EGOV-CeDEM-ePart

Addressing Lock-in Effects in the Public Sector: How Can Organisations Deploy a SaaS Solution While Maintaining Control of Their Digital Assets?

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

*University of Skövde, Sweden, bjorn.lundell@his.se
**University of Skövde, Sweden, jonas.gamalielsson@his.se
**University of Skövde, Sweden, Moorcrofts LLP, UK, andrew.katz@moorcrofts.com

Abstract: As software as a service (SaaS) adoption increases in both the public and private sectors, so does dependency on specific providers and technologies and the consequent danger of lock-in. This paper reports on how public sector organisations (PSOs) can, and should, avoid lock-in throughout the lifecycle (commissioning, deployment and decommissioning) of their deployment of the Microsoft Office 365 SaaS product (O365). We investigate how 33 PSOs address different lock-in effects, focussing on the City of Gothenburg, and show that none of the PSOs determined possible lock-in effects prior to implementation or were able to provide documented evidence that they would be able to independently access, process and maintain the digital assets processed by the SaaS solution after decommissioning. We also report on jurisdictional and data processing issues, with consequent impact on digital sovereignty.

Keywords: lock-in, public sector, SaaS solutions, cloud, open standards

Acknowledgement: This research has been financially supported by the Swedish Knowledge Foundation (KK-stiftelsen) and participating partner organisations in the LIM-IT project. The authors are grateful for the stimulating collaboration and support from colleagues and partner organisations, and for valuable discussions with Mathias Lindroth.

1. Introduction

Digital and data sovereignty is an increasing concern for countries wishing to maintain control of digital assets. At the same time, there is an increasing dependency on international providers of ICT solutions, and particularly cloud-based SaaS solutions (e.g. EC, 2020; Försäkringskassan, 2019; GAIA, 2020; Lundell et al., 2016; Radar, 2019) which process those assets. Research shows that lock-in effects can impose many different types of technical, legal, economic and societal challenges for public sector organisations ("PSOs") (Contreras, 2015; EC, 2014; Egyedi, 2007; Ghosh, 2005; Lundell et al., 2016; Lundell and Gamalielsson, 2018; Lundell et al., 2019). The overarching goal of this study is to investigate and explain how use of commercial SaaS solutions may cause different types of lock-in effects that impact on a PSO's ability to maintain control of its digital assets.

A number of initiatives that seek to mitigate problematic lock-in effects from technical, legal, and societal perspectives (e.g. Ghosh, 2005; Regeringen, 2009; SOU, 2009; NPS, 2016, 2019; Lundell et al., 2019) have been proposed. For example, several countries have published policies and strategies for open standards (e.g. NOC, 2007; UK, 2015; NPS, 2016) initiatives and proposals addressing digital and data sovereignty (e.g. GAIA, 2019). The public sector has seen significant deployment of SaaS solutions. For example, in August 2019 it was reported that, in Sweden, all large municipalities and about half of all municipalities used a specific SaaS solution, namely Microsoft Office 365 ("O365") (Radar, 2019). Such use implies that the municipalities' digital assets are processed and maintained in jurisdictions outside Sweden.

When using SaaS solutions to export files in closed file formats and closed standards it may be impossible to implement such formats and standards in third party software projects for a number of technical and legal reasons (Lundell et al., 2019), even if patent rights are available under so-called fair, reasonable and non-discriminatory (FRAND) terms. Research shows this may also be the case for open source software (OSS) projects (e.g. Blind and Böhm, 2019; Lundell et al., 2015, 2019). Accordingly, PSOs must ensure that, before adopting a SaaS solution, all processed data and metadata can be exported in files using open file formats (NPS, 2016) enabling them to be processed after use of the SaaS solution has ceased, through software sustainably implemented in OSS capable of processing all the relevant formats (Lundell et al., 2019).

The use of SaaS by PSOs also raises legal issues: a report from Radar (2019) shows that 88% of the 290 Swedish municipalities have undertaken a legal analysis on the use of cloud services (such analysis being undertaken either in-house or by external experts). However, previous research shows that there are several technical and legal challenges related to exit from a SaaS solution in terms of long-term maintenance of files after an organisation has ceased using it (Lundell et al., 2019). The study investigates the following research question (RQ): How do, and by which strategies should, public sector organisations address lock-in effects before use of commercial SaaS solutions?

The study explains how PSOs that have adopted SaaS solutions have considered and taken actions for maintaining control of their digital assets during the entire life-cycle of those assets. The investigation focuses on O365 and considers its adoption and use in the public sector. O365 is a widely deployed SaaS solution (which shares similar functionality with SaaS solutions from other vendors such as Google Gsuite), and a representative example of a cloud solution that has recently gained significant interest amongst PSOs.

The paper presents three principal contributions. First, we identify critical strategies for what to consider and how to take action before an organisation adopts and uses a SaaS solution. Second, we present insights from the adoption of O365 by 33 PSOs focusing on the risks for different types of lock-in effects, and in doing so we report on actions taken before adoption and identify strategies that would allow for a sustainable exit. Third, we report on strategies for how digital assets can, and should, be maintained after exit from a SaaS solution and specifically present novel findings concerning file format lock-in after exit from O365.

2. Research Approach

Through a review of the literature, which also considered published policies and strategies, strategies for how a PSO can avoid lock-in effects prior to adoption and use of a SaaS solution were identified (see Table 1). The review also considered strategies for how to maintain digital assets after a PSO has ceased to use a SaaS solution.

We initially investigated an influential large scale deployment of O365 in a large PSO – the City of Gothenburg ("CoG") (Gothenburg, 2018), a municipality with over half a million citizens and 56000 employees – that gained public exposure and public debate concerning the lawfulness of using O365 under Swedish law (Lindström, 2017; Nordström, 2020; SLK, 2017, 2019). We randomly selected 30 PSOs (and it was discovered that 29 of the 30 used O365) and selected 3 further PSOs that had publicly contributed to a report by SALAR (2019). Hence, public documents for a total of 33 PSOs were investigated for their adoption and use of O365.

The standards-setting process used by many standards setting organisations (SSOs), including ISO and ITU-T, allows organisations which claim to hold patents affecting implementation of standards to declare their claims in a publicly-accessible database maintained by the SSO. We reviewed such declarations which may impinge both on aspects of use of O365 and also the ability of customers to interpret and process files exported from their deployment of O365. Drawing from previous research, including Lundell et al. (2015, 2019), we reviewed how the PSOs have analysed patent risks and assessed if they have obtained third-party patent licences as mentioned in the Online Services Terms for O365 (e.g. OST, 2019). To investigate if PSOs have established sustainable exit strategies we investigated, through use of an action-case research approach, if it is possible to obtain patent licences allowing long-term maintenance of digital assets even after O365 is no longer used. To investigate whether it is possible to obtain necessary third party rights related specifically to the ITU-T H.265 standard (as detailed in the Online Services Terms for O365), we investigated all declarations made in the two relevant patent databases (ITU-T and ISO) and requested patent licences from all declarants. This phase of the study extends previous research (see Lundell et al., 2019) which seeks to obtain all necessary rights from third parties in order to allow for use and implementation of relevant standards (including the ITU-T H.265 standard) in software. The ITU-T H.265 standard investigated is jointly developed and provided by the ITU-T and ISO, so the investigation covered relevant information from patent databases provided by both ITU-T (2019) and ISO (2019). Specifically, we seek to obtain patent licences for the ITU-T H.265 standard essential patents which relate to all declarations in the specific patent databases. So that these licences can be used by a range of OSS projects, we explicitly request conditions compatible with establishing OSS projects under one (or several) of the three specific OSS licences: GPL 3.0, MPL 2.0, and Apache 2.0 (Lundell et al., 2019).

3. Results

Table 1 presents a conceptualisation of results, in the form of a set of factors with associated issues that a PSO should consider before adoption and use of a O365 solution, which evolved during the

review of the literature. The evolved factors and related issues constitute a basis for subsequent presentations of how PSOs have addressed the identified issues.

Table 1: Factors and Associated Issues to Consider Before Adoption and Use of a SaaS Solution

Factors (F1-F4) & issues	**Basis for evolved factors & issues include**
F1: Availability of all contract terms. Have all relevant contract terms been obtained, understood and accepted? Are relevant contract documents maintained?	Have you reviewed the agreement and understood the terms of the agreement, for example if the terms unilaterally can be changed by the supplier? (eSam, 2018)
F2: Availability of all necessary licences. Have relevant licences been identified? Have relevant licences been obtained?	Lawful use of certain file formats both during and after use of the SaaS solution may require patent and other licences. (Blind and Böhm, 2019; Contreras, 2015; Lundell et al., 2015, 2019; Lundell and Gamalielsson, 2018)
F3: Impact assessment. Is an impact assessment available? What are implications of data processing and potential disputes in different jurisdictions?	Impact assessment needs to show GDPR compliance (GDPR Article 35(4)), technically, procedurally, and legally (DI, 2019).
F4: Exit strategy. Is an effective exit strategy available? Have licences been obtained that allow for reuse of digital assets after exit? Is software (from different providers) available that allows for interpretation of files after exit from the SaaS solution?	Is there a strategy that allows for abandoning the cloud service in the future (an exit plan)? (eSam, 2018); Digital assets need to be exported in open standard formats (NPS, 2016; Lundell et al., 2019); PSOs need to obtain all licences and technical specifications to allow for interpretation of files after exit from a SaaS solution (Lundell et al., 2019; Lundell and Gamalielsson, 2018)

Concerning **availability of all contract terms** we find that no PSO has undertaken any action to obtain all contract terms related to third party rights as detailed in the online service terms (OST, 2019). Further, none of the PSOs have obtained and retained documentation of all contract terms despite having accepted the "Program Signature Form" which states: "By signing below, Customers and the Microsoft Affiliate agree that both parties (1) have received, read and understand the above contract documents, including any websites or documents incorporated by reference and any amendments and (2) agree to be bound by the terms of all such documents."

Concerning **availability of all necessary licences** which allow for use of digital assets we find that no PSO has obtained all licences from third parties as detailed in the contract terms for O365: "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, 2019) Therefore, the customer 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, it is currently unclear if it will be possible to obtain all necessary rights from all third party rights holders for the ITU-T H.265 standard that the PSOs are bound by when using O365. Crucially, this standard is normatively referenced (via other standards) in the ISO/IEC 29500 standard (OfficeOpen XML). Results from the investigation have found no indication to suggest that any of the 33 PSOs have obtained (or even considered the need to obtain) such licences. Hence, under the

assumption that the ISO/IEC 29500 standard is implemented by O365 it follows that data that is exported from O365 (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 O365 it follows that a customer signing the contract is exposed to certain risks (for no reason), but more importantly that customers exporting data from O365 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 O365 is unknown.

Concerning **impact assessment** we found that CoG and the most other PSOs have not undertaken an impact assessment (as detailed in GDPR's Article 35(4)) and, further that there is general unawareness concerning in which jurisdictions data processing and maintenance of each PSO's data has taken (and can take) place. It is clear that analyses of contract terms need to take into account different jurisdictions and legal systems, since jurisdiction and choice of law clauses covering the provision of O365 extends beyond Swedish law. Further, documentation provided by some PSOs referred to information provided by Microsoft which shows that many subprocessors based in different third countries (including Brazil, Chile, China, Egypt, India, Malaysia, Serbia, Singapore, South Korea, USA, and United Arab Emirates) are authorised to access customer data and personal data for provision of O365.

Concerning **exit strategy** which allow for reuse of digital assets we find that no PSO has access to an effective exit strategy that can be implemented after exit from O365 at short notice. An effective exit strategy will cover a PSO's continuing ability to make it possible to read and write files exported from O365, which will require software and associated licences covering those formats . It is clear that no PSO has sought to obtain licences to standard essential patents (SEPs) potentially impinging on the file formats referenced in the Online Services Terms for O365. There are a number of declarants of SEPs related to the ITU-T H.265 standard and there is no indication (in any of the responses) and no documentation from any of the PSOs that they have even considered the implications of the Online Services Terms for O365 they are bound by. Further, based on information provided during the study, we find no evidence that PSOs have considered potential risks related to SEPs that may arise from use of closed file formats. In addition, some files received during data collection from PSOs (including ".docx" and ".pdf" files) were themselves provided in several closed file formats that may impose significant challenges for any organisation that seeks to maintain files being exported from O365. These findings extend results from previous research, namely that it may not be possible to obtain licences necessary for legal reasons to interpret files in the PDF/A-3 format during the lifespan of SEPs declared in the ITU-T and ISO patent databases, potentially for many years (e.g. Lundell et al., 2019). Further, previous research also shows that it is unclear if the complete technical specification for ".docx" files exported from O365 can technically and legally be interpreted (Lundell et al., 2019). We find that PSOs are generally unaware of the complexities involved in interpreting the ISO/IEC 29500 file format standard (and all normative references included in several levels) and associated risks related to use and reuse of files represented in closed file formats that have been exported from O365. Overall, there is an overwhelming lack of documentation

showing analysis of the legal and technical challenges arising from continued use of files that have been exported from O365 without continued support from the current supplier.

4. Discussion and Conclusions

The study shows a widespread practice amongst PSOs to adopt and use a widely deployed SaaS solution from a global supplier under potentially problematic contract terms. The City of Gothenburg and most other PSOs use their adopted SaaS solution to process data on a large scale with users that are in a position of dependence without having carried out an impact assessment, despite the fact that PSOs are unaware of in which jurisdictions data can be, and have been, processed. Some PSOs identified prior to their adoption and use of their SaaS solution that the terms allow for data processing in several third countries. None of the organisations present any evidence to suggest that they have tried to obtain all necessary patent licences for the ITU-T H.265 standard from third parties which would allow for use of the adopted SaaS solution. Since these licences, in addition to licences for a large number of other standards, would also be needed to allow for implementation of the closed file format standards in software that can be provided by other suppliers it follows that organisations are potentially exposed to significant risks of losing control over their own digital assets.

Findings from the study also show that none of the investigated organisations present any strategy that would allow them 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 amongst the few PSOs that present some documented risk analysis there is strong faith that their current supplier will assist in a potential future situation if the PSO decides to abandon their current supplier.

Further, findings show that recommendations presented in the literature for how to maintain digital assets during their entire life-cycle have been ignored by all investigated PSOs. Before adoption of a SaaS solution, none of the organisations had investigated whether digital assets created and maintained in the SaaS solution can be exported in open file formats and open standards to allow use and reuse after exit. Further, none of the investigated PSOs have presented any analysis which addresses how to obtain all licences they require when, and after, the adopted SaaS solution is used. Hence, it is unclear if any of the organisations will be able to interpret their own files without support from their current supplier in a potential future situation when they have ceased to use the SaaS solution.

In summary, all investigated PSOs have failed successfully to address critical issues that need to be considered before adoption and use of a SaaS solution.

References

Blind, K. & 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.

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

DI (2019) List regarding Data Protection Impact Assessments according to article 35.4 of the Data Protection Regulation, Dnr. DI-2018-13200, Datainspektionen.

EC (2014). 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 Mar., ISBN 978-92-79-35991-0.

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 Feb.

Egyedi, T. (2007). Standard-compliant, but incompatible?!, Computer Standards & Interfaces, 29(6), 605-613.

eSam (2018). Checklista inför beslut om molntjänster i offentlig sektor, 31 October. Avaliable at: http://www.esamverka.se/stod-och-vagledning/rekommendationer-och-checklistor/checklista-infor-beslut-om-molntjanster-i-offenlig-sektor.html

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 Nov.

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, Oct.

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

Gothenburg (2018). City of Gothenburg: Annual Report 2018, Göteborgs Stad. www.goteborg.se

ISO (2019). ISO standards and Patents, International Organization for Standardization. https://www.iso.org/iso-standards-and-patents.html (Accessed 9 Jun. 2019).

ITU-T (2019). Intellectual property rights (IPR) in ITU Recommendations, International Telecommunication Union (ITU). https://www.itu.int/net4/ipr/search.aspx (Accessed 9 Jun. 2019).

Lindstrom, K. (2017). Göteborg stoppar Office 365-införande – av säkerhetsskäl, Computer Sweden, 5 Oct.

Lundell, B. & Gamalielsson, J. (2018). Sustainable digitalisation through different dimensions of openness: how can lock-in, interoperability, and long-term maintenance of IT systems be addressed?, In Proceedings of the 14th International Symposium on Open Collaboration (OpenSym '18), ACM, New York, ISBN: 978-1-4503-5936-8, Article 3, 10p.

Lundell, B., Gamalielsson, J. & 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, 13(1), 47-73.

Lundell, B., Gamalielsson, J. & 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, 10(2).

Lundell, B., Gamalielsson, J. & 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.

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, Ministry of Economic Affairs, The Hague, Nov.

Nordström, L. (2020). SKR: Välkommet att Göteborgs molntjänster granskas, Dagens Samhälle, 27 Jan.

NPS (2016). Open IT-standards, National Procurement Services, 7 Mar., Dnr 96-38-2014.

NPS (2019). Förstudierapport Webbaserat kontorsstöd, National Procurement Services, 22 Feb., Dnr 23.2-6283-18.

OST (2019). Online Services Terms Jun. 1, Microsoft.

Radar (2019). Moln över kommunerna: Hot eller möjlighet?, Radar Ecosystem Specialists, Stockholm.

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

SALAR (2019). Molntjänster och konfidentialitetsbedömning, Swedish Association of Local Authorities and Regions, Stockholm, 5 Nov.

SOU (2009). Strategi för myndigheternas arbete med e-förvaltning, Statens Offentliga Utredningar: SOU 2009:86, e-Delegationen, Finansdepartementet, Regeringskansliet, Stockholm, 19 Oct.

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

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

UK (2015). Open Standards Principles: For software interoperability, data and document formats in government IT specifications, HM Government, 7 Sep.

About the Authors

Björn Lundell

Björn Lundell is a senior researcher at the University of Skövde, Sweden. He leads the Software Systems Research Group, has conducted research related to free and open source software in a number of projects, and his research is reported in over 100 publications in international journals and conferences.

Jonas Gamalielsson

Jonas Gamalielsson is a researcher at the University of Skövde, Sweden. He has conducted research related to free and open source software in a number of projects, and his research is reported in a number of publications in international journals and conferences.

Andrew Katz

Andrew Katz is a visiting researcher at the University of Skövde, Sweden and a partner at boutique law firm Moorcrofts LLP, based in England's Thames Valley. Andrew specialises in technology law and has a particular interest in open design and development.