Anskaffning och användning av SaaS-lösningar under okända villkor

Har det utvecklats en kunskapsresistens bland myndigheter och leverantörer?

Professor Björn Lundell, Ph.D.
Software Systems Research Group (SSRG)
Högskolan i Skövde
bjorn.lundell@his.se
@
SUDO-projektet
Högskolan i Skövde
14 mars 2023

Introduktion – *anskaffning och användning av …*
… SaaS inom myndigheter – **Olämpligt** & **Olagligt**?

- Många svenska offentliga organisationer (PSOs) har anskaffat och använder **publika molntjänster**, däribland SaaS-lösningen **Microsoft 365** (M365) (Lundell et al., 2022b)
- '**contract terms** for the M365 solution require the customer to **acquire several third party patent licences** for specific formats **to allow for lawful use of M365** and **to allow for lawful long term maintenance of digital assets exported from M365**' (Lundell et al., 2022b)
- **Licenser** för HEVC (och andra patentbelastade format) som implementeras av M365 **behöver anskaffas** (Lundell et al., 2023a)

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)
- **SaaS-lösningar** – '*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)
- 'För att förhindra att en myndighets verksamhet eller uppgifter utsätts för särskilda risker i samband med **utkontraktering** eller samordning **av it-drift** anser regeringen alltså att **en uppgift ska få lämnas ut bara om det** med hänsyn till omständigheterna **inte är olämpligt**.' (Regeringen, 2023)

Olaglig & **olämplig** användning av **SaaS**-lösningar
Hur många ägg kan (och bör) läggas i samma korg?

- **97 %** (29 av 30) **av alla kommuner** som slumpmässigt valts ut för en studie använder **M365-lösningen** (Lundell et al., 2021b)
- '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 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)

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**

(Lundell et al., 2022b)

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**	**Tidsbegränsade licenser** ***Ev. supportkontrakt***	**Tidsbegränsade licenser** **Tidsbegränsade kontrakt**
	Öppen	**Eviga licenser** ***Ev. supportkontrakt***	**Eviga licenser** **Tidsbegränsade kontrakt**

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** orsakar **alltid olämplig** it-drift...

- ‘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
- 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
- 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

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

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
- 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, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning, Uppdragsforskningsrapport 2016:2, Konkurrensverket, ISSN: 1652-8089. http://www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/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

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
- 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
- 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.
- Regeringen (2023) Sekretessgenombrott vid teknisk bearbetning eller lagring av uppgifter, Lagrådsremiss, 26 januari.