EJLT European Journal of Law and Technology

Avoiding lock-in effects through obtaining all necessary licences before use of a SaaS solution in a public sector organisation: a case study

Björn Lundell, Jonas Gamalielsson, Andrew Katz, Mathias Lindroth*

Abstract

With increased adoption and use of cloud-based software-as-a-service (SaaS) solutions from international providers many public sector organisations expose themselves to a dependency on specific providers and a range of different lock-in effects. The article reports from a case study which investigated how a large Swedish public sector organisation addressed licensing issues and lock-in effects during adoption and use of a SaaS solution (Microsoft 365). The study identifies problematic licensing issues and presents a legal analysis related to the organisational implementation of the SaaS solution in the specific organisation. Findings show that the organisation has failed to successfully obtain all necessary licences and all necessary rights which would allow for long-term maintenance of all its digital assets independently of the SaaS solution currently in use.

* Björn Lundell and Jonas Gamalielsson are respectively Professor and Senior Lecturer in computer science, School of Informatics, University of Skövde, Sweden; Andrew Katz is Joint Managing Partner and Head of Technology Law at Moorcrofts LLP, Marlow, UK & visiting researcher at University of Skövde, Sweden; Mathias Lindroth is General Counsel, ACF Legal Intl AB, Sweden.

1. Introduction

Many organisations in the public sector are exposed to an increasing dependency on international providers of ICT solutions, and particularly cloud-based SaaS solutions (e.g. EC, 2020; eSam, 2021c; Försäkringskassan, 2019; GAIA, 2019; IMY, 2021, 2022; Lundell et al., 2016, 2020; Radar, 2019; Regeringskansliet, 2021; Skatteverket/Kronofogden, 2021a, 2021b).

The overarching goal of this paper is to report on how a large public sector organisation identifies and obtains all necessary licences for ensuring long-term maintenance of digital assets before use of a commercial SaaS solution provided by a global company. Specifically, the SaaS solution used by the public sector organisation which constitutes the context for the study is the Microsoft Office 365 solution[1] (hereafter referred to as 'M365', as we note that the solution was rebranded on 21 April 2020 when 'Office 365 became Microsoft 365' (Kaelin, 2020)).

Research shows that lock-in effects can impose many different types of technical, legal, economic and societal challenges for public sector organisations (Bekkers and Updegrove, 2013, p. 6; Blind and Böhm, 2019, p. 43; Contreras, 2015a, 2015b; EC, 2012, 2014a, 2014b; Egyedi, 2007; Egyedi and Hudson, 2005; Farrell and Klemperer, 2007; Ghosh, 2005; Katz, 2012; Kritikos et al., 2019; Lundell et al., 2016; Lundell et al., 2019; Mowbray, 2009; NPS, 2019). Further, the importance of avoiding lock-in effects and protecting digital sovereignty has been stressed by several large IT-intensive public sector organisations. For example, the Swedish Social Insurance Agency stresses the importance of reducing 'dependence on the provision of individual services by the private market' (Försäkringskassan, 2019) and the Swedish Tax Authority recognises the importance of avoiding lock-in effects related to potential adoption of SaaS solutions for video conferencing (Skatteverket/Kronofogden, 2021a, 2021b).

Over the years, many individuals, organisations and governments have taken various initiatives to strategically address problematic lock-in effects related to use of SaaS solutions. For example, policies and strategies for open standards have been published in several countries (e.g. Lundell et al., 2015; UK, 2012; NOC, 2007) and there are also initiatives and proposals addressing digital and data sovereignty (e.g. GAIA, 2019).

[1] When the study was initiated in 2017 the specific SaaS solution used by the public sector organisation was referred to as Microsoft Office 365.

Lock-in[2] is generally not a defined legal term. To cause lock-in, or becoming locked-in, is not illegal *per se*. The phenomenon of lock-in relates to several legal areas. For example, lock-in may be the result of breaches of competition law by the supplier, such as abuse of a dominant position. It may also arise from the customer's failure to fully comply with procurement law or regulations. In the case of public organisations in particular, it is virtually inevitable that lock-in leads to future infringements of procurement law, since the exit barriers so established make a fair and level tendering process impossible.

A commentary from the European Commission (EC, 2020) has highlighted the importance to the EU of 'technological sovereignty' and an extensive study undertaken on behalf of the Swedish Competition Authority which investigated current practice in IT projects undertaken in the public sector uncovered many examples of lock-in arising from both policy and practice related to adoption and use of cloud-based SaaS solutions in public sector organisations (Lundell et al., 2016).

In some countries, contemporary adoption and use of SaaS solutions by public sector organisations may seem a surprising development in light of previous policy initiatives. For example, the Swedish Government decided to establish a national delegation for e-Governance on 26 March 2009, and in so doing stressed the importance of utilising solutions based on open standards and open source software in order to avoid lock-in effects into specific platforms and solutions (Regeringen, 2009). In addition, in a public speech during the Swedish EU presidency on 5 November 2009, Mats Odell, then Swedish minister with responsibility for e-Governance, referred to the European Interoperability Framework version one (EC, 2004) when he stated that the 'use of open standards and open source solutions decreases the public sector's reliance on specific vendors and platforms' (Odell, 2009). Despite these initiatives in Sweden, in August 2019 it was reported that 88% of the 290 Swedish municipalities have undertaken a legal analysis on the use of cloud services and that all of the three largest cities in Sweden and about half of all municipalities used the M365 solution (Radar, 2019).

Contracting and licensing practices for SaaS solutions bring a range of potentially problematic issues. For example, it has long been known that contract amendment for

[2] Lock-in is said to occur whenever a switching to a potential competitor product is made more difficult by external factors. These may be human factors such as familiarity with the system's operation or user interface, development of internal work-arounds to tailor the system to a particular organisation's needs, or the natural desire to remain with the existing system since its shortcomings are at least known and understood: the devil you know. Other forms of lock-in may be technical, such as the file formats and APIs that a particular system uses not being compatible with a potential future replacement system. Lock-in is not unlawful *per se*, but it may in some circumstances have legal consequences. For example, lock-in imposed by a supplier may result in breaches of competition law, such as abuse of a dominant position. Lock-in may cause the customer to believe that there is, in practice, no alternative solution to that already implemented solution and thus lead to the customer's failure to fully comply with procurement law or regulations in seeking an alternative supplier.

SaaS solutions which are provided by global providers are often necessary 'because most contracts are indeed incomplete' (Aubert et al., 1998, p. 687). Moreover, previous research that investigated cloud computing established that even large purchasers face challenges related to 'missing contract terms or terms that are in conflict with' national law (McGillivray, 2016, p. 337). Based on a national review in the Swedish context, the National Audit Office (NAO) highlights that contract amendments can expose a public sector organisation to a number of risks, including unhealthy dependencies on its current supplier that can cause 'helplessness' for the customer (Riksrevisionen, 2011, p. 82). Also, based on recent dialogues between eSam (a group of public sector organisations[3]) and Microsoft concerning requirements for lawful and suitable SaaS solutions it was concluded by eSam that useful solutions are several years away in time. Further, public SaaS solutions offered by Microsoft would not fulfil eSam's requirements for lawful and useful solutions as detailed in a letter to Microsoft sent by the chair of eSam who is also the director general of the Swedish Tax Authority (eSam, 2021b). In addition, extensive investigations of a large number of projects undertaken by many different public sector organisations recognise that adoption and use of SaaS solutions provided by global providers typically involves dealing with complex and incomplete contracts which expose public sector organisations to a range of different lock-in effects (Lundell et al., 2016, 2019, 2020, 2021, 2022).

This paper reports from an investigation of the following research question:
How does, and by which strategies should, a public sector organisation identify and obtain all necessary licences to ensure long-term maintenance of digital assets before use of a commercial globally provided SaaS solution for addressing lock-in effects?

The focus of the paper is the practices and strategies of a public sector organisation. These are affected by several sets of laws and regulations in different areas, including but not limited to public law (including administrative law and law as it relates to retention, archiving and availability of data and materials by public sector organisations), procurement law, contract law, copyright law, patent law and the law of data protection and privacy. Specifically, we identify shortcomings in a specific public sector organisation's use of a specific SaaS solution, that raise additional issues relating to the GDPR (EU, 2016; IMY, 2022), the Swedish Public Access to Information and Secrecy Act (OSL, 2009; Regeringskansliet, 2021), the Administrative Procedure Act (FL, 2017; Furberg and Westberg, 2020/21), and regulations provided by the Swedish National Archives (Riksarkivet, 2009a, 2009b). Even if our primary interest is public law and rules directly governing the actions of the organisation, all the aforementioned legal aspects have to be taken into account when assessing the organisation's

[3] The eSamverkansprogrammet (in Sweden often abbreviated as 'eSam') is a collaboration between 32 central government agencies and the Swedish Association of Local Authorities and Regions (eSam, 2021a). When the national delegation for e-Governance had completed its mission the directors general for the authorities which participated in the national delegation voluntarily decided to establish the eSamverkansprogrammet in 2015. The collaboration addresses different aspects related to digitalisation and results from the collaboration are published in the form of guidelines and recommendations. For example, there is an expert group which focuses on legal issues.

strategies and practices. We have not set out to analyse exhaustively any individual legal question, or act by the organisation, and submit a detailed opinion. Rather, legal findings from the study relate broadly to obligations officials have in order to avoid unwanted dependencies and problematic lock-in effects, specifically by identifying and obtaining all necessary licences to allow for long-term maintenance of digital assets.

The paper presents several important contributions for organisations which consider adoption and use of a SaaS solution. First, we provide rich insights concerning licensing issues from one of the largest organisational implementations of the M365 solution in an EU-country which draws from an extensive data collection in a large public sector organisation (the second largest municipality) in Sweden. Second, we present a number of observations related to identifying and obtaining all necessary licences concerning use of the adopted M365 solution which impact on the conditions for use of M365 in public sector organisations. Third, we present and elaborate problematic licensing issues related to the implementation of M365 in a large public sector organisation. Fourth, we elaborate on legal analyses which we find should have been conducted related to the implementation and use of M365. Fifth, we present recommendations concerning licences for avoiding lock-in effects related to potential use of a SaaS solution.

2. On lock-in effects and SaaS solutions

For avoiding lock-in effects any organisation needs to obtain all licences necessary to ensure the long-term storage, maintenance, retrieval, and re-use of all its digital assets independently of the SaaS solution currently in use.

2.1 On licensing of software applications and formats for digital assets

In the early days of computing software 'was treated as a service' (Potter, 2000), and since the late 1960s several models for licensing and distribution of software have evolved (O'Rourke, 1995). Prior to the 1976 Copyright Act 'the scope of a programmer's copyright and patent rights in software was unclear' (Heffan, 1997, p. 1494). Over the years, a number of licences for software which rely on copyright have evolved, including Open Source Software licences which are licences that comply with the Open Source Definition (Unni, 2016). All Open Source Software licences approved by the organisation Open Source Initiative are provided under perpetual terms (Ballhausen, 2022, p. 129), something which promotes long-term maintenance of software applications and associated digital assets.

Each software application typically implements several different formats which are used for representation of digital assets. Many formats have been provided as formal standards by organisations such as ISO (International Organization for Standardization) and ITU-T (International Telecommunication Union). Related to several such standards there may be many patent holders which control patents ('standard-essential patents')

that impinge on those formats (Lundell et al., 2019). Consequently, before use of a format for which patent holders control patents it may be necessary to obtain patent licences from all rights holders to allow for lawful long-term maintenance of digital assets that use such formats over a time-period beyond that which the software application initially used. Moreover, there are also formats that are provided under conditions for which patent issues have been assessed to be unproblematic. For example, formats which comply with the definition of an open standard, where this definition constitutes the basis for a recommendation provided by the Swedish National Procurement Services, must be capable of implementation under conditions that do not require patent licences impinging on those formats (NPS, 2016) unless they are offered irrevocably on a royalty-free basis.

Prior to adoption and use of a software application in a public sector organisation ('PSO') it is necessary for the organisation to obtain all necessary rights that allow for lawful data processing and maintenance of each digital asset over its full life-cycle. This involves a need for the organisation to ensure that all necessary rights have been obtained from each rights holder for the software applications to be used (often involving a need to obtain software licences and in some cases patent licences) and also (where implementation or use of the format impinges on the intellectual property rights of third parties) for all formats implemented by each such application. Besides a need for each PSO to obtain all such necessary rights for the software applications it is also critical for the organisation to ensure that all necessary rights have been obtained for all such formats implemented and used by each application (typically involving a need to obtain patent licences for specific formats) in order to ensure lawful and appropriate long-term maintenance of each digital asset represented in those formats. These rights may be granted by the SaaS solution provider either directly (to the extent that it is itself a rights holder of necessary rights) or indirectly (by way of sub-licence) if the SaaS solution provider is authorised to do so by each rights holder, but it cannot automatically be assumed that all necessary licences will be granted by the SaaS solution provider in this way. In any event such licences are likely to be both limited in scope (covering only the implementation of the standards within the SaaS solution provided, but not within any other application used by the customer) and duration (for such time as the contract with the SaaS solution provider persists).

It follows, therefore, that since software applications (we use the term to include SaaS solutions) are typically provided under time-limited licences, commonly up to three years, any PSO needs to ensure long-term maintenance of its digital assets over much longer life-cycles. This has significant implications for each organisation to procure and use software applications which implement all formats used for representing digital assets over the full life-cycle for each digital asset (typically over several decades, as opposed to the life-cycle of the SaaS solution, which is likely to be much shorter). Note that even though the relevant patents themselves will have a limited term (of usually 20 years) it cannot be assumed that they will have expired by the time that the contract for the relevant SaaS solution has terminated (especially because it is in the nature of a SaaS solution that its functionality, and therefore the set of formats implemented, changes over time, and may therefore implement new formats during its life-cycle).

Thus, where a software application to be used by a PSO has implemented formats for which rights holders control patents that impinge on those formats the organisation may need to devote considerable efforts for obtaining all necessary rights for each format used for representation of digital assets, in order to allow for long-term maintenance of digital assets both during and also after the organisation has ceased to use that software application. It should be noted that prior research has shown that, even for some formats recognised as standards (e.g. ISO/IEC 29500) by formal standardisation organisations (ISO and ITU-T), it may be impossible to obtain all necessary patent licences under conditions which would allow for long-term maintenance of digital assets in those formats (Lundell et al., 2019).

Before a PSO uses a software application provided on a SaaS solution basis it is critical to establish that contract terms for the solution ensure that digital assets can be exported in formats for which the organisation has obtained all necessary rights (including all necessary patent licences) for each format used to allow for lawful long-term maintenance of digital assets that have been exported from the SaaS solution. Since prior research has shown that it may be impossible to obtain the complete technical specification for all versions and all editions of some formats (such as, for example, the ISO/IEC 29500 standard) that may have been faithfully implemented by specific SaaS solutions, each well-organised PSO also needs to consider if it is possible for the organisation to procure other software applications which allow for lawful and appropriate long-term maintenance of digital assets represented in specific formats after export from specific SaaS solutions used.

2.2 On licences for avoiding lock-in effects during and after use of a SaaS solution

The concept of 'lock-in' is a complex one that has received attention amongst researchers, practitioners, and policy makers for a long time (e.g. Aubert et al., 1998; David, 1985; Farrell and Klemperer, 2007; Ghosh, 2005; Kroes, 2008; Shapiro and Varian, 1999). For example, the EC commissioner who launched the Digital Agenda for Europe stressed the importance of interoperability between SaaS services as a means for avoiding lock-in as follows in a public speech: *'The development of electronic communications networks has seen a rise in the importance of interoperability between equipment used, between services provided, and between data exchanged. Interoperability encourages competition on the merits between technologies from different companies, and helps prevent lock-in.'* (Kroes, 2008)

Similarly, the European Commission has expressed concern for absence of interoperability and an inability to avoid lock-in when organisations adopt and use cloud solutions: *'Currently, individual vendors have an incentive to fight for dominance by locking in their customers, inhibiting standardised, industry-wide approaches. Despite numerous standardisation efforts, mostly led by suppliers, clouds may develop in a way that lacks interoperability, data portability and reversibility, all crucial for the avoidance of lock-in.'* (EC, 2012, p. 10)

Research shows that lock-in effects occur where (de facto) compatibility has developed as a result of market dominance (Egyedi and Hudson, 2005, p. 153). Further, findings from a study which investigated all 290 Swedish municipalities (with a 99% response rate) show that most Swedish municipalities are exposed to different types of lock-in effects, including file format lock-in and vendor lock-in (Lundell, 2011, p. 74). Conclusions from the same study show that most municipalities 'do not undertake (or even initiate) an evaluation before procurement of software and adoption of document formats' (Lundell, 2011, p. 75). Further, prior research which investigated legal issues related to cloud-based SaaS solutions identified risks for dependence on a solution from a specific provider as follows: 'A major lock-in concern is risk of dependence (or over-dependence) on one provider's, often proprietary, service. If the service is terminated for whatever reason, users wanted to recover all their data and metadata in formats that are easily accessible, readable, and importable into other applications, whether running internally or in another provider's cloud.' (Hon et al., 2012a, p. 116)

In acknowledging that several practitioner reports and research studies have highlighted that use of cloud and SaaS solutions in PSOs provides a range of different benefits we find that it has also been argued that despite 'numerous potential benefits of cloud computing usage, there are still some users reluctant to adopt this technology' (Yadegaridehkordi et al., 2020, p. 791). However, it has been argued that 'numerous applications have already been migrated to the Cloud' even though there are concerns for vendor lock-in (Kritikos et al., 2019, p. 1) and also other types of lock-in (e.g. Silva et al., 2013). Further, research shows that 'cloud computing raises legal issues beyond those encountered in more traditional IT outsourcing' (Bradshaw et al., 2011, p. 189). It has also been argued that legal challenges related to use of cloud and SaaS solutions include that 'we are likely to see legal disputes arising from geopolitical and jurisdictional issues' (Mowbray, 2009, p. 136).

Use of different licensing terms for provision of formats and standards which are implemented in software has been an issue that has triggered extensive discussions and controversy amongst policy makers, practitioners and researchers over the years (e.g. Contreras, 2015a, 2015b; EC, 2012; Kappos, 2017; Kesan and Hayes, 2014; Li, 2018; Lindberg, 2019; Lundell et al., 2015; Phipps, 2019). Previous research shows that 'it may be impossible to clarify conditions and obtain patent licences for standard essential patents (and all necessary rights) for use of specific ISO standards that are provided on FRAND-terms' (Lundell et al., 2019). Further, research shows that it may be impossible to even identify all standard essential patents which may impinge on a specific standard that are referred to by global providers of M365 and other SaaS solutions (Gamalielsson and Lundell, 2021; Lundell et al., 2015, 2019).

2.3 On obtaining licences for addressing lock-in effects in a SaaS context

Previous research has presented critical factors and associated issues that a PSO needs to consider before the organisation adopts and uses a SaaS solution in order to avoid

lock-in (Lundell et al., 2020). Specifically, ***availability of all necessary licences*** for the PSO is one important factor with associated critical issues that organisations need to consider:

- Have relevant licences been identified?
- Have relevant licences been obtained?

Previous research shows a number of fundamental challenges related to these issues (e.g. Lundell et al., 2019) and it has been shown that many PSOs have failed to successfully address these issues (e.g. Lundell et al., 2020). Specifically, it should be noted that lawful use of certain formats both during and after use of the SaaS solution may require patent licences and other types of licences (Blind and Böhm, 2019; Contreras, 2015a; Lundell et al., 2015, 2019).

It has been argued that licensees 'under standardized license agreements are deprived of an opportunity to influence the content of predefined indemnification provisions. As a result, licensees are open for third-party claims arising from infringement of intellectual property rights such as patent, copyright, and trademark, and misappropriation of trade secrets, which are not covered by indemnification provisions' (Savelyev, 2014, p. 565). Different cloud and SaaS solutions may be provided under different conditions and with different functionality, something which implies that an organisation needs to identify and obtain different types of licences for their specific usage scenarios. Further, SaaS solutions are typically provided under fixed-term contracts with renewal provisions that may change over time. This imposes specific risks related to an organisation's ability to exit from the solution with preserved digital assets. For example, conclusions from an investigation of contract terms for a specific SaaS solution (M365) which was undertaken by a Swedish PSO (the City of Stockholm) show that contract terms for the M365 solution can be changed at any time and that it is impossible for the PSO to determine if a tool can or cannot be lawfully used (Stockholm, 2021).

Fixed compatibility requirements (e.g. Microsoft APIs) and 'markets controlled by dominant suppliers' can create anti-competitive behaviour (Krechmer, 2013). For example, it has been argued that such anti-competitive behaviour 'can occur legally, as example, when multiple patent holders pool their intellectual property and require an expensive license to implement a standard' (Krechmer, 2013).

Since contract terms for a SaaS solution may require the customer to obtain patent licences from third parties, procurement of such licences may become a significant challenge. This may explain results from previous research which show that no PSO had obtained all licences from third parties as detailed in the contract terms for a specific SaaS solution (the M365 solution) they use in their own PSO (Lundell et al., 2020).

2.4 On legal requirements to obtain licences and avoid lock-in

As a general rule a PSO is not exempted from having to acquire licences for the software it intends to use, and licences for the maintenance of its digital assets over time. This is quite self-evident within western legal tradition, and explicit provisions to this extent will scarcely be found in primary legislation. Rather, a PSO's obligations in this regard may be derived from fundamental constitutional principles or sought in secondary, more detailed regulations issued by e.g, sector authorities or ministers by means of delegated norm-setting competence.

At the very foundation of all EU states is the rule of law. Exercise of public power under the law means that each PSO is obligated to comply with the law and, by extension, ensure that it does not put itself in a situation where infringements are unavoidable at a later stage (e.g. through lock-in). These fundamental principles usually apply without restriction also to the procurement by public authorities of software licences from private entities.

In Sweden, the principle of the rule of law can be found in Chapter 1, Section 1, paragraph 3 of the Instrument of Government (RF, 1974). The rule of law also forms part of the principles of good administration. The concept of good administration originates in Article 41 of the Charter of Fundamental Rights of the European Union (EU, 2012) and has been further developed in the Committee of Ministers' Recommendation to member states on good administration (CM, 2007). Again taking Sweden as example, the principles of good administration are found in Sections 5 to 8 of the 2017 Administrative Procedure Act (FL, 2017). Good administration encompasses *inter alia* principles of objectivity, proportionality, efficiency and availability. Also, as mentioned, it includes the principle of the rule of law and a general duty of care.

In 1976 the EEC (European Economic Community) laid down the first fundamental principles of public procurement in (what later became) the EU (EEC, 1976), including the principles of non-discrimination and equal treatment now found in Article 18 of the 2014 Public Procurement Directive (EU, 2014), stipulating amongst other things that the design of the procurement shall not be made with the intention of artificially narrowing competition, for instance by unduly favouring or disadvantaging certain economic operators. It can be argued that if a procurement causes lock-in, it also creates a distinct advantage for the same solution or provider in all future procurements of the same goods or services. The Court of Justice of the European Union, in its judgement on 19 June 2008 in case C-454/06 *Pressetext*, firmly rejected the practice of concluding a public services contract for an indefinite period, finding it to be 'at odds with the scheme and purpose of the Community rules governing public contracts' (EU, 2008). Accordingly, there must always be a next procurement, and EU procurement law imposes an obligation for each PSO to design procurements so that lock-in effects are avoided.

Detailed instructions and procedures for procuring office software may be found in various types of regulations applicable to different PSOs. The legal status of these is also likely to vary. In the best of worlds, this type of regulation contains instructions that ensure that the contracting PSO always complies with all legal requirements applicable to the particular procurement, including the obligation to avoid lock-in.

3. Research approach

Through a case study we investigated how a large PSO identified and obtained licences to ensure long-term maintenance of digital assets prior to use of the M365 solution. This investigation was part of a study which considered how a large PSO addressed lock-in effects related to its adoption, use, and large-scale organisational implementation of the M365 solution. The context for the case study was the *City of Gothenburg* (*Göteborgs Stad* in Swedish, 'CoG'), which is Sweden's second largest municipality 'with a population of just over half a million' in December 2016 (Got, 2017a, p. 5). The CoG is a politically governed organisation that is led by its city council (*Kommunfullmäktige* in Swedish, '*KF*') and its city executive board (*Kommunstyrelse* in Swedish, '*KS*'). The CoG had 54,200 employees at the end of 2016 (Got, 2016a, p. 6).

The CoG was purposefully selected as a highly relevant organisation for conduct of the case study. First, investigation of a large-scale adoption of M365 by a Swedish PSO (which during use of M365 involves data processing and maintenance of digital assets in different countries) is of particular relevance. There are Swedish national regulations (e.g. the Swedish Public Access to Information and Secrecy Act, in Swedish: 'Offentlighets- och sekretesslagen' (SFS 2009:400)) which need to be considered by a PSO considering the use of M365 (Regeringskansliet, 2021). Second, as an early adopter of M365 in the Swedish public sector (and one of the largest deployments in Sweden) the CoG is particularly influential. For example, representatives for several other Swedish PSOs have, in different contexts (including public events and discussion), referred to the CoG when presenting their own arguments and basis for adoption of M365 in other PSOs (e.g. Lundell et al., 2020). This includes a public event on 1 November 2017 during which two of the authors of this paper and a manager with influence over the M365 adoption in the CoG participated in discussions concerning the technical and legal analysis of M365 (Got, 2017d). Third, the organisational implementation of M365 gained public exposure and some public debate after it was temporarily suspended for legal and security reasons in October 2017 (Lindström, 2017). Fourth, a legal analysis of the lawfulness of using M365 under Swedish law was published soon after this suspension of deployment (SLK, 2017).

The basis for the study stems from discussions with representatives for the public sector related to public presentations and publication of results from a previous study (Lundell et al., 2016) which investigated licensing challenges, lock-in effects and strategies for exit in Swedish PSOs. During 2015–2016 the previous study was conducted on behalf of the Swedish Competition Authority and the results triggered extensive discussions with different representatives for the public sector in Sweden

and the EU. This, in turn, shaped ideas for a more focused study which evolved into conduct of the present case study. The case study was initiated in 2017 and has involved an extensive and complex data collection. A significant amount of material has successively been collected and obtained from the CoG and from other sources. This includes project documentation, contracts, and other publicly available sources. Amongst other sources of particular relevance is documentation from two legal analyses conducted by the legal experts at the CoG (SLK, 2017, 2019).

A large number of requests for information and data sources were sent (via email and via letters) and communicated (via phone dialogues and physical meetings) to representatives for the CoG, and an extensive amount of material was provided by the CoG. The collected material was systematically analysed as the data collection progressed, which in turn led to subsequent data collection as observations and results from the analysis evolved over time.

Since the public meeting with a representative for the CoG on 1 November 2017 the data collection involved dialogue with representatives for several organisations in the CoG, primarily the following three organisations (that will be presented in section 4): 'Förvaltningen för Intraservice', 'Förvaltningen för Inköp- och upphandling', and 'Stadsledningskontoret'. These organisations are, legally, different authorities in the CoG, which is of particular relevance for the analysis of findings from this study.

The CoG is a complex organisation, and it has internally been recognised that from a democratic perspective it is problematic that it may be perceived difficult to comprehend the organisation from an outside perspective. It may therefore seem natural that a major reorganisation of the CoG was prepared for 2021 (Got, 2020).

4. Observations from data collection and responses to requests

The adoption and deployment of M365 in the CoG represents one of the largest organisational implementations in Sweden (hereafter referred to as the implementation of M365), and it has therefore been highly influential in the Swedish context. For this reason, the implementation has, directly or indirectly, involved and affected a large number of individuals and other organisations, something which has contributed to a complex data collection and analysis process. Overall, the organisational implementation of M365 in the CoG can be characterised as a turbulent and politicised process during which the individuals, organisations and other stakeholders involved have faced significant tensions and a number of legal, organisational, technical and societal challenges.

The authority Intraservice (Swe. *Förvaltningen Intraservice*, '*Intra*') has responsibility for provision of the entire IT operations and other internal services within the CoG. A second organisation of particular relevance for the analysis is the authority Stadsledningskontoret (Swe. *Stadsledningskontoret*, hereafter referred to as *SLK*) which supports the city executive board (*KS*). Further, a third specifically relevant

organisation is the company *Göteborgs Stads Upphandlings AB* ('*UppAB*') which has been responsible for all public procurement in the CoG. This company was 100% owned by another company, *Göteborgs Stadshus AB*, which is the parent company for all operating companies in the CoG and it is wholly owned by the CoG (Got, 2018a). Also of relevance for the analysis is a reorganisation which followed a decision in the CoG during 2016 when it was decided that from January 2017 the operations in the company *UppAB* should be reorganised into an authority which is referred to as *Förvaltningen för inköp och upphandling* ('*Ink*'). The company *UppAB* exists during the life-cycle for already established and still active contracts, but new procurements and all operations should take place in the new authority *Ink*. Hence, the new authority *Ink* has from 2017 continued to constitute a strategic resource for the entire CoG related to public procurement.

From 1 June 2009 to 24 June 2021 the CoG has had a long-lasting relationship and several framework contracts with its partner *Atea Sverige AB* ('*Atea*') through which the CoG has been able to procure products and services from Microsoft (Got, 2009, 2011, 2013b, 2015f, 2016g, 2017f). The Swedish company *Atea* is the largest supplier of IT-products and services to Swedish PSOs with sales totalling 8422 MSEK (which represents 25% of the total Swedish public sector market of 34000 MSEK) during 2017 (DS, 2018). *Atea* was, at all relevant times, wholly owned by the Swedish company Atea Holding AB, which in turn has been wholly owned by the international company Atea ASA (Atea, 2014, 2022). The company Atea ASA is listed on the Norwegian stock exchange and the company has commercial operations in several other Nordic countries, including Denmark and Finland (ASA, 2020).

The M365 solution was launched by Microsoft in 2011 (PC, 2011) and we note that *Atea* has been the provider of products and services from Microsoft to the CoG over the entire time period during which M365 has been provided on the market (Got, 2009, 2011, 2013b, 2015f, 2016g, 2017f). On 5 April 2013 *Ink* presented tender documents for a framework agreement (Got, 2013a) which attracted three bids that resulted in a framework contract between the CoG and *Atea* for the time period (after two renewals) from 25 June 2013 to 24 June 2017 (Got, 2013b, 2015f, 2016g). Further, on 21 January 2017 *Ink* presented tender documents for a framework agreement (Got, 2017e) which attracted two bids that resulted in a framework contract between the CoG and *Atea* for the four-year time period from 25 June 2017 to 24 June 2021 (Got, 2017f).

The plans toward M365 usage in the CoG were shaped and became reality at some point during the four-year time period following the general election on 14 September 2014. Initial plans for an implementation of M365 in the CoG can be traced back to an item that allocated 10 minutes on the meeting agenda at an Intraservice board meeting on 21 June 2016, during which a presentation of IT strategies for the future was addressed by the IT manager at *Intra* (Got, 2016b). The minutes from this board meeting show that the IT manager at *Intra* explained that the administration made the assessment that the CoG needed to sign a new contract with Microsoft and that a change to a new version and a new licensing model would provide new opportunities

(Got, 2016c). From the minutes, it is clear that the IT-manager also explained that the CEO of *Intra* would present a time plan, cost estimates and suggestions for how to address security related to document management during the next Intraservice board meeting on 23 August 2016.

The conduct of the study has encompassed a complex data collection process which has involved many requests for data sources via a very large number of dialogues and contacts with different representatives for different organisations in the CoG. This includes both synchronous communication, through meetings and discussions (via face to face meetings and via phone) and also asynchronous communication (via email and letters). The website (and intranet, which during data collection has been publicly accessible via www.goteborg.se) provided by the CoG has also provided a valuable source from which an extensive amount of documentation has been systematically collected and analysed. During the study, one of the researchers (the first author) who coordinated the data collection has experienced many misunderstandings, something which to some extent may be seen as understandable due to the complexity, depth, and nature of the phenomena being scrutinised in the study. Overall, a very rich set of data sources has been collected from different informants and organisations both inside and outside the CoG, and as part of this a large set of files containing contract documents has been obtained from different authorities in the CoG.

Overall, during the entire data collection process we experienced that representatives for the CoG were reluctant to provide requested documents, and on several occasions also provided misleading information. For example, on 9 January 2018 we requested all applicable contract documents for the M365 solution, and during the interactions (which involved dialogue by phone) with the acting CIO at *Intra* we were informed that the CoG has, effectively, outsourced the CoG's decisions concerning whether or not to provide requested document (i.e. the CoG's decisions concerning the principle of public access to information, Swe. '*Offentlighetsprincipen*') to Microsoft. As an additional illustration of the unwillingness to provide the information requested we found that several (at least four) requested contract documents were withheld when the CoG on 23 February 2018 decided (Ref. 230/15) to provide only a subset of the requested contract documents (Got, 2018b, 2018c). We were able to identify this omission to provide all requested documents much later in the data collection process (after additional requests) and it was not until two years later (on 19 January 2020) that the CoG provided four additional contract documents which we initially requested on 9 January 2018 (i.e. more than two years earlier). Furthermore, we find that activities in relation to the acquisition of M365 in the CoG have received criticism, including from the city audit (Got, 2017g, 2018d, SVT, 2017; Spanaren, 2017).

5 Observations concerning availability of all necessary licences

Concerning **how the CoG took action for identifying and obtaining all necessary licences**, and the strategies it had adopted to this end, we found that the CoG was

organised in an adequate manner, and had adopted internal policy documents which are adequate for addressing a number of important issues. Moreover, we find that these policy documents constitute an eminently suitable starting point for the preparatory analysis necessary to avoid lock-in when acquiring software. Further, we note that the CoG was organised with a separate authority, *Intra*, with responsibility and specialist competence for the provision of the services in question, and another authority, *Ink*, with expertise in procurement. We note that the CoG had contracted a so-called licensing partner, *Atea*, whose role included the provision of business advice and active or background support, and participation in negotiations with software suppliers. The contracting of a neutral external expert could potentially provide very valuable competences concerning software and acquisition of licences, including the provision of support for complex public procurement projects. However, related to the actual behaviour of CoG and its licence partner we have made some observations on matters which we found problematic.

Concerning **availability of all necessary licences** for the adopted M365 solution we found that the CoG lacks access to all necessary licences for ensuring long-term maintenance of all its digital assets independently of the SaaS solution currently in use. This is despite the fact that the M365 solution has been used for several years by many individuals and organisations in the CoG.

The study has made a number of observations and identified several issues related to unavailability of all necessary licences that would allow for use of M365 to process digital assets in the CoG. Based on these observations our analysis identifies a number of findings which cause concern and call for actions amongst responsible decision makers.

First, we found that the CoG has not obtained all licences from third parties as detailed in the English version of the contract terms (dated 1 May 2017) for the M365 solution which are referenced in the legal review that was provided on 20 October 2017 by the CoG (SLK, 2017):

> 'Customer must obtain its own patent license(s) from any third party H.265/HEVC patent pools or rights holders before using Azure Media Services to encode or decode H.265/HEVC media.' (OST, 2017, p. 26)

Therefore, the customer (i.e. the CoG) must obtain its own licences from any third party rights holders related to the H.265/HEVC standard. Based on the information that has been provided during the study, we found that the CoG has not taken the action required to obtain all necessary rights from all third party rights holders for the ITU-T H.265 standard that the CoG is bound by when using the M365 solution. Crucially, this standard is normatively referenced (via other standards) in the ISO/IEC 29500 standard (OfficeOpen XML). Hence, under the assumption that the ISO/IEC 29500 standard is implemented in the M365 solution it follows that data that is exported from M365 (and stored locally as '.docx' files) may impinge on patents that have been declared as standard essential for the ITU-T H.265 standard (in the ISO and ITU-T patent databases,

see Lundell et al. (2019) for details). If, on the other hand, the ISO/IEC 29500 standard is not implemented by the M365 solution it follows that customers exporting data from M365 may be unable to interpret and maintain the files since the files (stored in '.docx') would in such a scenario fail to implement the ISO/IEC 29500 standard, which in turn may lead to loss of data since the file format actually implemented in M365 is unknown.

Second, based on the information that has been provided to us in response to a question sent to *Intra* and a City Legal Advisor at *SLK* who was also one of the authors of *SLK* (SLK, 2017), we find that the CoG has not taken any action to investigate availability of necessary licences as detailed in the online service terms (OST, 2017) which are referenced in SLK (2017). Specifically, we found that no action has been taken by the CoG in response to the following question[4] which was sent to one of the legal experts at *SLK* on 8 March 2020 and to *Intra* on 9 March 2020: '*What actions have you taken in order for Göteborg City to procure licences for the ITU-T H.265 standard?*'

Third, we found that the CoG has not obtained any licences related to the ITU-T H.264 and H.265 standards from third parties that would be necessary for ensuring long-term maintenance of all its digital assets independently of the SaaS solution currently in use. These standards are normatively referenced (via other standards) in the ISO/IEC 29500 standard (OfficeOpen XML) and under the assumption that the ISO/IEC 29500 standard is implemented in the M365 solution it follows that data that is exported from M365 (and stored locally as '.docx' files) may impinge on patents that have been declared as standard essential for the ITU-T H.264 and H.265 standards (see further Lundell et al. (2019)). During data collection, we experienced unawareness amongst decision makers at the CoG concerning the need to procure patent licences for (directly and indirectly) normatively referenced standards (such as the ITU-T H.264 and H.265) in the ISO/IEC 29500 standard.

6. Issues, implications and recommendations

Based on our analysis of publicly available sources and the information that has been provided in response to questions and requests for documentation during the study, we found a number of issues related to the implementation of the M365 solution in the CoG. We find that these issues have, potentially problematic, implications for individuals, organisations in the CoG, other organisations in Sweden, and society at large.

6.1 Issues related to obtaining licences before use of the M365 solution in the CoG

First, after the release of the M365 solution on 28 June 2011 (PC, 2011) and until the Intraservice board meeting on 21 June 2016 when the IT manager at *Intra* orally

[4] The Swedish wording used when posing this question (on 8 March 2020 to a City Legal Advisor at SLK and on 9 March 2020 to Intra) was: 'Vilka åtgärder har ni vidtagit för att till Göteborgs Stad anskaffa licenser för ITU-T H.265 standarden?'

presented the plan for use of M365 in the CoG (Got, 2016b, 2016c), we note a total absence of analyses covering potential licensing and lock-in issues. Specifically, before that board meeting no documentation referring to implications from use of M365 had been provided by *Intra* (Got, 2016c). Further, documentation from the board meeting (Got, 2016c) makes it clear that there had been a lack of discussion and a lack of any plan for how the CoG might effectively obtain all necessary licences and address lock-in challenges.

Second, on 9 August 2016 *Intra* supplemented the two-page document (Got, 2016d) with (version 1.0 of) an appendix (Got, 2016e) suggesting (*inter alia*) benefits of M365, costs, procurement, privacy, and licensing. Specifically, concerning licences, the appendix includes a comparison between M365 and the Office suite in use (Office 2007). Overall, we find that the document with its appendix (Got, 2016d, 2016e) lacks important content and presents misleading information which makes it inappropriate for use as a basis for any decision concerning a large investment. For example, there is no analysis covering adoption of a new licensing model (i.e. transition from use of software on-prem under perpetual terms to a periodically licensed SaaS solution) and associated lock-in effects. Hence, since this documentation provided by *Intra* also lacks critical details concerning costs, licences and other legal aspects, we find that the Intraservice board did not have a solid basis for a decision.

Third, based on the minutes from the two Intraservice board meetings on 21 June 2016 (Got, 2016c) and on 23 August 2016 (Got, 2016f) we find that no City Legal Advisor nor any other legal expert was present at either of the two board meetings when the proposal for the M365 solution was presented, and discussed (and finally decided at the Intraservice board meeting on 23 August 2016) (Got, 2016f). Under the assumption that licensing information and contract documents containing contract terms for M365 would have been provided to decision makers in advance, or brought to the meeting by any participant in either of these two meetings, we find that there would have been no real opportunity for the group to interpret, scrutinise, discuss, and clarify potential implications of various contract terms related to the licensing model for the M365 solution. However, based on the documented information that has been provided to us (and orally discussed during a meeting at *Intra* on 18 December 2018) we have no information which suggests that any licensing information or contract terms were provided and discussed before or during either meeting. Based on our experiences, we claim that even a legal expert with knowledge of the legal systems in all potentially relevant jurisdictions and the necessary technical skills and knowledge of relevant lock-in challenges would find it impossible to digest and analyse the necessary documentation (including complex contract terms and different types of licences) before an informed decision, even if that information had been made available on such short notice.

6.2 Issues related to obtaining licences to ensure long-term maintenance of digital assets

Fourth, we find that digital assets processed and exported from the CoG's M365 solution fail to fulfil the guidelines and regulations for archives (Regionarkivet, 2017a, 2017b) which the Intraservice board approved on 22 May 2017 (Got, 2017b, 2017c). Specifically, several files (with extensions '.docx' and '.pdf') created by use of the CoG's M365 solution and provided to us are inherently problematic from both legal and technical perspectives (e.g. Lundell et al., 2019). Further, files created in such formats fail to fulfil the regulations for archiving in the CoG (Got, 2017b, 2017c). The regulations for the CoG (in '7 §' of 'Arkivlagen' and 'Kommunallagen') state that technical requirements provided by Riksarkivet shall be fulfilled (Regionarkivet, 2017b). These technical requirements include digital assets (Swe. 'elektroniska handlingar'). Files provided with the extension '.docx' do not fulfil these requirements (Riksarkivet, 2009a, 2009b). In addition, the outcome of an analysis of files provided by *Intra* shows that PDF/A-files exported from the M365 solution fail to fulfil the requirements specified by Riksarkivet. Further, previous research shows that files provided by the CoG in the PDF/A-3 and PDF 1.7 formats are unsuitable for long-term maintenance (and thereby archiving) since it has been shown to be impossible to obtain all necessary rights for implementing these file formats in open source software projects that can be maintained over the full life-cycle of files produced in such file formats (e.g. Lundell et al., 2019).

Fifth, we find that decision makers at *Intra* and City Legal Advisors at *SLK* have taken no action to investigate the possibility of procuring patent licences covering the ITU-T H.264 and the ITU-T H.265 standards (as detailed in the Online Service Terms). Further, we find that the CoG has procured no patent licences related to either standard. We find that this omission exposes the CoG to the risks of patent infringement claims. Further, since both the ITU-T H.264 standard and the ITU-T H.265 standard are indirect normative references (via other standards) in the ISO/IEC 29500 standard we also find that omission in procuring patent licences for the ITU-T H.264 standard and the ITU-T H.265 standard exposes the CoG to significant risk of being unable to maintain its own digital assets over long life-cycles independently of the M365 solution. Should CoG, hypothetically, decide to cease using M365, the omission in procuring such patent licences will inhibit data sovereignty. This may cause significant issues related to interoperability and the ability to maintain digital assets over long life cycles. Further, since the CoG has procured no such patent licences we cannot undertake a legal analysis of their terms. Based on previous research that has investigated the possibility of obtaining all necessary patent licences for the ISO/IEC 29500 standard (Lundell et al., 2019), we find that the CoG is exposed to the risk of inability to maintain its own digital assets independently of the M365 solution.

6.3 Implications of discrepancy between policy and practice

We find that the documentation presented on 9 August 2016 by *Intra* (Got, 2016d, 2016e) as a basis for the proposed decision ignores many rules in the IT policy (Got, 2015b) which was approved in the CoG by the Intraservice board (Got, 2015c), by *KS* (Got, 2015d), and by *KF* (Got, 2015e). For example, the IT policy emphasises that procurement of IT solutions shall consider the importance of open standards and formats that allow for interoperability and long-term maintenance. Further, concerning contracts for global IT solutions in the CoG, we find that the IT policy makes it clear that all such contracts in the IT area shall be centrally analysed, signed and maintained. Based on our analysis of the documentation constituting the basis for the proposed decision we find that it does not address any of those issues and there is no sign of any analysis of licensing and contract terms that the CoG will be bound by if it decides to procure and use the M365 solution.

There is no legal definition of a municipal 'policy' in Sweden. Within the CoG, a policy constitutes a *governing document* (Swe. '*styrdokument*'). The CoG uses several different headings for governing documents and 'policy' is the one with least amount of concretisation. The purpose of a policy within the CoG is to express basic principles or values and to guide decision making. As such it is a type of document that officers within the CoG are duty-bound to take into account, but which will allow the decision makers a lot of discretion. Governing documents are not adopted on the basis of regulatory competence delegated to the municipality. A governing document is, per definition, not a legal norm in Sweden (Regeringen, 2012, p. 7) and the CoG itself as a legal entity is not compelled to abide by it. Each individual acting for the CoG, however, whether an officer or an elected official, is bound *vis-à-vis* the CoG to adhere to a policy when carrying out their duties.

Open standards and formats for interoperability and long-term maintenance of digital assets are something the CoG has committed itself to consider when the CoG procures IT solutions (Got, 2015b). Based on previous research (e.g. Lundell et al., 2015, 2016, 2019), we find it essential to use formats which fulfil the definition of an open standard (NPS, 2016) to ensure interoperability and long-term maintenance of digital assets. The open standards requirements in the CoG's IT policy is, therefore, appropriate. However, given that the IT policy seeks to promote interoperability through use of open standards and file formats the implementation of the M365 solution in the CoG is remarkable. Consequently, it seems clear that the CoG's IT policy has been ignored. Further, we find that through its use of closed file formats (such as PDF/A-3) the CoG fails to fulfil legal and technical requirements for use of file formats allowing for interoperability and are appropriate for long-term maintenance and archiving of files (e.g. Got, 2015b; NPS, 2016; Lundell et al., 2019). In addition, we also find that the CoG fails to fulfil regulations for archiving of digital assets (Got, 2015a, 2015b, 2015c, 2015d, 2015e, 2017b, 2017c; Regionarkivet, 2017b; Riksarkivet, 2009a, 2009b).

When an acting head of department at *Ink* signed a contract for the M365 solution (with E3 and E1 licences) on 28 June 2016 (Got, 2016h) we find that this action caused

vendor lock-in for the CoG. When the IT manager at *Intra* gave a short presentation of plans for M365 for the Intraservice board on 29 June 2016 and provided a documentation on 9 August 2016 the CoG was already bound by contracts for the M365 solution. Further, the documentation provided does not mention any risks and there is absence of analyses addressing any form of lock-in. For example, risks related to *standard-related lock-in*, *file format lock-in*, and *transformation lock-in*[5] related to the M365 solution were not mentioned. Hence, we find that the basis for the decision by the Intraservice board on 23 August 2016 was therefore misleading.

Findings from the study show that the implementation of the M365 solution in the CoG has caused a number of challenges and problematic lock-in effects for individuals and organisations (both inside and outside the CoG), and for society at large. These challenges have significant legal, technical, economic, and societal implications for the CoG, both during use of M365 and should the CoG cease to use M365 in the future. The study shows that lock-in effects relate both to the specific SaaS solution (M365) itself and digital assets that are imported, processed, maintained, and exported from the SaaS solution.

6.4 Lessons learnt and recommendations for addressing lock-in effects

During conduct of the study we have identified and analysed a number of problematic issues related to the implementation of the M365 solution in the CoG and specifically analysed several legal challenges and implications stemming from the adoption and use of M365. We find that several of the identified licensing issues have complex and problematic legal, technical, economic and societal implications. In this subsection we elaborate important lessons to be learnt and associated with each lesson we present recommendations for organisations which consider adoption and use of a SaaS solution.

The currently applicable IT policy was approved by the Intraservice board on 31 March 2015 (Got, 2015c), the *KS* on 23 September 2015 (Got, 2015d), and the *KF* on 8 October 2015 (Got, 2015e) in the CoG. The ***IT policy provides rules covering how contracts and licences should be handled and maintained*** in the CoG. They state that contracts for IT solutions applicable to the entire CoG shall be centrally signed and maintained and that all documentation related to software and licence terms shall be registered in a common register. Further, the rules also regulate the ***importance of licence management*** and state that all authorities and all companies in the CoG shall be responsible for ensuring that ***correct licences*** have been procured. Despite these ambitions, we find that only a subset of all contract documents which the CoG are bound by for the M365 solution are maintained by the CoG. Further, despite the applicable IT policy we also find that no organisation in the CoG has procured all

[5] It should be noted that an extensive study which investigated specific projects undertaken by municipalities and other PSOs in Sweden involving SaaS solutions shows that widely adopted work practices cause these and many other types of lock-in effects (Lundell et al., 2016).

necessary licences for M365 and that it therefore follows that no organisation in the CoG is correctly licensed to use the M365 solution. Hence, we strongly ***recommend*** that any PSO which is considering procurement and use of a SaaS solution (such as the M365 solution) ***adheres to the applicable IT policy*** and as part of such adherence makes sure that it ***maintains all relevant contract documents*** containing all contract terms and also ***procures all necessary licences*** for the specific SaaS solution which the PSO is bound by. Further, we ***recommend*** an authority maintains control of its own contract documents related to a specific SaaS solution and ***never outsources maintenance of contract documents containing contract terms that the authority is bound by to the supplier*** of the specific SaaS solution.

The ***limited scope of the legal analyses*** related to adoption and use of the specific SaaS solution (M365) in the CoG raises a number of unresolved issues and shows that several licensing and legal challenges have been ignored. For example, we find that the CoG has failed to undertake (and provide relevant documentation from) any comprehensive analysis of all contract terms they are bound by for use of the M365 solution in the CoG. Further, no legal analysis of the need for patent licences has been undertaken, something which impacts on the ability to process and maintain digital assets, both during use (as detailed in the contract terms for the M365 solution) and also after use of M365 in the CoG. Hence, we ***strongly recommend*** that a PSO which considers signing contracts for use of a SaaS solution (such as the M365 solution) always undertakes a ***comprehensive analysis of all contract terms*** (that includes analysis of effective strategies for procurement, and actual procurement of, all necessary patent licences) and conditions for ***identifying and obtaining all necessary licences to ensure long-term maintenance of digital assets independently of the specific SaaS solution***. Such an analysis needs to ***consider use*** and ***reuse of all digital assets*** that have been processed and maintained by the specific SaaS solution (such as the M365 solution), both ***during*** and ***after use*** of the specific SaaS solution (such as M365) in the specific PSO.

Based on reported experiences from other Swedish PSOs and findings from our investigation of the CoG's use of the M365 solution ***we recommend that the contract terms for the M365 solution are revised*** before a PSO uses the solution in order to allow for lawful and appropriate long-term maintenance of digital assets. Moreover, we also recommend that each PSO which considers use of a specific SaaS solution for long-term maintenance of its digital assets (in all formats used) over the full life-cycle for those assets, ensures that the solution is provided under lawful and appropriate contract terms which includes that the provider of the solution provides licences for each implemented format under perpetual terms. We find that this may require a need for a redesigned solution, for example, in order to allow for export of digital assets in formats that are suitable for long-term maintenance of digital assets.

In summary, we found that the CoG seems unaware of the inherent technical, legal and financial challenges related to use of closed formats (e.g. Lundell et al., 2019). We find that none of the authorities in the CoG has undertaken any analysis which indicates that they, for technical, legal, and financial reasons, will be able to use the files that

may be exported from the M365 solution. In addition, we find that the CoG has not obtained all necessary rights to allow for implementation of the closed file formats in software and that are needed to allow for use and reuse of files (represented in those closed file formats) after export from the SaaS solution M365.

7. Conclusions

The implementation of the M365 solution in the City of Gothenburg involves many different authorities, each one being responsible for its own operations. Procurement activities are managed by one authority (*Inköp- och upphandling*), the legal experts are based in another authority (*Stadsledningskontoret*), and the IT operations and overall responsibility for the M365 implementation is managed by yet another authority (*Intraservice*). From the study, it seems clear that there are tensions within the organisation which contributed to increased complexity in the data collection and analysis. Overall, despite these challenges, the study obtained a rich body of documentation related to licensing issues concerning the implementation of M365 in the City of Gothenburg. Even if the researchers encountered a number of misunderstandings and ignored requests for public documents that were sent to the City of Gothenburg, we find that the study reveals a rich description of the many obstacles, licensing challenges, and complexities encountered in the implementation of M365 in the City of Gothenburg.

As it seems, decision makers in the City of Gothenburg did not recognise the significance of the switch to a cloud-based SaaS solution. The transition was treated as an incremental, if conveniently refined, update of the long used existing solution from Microsoft. This can explain why the commendable IT policy for procurement of software, including strategies to identify and obtain all necessary licences, address lock-in challenges, and establishing an effective exit strategy to avoid consequences of lock-in, was not adhered to.

With regard to the investigation of, and acquisition of, the necessary licences during and after the deployment of M365, there is a lack of awareness and initiative within the City of Gothenburg. These issues are admittedly complicated, and it cannot be expected even from a large and well-organised authority that it should possess all the necessary specialist competences. The City of Gothenburg has contracted an external, 'neutral' licensing partner in *Atea*, but we have not found any evidence suggesting that *Atea* ever recommended any kind of analysis of the issues we investigated, i.e. the question of which licences are needed to ensure long-term maintenance of digital assets and avoid lock-in.

We find that the responsible authority (*Förvaltningen för Intraservice*) for the implementation of the M365 solution in the City of Gothenburg does not maintain all contract documents and lacks access to all contract terms the city has been bound by for use of the M365 solution despite the fact that contracts for the solution have been signed by representatives for the company *Göteborgs Stads Upphandlings AB* (until the

end of 2016) and the authority *Förvaltningen för Inköp- och upphandling* (from the beginning of January 2017) which have been responsible for procurement in the City of Gothenburg. Further, we also find that the responsible authority for the implementation of the M365 solution lacks documentation in the form of contract documents which detail how many licences of each type they have procured. Further, based on the information that has been provided from the City of Gothenburg during the study, it is clear that no organisation in the City of Gothenburg has addressed challenges related to standard essential patents which may impinge on formats being referenced in the online service terms for the M365 solution.

We find that the time-frame between 6 June 2016 and 24 August 2016 prevented any form of serious analysis of the need to identify and obtain licences that would allow for reuse and long-term maintenance of digital assets that political decision makers should have requested (in light of the absence of necessary relevant information from decision makers at the authority). Hence, we conclude that the actions taken by decision makers at the authority responsible for the M365 solution are far from what can be expected. Based on the information that was available on 23 August 2016 we find that the decision to adopt M365 should never have been taken. We conclude that decision makers at the responsible authority have omitted to thoroughly prepare for, and provide relevant documentation for the proposed decision, that could have been used as a comprehensive basis for strategic discussions concerning such an important decision.

Findings from the study also show that the City of Gothenburg has failed to identify and obtain all necessary licences to ensure long-term maintenance of digital assets. Further, none of the authorities and companies in the City of Gothenburg presents any strategy that would allow to cease using the SaaS solution in a way that exported digital assets can be used and reused by other software applications in the future. The study shows that the authority which is responsible for the M365 implementation, *Intra*, has not even considered a future possible need for ensuring long-term maintenance of digital assets and an effective exit strategy that can be implemented at short notice if necessary. Hence, we find that the City of Gothenburg is exposed to a significant risk of losing control of its own digital assets.

In conclusion, we find that any decision to implement a SaaS solution (such as the M365 solution) in a public sector organisation implies a number of legal, technical, economic, and societal challenges. The study has thoroughly analysed important licensing issues and challenges identified in an investigation of an implementation of a SaaS solution on a large scale in a complex organisation and reported on insights, lessons learnt and recommendations related to how the specific organisation (the City of Gothenburg) has addressed (and to large extent failed to successfully address) analysed licensing issues and challenges. Hence, we find that the study has made an important contribution to advance theory and practice in the area.

References

ASA (2020), 'Annual report 2019', ATEA ASA, 17 March.

Atea (2014), 'Årsredovisning ATEA Sverige AB', Org.nr. 556448-0282, Räkenskapsår 2013-01-01–2013-12-31, Stockholm, 22 May.

Atea (2022), 'Årsredovisning ATEA Sverige AB', Org.nr. 556448-0282, Räkenskapsår 2021-01-01–2021-12-31, Stockholm, 30 June.

Aubert, B A, Patry, M and Rivard, S (1998), 'Assessing the risk of IT outsourcing', in Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Volume VI, IEEE Computer Society, Los Alamitos, pp. 685–692.

Ballhausen, M (2022), 'Copyright Enforcement', In Brock, A. (ed) Open Source Law, Policy and Practice, 2nd edition, Oxford University Press, Oxford, ISBN 978-0-19-886234-5, pp. 126–140.

Bekkers, R and Updegrove, A (2013), 'IPR Policies and Practices of a Representative Group of Standards-Setting Organizations Worldwide', Commissioned by the Committee on Intellectual Property Management in Standard-Setting Processes, National Research Council, Washington, May.

Blind, K and Böhm, M (2019), 'The Relationship Between Open Source Software and Standard Setting', Thumm, N. (ed) EUR 29867 EN, JRC (Joint Research Centre) Science for Policy Report, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11593-9.

Bradshaw, S, Millard, C and Walden, I (2011), 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services', International Journal of Law and Information Technology, Vol. 19(3), pp. 187–223.

CM (2007), 'Recommendation CM/Rec(2007) of the Committee of Ministers to member states on good administration', The Council of Europe, 20 June 2007.

Contreras, J L (2015a), 'A Brief History of FRAND: Analyzing Current Debates in Standard Setting and Antitrust Through a Historical Lens', Antitrust Law Journal, Vol. 80(1), pp. 39–120

Contreras, J L (2015b), 'Patent Pledges', Arizona State Law Journal, Vol. 47(3), pp. 543–608.

David, P A (1985), 'Clio and the Economics of QWERTY', The American Economic Review, Vol. 75(2), pp. 332–337.

DS (2018), 'IT-köp dämpas trots digitala ambitioner', Dagens Samhälle, #28, 23 August, p. 4.

EC (2004), 'European Interoperability Framework for pan-European eGovernment Services', Version 1.0, European Commission, ISBN 92-894-8389-X.

EC (2012), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe', SWD(2012) 271 final, European Commission.

EC (2014a), 'Patents and Standards: A modern framework for IPR-based standardization', Final report, A study prepared for the European Commission Directorate-General for Enterprise and Industry, 25 March, ISBN 978-92-79-35991-0.

EC (2014b), 'Standard-essential patents, European Commission', Competition policy brief, Issue 8, June, ISBN 978-92-79-35553-0.

EC (2020), 'Shaping Europe's Digital Future, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions', European Commission, Communication, COM(2020) 67 final, 19 February.

EEC (1976), 'Council Directive 77/62/EEC of 21 December 1976 coordinating procedures for the award of public supply contracts', Official Journal of the European Communities, 21 December 1976.

Egyedi, T (2007), 'Standard-compliant, but incompatible?!', Computer Standards & Interfaces, Vol. 29(6), pp. 605–613.

Egyedi, T M and Hudson, J (2005), 'A standard's integrity: can it be safeguarded?', IEEE Communications Magazine, Vol. 43(2), pp. 151–155.

EU (2008), 'Judgment of the Court (Third Chamber) of 19 June 2008 (reference for a preliminary ruling from the Bundesvergabeamt, Austria) – pressetext Nachrichtenagentur GmbH v Republik Österreich (Bund), APA-OTS Originaltext – Service GmbH, APA Austria Presse Agentur registrierte Genossenschaft mit beschränkter Haftung', Case C-454/06, Public procurement – Directive 92/50/EEC – Procedures for the award of public service contracts – Concept of 'award of a contract', Official Journal of European Union, C 209/08, 15 August 2008.

EU (2012), 'Charter of the Fundamental Rights of the European Union', C 326/392, Official Journal of the European Union, 26 October 2012.

EU (2014), 'Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC', Official Journal of the European Union, 28 March 2014.

EU (2016), 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', Official Journal of the European Union, 4 May 2016.

eSam (2021a), 'Om eSam', eSam, Available at: https://www.esamverka.se/om-esam/om-esam.html (Accessed 7 December)

eSam (2021b), 'Uppföljning av möten mellan eSam och Microsoft', letter to Microsoft signed by the chair of eSam (who is also the director general of the Swedish Tax Authority), Dnr. 8-731121, 27 October, eSam.

eSam (2021c), 'Digital samarbetsplattform för offentlig sektor', 18 November, eSam. https://www.esamverka.se/aktuellt/nyheter/nyheter/2021-11-18-digital-samarbetsplattform---det-finns-lampliga-och-lagliga-alternativ-for-offentlig-sektor.html (Accessed 18 November)

Farrell, J and Klemperer, P (2007), 'Coordination and lock-in: Competition with switching costs and network effects', in Armstrong, M and Porter, R (eds) Handbook of Industrial Organization, Volume 3, Elsevier, pp. 1967–2072.

FL (2017), 'Förvaltningslag (2017:900)', SFS nr.: 2017:900, 28 September 2017.

Furberg, P and Westberg, M (2020/21), 'Måste myndigheter följa lagarna? Om utkontraktering och legalitet i digital miljö', Juridisk tidskrift, Vol. 2, pp. 406–417.

Försäkringskassan (2019), 'Cloud Services in Sustaining Societal Functions–Risks, Appropriateness and the Way Forward', Swedish Social Insurance Agency, Dnr. 013428-2019, Version 1.0, 18 November.

Gamalielsson, J and Lundell, B (2021) 'On Engagement With ICT Standards and Their Implementations in Open Source Software Projects: Experiences and Insights From the Multimedia Field', International Journal of Standardization Research (IJSR), Vol. 19(1), pp. 1–28.

GAIA (2019), 'Project GAIA-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem', Federal Ministry for Economic Affairs and Energy (BMWi), Berlin, October.

Ghosh, R A (2005), 'Open Standards and Interoperability Report: An Economic Basis for Open Standards', Deliverable D4, MERIT, University of Maastricht, December.

Got (2009), 'Ramavtal IK08335-01: Ramavtal avseende Large Account Reseller (LAR)', Dnr 335/08, Göteborgs Stads Upphandlings AB, Göteborgs Stad, 17 June.

Got (2011), 'Ramavtal IK08335-01 – Data – LAR, Dnr 335/08', Göteborgs Stads Upphandlings AB, Göteborgs Stad, 11 February.

Got (2013a), 'Förfrågningsunderlag', Dnr. 244/13, Göteborgs Stads Upphandlings AB, Göteborgs Stad, 5 April.

Got (2013b), 'Ramavtal programvarudistributör – LAR, Referensnr: UB30113354', Dnr 244/13, Göteborgs Stads Upphandlings AB, Göteborgs Stad.

Got (2015a), 'Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad', Dnr. 0113/11, Tjänsteutlåtande, Intraservice, Göteborgs Stad, 10 March.

Got (2015b), 'Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad', Appendix 2 in Got (2015a), Intraservice, Göteborgs Stad.

Got (2015c), 'Protokoll, § 40 0113/15 (Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad)', Intraservice, Göteborgs Stad, 31 March.

Got (2015d), 'Protokoll (nr 26), § 479 Dnr 1319/11 (Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad)', Kommunstyrelsen, Göteborgs Stad, 23 September.

Got (2015e), 'Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad', Handling 2015 nr 155, Kommunfullmäktige, Göteborgs Stad, 23 September.

Got (2015f), 'Förlängning av ramavtal, Referens: 354/13, 355/13, 356/13', Göteborgs Stads Upphandlings AB, Göteborgs Stad, 24 February.

Got (2016a), 'City of Gothenburg Annual Report 2015', Göteborgs Stad, 5 April 2016.

Got (2016b), 'Framtidsstrategier inom IT – information: Verksamhetschef (10 min.)', Föredragningslista, Intraservice, Göteborgs Stad, 21 June.

Got (2016c), 'Framtidsstrategier inom IT (§59)', Protokoll, Intraservice, Göteborgs Stad, 21 June.

Got (2016d), 'Införande av Office 365, Tjänsteutlåtande', 2 pages without Bilaga 1, Dnr. 0349/16, Intraservice, Göteborgs Stad, 29 June.

Got (2016e), 'Bilaga 1 Införande av Office 365', Version 1.0, Tjänsteutlåtande, Dnr. 0349/16, Intraservice, Göteborgs Stad, 8 August.

Got (2016f), 'Införande av Office 365 (§78 0349/16)', Protokoll, Intraservice, Göteborgs Stad, 23 August.

Got (2016g), 'Förlängning av ramavtal', Dnr: 354/13, 355/13, 356/13, Göteborgs Stads Upphandlings AB, Göteborgs Stad, 19 May.

Got (2016h) 'Formulär för undertecknande av program', Signed by acting head of department, Göteborg Stad Upphandlings AB' on 28 June, Volume Licensing, Microsoft, ProgramSignForm(MSSign)(EMEA)(SWE)(Oct2013).

Got (2017a), 'City of Gothenburg Annual Report 2016', Göteborgs Stad, 4 April 2017.

Got (2017b), 'Svar på förslag till Föreskrifter och riktlinjer om arkiv- och informationshantering i Göteborgs Stad', Tjänsteutlåtande, Dnr. 0252/17, Intraservice, Göteborgs Stad, 22 May.

Got (2017c), 'Remittering av förslag till Föreskrifter och riktlinjer om arkiv- och informationshantering i Göteborgs Stad (§ 66 0252/17)', Protokoll, Intraservice, Göteborgs Stad, 14 June.

Got (2017d), 'Presentation of Office 365 in Göteborgs Stad', the CEO at Intraservice, Göteborgs Stad, Sambruk & Kivos event, Mölndal, 1 November.

Got (2017e), 'Upphandlingsdokument, Upphandling Programvaror 2017: N050-0015/17', Göteborgs Stad Inköp och upphandling, Göteborgs Stad, 20 January.

Got (2017f), 'Programvaror 2017, Ref.nr.: IK17140-01', Dnr 244/13, Göteborgs Stads Inköp och upphandlings, Göteborgs Stad, 8 May.

Got (2017g), 'Revisionsrapport Stadsrevisionen, Nämnden för intraservice – granskning av utlandsresor', Stadsrevisionen i Göteborgs Stad, Dnr. 0288/17, 17 October.

Got (2018a), 'Årsredovisning för räkenskapsåret 2017-01-01–2017-12-31', Göteborgs Stad Upphandlings AB, Org.nr. 556070-5054, Dnr. 102/18, 19 June.

Got (2018b) 'Begäran om sekretessbeläggande', Göteborgs Stad, 26 January.

Got (2018c) 'Er begäran om att få ta del av allmänna handlingar avseende avtal med Microsoft', Göteborgs Stad, Dnr. 230/15, 23 January.

Got (2018d), 'Revisionsrapport Stadsrevisionen, Nämnden för intraservice – granskning av verksamhetsåret 2017', Granskningsredogörelse, Stadsrevisionen i Göteborg, Dnr. 0211/17, 6 March.

Got (2020), 'City of Gothenburg Annual Report 2019', Göteborgs Stad, 7 April 2020.

Heffan, I V (1997), 'Copyleft: Licensing collaborative works in the digital age', Stanford Law Review, Vol. 49(6), pp. 1487–1521.

Hon, W K, Millard, C and Walden, I (2012), 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now', Stanford Technology Law Review, Vol. 16(1), pp. 79–129.

IMY (2021), 'Integritetsskyddsrapport 2020: redovisning av utvecklingen på it-området när det gäller integritet och ny teknik', IMY rapport no. 1, Integritetsskyddsmyndigheten, Stockholm.

IMY (2022) Användning av molntjänster inom offentlig sektor – en sammanställning av en undersökning av sju myndigheter, Integritetsskyddsmyndigheten, Diarienummer: DI-2022-1985, 16 November.

Kaelin, M (2020), 'Office 365 is now Microsoft 365: What you need to know', Tech Republic, 27 April, https://www.techrepublic.com/article/office-365-is-now-microsoft-365-what-you-need-to-know/

Kappos, D J (2017), 'Open Source Software and Standards Development Organizations: Symbiotic Functions in the Innovation Equation', The Columbia Science & Technology Law Review, Vol. 18(2), pp. 259–267.

Katz, A (2012), 'Google, APIs and the Law. Use, Reuse and Lock-In', in Lopez-Tarruella, A (ed) Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, T.M.C. Asser Press, The Hague, ISBN 978-90-6704-845-3, pp. 287–301.

Kesan, J P and Hayes, C M (2014), 'FRAND's Forever: Standards, Patent Transfers, and Licensing Commitments', Indiana Law Journal, Vol. 89(1), pp. 231–314.

Krechmer, K (2013), 'Cloud computing standardization, in How does electrotechnology impact economic, social and environmental development? - Winning papers from the IEC-IEEE Challenge 2012', International Electrotechnical Commission, Geneva, pp. 11–21.

Kritikos, K, Zeginis, C, Iranzo, J, Gonzalez, R S, Seybold, D, Griesinger, F and Domaschka, J (2019), 'Multi-cloud provisioning of business processes', Journal of Cloud Computing, Vol. 8(1), Article number 18, pp. 1–29.

Kroes, N (2008), 'Being Open About Standards', Brussels, 10 June, SPEECH/08/317, European Commissioner for Competition Policy.

Li, J (2018), 'Intellectual property licensing tensions: utilising open source software in the formal standard-setting context', European Journal of Law and Technology, Vol. 9(2), https://ejlt.org/index.php/ejlt/article/view/593

Lindberg, V (2019), 'OSS and FRAND: Complementary Models for Innovation and Development', The Columbia Science & Technology Law Review, Vol. 20(2), pp. 251–270.

Lindström, K (2017), 'Göteborg stoppar Office 365-införande – av säkerhetsskäl', Computer Sweden, 5 October. https://computersweden.idg.se/2.2683/1.690037/gbg-stoppar-office365

Lundell, B (2011), 'e-Governance in public sector ICT procurement: what is shaping practice in Sweden?', European Journal of ePractice, Vol. 12(4), pp. 66–78.

Lundell, B, Gamalielsson, J and Katz, A (2015), 'On implementation of Open Standards in software: To what extent can ISO standards be implemented in open source software?', International Journal of Standardization Research, Vol. 13(1), 47–73.

Lundell, B, Gamalielsson, J and Katz, A (2019), 'Implementing IT Standards in Software: Challenges and Recommendations for Organisations Planning Software Development Covering IT Standards', European Journal of Law and Technology, Vol. 10(2), https://ejlt.org/index.php/ejlt/article/view/709/

Lundell, B, Gamalielsson, J and Katz, A (2020), 'Addressing lock-in effects in the public sector: how can organisations deploy a SaaS solution while maintaining control of their digital assets?', In Virkar, S. et al. (eds) CEUR Workshop Proceedings: EGOV-CeDEM-ePart 2020, Vol-2797, ISSN 1613-0073, pp. 289-296. http://ceur-ws.org/Vol-2797/paper28.pdf

Lundell, B, Gamalielsson, J, Katz, A and Lindroth, M (2021), 'Perceived and Actual Lock-in Effects Amongst Swedish Public Sector Organisations when Using a SaaS Solution', In Scholl, H. J. et al. (eds) EGOV 2021: Electronic Government, Lecture Notes in Computer Science, Vol. 12850, Springer, Cham, pp. 59–72.

Lundell, B, Gamalielsson, J, Katz, A and Lindroth, M (2022), 'Use of Commercial SaaS Solutions in Swedish Public Sector Organisations under Unknown Contract Terms', In Janssen, M. et al. (eds) EGOV 2022: Electronic Government, Lecture Notes in Computer Science, Vol 13391, Springer, Cham, pp. 73–92.

Lundell, B, Gamalielsson, J and Tengblad, S (2016), 'IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning',

Uppdragsforskningsrapport 2016:2, Konkurrensverket (the Swedish Competition Authority), ISSN: 1652-8089. http://www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/forsk_rapport_2016-2.pdf

McGillivray, K (2016), 'FedRAMP, Contracts, and the U.S. Federal Government's Move to Cloud Computing: If an 800-pound Gorilla Can't Tame the Cloud, Who Can?', Science and Technology Law Review, Vol. 17(2), pp. 336–401.

Microsoft (2018), 'Campus and School Agreement', Microsoft, November.

Mowbray, M (2009), 'The Fog over the Grimpen Mire: Cloud Computing and the Law', SCRIPTed, Vol. 6(1), pp. 132–146.

NOC (2007), 'The Netherlands in Open Connection: An action plan for the use of Open Standards and Open Source Software in the public and semi-public sector', The Ministry of Economic Affairs, The Hague, November.

NPS (2016), 'Open IT-standards', National Procurement Services, Kammarkollegiet, Dnr 96-38-2014, 7 March. https://www.avropa.se/globalassets/dokument/open-it-standards.pdf

NPS (2019), 'Förstudierapport Webbaserat kontorsstöd', National Procurement Services, Kammarkollegiet, Dnr 23.2-6283-18, 22 February. https://www.avropa.se/globalassets/forstudierapporter-vt--it/forstudierapport-webbaserat-kontorsstod2.pdf

Odell, M (2009), 'Innovations for Europe: Increasing Public Value, European Public Sector Award', Public Speech, Maastricht, 5 November.

O'Rourke, M A (1995), 'Drawing the Boundary between copyright and contract: Copyright preemption of software license terms', Duke Law Journal, Vol. 45(3), pp. 479–558.

OSL (2009), 'Offentlighets- och sekretesslag (2009:400)', SFS nr.: 2009:400, 20 May 2009.

OST (2017), 'Online Services Terms May 1, Microsoft Volume Licensing Online Services Terms (Worldwide English, May 2017)', Microsoft.

PC (2011), 'Microsoft Office 365 Launching June 28', PC Magazine, 6 June, https://uk.pcmag.com/news/106899/microsoft-office-365-launching-june-28

Phipps, S (2019) Open Source and FRAND: Why Legal Issues Are The Wrong Lens, OpenForum Academy, Open Forum Europe, March.

http://www.openforumeurope.org/wp-content/uploads/2019/03/OFA_-_Opinion_Paper_-_Simon_Phipps_-_OSS_and_FRAND.pdf

Potter, S W (2000), 'Opening Up to Open Source', Richmond Journal of Law and Technology, Vol. 6(5). http://jolt.richmond.edu/jolt-archive/v6i5/article3.html

Radar (2019), 'Moln över kommunerna: hot eller möjlighet?', Radar Ecosytem Specialists, Stockholm.

Regeringen (2009), 'Delegation för e-förvaltning', Dir. 2009:19, Swedish Government, 26 March.

Regeringen (2012), 'Bättre tillgång till kommunala föreskrifter', Regeringens proposition 2011/12:149, 16 May.

Regeringskansliet (2021), 'Säker och kostnadseffektiv it-drift: rättsliga förutsättningar för utkontraktering', Delbetänkande av It-driftsutredningen, Statens Offentliga Utredningar, SOU 2021:1, Stockholm, ISBN 978-91-525-0001-9, ISSN 0375-250X.

Regionarkivet (2017a), 'Remittering av föreskrifter och riktlinjer om arkiv- och informationshantering i Göteborgs Stad', Dnr. AN-1858/16, Västra Götalandsregionen och Göteborgs Stad, 11 April.

Regionarkivet (2017b), 'Bilaga 1: Remittering av föreskrifter och riktlinjer om arkiv- och informationshantering i Göteborgs Stad', Dnr. AN-1858/16, Västra Götalandsregionen och Göteborgs Stad, 11 April.

RF (1974), 'Kungörelse (1974:152) om beslutad ny regeringsform', SFS nr.: 1974:152, 28 Februari 1974.

Riksarkivet (2009a), 'Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)', Riksarkivets författningssamling, RA-FS 2009:1, Riksarkivet, ISSN 0283-2941.

Riksarkivet (2009b), 'Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling), Riksarkivets författningssamling', RA-FS 2009:2, Riksarkivet, ISSN 0283-2941.

Riksrevisionen (2011), 'IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?', RiR 2011:4, Riksrevisionen, Stockholm, ISBN 978 91 7086 241 0.

Savelyev, A (2014), 'Software-as-a-service – Legal nature: Shifting the existing paradigm of copyright law', Computer Law & Security Review, Vol. 30(5), pp. 560–568.

Shapiro, C and Varian, H R (1999), 'The Art of Standards Wards', California Management Review, Vol. 41(2), pp. 8–32.

Silva, G C, Rose, L M and Calinescu, R (2013), 'A Systematic Review of Cloud Lock-In Solutions', in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, IEEE Computer Society, Los Alamitos, pp. 363–368.

Skatteverket/Kronofogden (2021a), 'Beslut: Promemoria om ersättning av Skype i Skatteverkets och Kronofogdens verksamhet', Memorandum regarding the replacement of Skype in the Swedish Tax Agency's and Swedish Enforcement Authority's operations, Decision, 3 May, The Swedish Tax Agency, Dnr. 8-958696, The Swedish Enforcement Authority, Dnr. KFM 10419–2021.

Skatteverket/Kronofogden (2021b), 'Decision: Memorandum regarding the replacement of Skype in the Swedish Tax Agency's and Swedish Enforcement Authority's operations', 3 May, The Swedish Tax Agency, Reference no.: 8-958696, The Swedish Enforcement Authority, Reference no.: KFM 10419–2021.

SLK (2017), 'Promemoria avseende Office 365', Stadsledningskontoret, Göteborgs Stad, 20 October.

SLK (2019), 'Office 365 – bedömning om röjande enligt OSL', Stadsledningskontoret, Göteborgs Stad, 14 November.

Spanaren (2017), 'Revisorskritik: Intraservice bryter mot stadens policy mot mutor', spanaren.se, 17 October. https://spanaren.se/2017/10/17/revisorskritik-intraservice-bryter-mot-stadens-policy-mot-mutor/

Stockholm (2021), 'Underlag för inriktningsbeslut avseende Microsoft 365 och andra molntjänster', Dnr KS 2021/581, Stadsledningskontoret, Stockholm Stad, 9 December.

SVT (2017), 'Politiker från Göteborg på dyr konferens i Seattle', SVT (the Swedish public service television company), 8 July.

UK (2012), 'Open Standards Principles: For software interoperability, data and document formats in government IT specifications', HM Government, 7 September. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/459074/Open-Standards-Principles-2012.pdf

Unni, V K (2016), 'Fifty Years of Open Source Movement: An Analysis through the Prism of Copyright Law', Southern Illinois University Law Journal, Vol. 40(2), pp. 271–300.

Yadegaridehkordi, E, Nilashi, M, Shuib, L and Samad, S (2020), 'A behavioral intention model for SaaS-based collaboration services in higher education', Education and Information Technologies, Vol. 25(2), pp. 791–816.