting Authorities and Strategic Goals of Public Procurement – A Relationship Defined by Discretion?' in Sanja Bogojević, Xavier Groussot and Jörgen Hettne (eds), *Discretion in EU Public Procurement Law* (Hart Publishing 2018)

Arezzo E and Ghidini G, 'On the Intersection of IPRS and Competition Law with Regard to Information Technology Markets' (2006), accessed 30 April 2021

Audi, 'Power of attorney: Rights of data subjects', accessed on 26 April 2021

Banda C, 'Enforcing Data Portability in the Context of EU Competition Law and the GDPR' (2017) MIPLC Master Thesis Series (2016/17), accessed 29 November 2020

Chýle J, 'Jaké otázky si klást v IT veřejných zakázkách před zahájením migrace dat a problematika vendor lock-in' (2017) Informační list 2017 - Zakázkové právo v oblasti ICT a další aktuální témata, accessed 29 November 2020.

Davilla M, 'Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules' (2017) *Journal of European Competition Law & Practice*

[175] This article is based on the author's LLM thesis defended at Tilburg University.

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds) *Reinventing data protection?* (Springer 2009)

Druey JN, 'Information Cannot Be Owned: There is More a Difference than Many Think' (2004) Harvard Law School Public Law Research Paper Series, Research Paper no 96

Dvořák D and others, *Zákon o zadávání veřejných zakázek: Komentář* (CH Beck 2017)

Elfering S, 'Unlocking the Right to Data Portability – An Analysis of the Interface with the Sui Generis Database Right' (2019) 38 Munich Intellectual Property Law Center - MIPLC Studies, accessed 29 November 2020

Graef I, Husovec M and Purtova N, 'Data portability and data control: Lessons for an emerging concept in EU law' (2018) 19 6 German Law Journal, accessed 29 November 2020

Graells AS, *Public Procurement and the EU Competition Rules* (Hart Publishing 2011)

Herrera S and Ouedraogo A, 'Efficiency of Public Spending in Education, Health, and Infrastructure – An International Benchmarking Exercise' (Word Bank Group 2018), accessed 4 January 2021

Hijmans H, 'Article 1 Subject-matter and objectives' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford 2020)

Hou L, 'Refusal to Deal within EU Competition Law' (2010) SSRN Electronic Journal, accessed 30 April 2021

Kaplow L, 'Market Definition and the Merger Guidelines' (2011) The Harvard John M. Olin Discussion Paper Series, accessed on 20 April 2021

Kelman S, 'Goals, Constraints, and the Design of a Public Procurement System' in *The Costs of Different Goals of Public Procurement* (Konkurrensverket 2012), accessed 4 January 2021

Lindqvist J, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (2018) 1 26 International Journal of Law and Information Technology, accessed 1 January 2021

Mäger T and Neideck PO, 'European Union – Data-related Abuse of Dominance' in Claire Jeffs (ed), *E-Commerce Competition Enforcement Guide* (Global Competition Review 2018), accessed 30 April 2021

Meinhardt M, Waser A and Merkt B, 'New Swiss unilateral conduct rules significantly broadened' (Lexology, 2021), accessed on 26 April 2021

Míšek J, *Moderní regulatorní metody ochrany osobních údajů* (Masarykova univerzita 2020)

Mišúr P, 'Evropský parlament schválil nařízení o volném pohybu neosobních údajů v EU' (CH Beck 2018) Obchodněprávní revue

O'Donoghue R and Padilla J, *The Law and Economics of Article 102 TFEU* (3rd edn, Hart Publishing 2020)

Opara-Martins J, Sahandi R and Tian F, 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective' (2016), accessed 5 September 2020

Purtova N, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?' (2017) Tilburg Law School Legal Studies Research Paper Series No. 21/2017, accessed on 2 February 2021

Ritter J and Mayer A, 'Regulating data as property, a new construct for moving forward' (2018) Duke Law & Technology Review 1 16, accessed 2 February 2021

Shah RC, Kesan JP and Kennis AC, 'Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience' (2007) Illinois Public Law Research Paper No. 07-13, accessed 5 September 2020

Sjoerdstra B, 'Dealing with Vendor Lock-in' (University of Twente 2016), accessed 5 September 2020

Sventesson D and Polčák R *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law* Edward Elgar Publishing 2017)

Svoboda J, 'Veřejné zakázky v oblasti ICT a problém závislosti zadavatele' (2019) 10 19 Revue pro právo a technologie, accessed 14 November 2020

SWIPO, 'About SWIPO', accessed 21 April 2021

SWIPO, 'SWIPO codes published', accessed 29 November 2020

Swire P and Lagos Y, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review, accessed 30 April 2021

'Types of abuse of dominant position related to pricing' (Finnish Competition and Consumer Authority 2014), accessed on 27 April 2021

Vévoda P, 'Data obsažená v IT systémech, jejich vlastnictví a zakázkové právo' (2017) Zakázkové právo v oblasti ICT a další aktuální témata - Informační list 1 17, accessed 5 February 2021

Warrington G, 'Competition law, data sharing and connected vehicles aftermarkets' (Pinsent Masons 2020), accessed on 25 April 2021

Wijckmans F and Tuytschaever F, *Vertical Agreements in EU Competition Law* (Oxford 2018)

Wong J and Henderson T. 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR' (2019) 9 3 International Data Privacy Law, accessed on 26 April 2021

World Law Direct 'Prohibited Anti-Competitive Behavior', accessed 22 June 2021

Zech H, 'A legal framework for a data economy in the European Digital Single Market: rights to use data' (2016) 11 6 Journal of Intellectual Property Law & Practice, accessed on 19 April 2021