

Migrating to OpenSource

Motion for ICGP AGM

Proposed by: Dr Greg Pszkit

Seconded by: Dr Colman Byrne

Summary

We propose that the Louth Faculty mandates the ICGP to institute a strategic review and planning process to progressively migrate its core IT infrastructure and software from closed-source, predominantly US-owned platforms (such as Microsoft products) toward open-source, Linux-based alternatives, in line with European digital-sovereignty and EU-open-source-software policy objectives.

Details

Examples of successful and planned migrations:

Several European cities—such as Munich, Schleswig-Holstein, and Lyon—have already begun or completed large-scale migrations from Microsoft to Linux-based open-source stacks, in pursuit of digital sovereignty, cost control, and local IT development. National policies for Germany and France were recently introduced as well:

1. **Munich, Germany** – The city ran the “LiMux” project from 2004 onward, migrating roughly 12,600 of its 15,500 desktops from Windows to a Linux-based solution, explicitly to reduce dependence on a single US vendor and foster local IT services.¹
2. **Schleswig-Holstein, Germany** – This northern state is migrating around 30,000 public-sector workstations from Windows and Microsoft Office to Linux and LibreOffice, explicitly to achieve “digital sovereignty” and switch to locally-supported, open-source tools.²
3. **Lyon, France** – The city has begun phasing out Microsoft Office and Windows in favour of Linux, OnlyOffice, and PostgreSQL, as part of a “Territoire Numérique Ouvert” (Open Digital Territory) platform emphasizing data control, transparency, and regional economic development.³
4. **Cities in Denmark and other EU states** – Several Danish cities (e.g., Aarhus, Copenhagen) and administrations in Spain, Italy, and elsewhere have also moved toward open-source office suites and Linux, often citing savings on licensing and reduced vendor lock-in.

¹ <https://opensource.com/government/14/5/how-munich-switched-15000-pcs-windows-linux>

² https://www.theregister.com/2024/04/04/germanys_northernmost_state_ditches_windows/

³ <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/municipality-lyon-moves-towards-open-source>

5. Also, Germany's federal government just incorporated this move into the **Deutschland-Stack** framework, published by the Federal Ministry for Digital and State Modernization. It requires **ODF (Open Document Format)** and **PDF/UA** as the only permitted formats for documents across **all public administration levels**—from federal ministries to local offices—under the "Semantic Technologies and Real-Time Analytics" pillar.⁴
6. **France's Interministerial Digital Directorate (DINUM)** announced on 8 April 2026 that it is migrating its own workstations from Windows to Linux and **has ordered every government ministry to formalise a plan to eliminate extra-European digital dependencies by autumn 2026**. It is not just a casual suggestion for the public sector; it is an official directive/mandate for ministries to plan and formalize the transition.⁵

European Commission position

The European Commission's open-source-software strategy and emerging sovereign-tech proposals explicitly encourage public administrations to increase their use of open-source tools. By aligning with this trajectory, the ICGP can proactively support digital sovereignty and interoperability rather than lag behind EU-level policy.

1. The **European Commission's Open Source Software Strategy** (2020-2023 and follow-ups) explicitly promotes open-source software across EU institutions, including setting up an Open Source Programme Office, revising software-distribution practices, and integrating open source into IT governance and security.⁶
2. The **Interoperable Europe / JoinUp** initiative has long highlighted thousands of EU cities and regions using free/open-source software, and the Commission is steadily increasing the role of open-source in its own ICT services.⁷
3. Newer initiatives, such as proposals for an **EU Sovereign Tech Fund** and an **Open Source expert group**, aim to support strategically important open-source projects and tailor features requested by European public administrations, reinforcing the policy-level push toward open-source ecosystems.⁸

Why inertia is not optimal approach

Enshittification

Enshittification, also known as platform decay, is a process in which two-sided online products and services decline in quality over time. Initially, vendors create high-quality offerings to attract users,

⁴ <https://blog.documentfoundation.org/blog/2026/03/20/big-news-germany-has-just-made-odf-mandatory/>

⁵ <https://thenextweb.com/news/france-linux-windows-migration-digital-sovereignty>

⁶ https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open-source-software-strategy_en

⁷ <https://ajuntamentdebarcelona.github.io/ethical-digital-standards-site/tech-sovereignty/0.1/public-administration.html>

⁸ <https://opensource.org/blog/europes-open-source-opportunity-our-vision-for-the-eu-open-digital-ecosystems-strategy>

then they degrade those offerings to better serve business customers, and finally degrade their services to both users and business customers to maximize short-term profits for shareholders.

Canadian writer Cory Doctorow coined the neologism enshittification in November 2022. The American Dialect Society selected it as its 2023 Word of the Year, with Australia's Macquarie Dictionary following suit for 2024. Merriam-Webster and Dictionary.com also list enshittification as a word.⁹

And this is exactly the reason for:

Long history of Microsoft's frivolous approach to reported issues

- Microsoft sat on a critical **JavaScript-engine zero-day** (related to Edge / Chakra) for about **90 days** after being told of it. The flaw was **already being exploited** in the wild when they finally patched it. Trend Micro's Zero Day Initiative (ZDI) reported it to Microsoft, pointed out that 90 days had passed, and Microsoft only fixed it after pressure and disclosure talk.¹⁰
- Microsoft **knew about a serious Windows Print Spooler RCE (CVE-2021-36958)** since **December 2020**, but left it unfixed until **August 2021**, when exploitation was obvious and another Print Spooler RCE (PrintNightmare) was already under active attack. Microsoft was sitting on it for **eight months** while **customers were being hit** (ransomware and lateral-movement attacks).^{11 12}
- "Midnight Blizzard" - Russian state sponsored group, originally known as NOBELIUM, which managed to crawl inside **Microsoft's** network to obtain access to data belonging to their **upper-most top level executives** as well as certain **corporate customers** and a number of **federal agencies**.^{13 14}
 - Microsoft is using their own security flaws as an opportunity to **upsell** their **Entra ID Protection** and **Purview Audit (Premium)** capabilities¹⁵:
 - *"Detect, investigate, and remediate identity-based attacks using solutions like Microsoft Entra ID Protection.*
 - *Investigate compromised accounts using Microsoft Purview Audit (Premium).*
 - *Enforce on-premises Microsoft Entra Password Protection for Microsoft Active Directory Domain Services."*
- The federal Cyber Safety Review Board released a long-anticipated report which showed the company **failed to prevent** a massive 2023 hack of its **Microsoft Exchange** Online environment. The hack by a People's Republic of China-linked espionage actor led to the theft of 60,000 **State Department** emails and gained access to other **high-profile officials**¹⁶
 - AJ Grotto, the director of the Program of Geopolitics, Technology and Governance at the Stanford Cyber Policy Center and a former White House director for cyber policy said: *"In a healthy marketplace, **these would be fireable offenses**. Regrettably, the*

⁹ <https://en.wikipedia.org/wiki/Enshittification>

¹⁰ <https://www.zerodayinitiative.com/advisories/ZDI-18-1350/>

¹¹ <https://thehackernews.com/2021/08/microsoft-security-bulletin-warns-of.html>

¹² <https://www.hipaajournal.com/exploit-released-printnightmare-zero-day-windows-print-spooler-rce-vulnerability/>

¹³ <https://www.theverge.com/2024/7/4/24192159/microsoft-midnight-blizzard-hack-targets>

¹⁴ <https://www.techmonitor.ai/technology/cybersecurity/midnight-blizzard-microsoft-breach?cf-view>

¹⁵ <https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/>

¹⁶ <https://industrialcyber.co/reports/csrbs-reports-microsoft-exchange-breach-by-storm-0558-urges-security-reforms-following-espionage-incident/>

marketplace is far from healthy — Microsoft has the government locked in as a customer, so the government's options for forcing change at Microsoft are limited, at least in the short term."

- Taiwanese security researcher Orange Tsai published a blog post laying out the details of a security vulnerability in Microsoft Exchange. Tsai warned Microsoft about this vulnerability as early as June of 2021, and while the company responded by releasing some partial fixes, it took Microsoft **14 months to fully resolve** the underlying security problem. Tsai had earlier reported a related vulnerability in Exchange that was massively exploited by a group of Chinese state-sponsored hackers known as Hafnium, which last year penetrated more than 30,000 targets by some counts. Yet according to the timeline described in Tsai's post this week, Microsoft **repeatedly delayed fixing** the newer variation of that same vulnerability, assuring Tsai no fewer than four times that it would patch the bug before pushing off a full patch for months longer. When Microsoft finally released a fix, Tsai wrote, it still required manual activation and lacked any documentation for four more months¹⁷
- Microsoft has repeatedly **down-played serious issues, taken too long to fix them, and then only acted after public or regulatory pressure**, including Exchange-related bugs that were exploited before patches shipped. HealthMail is based on Exchange.

We are in a walled garden and on one company's mercy

We no longer truly own any software; we only use it as a service, which means paying forever. On top of that, at any moment a private company can arbitrarily decide to end support and force users to buy a new version.

- Windows 10 and the forced upgrade to Windows 11 – this often required a hardware upgrade even when **it wasn't technically necessary**; there are well known software workarounds to bypass the artificial requirements.¹⁸ Credit to the EU for making Microsoft extend Windows 10 support longer in Europe.¹⁹
- Forcing Exchange Server upgrades by **refusing to accept email from servers on older versions** – one could argue this was effectively extorting additional licensing fees from existing customers, dressed up as a "security risk." Yet any security flaws in Exchange Server are Microsoft's own responsibility. Now they claim they're afraid of receiving email that earlier versions of their own software might send to their newer versions.

They can decide to **introduce a feature we do not want, do not need, or even consider dangerous**— and we have no real say in the matter, unless it escalates into a major public controversy. Take Recall, for example: a feature that would take a screenshot every few seconds and store it "securely" (if you revisit the list above, do you still trust their definition of "secure"?), all in the name of easier searching via AI agents. That would mean every consultation note could end up stored and processed by Microsoft. Only after significant backlash did Microsoft decide to make the feature opt-in, whereas it was originally intended to be enabled by default.²⁰

¹⁷ <https://www.wired.com/story/microsoft-exchange-server-vulnerabilities/>

¹⁸ <https://www.zdnet.com/article/how-to-upgrade-your-incompatible-windows-10-pc-to-windows-11/>

¹⁹ <https://forums.steinberg.net/t/windows-10-extended-support-to-be-free-for-one-year-in-europe/1009591>

²⁰ <https://support.microsoft.com/en-us/windows/retrace-your-steps-with-recall-aa03f8a0-a78b-4b3e-b0a1-2eb8ac48701c>

The same risk applies to GP-level IT systems, where the lack of meaningful competition leaves clinicians with little choice and even less control over what features are imposed on them.

What are benefits

Digital sovereignty and data control

- Reducing reliance on closed-source, US-centric platforms gives the ICGP greater oversight of software, data handling, update policies, and security practices.
- This aligns with the European trend toward “digital sovereignty” and independence from single foreign vendors.

Cost-effectiveness and sustainability

- Open-source software often carries no per-user licensing fees and can run on existing or lower-spec hardware, lowering long-term IT running costs.
- In situation of any disagreement with maintainer of any software, OpenSource project can be forked and maintained by a new team.

Compliance with emerging EU policy

- The EU’s explicit encouragement of open-source software in public administration means that ICGP can proactively align with broader European digital-governance standards instead of reacting to later mandates.

Transparency and interoperability

- Open-source tools typically support open standards, which improves interoperability with other health-IT systems and facilitates easier data-sharing and auditing.

Safety and security

- Open-source projects, by their nature of having source code public, are much safer. Any bug can be identified by number of maintainers or security researchers with prompt patching.

ENDS