JeDEM 14(2): 214-234, 2022
ISSN 2075-9517
http://www.jedem.org
Date of submission: 06.12.2021
Date of acceptance: 27.07.2022
Article DOI: 10.29379/jedem.v14i2.749

Data Processing and Maintenance in Different Jurisdictions When Using a SaaS Solution in a Public Sector Organisation

Björn Lundell[1*], Jonas Gamalielsson[2], Andrew Katz[3], Mathias Lindroth[4]

[1] ORCID Nr: 0000-0002-2825-135X*
University of Skövde, Skövde, Sweden, bjorn.lundell@his.se

[2] ORCID Nr: 0000-0003-2700-2535
University of Skövde, Skövde, Sweden, jonas.gamalielsson@his.se

[3] ORCID Nr: 0000-0002-1001-0283
Moorcrofts LLP, Marlow, UK & University of Skövde, Skövde, Sweden, andrew.katz@moorcrofts.com

[4] ORCID Nr: 0000-0003-1866-713X
ACF Legal Intl. AB, Malmö, Sweden, mathias.lindroth@acflegal.org

Abstract: Many public sector organisations (PSO) use SaaS solutions from dominant global providers. Implementation of these solutions may raise issues concerning both lawful data processing, and the obligations that those PSOs have to maintain their digital assets. One example is a large Swedish PSO which addressed these issues as part of the adoption and implementation of Microsoft 365. The study identifies challenges and presents an analysis of the organisational implementation of that SaaS solution, exposing legal issues that arose in that context. Findings show an absence of a documented risk analysis related to the PSO's use of that SaaS solution, covering data processing and maintenance of its digital assets. Recommendations are presented to facilitate a PSO's procurement and implementation of such a SaaS solution to address issues around data processing and the processing of digital assets.

Keywords: SaaS, lock-in, Microsoft 365, public procurement, contract terms, GDPR, case study

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.

1. Introduction

Public sector organisations (PSOs) are prone to dependence on international providers of cloud-based SaaS (Software-as-a-Service[1]) solutions involving data processing and maintenance of digital assets. In many cases, the provision of those services crosses one or more jurisdictional boundaries (e.g. EC, 2020; Försäkringskassan, 2019; IMY, 2021; Lundell et al., 2016, 2020; Regeringskansliet, 2021; SKV/KFM, 2021). The overarching goal of this paper is to report on how a large PSO can ensure lawful and appropriate data processing and maintenance of its digital assets[2] when using a globally available commercial SaaS solution. The SaaS solution studied herein is Microsoft 365[3] (M365) (Kaelin, 2020).

Implementation of such SaaS solutions may raise issues concerning both lawful data processing, and the obligations that an organisation has to maintain its digital assets. Previous studies have scrutinised the potential for lawful and appropriate use of cloud-based SaaS solutions in Swedish PSOs and identified a range of challenges (Stockholm, 2021; IMY, 2021; SKV/KFM, 2021; eSam, 2018; Lundell et al., 2016, 2021; Opara-Martins et al., 2016). For example, during 2020 and 2021 the municipal board of the City of Stockholm undertook an investigation of the potential adoption of M365 and presented three main reasons for refraining from use of M365 in its report (Stockholm, 2021).

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 conclude that "we are likely to see legal disputes arising from geopolitical and jurisdictional issues" (Mowbray, 2009, p. 136).

Adoption and use of a SaaS solution imposes challenges related to lawful data processing and digital asset maintenance, which are inherently different from those arising from the use of on-prem software under perpetual terms (Bradshaw et al., 2011; Janssen and Joha, 2011; Lundell et al., 2021; Opara-Martins et al., 2016; Stockholm, 2021). Use of such SaaS solutions imposes, amongst others, a number of additional technical, legal, economic, and societal challenges which have been addressed in previous studies.

Based on a review of previous studies (Lundell et al., 2016; Wagle, 2016) we have identified and elaborated seven such challenges. We identify challenges relating to comprehending how a SaaS solution functions (e.g. Lundell et al., 2016; Wagle, 2016), determining which parties will be involved in providing the solution (e.g. Lundell et al., 2020), and the legal implications thereof (e.g. Furberg and Westberg, 2020/21; Stockholm, 2021). Further challenges relate to legal restrictions on the free

1 "*Software as a Service (SaaS)*. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure." (NIST, 2011)

2 "A digital asset is anything that is stored digitally and is uniquely identifiable that organizations can use to realize value. Examples of digital assets include documents, audio, videos, logos, slide presentations, spreadsheets and websites." (Gartner, 2022)

3 When the study was initiated in 2017 the specific SaaS solution used by the public sector organisation was referred to as Microsoft Office 365. In acknowledging that many practitioners for a long time have referred to the specific SaaS solution as 'Office 365' we note that on 21 April 2020 it was rebranded and "Office 365 became Microsoft 365" (Kaelin, 2020).

flow of data (e.g. CJEU, 2020; Shurson, 2020), such as restrictions relating to the protection of personal data, national security interests (e.g. Liu, 2016; MS, 2019) or a general duty of confidentiality in public administration (e.g. eSam, 2018; SKV/KFM, 2021).

Based on these challenges, the study investigates the following research question: How does, and by which strategies should, a public sector organisation ensure lawful and appropriate data processing and maintenance of its digital assets when using a commercial SaaS solution that is globally provided by a dominant actor?

The paper presents several contributions for organisations considering adoption and use of a SaaS solution. First, we identify challenges concerning lawful and appropriate data processing and maintenance of digital assets and provide rich insights from one of the largest organisational implementations of the M365 solution in an EU-country. Second, we present seven main findings related to adoption and use of M365 in the second largest municipality in Sweden. Third, we present and elaborate problematic data processing and maintenance issues related to the implementation of the M365 solution, and present an associated strategy with recommendations for ensuring lawful and appropriate data processing and maintenance of an organisation's digital assets related to use of a globally provided SaaS solution.

2. On use of SaaS solutions for data processing and maintenance of digital assets

The phrase 'lawful and appropriate', throughout this paper, refers to all the requirements imposed on each PSO within the EU in accordance with applicable legislation, as well as the principles of good administration whether codified or not. 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).

Good administration encompasses *inter alia* principles of objectivity, proportionality, efficiency and availability. Also, and even more importantly for the purpose of this study, it encompasses the fundamental principle of the rule of law and a general duty of care. The principles of good administration are codified by various means in many member states. In Sweden, for instance, the principle of the rule of law can be found in Chapter 1, Section 1, paragraph 3 of the Constitution (RF, 1974), and the principles of good administration in Sections 5 through 8 of the 2017 Administrative Procedure Act (FL, 2017). Notably there is also a provision in the following section, Section 9, of the same act, which stipulates that administrative matters shall be processed in writing.

The phrase 'processing and maintenance of digital assets' is intended to cover the processing, maintenance and storage of documents and other types of digital assets in a broad sense, both within the particular SaaS solution and outside of it, i.e. with regard to assets created or exported for the purpose of being transferred to another recipient, to a new solution, or for archiving, during and after an organisation has ceased to use the solution. In order to allow for interoperability and long-term maintenance of digital assets that have been processed during an organisation's use of a SaaS

solution it is critical that the solution supports export of assets in appropriate file formats[4] that promote longevity of digital assets and also conforms to the regulations stipulated by the Swedish national archives concerning use of formats (Riksarkivet, 2009). Additionally, conditions for use of a SaaS solution in a PSO must allow for lawful and appropriate data processing of digital assets, irrespectively of whether the organisation has (or lacks) copyright for each asset, both during and after the organisation has ceased to use the solution.

We have identified and conceptualised seven separate challenges that any organisation considering adopting such a SaaS solution needs to address.

First, before adoption and use of a SaaS solution in a PSO the organisation must understand how the solution functions in all aspects, including technical and legal. This presupposes that the organisation obtains (and files) and analyses all applicable contract terms to determine the conditions in which the organisation's digital assets would be processed and maintained. Previous research shows that PSOs commonly use M365 without having obtained and analysed all applicable contract terms (Lundell et al., 2021). This implies that each such organisation is unable to assess the legal context in which its digital assets may be processed by the solution (Lundell et al., 2021). So-called dynamic contract terms, which may be unilaterally amended by the service provider, are another aspect of this challenge. For example, a report by the municipal board of the City of Stockholm found that potential adoption of the M365 solution would imply use of M365 under unknown and dynamic conditions which the supplier may unilaterally change any time (Stockholm, 2021).

Second, based on the understanding gained from the investigation of the functionality and terms offered by each provider of a specific SaaS solution, it is critical to assess if the specific SaaS solution is appropriate for the organisation's needs and would allow for legal processing and maintenance of its digital assets (Melin et al., 2019). This entails revisiting and analysing all legal requirements which may apply to the adoption, implementation, operation and decommissioning of the solution. A solution relying on external data processing may introduce significant new technical and legal issues, including uncertainty under which laws and regulation will be applicable on the intended use and exit from a specific solution. Technical expertise is equally important during adoption and use of such a solution. It is critical, before a PSO uses a SaaS solution for data processing of digital assets, to ensure longevity of the organisation's assets through interoperability with other systems. For example, previous research shows that M365 may be unable to export certain digital assets in a way that allows for their continued lawful and appropriate data processing and maintenance (Lundell et al., 2019, 2020, 2021).

Third, a particular legal challenge concerns GDPR compliance. Research shows that use of a SaaS solution from global providers has raised data privacy concerns for organisations based in the EU (EDPS, 2020, 2021; Shurson, 2020; Svantesson, 2012; Tracol, 2021). With use of a globally provided

[4] File formats are provided under different terms which (for technical and legal reasons) may allow for (or inhibit) implementation of a format in software (Lundell et al., 2019). To ensure the long-term maintenance of digital assets exported from a SaaS solution it is critical that each file format used has been implemented in software under perpetual terms which comply with the Open Source Definition (Lundell et al., 2019).

SaaS solution it follows that data export to several third countries may occur, which must be addressed in order to avoid unlawful data processing in breach of the GDPR (DI, 2019; IMY, 2021; SKV/KFM, 2021). For example, an investigation of data processing and maintenance of digital assets by a Swedish PSO ('Transportstyrelsen', eng. the Swedish Transport Agency) exposed, *inter alia*, sensitive data to Serbian jurisdiction, something which was criticised by the Swedish Government Offices (Regeringskansliet, 2018). A PSO's use of a SaaS solution from a global provider (such as M365) will often involve data processing by several additional parties, retained by the service provider in the role as subprocessors, based in different countries. Specifically, on 5 September 2019 Microsoft presented a list of "the subprocessors authorized to access customer data and personal data in Microsoft's Online Services" which lists several companies based in many different countries, including China, India, Serbia, USA and United Arab Emirates (Microsoft, 2019c). Several lists have subsequently been presented, including a list on 24 September 2021 which 'identifies the subprocessors authorized to access both (i) customer data and personal data contained within it in Microsoft's Online Services (referred to as "Customer Data" in the table below), as well as (ii) personal data other than that contained in Customer Data.' (Microsoft, 2021b) Further, research which investigated adoption and use of M365 by Swedish PSOs found that several organisations "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" the solution (Lundell et al., 2020).

Fourth, data processing and maintenance of an organisation's digital assets in certain countries may cause security challenges (e.g. Säpo, 2019). For example, research shows that use of the M365 solution in Swedish PSOs may expose each organisation's own digital assets to certain foreign laws and regulations (Lundell et al., 2020), such as FISA (Foreign Intelligence Surveillance Act) 702 (Liu, 2016; NPS, 2019; SKV/KFM, 2021) and the Chinese NIL (National Intelligence Law) (MS, 2019).

Fifth, use of SaaS solutions which are provided by companies that have operations in tax havens may cause financial (tax related) challenges (EC, 2017a, 2019). Moreover, if a (tax funded) PSO procures services from a provider of a SaaS solution involving companies based in tax havens, this could be seen as contrary to the concept of fair competition. Hence, use of such a SaaS solution could be considered inappropriate if provided by a company that is wholly owned by another company based in a country that has been included on the "EU list of non-cooperative jurisdictions for tax purposes" (EC, 2017a).

Sixth, for a Swedish PSO, the Swedish Public Access to Information and Secrecy Act[5] (OSL) (OSL, 2009), causes issues where data processing is to be carried out by external IT-operations. Disclosure of any piece of information held by a Swedish PSO presupposes a prior assessment under the OSL, and the possibility of 'bulk disclosure' to the service provider of all data in the solution poses a particular problem. This has been recognised by the Swedish Government Offices in a report that focused on the conditions for the outsourcing of IT operations by government agencies, municipalities, and regions in Sweden (Regeringskansliet, 2021). Further, a group of legal experts at eSam (who represent several large it-intensive Swedish PSOs) concluded that use of cloud based

5 In Swedish: 'Offentlighets- och sekretesslag' (OSL, 2009).

SaaS solutions by a Swedish PSO imposes specific challenges. Specifically, "eSam's group of legal experts concluded on 23 October 2018 that if information is made technically available to an IT service provider that is bound by the rules of another country due to ownership conditions, according to which the service provider may be obliged to provide information, the information should be considered divulged." (SKV/KFM, 2021).

Seventh, research shows that use of SaaS solutions from international providers may cause the organisation's data processing and maintenance of digital assets to be governed by the laws of other countries rather than Swedish law, by means of choice of law clauses contained in the terms and conditions for the solution. Such exposure may be legally questionable under Swedish law (Furberg and Westberg, 2020/21). For example, an analysis by Swedish legal experts argued that it is contrary to the principle of legality for a Swedish PSO to enter into contracts governed by the laws of a foreign country, in instances where the choice of law will affect the performance of the official duties of the organisation (Furberg and Westberg, 2020/21). These tasks, argued the authors, shall be governed only by the laws of Sweden and the EU.

Global providers of cloud-based SaaS solutions may have strong incentives for causing dependencies and different types of lock-in effects in order to retain customers (Opara-Martins et al., 2016; Xiao et al., 2020). For example, research shows that increased "customer retention and preventing customers from replacing the adopted SaaS applications has become a crucial task for all SaaS vendors" (Xiao et al., 2020). Moreover, both technical and non-technical lock-in effects are seen as essential strategies for retaining customers when reporting that "it is crucial for SaaS vendors to increase customers' commitment to the application" (Xiao et al., 2020). Similarly, a study of a globally provided cloud-platform stresses the importance for the platform owner of establishing relationships and dependencies amongst its customers (Schreieck et al., 2021, p. 379).

For all these reasons, it follows that it would be unwise for a PSO to uncritically assume that data processing and maintenance of the organisation's digital assets through use of a cloud-based globally provided SaaS solution would be lawful and appropriate.

3. Research approach

To gain understanding of how a large PSO ensured lawful and appropriate data processing and maintenance of its digital assets related to its adoption, use, and large-scale organisational implementation of the SaaS solution M365 we utilised an interpretive case study approach for our investigation (Walsham, 1993, 1995; Braa and Vidgen, 1999).

During research design and conduct of the case study we considered validity threats and aspects of trustworthiness, which also considered experiences from prior research on method transfer and research methods (Guba, 1981; Lings and Lundell, 2004). The research design for the study was informed by experiences from previous research on qualitative techniques conducted in the software systems domain, which includes the first author's experiences from research on Glaser's strand of Grounded Theory (Lings and Lundell, 2005). Based on our experiences, we consider it essential for researchers in this area to be "knowledgable" in conditions for use of the technologies under

instigation (Lings and Lundell, 2005), which necessitates understanding of both technical and legal challenges related to globally provided SaaS solutions.

The context for the case study was the *City of Gothenburg*[6] (CoG), which was selected for a number of reasons.

First, the CoG is a large PSO which consists of several independent authorities and, as such, can be expected to have the resources to be able to undertake a comprehensive analysis prior to the adoption and use of M365. The CoG is Sweden's second largest municipality 'with a population of just over half a million' in December 2016 (Got, 2017a, p. 5) and 'a population of almost 600,000' in 2020 (Got, 2021, p. 9). In April 2017, it was reported that the CoG had 54200 employees at the end of 2016 (Got, 2017a, p. 6).

Second, investigation of a large scale adoption of M365 by a Swedish PSO (which during use of M365 involves data export to third countries) is of particular relevance. There was an early awareness on regulating data export in Sweden, in fact, in 1973 Sweden was the first country that regulated 'data exports to third countries' (Wagner, 2018, p. 319).

Third, since the CoG consists of several different (and legally independent) authorities[7] adoption of M365 imposes specific challenges related to the Swedish Public Access to Information and Secrecy Act (OSL, 2009) which need to be considered by a PSO regarding the use of M365 (Regeringskansliet, 2021).

Fourth, as an early adopter and one of the largest deployments of M365 in the Swedish public sector, the CoG is particularly influential. For example, representatives for several other Swedish PSOs have, in different contexts, 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).

Fifth, the organisational implementation of M365 gained public exposure and public debate after it was temporarily suspended for legal and security reasons in October 2017 (Lindström, 2017).

Sixth, a legal analysis of the lawfulness of using M365 under Swedish law was published soon after this suspension of deployment (SLK, 2017).

The study was motivated by discussions with representatives for the public sector related to public presentations and the publication of results from a previous study (Lundell et al., 2016) which investigated a range of lock-in challenges, including data processing and maintenance of digital assets through use of SaaS solutions in Swedish PSOs that are exposed to various laws and regulations in different jurisdictions. During 2015-2016 the previous study was conducted on behalf

6 In Swedish: 'Göteborgs Stad'.

7 The CoG consists of several different authorities which imposes challenges concerning use of external it-operations (including any form of outsourcing and use of a globally provided SaaS solution) related to the Swedish Public Access to Information and Secrecy Act (OSL, 2009).

of the Swedish Competition Authority, and the results triggered extensive discussions with representatives for the public sector in Sweden and the EU. This, in turn, shaped ideas and focus for the present case study which was initiated in 2017.

The study involved an extensive and complex data collection and analysis. Data collection was coordinated by the first author and analysis of the rich resource of collected data involved all four authors, a methodology which brought valuable supplementary experiences to the technical and legal analysis. During data collection we requested and obtained a rich corpus of public documents related to the adoption of M365 from the CoG. Data collection requested all applicable contract documents, documentation of decisions and plans for the organisational implementation of M365, and documentation of analyses related to the adoption, data processing, use, and deployment of M365 undertaken with different foci (legal, technical, organisational, security, privacy, etc.). In cases when requested documents were unavailable, supplementary questions and requests for documents were sent. A significant amount of documents and other material has successively been collected from the CoG and from other sources. Material analysed 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).

Since the public meeting with a representative for the CoG on 1 November 2017 the data collection has involved dialogue with representatives for several organisations in the CoG, primarily the following three organisations: the agency with responsibility for provision of infrastructure services which includes provision of M365 within the CoG (Swe. 'Förvaltningen Intraservice', hereafter referred to as *Intra*), the agency with responsibility for all public procurement in the CoG (Swe. 'Förvaltningen Inköp- och upphandling', hereafter referred to as *Ink*), and the agency which supports the City Executive Board under leadership of the City Director (Swe. 'Stadsledningskontoret', hereafter referred to as SLK). Documentation and responses to requests for information from these organisations (which legally constitute different authorities in the CoG) have been of particular relevance for the analysis of findings from the case.

A large number of requests for information and data sources have been sent (primarily via email, and to a limited extent also via letters). Data were also obtained from the CoG website (accessed via www.goteborg.se). To a limited extent, data collection has also involved synchronous communication (via phone dialogues and physical meetings) to representatives of the CoG in order to clarify misunderstandings. The collected material (including contract documents, reports, documents, responses to requests for clarifications) has been systematically analysed and emergent issues have been conceptualised and discussed amongst all researchers, in order to gain several perspectives and account for validity threats. This analysis was performed as the data collection progressed, allowing subsequent data collection to evolve with the results of the analysis.

4. Observations from the case

The adoption and deployment of M365 in the CoG has, directly or indirectly, involved and affected a large number of individuals and organisations. We characterise the deployment of M365 in the CoG as a turbulent and politicised process, during which the individuals, organisations and other

stakeholders involved have faced significant tensions and a range of legal, organisational, technical and societal challenges.

From 1 June 2009 to 24 June 2021 the CoG had a long-lasting relationship and several framework contracts with its partner *Atea Sverige AB* (hereafter referred to as *Atea*), through which it was able to procure products and services from Microsoft (Got, 2009, 2011, 2013, 2015, 2016c). The Swedish company *Atea* is the largest supplier of IT-products and services to Swedish PSOs with sales representing 25% of the total Swedish public sector market during 2017 (DS, 2018). 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 the M365 solution has been provided on the market. In particular, 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 CoG shaped plans toward M365 usage at some point during the four year time period following the general election on 14 September 2014. In particular, plans for an organisational 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 given by the IT manager at *Intra* (Got, 2016a). Minutes from this board meeting state that this presentation explained that the administration had 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, 2016b). In addition, 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.

Conduct of the study encountered unwillingness to provide the information requested. We found that this was largely caused by the supplier's desire that the contract terms and contract documents be kept confidential. Eventually, through a very complex and time-consuming process the study obtained a rich body of documentation which the researchers analysed during conduct of the study.

5. Case findings

Concerning lawful and appropriate *data processing and maintenance of digital assets,* we found that the CoG lacks any comprehensive analysis related to its use of M365. Based on our analysis the study presents seven main *findings,* related to the adoption and use of the M365 solution in the CoG, which cause concern and call for actions amongst responsible decision makers in the CoG.

First, we found that neither *Intra* (i.e. the responsible authority for the M365 deployment in the CoG) nor any other organisation in the CoG have obtained (and filed) all applicable contract terms for the M365 solution prior to use of the solution. Hence, it follows that the CoG is unable to assess under which conditions data processing and maintenance of its digital assets may take place.

Second, based on the information that has been provided to us by *Intra*, we found that the M365 solution does not ensure long-term maintenance of the specific functionality for transformation between different representations of digital assets (i.e. the functionality provided for transforming digital assets between different representations[8]) when the M365 solution is being used. From analysis of the contracts, we identified a lack of long-term support for specific transformations. For example, the technical specification of the ISO/IEC 29500 standard has evolved over time and the extent to which specific transformations and formats are (still being) supported, and over time have been supported, is unclear. Hence, from our analysis of the contracts, we found no assurance (on perpetual terms) that all functionality for transformations that has been provided by M365 will forever remain unmodified in order to ensure long-term support for specific transformations. It should be noted that such support is critical for long-term maintenance of digital assets and in particular when digital assets are being transformed to (and from) an internal representation in the M365 solution (e.g. when the content of a file being represented in a specific version of a '.docx' format is being imported to the M365 solution, thereafter being modified through use of M365, and later being exported from the M365 solution to a '.docx' format for data processing with other software applications outside the M365 solution). Moreover, we also find that the CoG has been unable to provide digital assets (by export from M365) in the PDF/A-1 file format which is an appropriate format for long-term maintenance of digital assets. It should be noted that PDF/A-1 fulfils the Swedish national regulations, as detailed by the Swedish National Archives (Riksarkivet, 2009), whereas PDF/A-3 is an inappropriate format which does not fulfil the same regulations. In summary, we found that the M365 solution used in the CoG does not prevent transform lock-in, something which may cause severe challenges for long-term maintenance of digital assets in the CoG.

Third, despite use of M365 at a large scale in the CoG for purposes including processing of vast amounts of personal data, we found that neither *Intra* nor any other organisation in the CoG (of a total of 28 PSOs that we contacted two years after the GDPR came into force) have undertaken and provided any impact assessment as detailed in GDPR's Article 35 and by the Swedish Data Protection Authority (DI, 2019). We find this particularly noteworthy, given that the M365 solution has been used for several years by many individuals and organisations in the CoG.

Fourth, based on the information that has been provided to us by *Intra* (i.e. the responsible authority for the M365 implementation in the CoG), we found that the CoG does not know in which countries data processing and maintenance of digital assets from the CoG *has* taken place. Nor in which countries data processing and maintenance of digital assets from the CoG *may* take place, according to the contracts with the providers of the M365 solution. In addition, based on our analysis of the contract terms in a contract document (OST, 2017) which is referenced in the legal review provided by *SLK* (SLK, 2017) we found that the CoG is bound by contract terms concerning 'Location

[8] During a public meeting on 1 November 2017 the first author of this paper posed a specific question to the CEO at *Intra* which probed if the CoG had analysed risks concerning transform lock-in prior to adoption of M365 (Got, 2017d). Based on the response and subsequent clarifications from other representatives at *Intra* during conduct of the study (including during a meeting at *Intra* on 18 December 2019) it was clarified by representatives for *Intra* that no such analysis had been conducted.

of Data Processing' which state that customer data may be transferred to, stored and processed outside the EU:

> *"Except as described elsewhere in the OST, Customer Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland. In addition to Microsoft's commitments under the Standard Contractual Clauses and other model contracts, Microsoft is certified to the EU-U.S. Privacy Shield Framework and the commitments it entails."*

Fifth, we found that signing a contract with a company that is wholly owned by a company based in a non-cooperative tax jurisdiction for data processing of a PSO's digital assets through use of M365, that has been (and at time of writing still is) used in the CoG, has raised concern amongst some political decision makers in the CoG. Specifically, on 24 March 2018 a representative for *Intra* signed a contract[9] with Microsoft AB which on 24 March 2018 was a company that was a wholly owned subsidiary to the Bermuda-based company MBH Ltd (Microsoft, 2019a). The contract was signed by *Intra* despite the fact that Bermuda, at the time for signing the contract, was included on EU's list of "tax regimes that facilitate office structure which attract profits without real economic activity" (EC, 2017a, p. 16) that has been created as part of the EU's work "to deal more robustly with external threats to Member States' tax bases and to tackle third countries that consistently refuse to play fair on tax matters" (EC, 2017b). In response to a question posed (on 20 and 21 January 2020) to all ordinary members (101 decision makers) in the Intraservice board, the board for *Ink*, the City Executive Board, and the City Council in the CoG and amongst the (15) responses there seemed to be an unawareness of the situation. Only two decision makers clearly articulated that they considered it to be inappropriate to sign contracts with a company that is wholly owned by another company which is based in country that is included in EU's list of tax havens. In acknowledging that there may be different political views concerning the relevance of EU's efforts related to tax matters (EC, 2017a, 2017b) we find that a PSO which considers procurement and signing contracts for use of a SaaS solution (such as the M365 solution) needs to consider societal implications before signing a contract with companies wholly owned by other companies based in countries assessed to be tax havens by the EU or some other authority.

Sixth, we found that in October 2017 the city legal advisors decided to temporarily suspend the implementation of M365 for reasons of concern related to OSL, something which received national attention in the press (GP, 2017; Lindström, 2017). On 20 October 2017 a legal analysis was presented by the city legal advisors at *SLK* which led to the implementation of M365 being resumed (SLK, 2017). The analysis presented by *SLK* addressed risks stemming from provision of a large amount of information to Microsoft without prior assessment of each piece of data. A new supplementary contract with Microsoft (Microsoft, 2017) would resolve any issues. Besides Customer Lockbox (which is a new contract that is signed and maintained by *Intra*, i.e. a different authority from *SLK*

[9] 'Microsoft Enterprise Services Work Order', Work Order Number: 6SWE184-16189-194255 (Dnr: 0354/18)

where the City Lawyers are based) we find that the City Legal Advisor's analysis merely refers to one single contract document, namely the English edition of the contract document 'Microsoft Volume Licensing Online Service Terms May 1, 2017' (OST, 2017). In addition, during the spring of 2018, *Intra* requested an assessment of the Customer Lockbox functionality by a security expert at *Intra*, whose findings were presented in a memo to the Intraservice board meeting on 23 May 2018 (Got, 2018). This security expert noted that Microsoft had been asked, but was unable, to provide a detailed description of the service. Further, it had been confirmed that the functionality was not at all unique and tailored to the city as promised. Most importantly, this security expert concluded that Customer Lockbox was useless for the purpose of avoiding unlawful disclosure of classified information. Besides, according to this security expert, Customer Lockbox did not cover all services supplied by Microsoft. His conclusion was contrary to that of the City Legal Advisors in October 2017 (SLK, 2017), in that he found that the Customer Lockbox functionality did not solve the OSL disclosure issue.

Seventh, we found that analyses of contract terms and licences need to take into account different jurisdictions and legal systems, since the applicable law for the contract terms and interpretation of a licence that a Swedish PSO is bound by for the M365 solution is not only the Swedish law. For example, *Intra* provided the Swedish version[10] of the 'Campus and School Agreement', which contains the following contract terms:

> "***Applicable law.*** *The terms of this agreement and each Enrollment entered into with any Microsoft Affiliate located outside of Europe will be governed by and construed in accordance with the laws of the State of Washington and federal laws of the United States. The terms of this agreement and each Enrollment entered into with a Microsoft Affiliate located in Europe will be governed by and construed in accordance with the laws of Ireland."*

Moreover, we found that exposure of children's data processing to unknown jurisdictions may cause privacy concerns. Further, since different countries have different copyright legislation (and given that the CoG does not know in which countries its data is being processed and maintained), we found that different employed and not employed (e.g. children in public schools) users of the M365 solution in the CoG have potentially been exposed to the legislation of a number of different jurisdictions when they create and modify digital assets under different copyright regimes in different jurisdictions. Further, since use of the M365 solution requires that the CoG grants a royalty-free licence[11] for all digital assets being processed by the solution, there may be serious copyright issues since the CoG lacks copyright (or an appropriate licence which permits sub-licensing) for all assets that may be processed by the solution.

[10] On 6 December 2018 a representative for *Intra* signed the Swedish version of this contract: 'Campus- och School-avtal'.

[11] "To the extent necessary to provide the Services to you and others, to protect you and the Services, and to improve Microsoft products and services, you grant to Microsoft a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services" (Microsoft, 2021d)

6. Issues and implications

Based on our analysis of the information that has been provided to us in response to questions and requests for documentation during the study, which evolved and became conceptualised into seven main findings (presented in the previous section), we highlight three problematic *issues* related to the organisational implementation of the M365 solution for data processing and maintenance of digital assets in the investigated PSO (CoG). These three issues have potentially very problematic implications for individuals, organisations in the PSO, other organisations in Sweden, and society at large. Moreover, related to each *issue*, we present an associated *strategy* containing a recommendation concerning what each PSO should do in order to ensure lawful and appropriate data processing and maintenance of its digital assets when using a globally provided SaaS solution.

First, based on the finding that the PSO (CoG) lacks all contract terms for the M365 solution, and therefore is unable to assess under which conditions use of M365 for data processing and maintenance of its digital assets would take place, it follows that digital assets are exposed at significant risks. Hence, for each PSO which is exposed to such risks, we recommend that the PSO immediately adopts and executes a *strategy* for obtaining, filing and analysing all contract terms for the M365 solution (before continued use of M365), in order to establish *whether* lawful and appropriate data processing and maintenance of the PSO's digital assets can take place through use of the M365 solution.

Previous research shows that it may be impossible for a PSO to obtain all applicable contract terms for M365 (Lundell et al., 2021). Moreover, studies have shown that it is impossible for a PSO to analyse under which conditions M365 will be provided and that the PSO lacks influence over the contract for the M365 solution which may be changed at any time (e.g. Stockholm, 2021).

Second, based on the findings that the PSO (CoG) lacks information detailing in which countries data processing and maintenance of digital assets from the CoG *has taken place,* it follows that data exports of CoG's digital assets may have taken place to a range of different third countries over the years. Further, since the CoG also lacks access to all contract terms they are bound by for the M365 solution, it also follows that the CoG lacks information concerning in which countries data processing and maintenance of CoG's digital assets *may take place* according to the contracts with the providers of M365. We find that this unawareness concerning applicable jurisdictions prevents analysis of risks related to data processing and maintenance of CoG's digital assets under different (unknown) copyright regimes, and that it also prevents opportunities for conduct of any impact assessment as detailed in GDPR's Article 35. We find this inappropriate given the large-scale use of M365 in the CoG. Based on the contract terms that the CoG actually has provided in response to requests, we conclude that the CoG's data may be transferred to "the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities" (OST, 2017). Consequently, we find that the PSO's data processing and maintenance of its digital assets is exposed to significant risks. Hence, for each PSO which is exposed to such risks, *we recommend* that the PSO undertakes an impact assessment as detailed in GDPR's Article 35 which at least must assess possible impacts of data processing and maintenance of CoG's digital assets through use of subprocessors based in all countries which Microsoft has published, including lists published on 22 February 2019 (Microsoft, 2019b), on 5 September 2019 (Microsoft, 2019c), on 31 July 2020 (Microsoft,

2020), on 13 August 2021 (Microsoft, 2021a), on 24 September 2021 (Microsoft, 2021b), and on 23 November 2021 (Microsoft, 2021c). In particular, this recommendation includes a need to analyse implications of possible data export from a Swedish PSO to several countries which previously have been analysed as problematic, including China (Säpo, 2019; MS, 2019), Serbia (Regeringskansliet, 2018), and USA (SKV/KFM, 2021). Further, beyond a PSO's analysis of the GDPR (Nas and Roosendall, 2018; IMY, 2021) which includes analyses of each potential subprocessor, we *recommend* that a solid analysis of data processing and maintenance of a Swedish PSO's digital assets must also consider a number of other legislations, including Förvaltningslagen (e.g. Furberg and Westberg, 2020/21), Säkerhetsskyddslagen (e.g. Säpo, 2019), and a number of national laws and regulations such as NIS[12], FISA 702[13] (NPS, 2019; SKV/KFM, 2021) and NIL (MS, 2019). Consequently, we find that the scope of the legal analysis presented by *SLK* on 20 October 2017 (SLK, 2017) was too limited to constitute a solid basis for a decision concerning continued implementation of the M365 solution in the CoG. In addition, we note that the outcome of the legal analyses of OSL, in two different analyses by the city legal advisors in the CoG (SLK, 2017, 2019), have reached substantially different conclusions than those presented by other legal experts (e.g. eSam, 2018, 2021; NPS, 2019; Regeringskansliet, 2021).

Third, based on the finding that all digital assets which the PSO (CoG) has processed and exported from the M365 solution have been exported in formats that are unsuitable for long-term maintenance of digital assets (Lundell et al., 2019, 2021) and that formats used for these digital assets also fail to fulfil requirements for long-term maintenance of digital assets as required by the Swedish National Archives (Riksarkivet, 2009), we find that the PSO exposes its digital assets for significant risks. Further, the PSO's data processing fails to fulfil the guidelines and regulations for archives (Regionarkivet, 2017a, 2017b) which the Intraservice board has approved on 22 May 2017 (Got, 2017b, 2017c). Consequently, it follows that the PSO also fails to fulfil its own regulations. Specifically, several files (with filename extensions '.docx' and '.pdf') that have been created by use of the M365 solution used in the CoG 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). It should be noted that this includes technical requirements for digital assets (Swe. 'elektroniska handlingar') which makes it clear that files provided with the extension '.docx' do not fulfil these requirements (Riksarkivet, 2009). Consequently, we find that the PSO's data processing and maintenance of its digital assets is exposed to significant risks. Hence, for each PSO which is exposed to such risks, we *recommend* that the PSO immediately adopts and executes a *strategy* for ensuring that data processing and maintenance of digital assets, through use of M365, allows for export of digital assets in formats which are (technically and legally) suitable for long-term maintenance beyond the time period for use of M365 in the specific PSO. Previous research shows that export of digital assets in formats which fulfil regulations and are suitable for long-term maintenance, beyond the time period during which a PSO uses M365, may require negotiations with the supplier and redesign of the M365 solution (e.g. Lundell et al., 2019),

[12] The Directive on security of network and information systems.

[13] Foreign Intelligence Surveillance Act.

something which may prevent lawful and appropriate data processing and maintenance of digital assets in a PSO (eSam, 2021).

7. Conclusions

The study shows that a dependency on international providers for data processing and maintenance of the City of Gothenburg's digital assets through use of the M365 solution has been, and continues to be, inappropriate for a range of different reasons. Findings from the study show that the City of Gothenburg failed to recognise the significance of the implementation of the cloud-based SaaS solution. In particular, the transition from on-premise deployment (with licences provided on perpetual terms) to a cloud-based SaaS solution (with time limited licences) is a radical change. This implies a new set of risks as the customer will no longer exercise direct and exclusive control over its information.

From a societal perspective, we find it inappropriate for a public sector organisation within the EU to engage and sign contracts with a provider that is wholly owned by a company that is based in a country that has been included in the EU list of non-cooperative tax jurisdictions. We note that the vast majority of political decision makers in the City Executive Board and the City Council at the City of Gothenburg had no issue with this arrangement when asked during conduct of the study. Further, we also find it inappropriate to allow for data processing and maintenance of the City of Gothenburg's digital assets in unknown jurisdictions through use of a SaaS solution that may involve subprocessors in a range of different countries. In particular, given that the list of subprocessors used by Microsoft includes organisations from countries which have been identified as potentially problematic in different analyses, including an analysis presented by the Swedish Security Service and an analysis presented by a Swedish law firm, we find it remarkable that no authority in the City of Gothenburg had undertaken any Data Processing Impact Assessment (DPIA) in accordance with GDPR Article 35 one year after specific guidelines had been published by the Swedish authority for data protection and within two years after the GDPR came into force. In addition, we find that use of the M365 solution for data processing of sensitive information and processing of digital assets for which the City lacks copyright (or an appropriate licence) may cause a number of unforeseen and undesirable legal issues, for example, exposure to different copyright laws and risks for disputes in different jurisdictions. We note that none of these issues have been analysed by the CoG.

In conclusion, the study highlights several unresolved challenges and recommendations related to prerequisites for lawful and appropriate adoption and use of a globally provided cloud-based SaaS solution for data processing and maintenance of digital assets in a large public sector organisation. Adoption and use of a cloud-based SaaS solution under unknown contract terms in a public sector organisation, which may involve several subprocessors based in different countries, would expose the organisation's data processing and maintenance of its digital assets to several unknown regulations and laws applicable in different countries. Use of a SaaS solution under such circumstances would expose the organisation's digital assets to significant risks. An omission to obtain, file and analyse all applicable contract terms before potential use of a commercial SaaS solution that is globally provided should always be avoided.

References

Braa, K. & Vidgen, R.T. (1999). Interpretation, intervention and reduction in the organizational laboratory: a framework for in-context information systems research, Information and Organization, 9(1), 25-47.

Bradshaw, S. & Millard, C. & 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, 19(3), 187-223.

CJEU (2020). The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, Judgment in Case C-311/18, Press Release No 91/20, Court of Justice of the European Union, Luxenbourg, 16 July. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

CM (2007). Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration, The Council of Europe, 20 June.

DI (2019). List regarding Data Protection Impact Assessments according to article 35.4 of the Data Protection Regulation, Dnr. DI-2018-13200, Datainspektionen (The Swedish Data Protection Authority), Stockholm, 16 January.

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

EC (2017a). The EU list of non-cooperative jurisdictions for tax purposes, 15429/27, Council of the European Union, 5 December 2017. https://data.consilium.europa.eu/doc/document/ST-15429-2017-INIT/en/pdf

EC (2017b). Questions and Answers on the EU list of non-cooperative tax jurisdictions, Fact Sheet: MEMO/17/5122, European Commission, 5 December. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_5122

EC (2019). The revised EU list of non-cooperative jurisdictions for tax purposes – Council conclusions (12 March 2019), 7441/19, Council of the European Union, 12 March. https://data.consilium.europa.eu/doc/document/ST-7441-2019-INIT/en/pdf

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.

EDPS (2020). EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, European Data Protection Supervisor, Publications Office of the European Union, Luxembourg, ISBN 978-92-9242-567-8, 2 July.

EDPS (2021). The EDPS opens two investigations following the "Schrems II" Judgement, Press Release, EDPS/2021/11, European Data Protection Supervisor, 27 May.

eSam (2018). Rättsligt uttalande om röjande och molntjänster, VER 2018:57, eSam, 23 October.

eSam (2021). 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.

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

FL (2017). Förvaltningslag (2017:900), SFS nr: 2017:900, 28 September. https://rkrattsbaser.gov.se/sfst?bet=2017:900

Furberg, P. & Westberg, M. (2020/21). Måste myndigheter följa lagarna? Om utkontraktering och legalitet i digital miljö, Juridisk tidskrift, 2, 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.

Gartner (2022). Digital Assets, Gartner Glossary. https://www.gartner.com/en/finance/glossary/digital-assets (Accessed 5 April 2022)

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

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

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

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

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

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 @ 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 (2018). Bedömning av Customer Lockbox, Intraservice, Göteborgs Stad, 21 May.

GP (2017). GÖTEBORG AVBRYTER OSÄKERT IT-PROJEKT, Göteborgs-Posten, Göteborg, 7 October, p. 1.

Guba, E. G. (1981). Criteria for Assessing the Trustworthiness of Naturalistic Inquiries, Educational Communication and Technology, 29(2), 75-91.

IMY (2021). Förhandssamråd om Azure AD och Teams, Integritetsskyddsmyndigheten, Dnr. DI-2021-1513, Stockholm, 2 June.

Janssen, M. & Joha, A. (2011). Challenges for Adopting Cloud-Based Software as a Service (SaaS) in the public sector, in Proceedings of the European Conference on Information Systems (ECIS 2011), http://aisel.aisnet.org/ecis2011/80

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/

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

Lings, B. & Lundell, B. (2004). On Transferring a Method into a Usage Situation, in Kaplan, B., Truex III, D.P, Wastell, D., Wood-Harper, A.T and DeGross, J.I. (eds.) Information Systems Research: IFIP Working Group 8.2 – IS Research Methods Conference – "Relevant Theory and Informed Practice: looking forward from a 20 year perspective on IS research", Kluwer, Boston, pp. 535-553.

Lings, B. & Lundell, B. (2005). On the adaptation of Grounded Theory procedures: insights from the evolution of the *2G* method, Information, Technology & People, 18(3): 196-211.

Liu, E. C. (2016). Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), Congressional Research Service, Report#: R44457, CRS Report, 13 April. https://crsreports.congress.gov/product/pdf/R/R44457/3

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). https://ejlt.org/index.php/ejlt/article/view/709/

Lundell, B. & Gamalielsson, J. & 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. & 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. & 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

MS (2019). Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities, Mannheimer Swartling AB, Stockholm, January. https://www.mannheimerswartling.se/app/uploads/2021/04/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf

Melin, U., Sarkar, P. K. & Young, L. W. (2019). To couple or not to couple: A case study of institutional legitimacy relating to SaaS applications in two universities, Information Technology & People, 33(4), 1149-1173.

Microsoft (2017). Formulär för undertecknande av program, Volume licensing, Microsoft, 19 October.

Microsoft (2019a). Årsredovisning Microsoft Aktiebolag: Räkenskapsår 2017-07-01 - 2018-06-30, Microsoft Aktiebolag, Org.nr 556233-4804, 16 February 2019.

Microsoft (2019b). Microsoft Core Online Services Subprocessor List, Microsoft Corporation, 22 February.

Microsoft (2019c). Microsoft Online Services Subprocessors List, Microsoft Corporation, 5 September.

Microsoft (2020). Microsoft Online Services Subprocessors List, Microsoft Corporation, 31 July.

Microsoft (2021a). Microsoft Commercial Support Subcontractors, Microsoft Corporation, 13 August.

Microsoft (2021b). Microsoft Online Services Subprocessors List, Microsoft Corporation, 24 September.

Microsoft (2021c) Microsoft Online Services Subprocessors List, Microsoft Corporation, 23 November. https://go.microsoft.com/fwlink/p/?linkid=2096306 (Accessed 14 April 2022)

Microsoft (2021d) Microsoft Services Agreement, Published 1 April 2021, Effective 15 June 2021. https://www.microsoft.com/en-us/servicesagreement (As is: 3 April 2022).

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

Nas, S. & Roosendaal, A. (2018). DPIA Diagnostic Data in Microsoft Office Proplus, Study Commissioned by the Ministry of Justice and Security for the benefit of SLM Rijk Vendor Management (Strategic Microsoft Dutch Government), Privacy Company, 5 November. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf

NIST (2011) The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg. https://doi.org/10.6028/NIST.SP.800-145

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

Opara-Martins, J., Sahandi, R. & Tian, F. (2016) Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective, Journal of Cloud Computing, 5(4). https://doi.org/10.1186/s13677-016-0054-z

OSL (2009). Offentlighets- och sekretesslag (2009:400), SFS nr: 2009:400, 20 May. https://rkrattsbaser.gov.se/sfst?bet=2009:400

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

Regeringskansliet (2018). Granskning av Transportstyrelsens upphandling av it-drift, Ds 2018:6, February, Regeringskansliet, ISBN 978-91-38-24768-6.

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 February. https://rkrattsbaser.gov.se/sfst?bet=1974:152

Riksarkivet (2009). 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. https://riksarkivet.se/rafs?pdf=rafs/RA-FS%202009-02.pdf

Schreieck, M., Wiesche, M. & Krcmar, H. (2021). Capabilities for value co-creation and value capture in emergent platform ecosystems: A longitudinal case study of SAP's cloud platform, Journal of Information Technology, 36(4), 365–390.

Säpo (2019). Säkerhetspolisens årsbok 2019, ISBN: 978-91-86661-17-5, Stockholm.

Shurson, J. (2020). Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law, International Journal of Law and Information Technology, 28(2), 167-184.

SKV/KFM (2021). 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.

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

Svantesson, D. J. B. (2012). Data protection in cloud computing – The Swedish perspective, Computer Law & Security Review, 28(4), 476-480.

Tracol, X. (2021). Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations, ERA Forum, https://doi.org/10.1007/s12027-021-00679-1

Wagle, S. S. (2016). Cloud Computing Contracts, In Lehmann, A. et al. (Eds.) Privacy and Identity Management: Facing up to Next Steps, IFIP Advances in Information and Communication Technology, Vol. 498, Springer, Cham, ISSN 1868-4238, ISBN 978-3-319-55782-3, pp. 182-198.

Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?', International Data Privacy Law, 8(4), 318-337.

Walsham, G. (1993) Interpreting Information Systems in Organizations, Wiley, Chichester.

Walsham, G. (1995) Interpretive case studies in IS research: nature and method, European Journal of Information Systems, 4(2), 74-81.

About the Authors

Björn Lundell

Björn Lundell is a professor at the University of Skövde, Skövde, Sweden, where he leads the Software Systems Research Group. His research interests include fundamental sociotechnical challenges concerning software systems, focusing on different aspects of lock-in, interoperability, and longevity of systems. Lundell received his Ph.D. from the University of Exeter in 2001.

Jonas Gamalielsson

Jonas Gamalielsson is a researcher and senior lecturer at the University of Skövde, Skövde, Sweden, where he is a member of the Software Systems Research Group. His research interests include open source software and open standards for addressing challenges related to lock-in, interoperability, and longevity of systems. Gamalielsson received his Ph.D. from Heriot Watt University in 2009.

Andrew Katz

Andrew Katz is a visiting researcher in the Software Systems Research Group, University of Skövde, Skövde, Sweden, and a partner at the law firm Moorcrofts, Marlow, U.K. His research focuses on technology law with a particular interest in open source software, open design (including hardware), development, and licensing. Katz received his M.A. in law from Cambridge University, U.K. and qualified as a barrister at the Inns of Court School of Law in London, before requalifying as a solicitor, practising in England and Wales. Further information about him can be found at https://moorcrofts.com/team/andrew-katz/

Mathias Lindroth

Mathias Lindroth is a Swedish lawyer specialising in the fields of intellectual property, IT and privacy law. Since 2001 he has advised both public and private sector clients in matters relating to their use of information technology. He has cooperated with the researchers at the Software Systems Research Group at Skövde University in several projects. He also serves on the board of directors of the Swedish Open Source industry association (Open Source Sweden).

