

# Anskaffning och användning av programvara som tjänst (SaaS-lösningar) inom myndigheter

Resultat och erfarenheter från en studie av en stor  
offentlig organisations anskaffning av M365-lösningen

Professor Björn Lundell, Ph.D.

Software Systems Research Group (SSRG)

Högskolan i Skövde

[bjorn.lundell@his.se](mailto:bjorn.lundell@his.se)

@

Sambruk, Nätverk – Digitala samverkansplattformar

16 mars 2023

# Introduktion – *en fallstudie av en stor PSO som ... anskaffat och använder Microsoft 365-lösningen*

- Många offentliga organisationer (PSOs) har anskaffat och använder **publika molntjänster**, däribland SaaS-lösningen **Microsoft 365** (M365) (Lundell et al., 2022b)
- En **fallstudie** av en **PSO** som anskaffat och använder **M365** redovisar ett olämpligt **leverantörsberoende** (Lundell et al., 2022c)
- ‘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’ (Lundell et al., 2022c)

# Resultat från fallstudien (1/3) ...

*... identifierar flera problem och brister, däribland ...*

- '[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' (Lundell et al., 2022c)
- 'we find it **inappropriate for a public sector organisation** within the EU [CoG] **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.**' (Lundell et al., 2022c)

# Resultat från fallstudien (2/3) ...

*... identifierar flera problem och brister, däribland ...*

- Det underlag för beslut om fortsatt användning av M365 som redovisades den 20 oktober 2017 ‘was too limited to constitute a solid basis for a decision’ (Lundell et al., 2022c)
- Göteborgs Stad ‘**lacks information detailing in which countries data processing and maintenance of digital assets** from the CoG *has taken place*’ (Lundell et al., 2022c)
- ‘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**’ (Lundell et al., 2022c)

# Resultat från fallstudien (3/3) ...

... identifierar flera problem och brister, däribland ...

- ‘neither *Intra* nor any other organisation in the CoG (of a total of 28 PSO’s 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’ (Lundell et al., 2022c)
- ‘since use of the M365 solution requires that the CoG grants a royalty-free licence 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**’ (Lundell et al., 2022c)

# Olaglig & olämplig användning av molntjänster ... & programvara som tjänst (SaaS-lösningar)?

- **Molntjänst** – 'en tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser'  
(2 § 7 p. i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster)
- **Cloud computing** 'is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'  
(NIST, 2011)
- **SaaS**: 'The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure' (NIST, 2011)

# Olaglig & olämplig användning av SaaS-lösningar

## Hur många ägg kan (och bör) läggas i samma korg?



- ‘for a PSO that has not yet adopted M365 **it would be “completely insane”** (Swe. ‘helt vansinnigt’) **to adopt and use the solution under current conditions as it is “unlawful”** (Swe. ‘inte lagligt’)’ (Lundell et al., 2022b)
- ‘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’ (Lundell et al., 2022c)
- **97 % (29 av 30) av alla kommuner** som slumpmässigt valts ut för en studie använder **M365-lösningen** (Lundell et al., 2021b)

# Av alla undersökta myndigheter som anskaffat & ... ... använder **M365**-lösningen **har ingen myndighet** ...

- ... identifierat alla relevanta **avtalsvillkor**
- ... identifierat alla relevanta **licenser** för format
- ... identifierat relevanta **säkerhetsrisker (NIL)**
- ... tillgång till en lämplig **exitstrategi** som möjliggör att användningen av M365 kan avslutas med en god förvaltning
- ... analyserat risker avseende **patent (SEPs)**
- ... analyserat risker avseende **upphovsrätt**
- ... analyserat användning av underbiträden för behandling av uppgifter i länder utanför EU, däribland **Kina & Serbien**



# Datasuveränitet (eng. Data sovereignty) ... ... förutsätter upprätthållande av en **god förvaltning**

- **Datasuveränitet *förutsätter*** anskaffning, utveckling och nyttjande av system och programvara som möjliggör **behandling** och en **god förvaltning** av **uppgifter och handlingar** (data, dokument & andra typer av digitala representationer, exvis data i databaser) i **öppna format** och **öppna standarder** som ***har implementerats*** av hållbara programvaruprojekt som tillhandahåller **öppen programvara**
- “Data sovereignty refers to the capability of a legal entity or natural person to determine and execute usage rights when it comes to their data.” (Otto, 2022)

# En god förvaltning – undviker inlåsnings ...

- 'Inlåsnings effekter kan uppstå om myndigheten på ett eller annat sätt har ett **beroende** till en specifik leverantör. De kan bland annat uppstå på grund av en viss leverantörs specifika **produkter, tjänster** eller **teknologi**. Det kan även bero på **kompetensmässiga** och **rättsliga skäl**, vilket kan medföra att tjänsten varken kan eller får förvaltas av någon annan än den som levererar den för tillfället.' (Pensionsmyndigheten, 2015)
- 'A major **lock-in concern** is **risk of dependence** (or over-dependence) on **one provider's**, often proprietary, **service**' (Hon et al., 2012)

# En **god förvaltning** – *undviker inlåsning genom ...* *... öppna format som implementeras i programvara*

- Ett **format** som tillhandahålls under villkor som uppfyller definitionen av öppen standard enligt EIF 1.0 (EU:s interoperabilitetsramverk version 1.0) är ett **öppet format**
- **Öppna format *kan implementeras*** av programvaruprojekt som distribuerar programvara under licenser för **slutna programvara** och ***alla licenser för öppen programvara*** (eng. **Open Source Software**, [opensource.org](https://opensource.org))
- **Slutna format** som tillhandahålls under s.k. FRAND-villkor orsakar inlåsning, interoperabilitetsproblem, samt hinder för öppen programvara (Lundell, 2020; Lundell et al., 2015, 2019, 2023)

# En **öppen programvara** (Open Source Software)

*... är en delmängd av all programvara ...*

- En **öppen programvara** (Open Source Software, OSS) är en programvara som tillhandahålls under **villkor** som uppfyller **definitionen av öppen programvara** ([opensource.org/osd](https://opensource.org/osd)) och som tillgängliggjorts under en licens vilken godkänts av organisationen Open Source Initiative (**OSI**, [opensource.org](https://opensource.org))
- OSI förvaltar definitionen som har etablerats för att precisera vad som utgör öppen programvara (Perens, 1999; Lundell, 2020)
- Ett **fåtal** populära **licenser** för öppen programvara används av en mycket **stor andel** av de **programvaruprojekt** som tillhandahåller öppen programvara ([opensource.org/licenses](https://opensource.org/licenses))

# Utveckling av öppen vs. sluten programvara ... ... användning med intern vs. extern it-drift ...

		Användning av programvara ...	
		Intern it-drift	Extern it-drift
Utveckling av programvara ...	Sluten	<b>Tidsbegränsade licenser</b> <i>Ev. supportkontrakt</i>	<b>Tidsbegränsade licenser</b> <b>Tidsbegränsade kontrakt</b>
	Öppen	<b>Eviga licenser</b> <i>Ev. supportkontrakt</i>	<b>Eviga licenser</b> <b>Tidsbegränsade kontrakt</b>

*Baserat på Lundell et al. (2021a, 2022b, 2023b)*

- **Öppen programvara** (kund har kontroll): Kan användas med såväl **intern** (lokalt installerad) som **extern** drift genom myndighetssamverkan *eller* drift av privat leverantör (SaaS)
- **Sluten programvara** (lev. har kontroll över villkor för it-drift)

# Laglig & lämplig behandling och förvaltning av ... ... uppgifter och handlingar med SaaS-lösningar ...

- ‘Lawful and appropriate use of cloud-based globally provided Software-as-a-Service (SaaS) solutions by a public sector organisation (PSO) for **data processing** and **maintenance of digital assets presupposes an investigation of all relevant contract terms.**’ (Lundell et al., 2022b)
- Okända villkor omöjliggör analys av laglighet och lämplighet

**Olaglig & olämplig databehandling och förvaltning ...**

**Okända villkor för databehandling och förvaltning ...**

**Laglig & lämplig databehandling och förvaltning ...**

**... av uppgifter och handlingar**

# Användning av en **SaaS-lösning** under ... ... **okända villkor** är **alltid olämplig** ...

- ‘The fact that public bodies have actually no control over the engagement of processors and sub-processors makes it difficult for them to ensure that the processing is compliant with the provisions of the GDPR, especially regarding transfers to third countries. However, it must be emphasised that this difficulty does not, in itself, exonerate the controller from its responsibilities in the processing.’ (EDPB, 2023, s. 16)
- För en myndighet som **använder en SaaS-lösning under okända villkor** för att behandla och förvalta uppgifter och handlingar inom myndigheten **är det omöjligt att visa att myndighetens användning av lösningen inte är olämplig**

# Referenser (1/6) ...

- Bendiek, A. & Stürzer, I. (2022) Advancing European Internal and External Digital Sovereignty, German Institute for International and Security Affairs, SWP Comment 2022/C 20, 11 March. <https://doi.org/10.18449/2022C20>
- EC (2020a) A European strategy for data, COM(2020) 66 final, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, European Commission, 19 February. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>
- EC (2020b) Inception Impact Assessment, Legislative framework for the governance of common European data spaces, CENCT/G1, Legislative Proposal, Ref. Ares(2021)3527151, European Commission, 2 July. <https://ec.europa.eu/info/law/better-regulation/>
- EC (2022) European Commission digital strategy Next generation digital Commission, C(2022) 4388 final, Communication to the Commission, European Commission, 30 June. [https://ec.europa.eu/info/publications/EC-Digital-Strategy\\_en](https://ec.europa.eu/info/publications/EC-Digital-Strategy_en)
- EDPB (2023) 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, European Data Protection Board, Adopted on 17 January. [https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en)
- EK (2020a) En EU-strategi för data, COM(2020) 66 final, Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, Europeiska kommissionen, 19 februari. <https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020DC0066&from=SV>



# Referenser (2/6) ...

- Fischer, T., Lundell, B. & Gamalielsson, J. (2021) Achieving Conformance to Document Standards: Can PDF Files Conform to the PDF/A-1b Specification?, International Journal of Standardization Research (IJSR), Vol. 19(1), pp. 1-32. <http://doi.org/10.4018/IJSR.288523>
- Försäkringskassan (2019) Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt, Dnr. 013428-2019, Version 1.0, 18 november, <https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf?MOD=AJPERES&CVID=>
- GAIA (2020) Technical Architecture, Federal Ministry for Economic Affairs and Energy (BMWi), Berlin, June. <https://www.bmwk.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.html>
- Gamalielsson, J. & Lundell, B. (2017) On licensing and other conditions for contributing to widely used open source projects: an exploratory analysis, In Proceedings of the 13th International Symposium on Open Collaboration (OpenSym '17). ACM, New York, NY, USA, Article 9, 14p. <http://doi.org/10.1145/3125433.3125456>
- Hon, W. K., Millard, C. & Walden, I. (2012) Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now, Stanford Technology Law Review, Vol. 16(1), pp. 79-129.
- Lundell, B. (2020) Analys av DIGG:s policy för utveckling av programvara, version 1.0, 20 maj, Skövde University Studies in Informatics 2020:1, ISSN 1653-2325, ISBN: 978-91-983667-6-1, University of Skövde, Skövde, Sweden. <http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-18895>
- Lundell, B. (2021) Yttrande över betänkandet Säker och kostnadseffektiv IT-drift (SOU 2021:1), Dnr. HS 2021/469, Högskolan i Skövde, Skövde, 7 maj.

# Referenser (3/6) ...

- Lundell, B. (2022) Förutsättningar för datadelning genom öppna ekosystem: ett perspektiv på möjligheter och hinder, Dnr. FP 2021/87, 14 Feb. 2022, Högskolan i Skövde, Inkluderad i Vinnovas slutrapport "Uppdrag att kartlägga behov av utvecklingsinsatser för datadelning" från regeringsuppdrag (Dnr. I2021/02737).  
<https://www.vinnova.se/contentassets/41641cacf8a24d0782c88fb18259fd3b/2021-04320-slutrapport.pdf>
- Lundell, B., Butler, S., Fischer, T., Gamalielsson, J., Brax, C., Feist, J., Gustavsson, T., Katz, A., Kvarnström, B., Lönroth, E. & Mattsson, A. (2022a) Effective Strategies for Using Open Source Software and Open Standards in Organizational Contexts – Experiences From the Primary and Secondary Software Sectors, IEEE Software, Vol. 39(1), pp. 84-92.  
<https://doi.org/10.1109/MS.2021.3059036>
- Lundell, B. & Gamalielsson, J. (2018) Sustainable digitalisation through different dimensions of openness: how can lock-in, interoperability, and long-term maintenance of IT systems be addressed?, In Proceedings of the 14th International Symposium on Open Collaboration (OpenSym '18), ACM, New York, ISBN: 978-1-4503-5936-8, Article 3, 10p. <https://doi.org/10.1145/3233391.3233527>
- Lundell B., Gamalielsson, J., Butler, S., Brax, C., Persson, T., Mattsson, A., Gustavsson, T., Feist, J. & Öberg, J. (2021a) Enabling OSS usage through procurement projects: How can lock-in effects be avoided?, In Taibi, D. et al. (Eds.), The 13th International Conference on Open Source Systems (OSS 2021), IFIP AICT 624, Springer, pp. 1-12. [https://doi.org/10.1007/978-3-030-75251-4\\_2](https://doi.org/10.1007/978-3-030-75251-4_2)

# Referenser (4/6) ...

- Lundell, B., Gamalielsson, J. & Katz, A. (2015) On implementation of Open Standards in software: To what extent can ISO standards be implemented in open source software?, *International Journal of Standardization Research*, Vol. 13(1), pp. 47-73. <https://dx.doi.org/10.4018/IJSR.2015010103>
- 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*, Vol. 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. (2023a) Implementing the HEVC standard in software: Challenges and Recommendations for organisations planning development and deployment of software, *Journal of Standardisation*, Vol. 2. <https://doi.org/10.18757/jos.2022.6695>
- Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2021b) 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. [https://doi.org/10.1007/978-3-030-84789-0\\_5](https://doi.org/10.1007/978-3-030-84789-0_5)

# Referenser (5/6) ...

- Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2022b) Use of Commercial SaaS Solutions in Swedish Public Sector Organisations under Unknown Contract Terms, In Janssen, M. et al. (Eds.) EGOV 2022: Electronic Government, Lecture Notes in Computer Science, Vol 13391, Springer, Cham, pp. 73-92. [https://doi.org/10.1007/978-3-031-15086-9\\_6](https://doi.org/10.1007/978-3-031-15086-9_6)
- Lundell, B., Gamalielsson, J., Katz, A., & Lindroth, M. (2022c) Data Processing and Maintenance in Different Jurisdictions When Using a SaaS Solution in a Public Sector Organisation, JeDEM – EJournal of EDemocracy and Open Government, Vol. 14(2), pp. 214–234. <https://doi.org/10.29379/jedem.v14i2.749>
- Lundell, B., Gamalielsson, J., Katz, A., & Lindroth, M. (2023b) Avoiding lock-in effects through obtaining all necessary licences before use of a SaaS solution in a public sector organisation: a case study, European Journal of Law and Technology, Vol. 14(1) (to appear).
- Lundell, B., Gamalielsson, J. & Tengblad, S. (2016) IT-standarder, inlåsnings och konkurrens: En analys av policy och praktik inom svensk förvaltning, Uppdragsforskningsrapport 2016:2, Konkurrensverket, ISSN: 1652-8089. [http://www.konkurrensverket.se/globalassets/publikationer/uppdagsforskning/forsk\\_rapport\\_2016-2.pdf](http://www.konkurrensverket.se/globalassets/publikationer/uppdagsforskning/forsk_rapport_2016-2.pdf)
- Lundell, B., Gamalielsson, J., Tengblad, S., Hooshyar Yousefi, B., Fischer, T., Johansson, G., Rodung, R., Mattsson, A., Oppmark, J., Gustavsson, T., Feist, J., Landemoo, S. & Lönroth, E. (2017) Addressing lock-in, interoperability, and long-term maintenance challenges through Open Source: How can companies strategically use Open Source?, In Balaguer et al. (Eds.) The 13th International Conference on Open Source Systems (OSS 2017), IFIP AICT 496, Springer, pp. 80-88. [http://dx.doi.org/10.1007/978-3-319-57735-7\\_9](http://dx.doi.org/10.1007/978-3-319-57735-7_9)

# Referenser (6/6) ...

- › Lundell, B. & van der Linden, F. (2012) Open Source Software as Open Innovation: Experiences from the Medical Domain, In Eriksson Lundström et al. (Eds.) *Managing open innovation technologies*, Springer, pp. 3-16. [https://doi.org/10.1007/978-3-642-31650-0\\_1](https://doi.org/10.1007/978-3-642-31650-0_1)
- › Meeker, H. (2020) *Open (Source) for Business: A Practical Guide to Open Source Software Licensing*, Third edition, Kindle Direct Publishing Platform, Seattle, ISBN-13: 979-8618201773.
- › NIST (2011) *The NIST Definition of Cloud Computing*, Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, September. <https://doi.org/10.6028/NIST.SP.800-145>
- › NPS (2016) *Open IT-standards*, National Procurement Services, Kammarkollegiet, 7 mars, Dnr 96-38-2014, <https://www.avropa.se/globalassets/dokument/open-it-standards.pdf>
- › Otto, B. (2022) *The Evolution of Data Spaces*, In Otto et al. (Eds), *Designing Data Spaces*, Springer, Cham. pp. 3-15. [https://doi.org/10.1007/978-3-030-93975-5\\_1](https://doi.org/10.1007/978-3-030-93975-5_1)
- › Pensionsmyndigheten (2015) *Molntjänster i staten: en ny generation av outsourcing*, Pensionsmyndigheten, Version 1.0, 28 december.
- › Perens, B. (1999) *The Open Source Definition*, In DiBona, C. et al. (Eds.) *Open Sources: Voices from the Open Source Revolution*, O'Reilly & Associates, ISBN: 1-56592-582-3, pp. 79-86.