Perceived and Actual Lock-in Effects Amongst Swedish Public Sector Organisations When Using a SaaS Solution

Björn Lundell, Jonas Gamalielsson, Andrew Katz, Mathias Lindroth

Perceived and Actual Lock-in Effects Amongst Swedish Public Sector Organisations when Using a SaaS Solution

Björn Lundell[1], Jonas Gamalielsson[1], Andrew Katz[1,2], Mathias Lindroth[3]

[1] University of Skövde, Sweden
[2] Moorcrofts LLP, UK
[3]ACF Legal Intl. AB, Sweden
{bjorn.lundell|jonas.gamalielsson@his.se,
andrew.katz@moorcrofts.com, mathias.lindroth@acflegal.org}

Abstract. When a public sector organisation (PSO) uses a software as a service (SaaS) solution from a global provider this imposes risks for different types of lock-in effects. In turn, use of such solutions by PSOs may prevent full control of digital assets that need to be created, processed, maintained, and archived for use and reuse over long life-cycles. This paper addresses perceived and actual lock-in effects related to use of SaaS solutions in the public sector. We review perceptions of lock-in amongst government agencies and investigate how 46 PSOs have addressed challenges related to obtaining licences and an effective exit plan related to use of the Microsoft Office 365 SaaS solution. Through a review of responses to a survey conducted by the Swedish Government Offices we find significant misconceptions concerning lock-in effects. We find that every one of the 46 PSOs investigated neither obtained necessary licences nor established an effective exit strategy to allow the PSO to independently access, process and maintain digital assets processed by the SaaS solution after decommissioning. We present recommendations for any PSO considering use of a SaaS solution.

1 Introduction

On 26 September 2019 the Swedish Government issued a directive which commissioned an investigation relating to secure and cost-effective IT operations for the Swedish public sector [32]. On 15 January 2021 the Swedish Government Offices presented a report from that investigation which "focus[es] on the conditions for the outsourcing of IT operations by government agencies, municipalities and regions" [37]. The report shows extensive use of SaaS (Software as a Service) solutions amongst governmental agencies and reports that 95% of the agencies "use some form of Software as a Service" [37]. The overarching goal of this study is to investigate and explain critical aspects of how perceived and actual lock-in effects in the Swedish public sector impact on a public sector organisation's ability to conduct lawful and cost-effective IT operations through use of a SaaS solution from a global provider.

The European Commission has highlighted the importance to the EU of "technological sovereignty" [8] and there are initiatives for addressing digital and data

sovereignty [14]. Many individuals, organisations, and member states in the EU are concerned over exposure and an increasing dependency on global providers of cloud-based SaaS solutions [8, 12, 14, 22, 23, 28, 30, 37]. For example, as stated by Hon et al. [17]: *"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."* Further, a study of a widely deployed SaaS solution from a global provider: Microsoft (Office 365, the Microsoft Office 365-solution, hereinafter referred to as 'O365') shows that the customer is required to acquire patent licences for the ITU-T H.265 standard and findings show that the 33 investigated public sector organisations (PSOs) have failed to obtain all necessary patent licences *"which would allow for use of the adopted SaaS solution"* [22].

Extensive investigations of a large number of projects undertaken by many different PSOs recognise that adoption and use of SaaS solutions provided by global providers typically involves dealing with complex and incomplete contracts which expose organisations to a range of different lock-in effects [21, 22, 23]. For example, a study which investigated 33 PSOs that have adopted and use O365 found that "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" [22]. Further, the same study found that no PSO "has obtained all licences from third parties as detailed in the contract terms for" the specific SaaS solution [22]. In addition, findings also show that 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" [22]. It should be noted that such an exit-strategy requires the use of software and its associated licences as well as (potentially) licences covering file formats used when exporting files.

This study investigates the *following research questions*:

RQ1: How do public sector organisations that use commercial SaaS solutions perceive lock-in effects?

RQ2: How are public sector organisations that use commercial SaaS solutions actually locked-in?

The paper presents three principal contributions. First, we identify perceptions of lock-in amongst the Swedish Government, the Swedish Government Offices, and Swedish PSOs through a review of a directive [32] and a report which investigated IT operations for the Swedish public sector [37]. Specifically, we identify perceptions of lock-in amongst governmental agencies through a critical review of survey results in order to report on how the investigation has addressed its directive related to analysis of lock-in effects (section 4). Second, for addressing the second research question we investigate use of a widely deployed SaaS solution (O365) amongst 46 PSOs with a focus on licences and the risks of lock-in effects, and report on actions taken by organisations before use with a review of availability of licenses for lawful use and strategies that would allow for a sustainable exit (section 5). Hence, the present investigation of actual lock-in related to use of O365 extends previous research which also investigated use of O365 amongst 33 other PSOs [22]. Third, we present five key

questions which any organisation needs to analyse and answer in the affirmative before (and during the entire life-cycle for when) a SaaS solution from a global provider is used (section 6).

2 On lock-in effects and SaaS solutions

Interoperability amongst heterogeneous ICT solutions is essential for long-term maintenance of digital assets and the success of effective eGovernment solutions. Faithful implementations of open ICT standards and open file formats promote software interoperability and avoid lock-in effects, which are essential prerequisites for cost-effective eGovernment solutions. Research shows that lock-in effects can impose many different types of technical, legal, economic and societal challenges for PSOs [1, 2, 3, 5, 6, 7, 9, 10, 15, 18, 19, 23, 25]. For example, challenges related to use of cloud and SaaS solutions from global providers have been elaborated as follows [14]: *"**Lock-in effects** emerge between customers and providers of cloud services if the switchover to an alternative provider of solutions or services is made more difficult, or indeed impossible, by switchover costs and barriers. The barriers to a switchover can be of a technical-functional kind (dependence on the specific features of certain providers); they can arise from contractual agreements (e.g. license models and penalty costs), but also result from a high, customer-specific degree of personalisation, from familiarisation effects, or from the sheer data volume that is to be migrated."*

The public sector has seen significant deployment of SaaS solutions over the past few years. For example, in August 2019 it was reported that, in Sweden, all large municipalities and about half of all municipalities of any size used O365 [30]. Further, recent research indicates that use of O365 amongst all 290 Swedish municipalities may be even more widespread, in light of the observation that 97% (29 of 30) of the municipalities that were randomly selected for a study used the solution [22].

For several decades, PSOs have considered standardisation and utilisation of standards as a strategy for avoiding problematic lock-in effects [16] and studies have recognised the importance of open source software projects for implementation of standards [2]. However, research shows that it may be impossible to clarify conditions and obtain all patent licences for standard essential patents (and all necessary rights) for use of the O365 solution [21]. In fact, use of specific formal standards that are provided on FRAND-terms may inhibit implementation in software projects [20, 21]. Such conditions may significantly inhibit an effective exit-strategy for a PSO that wishes to abandon use of a specific SaaS solution.

The importance of an exit strategy has been stressed by various policy recommendations [11, 23, 38]. For example, the UK Government has stated that exit costs from an IT solution used by a government authority must be associated with the initial investment: *"As part of examining the total cost of ownership of a government IT solution, the costs of exit for a component should be estimated at the start of implementation. As unlocking costs are identified, these must be associated with the incumbent supplier/system and not be associated with cost of new IT projects."* [38] Further, to promote software interoperability and avoid lock-in effects, the UK

Government highlights the importance of open standards when formulating an exit strategy: *"In preparation for any technical refresh projects, or in exceptional circumstances, where extensions to IT contracts or to legacy solutions have been agreed, government bodies must formulate a pragmatic exit management strategy. These must describe publicly the existing standards used together with the transition to open standards and compulsory open standards."* [38]

Policy initiatives in several countries have recognised the importance of open standards and open file formats in order to avoid lock-in effects into specific platforms and solutions [20, 26, 27, 31, 38]. To avoid lock-in effects, it is important that an adopted SaaS solution is able to export digital assets in open standards and open file formats [21, 27].

3 Research approach

We investigated *perceived lock-in effects* amongst PSOs as follows (RQ1). First, through a review of how lock-in effects have been considered by the Swedish Government as presented in its directive for an investigation of secure and cost-effective IT operations for the Swedish public sector [32], we establish a contemporary national policy goal for public administration related to lock-in effects. Second, through a critical review of the report [37], we establish how the investigation undertaken by the Swedish Government Offices has fulfilled their task (as detailed in the directive [32]). Third, through a review of responses from Swedish PSOs (in this case, governmental agencies) to a questionnaire and an analysis of how the report presents perceived lock-in effects, we consider the extent to which the report [37] reflects responses to the questionnaire by PSOs and considers fulfilment of the directive related to policy goals concerning planned investigation of how PSOs are able to address lock-in effects as presented in the directive [32].

We investigated *actual lock-in effects* amongst PSOs (RQ2) by drawing from a previously conducted literature review which identified four essential factors that impact on a PSO's ability to lawfully use a SaaS solution from a global provider [22]. This study considers two of those four factors, namely *availability of all necessary licences* and *availability of an effective exit strategy*, that impact on a PSO's ability to lawfully use the O365 solution whilst maintaining control of their digital assets, both during and after use of O365. First, we selected 46 PSOs that use O365 (based on indications of use presented in public sources) for investigation of the two factors. The selected PSOs comprised 13 PSOs under the government, 8 regional PSOs, and 25 local authorities (municipalities). None of these 46 PSOs were investigated in the previous study [22] covering O365-using PSOs. Second, we reviewed the *availability of all necessary licences* based on documentation we requested from each PSO. We analysed the contract terms and licences provided as part of that documentation with a view to considering whether each PSO had obtained all licences necessary for using O365 (as detailed in the applicable O365 contract terms) and also whether manipulation, import and export of digital assets was possible independently of the O365 solution. Third, we reviewed the *availability of an effective exit strategy* based on an analysis of the

documentation we requested from each PSO. In particular, we considered whether the exit strategy included provision for continued maintenance and re-use of digital assets should the PSO cease to use the O365 solution.

4 Observations on perceived lock-in amongst public sector organisations

The importance of obtaining all necessary licences for lawful and effective data processing of digital assets has been recognised in different contexts [21, 22, 38]. Related to a national eGovernance initiative, the Swedish Government has stressed the importance of open standards for avoiding dependence on specific platforms and solutions [31]. We find that the first report from the national eGov initiative recognised the importance of using open standards for avoiding lock-in [36]. Further, on 31 October 2018 we find that eSam (a subsequent Swedish national initiative) presented a checklist for PSOs related to use of cloud and SaaS solutions which stresses the importance of availability of a plan for exit [11].

The recent Swedish government directive recognises lock-in effects as an important factor which needs to be considered when analysing cost-effective IT operations and emphasises that a task for the investigation is to review the ability amongst PSOs to identify risks for lock-in effects [32]. Specifically, the directive states that the investigator shall survey PSOs' ability to identify risks for lock-in effects [32].

The survey is based on a questionnaire to *"government agencies, case studies of five agencies and a workshop attended by representatives of 16 agencies"* [37]. On 17 March 2020 the Swedish Government Offices sent the questionnaire (containing 31 questions) to 180 Swedish government agencies[1] (see Appendix 3 [37]) with a request for responses to the questionnaire no later than 31 March 2020. Amongst the respondents, 158 government agencies in total responded to (at least some) questions in the questionnaire [37].

The report includes results from the survey conducted amongst governmental agencies which show that "lock-in effects" are major obstacles preventing "cost effective IT operation" [37]. Specifically, the report presents findings from the survey as follows [37]: *"The greatest obstacles to secure IT operations are deficient information classification and a lack of expertise in IT and security, as well as of procurement expertise. Lack of expertise is seen as a risk factor for secure IT operations among both small and large agencies. The greatest obstacles to cost-effective IT operations are high security requirements and various types of lock-in effects, as well as shortages of expertise."*

We find that 52 government agencies provided a response to the questionnaire with comments related to *vendor lock-in or other lock-in effects* which is included as one (of a total of six) potential factors (in question 27 of the questionnaire) that may prevent

[1] The report states that the survey is based on a questionnaire to 200 government agencies [37]. However, on 24 March 2020 it was clarified (by a representative from the Swedish Government Offices) that the survey was sent to 180 government agencies.

cost-effective IT operations. Further, we find that 83 government agencies provided a response with comments related to *other* as another potential factor (in question 27) and that several of these comments also indicate perceived lock-in effects amongst respondents. In addition, we find that 88 government agencies provided additional comments (of which some government agencies highlighted challenges related to lock-in) in their response to a question about *other* issues that a respondent wanted to add or clarify as part of their response (question 31 of the questionnaire).

Further, we note that amongst government agencies which provided a response to *other* (in question 31), several of these agencies did not provide a response related to the factor *vendor lock-in or other lock-in effects*. This, in turn, shows that any thorough analysis of perceived lock-in effects amongst respondents needs to consider, at least, all responses and comments related to *vendor lock-in or other lock-in effects* and *other* issues (related to question 27) and also other issues (related to question 31). However, we find that the report fails to present such a thorough analysis, and several critical aspects of lock-in which have been raised and highlighted by respondents in responses to the questionnaire have been ignored by the investigation.

The report [37] states (in Figure 4.4) that 21% of the government agencies express that *vendor lock-in or other lock-in effects* prevent cost-effective IT operations. However, from analysis of responses to the questionnaire we find that this is misleading. In fact, we find that the proportion of government agencies which in their responses have expressed that *vendor lock-in or other lock-in effects* prevent their cost-effective IT operations is much higher.

Based on a dialogue with representatives for the investigation we have received information[2] which stresses that 33% of the government agencies express that *vendor lock-in or other lock-in effects* prevent cost-effective IT operations. However, from analysis of responses we find that this number is also misleading (since responses related to lock-in effects have been reported under others and also that this proportion is based on the total number of government agencies (i.e. 158) which responded to some questions). Hence, since only 52 government agencies responded (and of which more than 80% report lock-in effects) we find the report is misleading concerning the proportion of agencies that have experienced lock-in effects.

Many government agencies state in their respective response to the questionnaire that they experience different types of lock-in effects which prevent cost-effective IT operations for their own agency. Several respondents experience vendor lock-in and express concern over dependence of specific global suppliers that prevent cost-effective IT operations. For example, amongst responses we observe government agencies which express dependence on a global supplier of a SaaS solution (e.g. responses mention dependence on Microsoft for O365) and others which express dependence on Swedish suppliers (e.g. Statens Servicecenter, Ladok, and Försäkringskassan). We also observe concern over problematic dependencies between software and hardware which imply problematic dependencies on specific suppliers. Further, some respondents express

[2] For example, on 3 February 2021 a representative for the investigation explained that analysis of responses to the questionnaire (which reports 21%) is based on consideration of all six factors under question 27 which includes several factors that are unrelated to lock-in.

concern over *contract lock-in* and yet other over *competence lock-in* related to use of external suppliers (cloud and SaaS solutions). Some respondents raise legacy issues with already procured licences as inhibitors which cause lock-in. In addition, *format lock-in* is also mentioned amongst respondents as a concern which prevents cost effective IT operations, and mention that they try to use open standards to mitigate such lock-in. One governmental agency also highlights legal issues related to format lock-in as a serious risk which prevents longevity of digital assets. This, in turn, inhibits cost-effective IT operations.

Amongst responses we observe government agencies which express positive experiences from their use of SaaS solutions from global suppliers (e.g. several mention Microsoft 365). Further, one respondent raises concern over risks that government agencies become dependent on solutions from three specific global providers (Amazon, Google, and Microsoft), whilst at the same time highlighting that it may be unrealistic for organisations to develop alternatives without international collaboration.

Respondents express different views concerning whether SaaS solutions are cost-effective. For example, as expressed by one respondent: *"We currently have cost-effective IT operations which fulfil the needs for our organisation. To only use SaaS solutions or to outsource IT operations in a traditional sense cannot be motivated from a cost nor a functionality perspective."* On the contrary, another respondent (representing a small governmental agency) expresses that the internal policy is to avoid using a SaaS solution from a global provider for legal reasons, even though such solutions may be more cost-effective.

Several respondents express concern related to legal issues and we find that the report only addresses a few of these legal issues which may impact on IT operations. Further, responses to the questionnaire, observations from case studies of the five selected government agencies, and the workshop (attended by representatives of 16 agencies) highlight challenges under different jurisdictions for any PSO that uses (or plans to use) cloud and SaaS solutions from global providers. For example, we find that the report does not address several critical technical and legal issues related to lock-in and use of a widely deployed SaaS solution (specifically, O365): copyright, patents, archiving, laws related to governance of digital assets, and national laws (in Sweden and other countries) which may impact on data processing when PSOs use O365 (e.g. the Swedish Säkerhetsskyddslagen and the Chinese NIL [24]). Reports from the questionnaire and the case studies [37] show that O365 is used in a number of government agencies. However, critical licensing issues, lock-in challenges, and several legal challenges identified in responses to the questionnaire and the five case studies are not addressed in the report [37]. In addition, we find that the report lacks a comprehensive coverage of several other legal issues and regulations which impact on widely used SaaS solutions from global providers, especially in light of the observation that many SaaS solutions use subprocessors for data processing in several different countries [22].

Further, the directive highlights that public procurement impacts on lock-in effects [22]. However, we find that the report from the investigation fails to analyse important strategies for addressing lock-in effects, including experiences from other countries (despite that a goal for the investigation is to review experiences from the UK). This

includes published strategies for addressing exit costs which have been presented by eSam [11], adopted in the UK [38] and recommended in a report from commissioned research published by the Swedish competition authority [23].

5 Observations on actual lock-in amongst public sector organisations

Concerning availability of all licences necessary for the use of digital assets created and processed by O365 we find that no PSO has obtained all third party licences as detailed in the contract terms for the O365 solution. Specifically, the contract terms state: *"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."* [29] Hence, since the O365 licence explicitly does not provide such licences, the customer must obtain its own licences from any third party rights holders related to the ITU-T H.265 standard.

Based on the information that has been provided during the study, we find that it is unclear if it will be possible to obtain all necessary rights from all third party rights holders for the ITU-T H.265 standard which the PSOs are bound by when using the O365 solution. Further, this standard is normatively referenced (via other standards) in the ISO/IEC 29500 standard (OfficeOpen XML). Observations from the study showed no indication to suggest that any of the 46 PSOs have obtained (or even considered the need to obtain) such licences. Consequently, under the assumption that the ISO/IEC 29500 standard is faithfully implemented by the O365 solution it follows that digital assets exported from the O365 solution (and stored locally as '.docx' files) may impinge on patents that have been declared as standard essential for the ISO/IEC 29500 standard (and including all its normative references) in the ISO and ITU-T patent databases (and also on patents which may be standard essential patents (SEPs) even if those have not been declared in any of these patent databases).

Concerning availability of an exit strategy which allows for reuse of digital assets we find that no PSO has access to an effective exit strategy that can be implemented after exit from the O365 solution at short notice. We find that any effective exit strategy must cover a PSO's continuing ability to make it possible to read and write files exported from the O365 solution. This will require software and associated licences which cover those formats. It is clear that no PSO has sought to obtain licences for SEPs potentially impinging on the file format referenced in the Online Services Terms for the O365 solution. Hence, it follows that no PSO has considered all costs (i.e. costs including potential fees covering all applicable licences) related to their ability to create and maintain their digital assets during (and after) use of the O365 solution.

Further, we find that all PSOs have been unable to export files in the PDF/A-1 format from the O365 solution. The PDF/A-1 format is an open file format [27] which is suitable for long-term maintenance of digital assets and required by Riksarkivet for archiving [34, 35]. Hence, it follows that all PSOs that use the O365 solution fail to fulfil requirements for archiving expressed by Riksarkivet. In addition, any effective exit strategy needs to consider how to address exit costs at time for the initial

investment, for example, as detailed in the UK policy [38]. However, we note that none of the 46 respondents have adopted a strategy for how to address exit costs as part of the initial investment (i.e. at the time for when the PSO procured the O365 solution). Hence, hidden costs (at time for the initial investment) are ignored by all respondents. Finally, in response to requests during data collection we find that some PSOs are able to provide files in the closed file format standard PDF/A-3 and other PSOs in other closed file formats (e.g. PDF 1.5) which are not even recognised as international standards. In general, we find significant unawareness amongst PSOs of the need to obtain licences that would prevent format lock-in.

6 Analysis

Our study shows that the Swedish Government, the Swedish Government Offices, and Swedish Government Authorities each have significantly diverging views on the importance of analysing and addressing lock-in challenges related to the investigation of cost-effective IT operations for the Swedish public sector.

Concerning *perceived lock-in effects*, our analysis shows a number of misconceptions related to importance of addressing technical, legal, and societal implications of different types of lock-in effects amongst key stakeholders which, in turn, have significant impact on prerequisites for cost-effective IT operations. We specifically elaborate three critical misconceptions.

First, in acknowledging that the directive [32] states that the investigation shall analyse risks related to lock-in effects, we find that the directive indicates problematic misconceptions concerning the opportunities provided by effective public procurement (with reference to the national procurement strategy, see [33]). Specifically, we find that underlying assumptions in the directive convey problematic misconceptions concerning regulations and current practice for public procurement in the IT domain. For example, we find problematic misconceptions concerning the relationship between opportunities for use of international standards and how such standards may impact on lock-in effects [21, 23]. We note that the directive does not refer to previously published studies from commissioned research, studies which are published by several Swedish government authorities, including the Swedish competition authority [23], the Swedish national agency responsible for all framework agreements for public procurement which are to be used by all Swedish government agencies [27], and an independent analysis of a strategy presented by the Swedish Agency for Digital Government [4] that addresses licensing of software recommended for PSOs. In addition, we note that the directive [32] also lacks recognition of the importance of open standards. The Swedish Government, it should be noted, stressed the importance of open standards for addressing lock-in in its directive for the Swedish e-Government initiative [31] and by Swedish PSOs in the first report from that initiative [36].

Second, we find that the report [37] lacks a thorough analysis of lock-in effects and related challenges which impact on cost-effective IT operations through use of cloud and SaaS solutions. Further, the report fails to recognise significant technical and legal obstacles related to use of such solutions. We find that lock-in effects prevent lawful

creation, processing, maintenance, and archiving of digital assets through use of SaaS solutions from global providers that currently are widely deployed amongst Swedish PSOs. Further, we lack analysis related to patent laws that would address identified challenges related to format lock-in [20, 21]. We also lack a comprehensive analysis of laws and regulations (potentially with proposals for revised laws and regulations) related to archiving [34, 35] and long-term maintenance of digital assets [13], which considers the potential for lawful use of SaaS solutions (such as O365) from global providers.

Third, we find that the report [37] ignores important policy recommendations presented by a national policy in the UK [38] which emphasise the importance of using open standards for promoting software interoperability and avoiding lock-in effects (to avoid hidden costs caused by unsuitable procurement practices) by stressing the importance of exit strategies.

Concerning *actual lock-in* amongst PSOs, we find significant confusion amongst PSOs related to critical prerequisites which would ensure that an organisation, technically and lawfully, can create, process, maintain, and archive digital assets during and after use of a SaaS solution. Specifically, results from the study show that amongst 46 investigated PSOs that use the O365 solution there is significant confusion related to the need for obtaining licences and an effective exit-strategy that, technically and legally, would allow for use and reuse of digital assets created by a PSO during and after use of the specific SaaS solution. Hence, given that none of the 46 organisations has obtained all necessary licences for the SaaS solution it follows that any analysis of actual costs for use of the solution will be misleading. Consequently, any analysis of cost-effective IT operations for use and reuse of digital assets created, processed, maintained, and archived by PSOs will be based on misleading and incorrect underlying assumptions.

Further, despite the fact that the investigation undertaken by the Swedish Government Offices has received details concerning challenges related to format lock-in and research results concerning the need for obtaining licences related to SEPs for a commonly used SaaS solution, we note that the investigation has chosen to ignore those issues in the report [37]. Hence, since research shows that patent issues and format lock-in cause significant costs it follows that any assessment of cost-effectiveness neglecting those costs becomes speculative.

In summary, since none of the 46 PSOs that use O365 has obtained all necessary licences and all lack an effective exit strategy (which considers costs for exit) we find that their actual lock-in may be significantly worse than their (self-assessed) perceived lock-in. Unavailability of all necessary licences which would allow for data processing and maintenance of a PSOs own digital assets also implies significant other risks, beyond risks related to cost issues.

Finally, based on our analysis of results from the present study and results from previous research [22], we recommend that any PSO undertakes an analysis which includes consideration of the following five questions, each requiring a clear "yes" both prior to adoption and throughout the entire life-cycle of deployment and use of a SaaS solution from a global provider:

(1) Is the text of all applicable contract terms for the SaaS solution available and maintained by the PSO?;

(2) Has the PSO obtained all applicable licences for the SaaS solution that provide the PSO all technical abilities and all necessary rights that allow for creation, processing, maintenance, and archiving of digital assets during use of the SaaS solution?;

(3) Has the PSO obtained all applicable licences for the SaaS solution that provide the PSO all technical abilities and all necessary rights that allow for creation, processing, maintenance, and archiving of digital assets with available software (provided under open source software licences) after the PSO has ceased to use the SaaS solution (i.e. after exit)?;

(4) Is the PSO only exposed to Swedish law for data processing and maintenance of digital assets when the SaaS solution is used?;

(5) Has the PSO control over which foreign laws, regulations, and jurisdictions may impact on data processing and maintenance of the PSO's digital assets when the SaaS solution is used?

We find that none of the 46 PSOs in the present study and none of the other 33 PSOs in a previous study [22] fulfils all these five recommendations (i.e. none of 79 PSOs in total).

7 Conclusions

Fundamental to IT operations for any public sector organisation is the ability to create, process, maintain, and archive digital assets that are relevant for individuals, organisations and society at large. When an organisation creates, processes, maintains, and archives digital assets through use of IT solutions it is critical that the organisation has autonomy and full control of all its digital assets over the full life-cycle of those assets. Further, for society at large it is critical to maintain digital and data sovereignty which allows for cost effective, technically suitable, and lawful IT operations of digital assets that allow for use and reuse of those assets amongst all public sector organisations. In particular, for a public sector organisation which uses cloud and SaaS solutions from global providers there are a number of additional challenges that impact on the organisation's ability to maintain autonomy and full control of its digital assets. In conclusion, we find that the investigation undertaken by the Swedish Government Offices has failed to address several critical factors in its report [37] in order for it to successfully address the goals detailed in the directive [32].

Any analysis of cost-effective IT operations needs to be grounded in some sort of realistic perception of actual costs. We find that the investigation by the Swedish Government Offices fails to address critical aspects which impact on actual costs for use of commonly used SaaS solutions. Critical aspects, such as exit costs and hidden costs for IT-operations, are omitted despite the fact that responses to the questionnaire have highlighted the importance of such aspects. Specifically, the report lacks coverage of how to address exit costs at time for procurement of an IT solution to be used by a public sector organisation.

The study shows stark unawareness of critical technical, legal, and societal challenges which impact on digital and data sovereignty that impact on cost effective IT operations for public sector organisations. For example, the review of the UK presented in the Swedish report [37] fails to address effective exit strategies, despite the fact that the directive from the Government explicitly mentions that experiences from the UK should be reviewed. We find that exit strategies have been elaborated and recommended in the UK as a critical factor which needs to be analysed as it often represents a 'hidden cost' for IT operations [38].

Findings show that none of the 46 investigated public sector organisations have successfully addressed critical issues that need to be considered before adoption and use of a specific SaaS solution (Microsoft Office 365) from a global provider. Amongst the 46 public sector organisations the study shows that no organisation has acquired all licences which are needed for IT operations of this SaaS solution. Further, the same 46 organisations have also failed successfully to obtain all necessary licences which allow for continued use of all digital assets exported from the SaaS solution in a potential future scenario if the organisation will cease to use the SaaS solution.

Related to *perceived lock-in* amongst public sector organisations, we find that the vast majority of organisations in the Swedish public sector express significant concern related to use of SaaS solutions from global providers. Further, based on our analysis of the directive provided by the Swedish government and the report provided by the Swedish Government Offices, the study shows stark unawareness of critical factors that impact on previously investigated lock-in effects, and consequently fail to recognise important prerequisites for any analysis of cost effectiveness of IT operations.

Related to *actual lock-in* amongst public sector organisations, we find no single example of any public sector organisation that has obtained all necessary licences that allow for use of a commonly deployed SaaS solution, and no single example of any organisation which has access to an effective exit strategy that allows for continued use and reuse of an organisation's own digital assets after exit from the specific SaaS solution currently used. Hence, it follows that no public sector organisation that has adopted a commonly deployed SaaS solution (Microsoft Office 365) has any idea about the actual cost for IT operations related to creation, processing, maintenance, and archiving of the organisation's own digital assets during and after use of the SaaS solution. As many public sector organisations lack access to the text of all applicable contract terms for the specific SaaS solution used (and instead rely on the supplier for maintenance of its own contracts) we find widespread lack of autonomy and control amongst public sector organisations. Further, we find that the Swedish Government Offices has failed to recognise critical factors, such as the need for obtaining licences and calculation of exit costs, which impact on cost effective IT-operations.

Acknowledgement. This research has been financially supported by the Swedish Knowledge Foundation (KK-stiftelsen) and participating partner organisations in the SUDO project. The authors are grateful for the stimulating collaboration and support from colleagues and partner organisations.

References

1. Bekkers, R., Updegrove, A.: 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 (2013)
2. Blind, K., Böhm, M.: The Relationship Between Open Source Software and Standard Setting. In: 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 (2019)
3. Contreras, J. L.: A Brief History of FRAND: Analyzing Current Debates in Standard Setting and Antitrust Through a Historical Lens. Antitrust Law Journal 80(1), 39-120 (2015)
4. DIGG: Analys av DIGG:s policy för utveckling av programvara. Agency for Digital Government. 3 June (2020) https://www.digg.se/om-oss/nyheter/2020/analys-av-diggs-policy-for-utveckling-av-programvara
5. EC: 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
6. EC: 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 (2014)
7. EC: Standard-essential patents. European Commission, Competition policy brief, Issue 8, June, ISBN 978-92-79-35553-0 (2014)
8. EC: 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 (2020)
9. Egyedi, T.: Standard-compliant, but incompatible?!. Computer Standards & Interfaces 29(6), 605-613 (2007)
10. Egyedi, T. M., Hudson, J.: A standard's integrity: can it be safeguarded?. IEEE Communications Magazine 43(2), 151-155 (2005)
11. eSam: Checklista inför beslut om molntjänster i offentlig sektor. eSam, 31 October, www.esamverka.se (2018)
12. Försäkringskassan: Cloud Services in Sustaining Societal Functions–Risks, Appropriateness and the Way Forward, Swedish Social Insurance Agency, Dnr. 013428-2019, Version 1.0, 18 November (2019)
13. Furberg, P., Westberg, M.: Måste myndigheter följa lagarna? Om utkontraktering och legalitet i digital miljö. Juridisk tidskrift 2, 406-417 (2020/21)
14. GAIA: 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 (2019)
15. Ghosh, R. A.: Open Standards and Interoperability Report: An Economic Basis for Open Standards. Deliverable D4, MERIT, University of Maastricht, December (2005)
16. Guijarro, L.: Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States. Government Information Quarterly 24(1), 89-101 (2007)
17. Hon, W. K., Millard, C., Walden, I.: Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now. Stanford Technology Law Review 16(1), 79-129 (2012)

18. Katz, A.: 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 (2012)
19. Kritikos, K., Zeginis, C., Iranzo, J., Gonzalez, R. S., Seybold, D., Griesinger, F., Domaschka, J.: Multi-cloud provisioning of business processes. Journal of Cloud Computing 8(1), Article number 18, 1-29 (2019)
20. Lundell, B., Gamalielsson, J., Katz, A.: 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 (2015)
21. Lundell, B., Gamalielsson, J., Katz, A.: Implementing IT Standards in Software: Challenges and Recommendations for Organisations Planning Software Development Covering IT Standards. European Journal of Law and Technology 10(2) (2019)
22. Lundell, B., Gamalielsson, J., Katz, A.: 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 (2020)
23. Lundell, B., Gamalielsson, J., Tengblad, S.: 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 (2016)
24. Mannheimer Swartling: Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities, Mannheimer Swartling AB, Stockholm, January.
25. Mowbray, M.: The Fog over the Grimpen Mire: Cloud Computing and the Law. SCRIPTed 6(1), 132-146 (2009)
26. NOC: 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 (2007)
27. NPS: Open IT-standards. National Procurement Services, Kammarkollegiet, Stockholm, Dnr 96-38-2014, 7 March (2016)
28. NPS: Förstudierapport Webbaserat kontorsstöd. National Procurement Services, Kammarkollegiet, Stockholm, Dnr 23.2-6283-18, 22 February (2019)
29. Online Services Terms: February 2021. Microsoft Volume Licensing Online Services Terms (Worldwide English, February 2021), Microsoft.
30. Radar: Moln över kommunerna: hot eller möjlighet?. Radar Ecosytem Specialists, Stockholm. radareco.se (2019)
31. Regeringen: Delegation för e-förvaltning. Dir. 2009:19, Swedish Government, 26 March (2009)
32. Regeringen: Säker och kostnadseffektiv it-drift för den offentliga förvaltningen. Kommittédirektiv, Dir. 2019:64, Infrastrukturdepartementet, Regeringen, 26 September (2019)
33. Regeringskansliet: Nationella upphandlingsstrategin, Finansdepartementet, Stockholm (2016)
34. Riksarkivet: Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling). Riksarkivets författningssamling, RA-FS 2009:1, Riksarkivet, ISSN 0283-2941 (2009)
35. Riksarkivet: 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 (2009)

36. SOU: Strategi för myndigheternas arbete med e-förvaltning. Statens Offentliga Utredningar: SOU 2009:86. e-Delegationen, Finansdepartementet, Regeringskansliet, Stockholm, 19 October (2009)
37. SOU: Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Statens Offentliga Utredningar, SOU 2021:1, Delbetänkande från IT-driftsutredningen, Stockholm, ISBN 978-91-525-0001-9 (2021)
38. UK: Open Standards Principles: For software interoperability, data and document formats in government IT specifications. HM Government, 7 September (2012)