# Software Alternatives to Large-Scale Providers

Workshop #2

49th EDPS-DPO Meeting

June 4th, 2021

Your Facilitators:

Constantin CHIRA-PASCANUT, EDPS DPO
[email address redacted]

Robert RIEMANN, EDPS Technology and Privacy
[email address redacted]

# Workshop Schedule

| | | |
|---|---|---|
| 10 min | Warm-Up 🔥 | |
| 10 min | Introduction | Constantin CHIRA-PASCANUT and Robert RIEMANN (EDPS) |
| 10 min | Case Study: Microsoft Office | Elisa MORO (Council DPO Office) |
| 10 min | Case Study: Free Software | Franz RITSCHEL (Carl Duisberg Centren, DPO) |
| 50 min | Discussion 💬 | |

ℹ *Chatham House Rule* for an open discussion within our workshop!

# EDPS IT Today

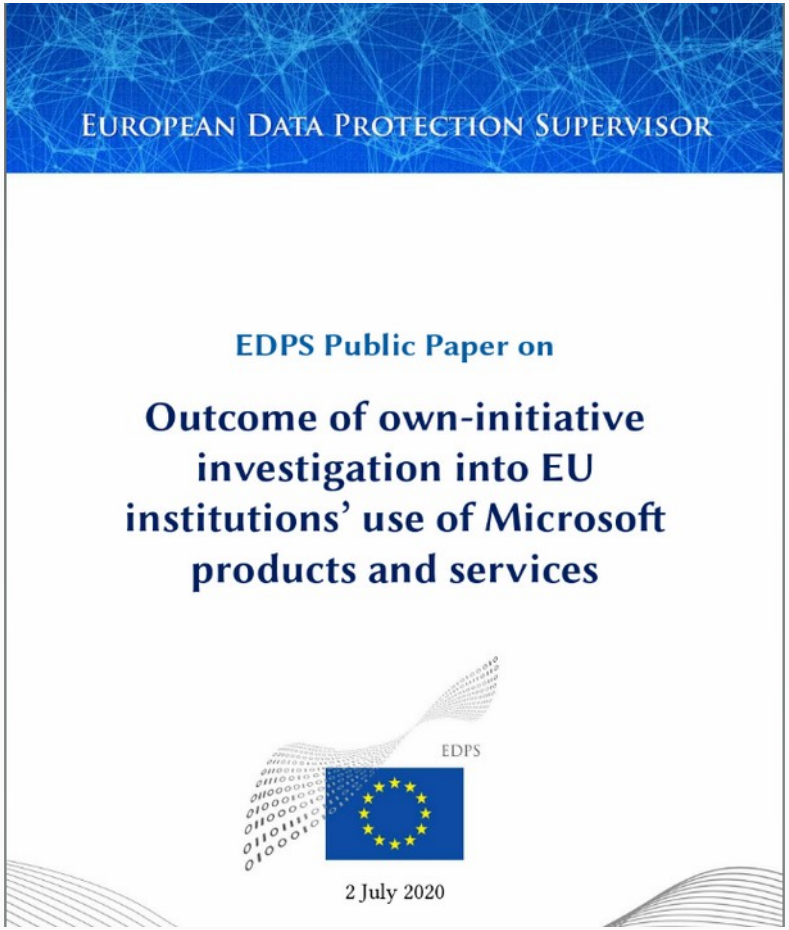
# EDPS Use of Software from Large-Scale Providers

## Also the EDPS depends on software from large-scale providers

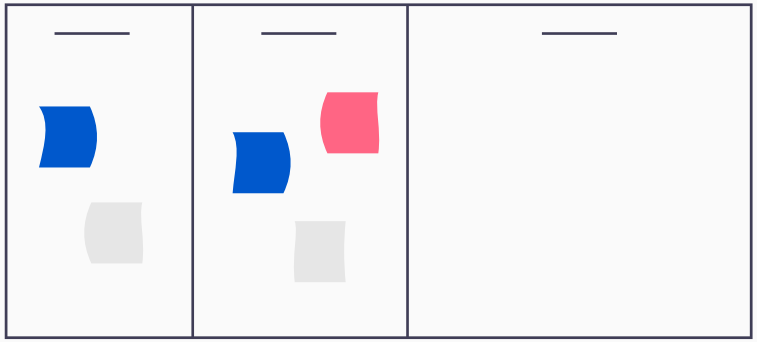
- Twitter
- LinkedIn
- Youtube
- Microsoft Office 2016 (dominant use)
- Microsoft OneDrive/Sharepoint
  (early access via EP provided EDPS IT accounts/devices)

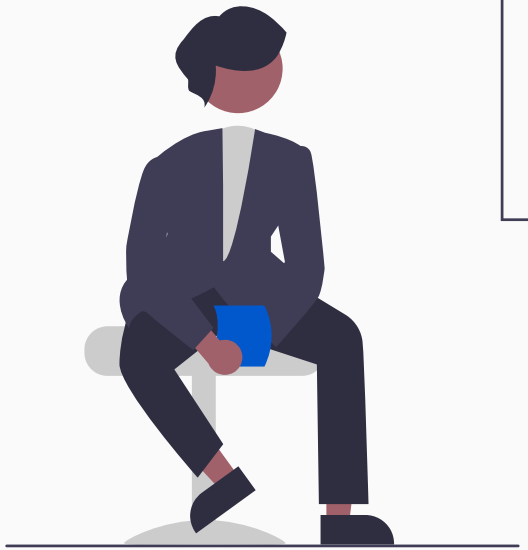
# EDPS Investigation into Microsoft Office

- Not data protection compliant by design
  - Telemetry data
  - Schrems II
  - Blocking of online features (e.g. dictionary)
- Complex to audit properly
- Challenging and expensive negotiations with Microsoft (more: The Hague Forum)



# EDPS IT Strategy





# EDPS Strategy to advance State of the IT/Art

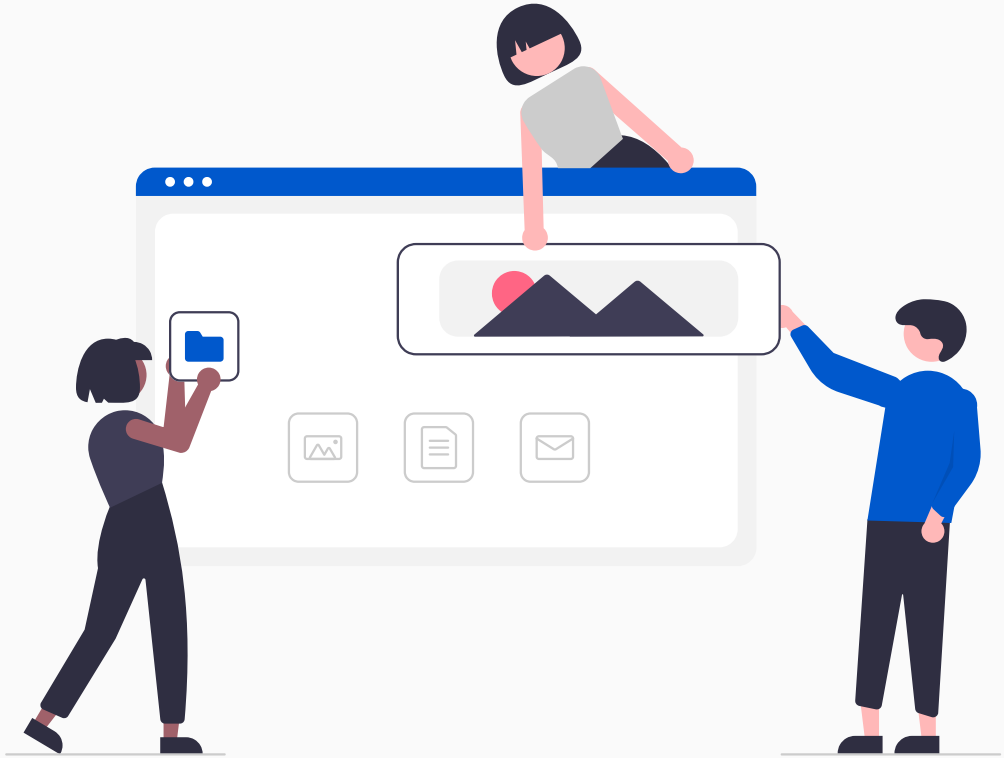
## EDPS Strategy for 2020-2024

> "The EDPS is interested in policy initiatives to achieve 'digital sovereignty', where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. At the same time, we are committed to overcome the detrimental vendor's lock-in syndrome in EUI."

## EDPS on-going Initatives

- IT Gap-Analysis to be followed by a study how to modernise EDPS IT
- Pageflow for Interactive Story-Telling in the Web: https://edpb.edps.europa.eu/europe-day-2021
- Pilot test: Nextcloud with LibreOffice Online
- Public pilot test: Mastodon (Twitter clone)
- Public pilot test: Peertube (Youtube clone)
- EUI Awareness Raising (e.g. workshop at 49$^{th}$ EDPS-DPO meeting)

# EDPS IT Tomorrow ?



# EDPS Social Media Pilots

- Offer citizen full access to public service in a full GDPR-compliant way.
- Use **federated networks** (think of email network) and **APIs** (think of RSS).
- EDPS set to explore in public pilot test two alternative channels:

**Mastodon** (Twitter/Instagram)

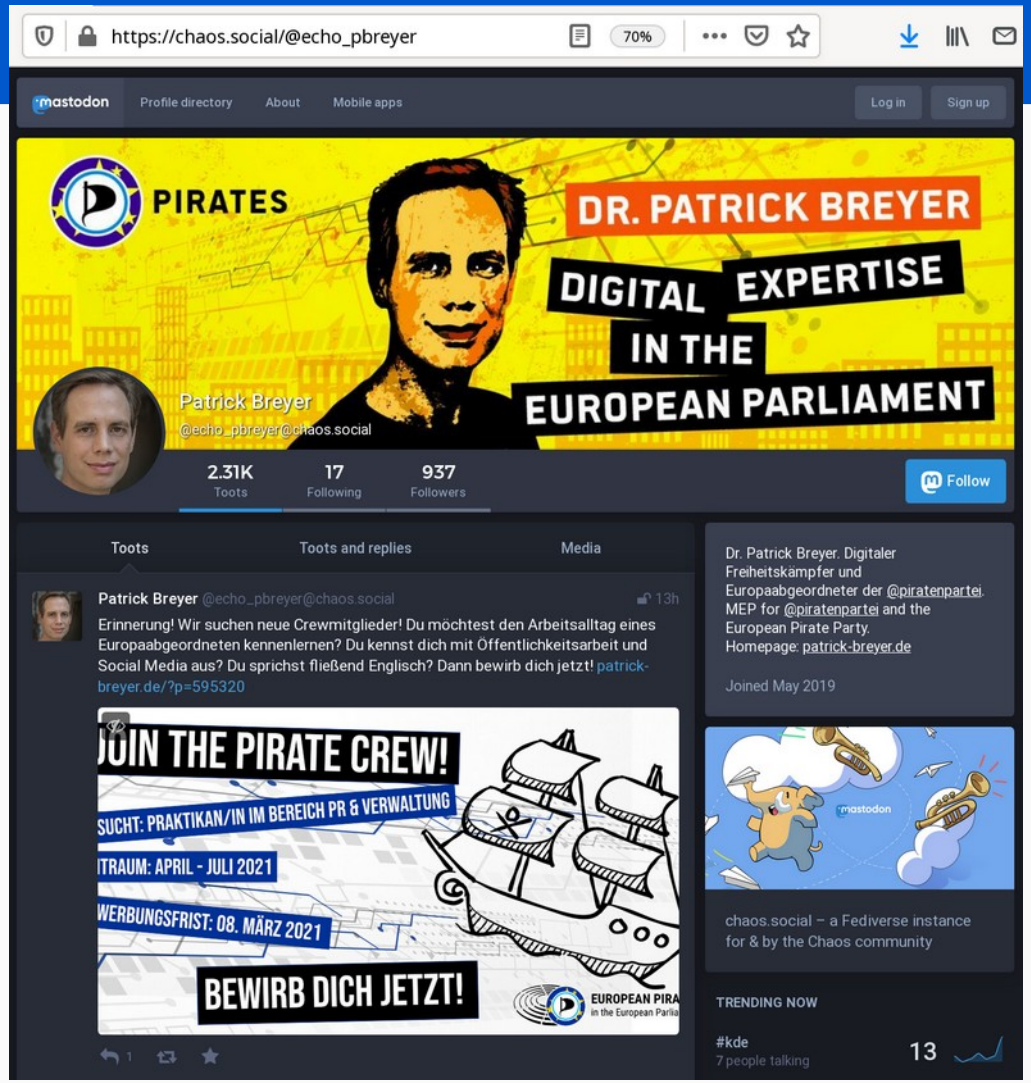
- https://joinmastodon.org
- Examples: https://social.bund.de/@bfdi, https://chaos.social/@echo_pbreyer, https://mastodon.social/@RegierungBW, https://bawü.social/explore

**Peertube** (Youtube)

- https://joinpeertube.org
- Examples: https://media.privacyinternational.org, https://peertube.european-pirates.eu

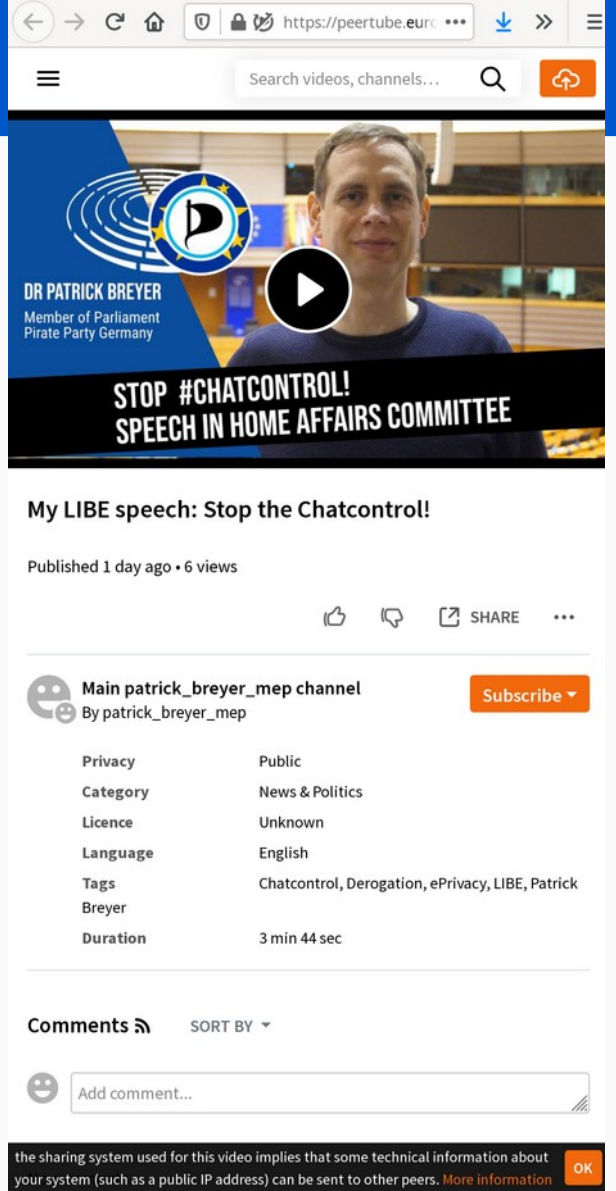
# Quick glimpse into Mastodon

- Stream of *toots* with a upper limit of usually 500 characters and images
- User access toots via website or their own Mastodon account on a (different) Mastodon website
- Open source, customisable and interoperable (ActivityPub)
- Bring your own privacy policy
- Bring your own moderation policy
- EU server without citizen accounts: less personal data processing



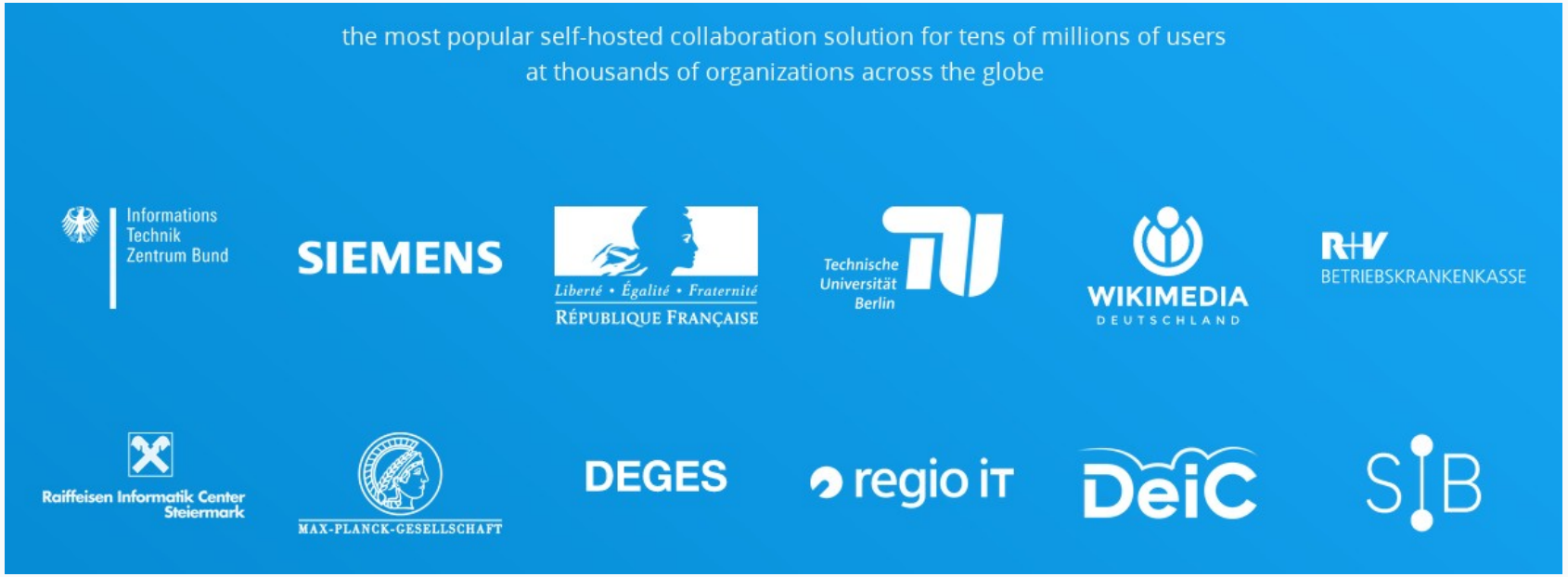
# Quick glimpse into Peertube

- In few words: Youtube clone with accounts and channels
- User access videos via website or video embeds on other websites or e.g. Mastodon
- Open source, customisable and interoperable (ActivityPub)
- Bring your own privacy policy
- Bring your own moderation policy
- Optional: WebTorrent P2P support (not recommended for pilot test)
- Optional: live broadcasting support (P2P?)

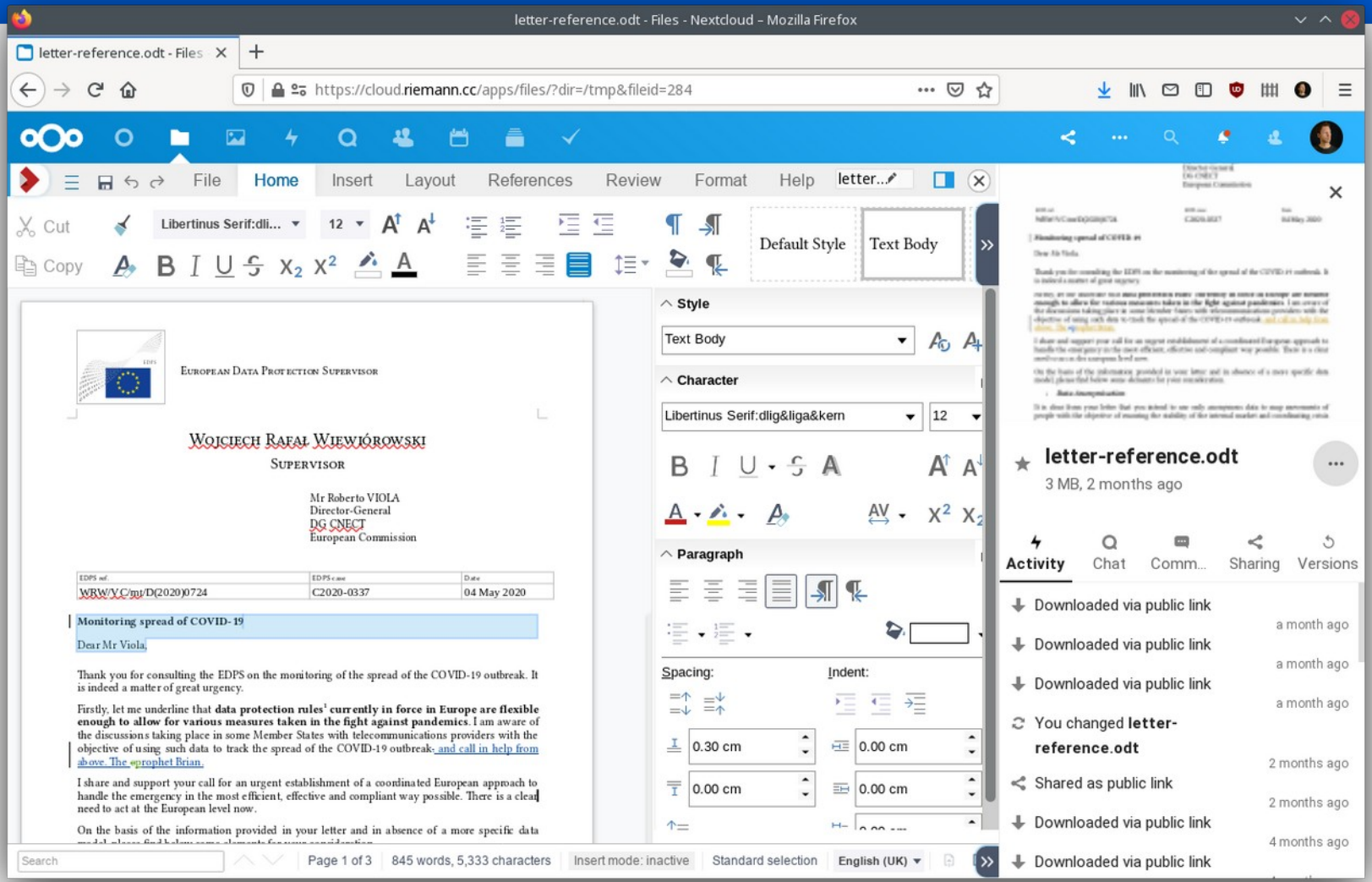


# Quick glimpse into Nextcloud

- Nextcloud is a Dropbox clone with plugins for
  Office productivity, video conferencing, project management, etc.
- Free Software, Open Standards (CalDav, WebDAV, CardDav)
- Bring your own privacy policy



# Example: Robert's Personal Nextcloud hosted in Germany and France



# EDPS Data Protection Assessment of Software Alternatives Providers

## Holistic Approach

- questionnaire
- research, including on sub-processors (i.e. documentation published, business model)
- Know your (prospective) providers
- documentation requested (i.e. copies of data protection documentation available-DPA; procedures)
- documentation proposed (i.e. EDPS DPA)

| | |
|---|---|
| **1.7.** | Does your organisation have a personal data breach management process?<br><br>If yes, please briefly describe it in the "Comment" field and provide us a copy of this procedure. |
| **1.10.** | Will the EDPS's data be separated from other clients (other instance on same machine/other virtual machine/other physical machine) and/or encrypted?<br><br>If yes, please provide more details in the "Comment" field. |
| **1.11.** | Does your organisation offer automatic data/document deletion after a certain period?<br><br>If yes, please provide more details in the "Comment" field. |
| **1.12.** | Can data be destroyed in a secure way after the retention period was reached and/or when the contract ends?<br><br>If yes, please provide more details in the "Comment" field. |
| **1.13.** | Does your organisation maintain a full audit trail of access made to the EDPS' data (read/copy/modify/delete) retaining who processed how, when and which data?<br><br>If yes, please provide more details in the "Comment" field. |

# EDPS Assessing Data Protection of Alternative Software as a Service (SaaS)

**Reactions of Service Providers**

- At times refusal to provide info ('not economically viable')
- Willingness to cooperate

**Internal Assessment**

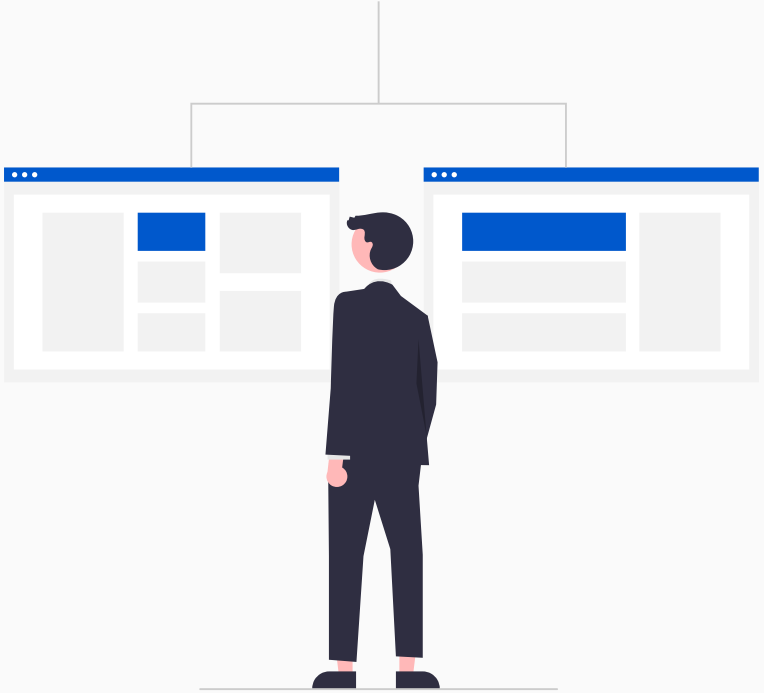
- identify, assess and decide on risks (i.e. sub-processors; data storage; transfers)

**Risk Management**

- Provider (i.e. alternative cloud providers)
- Internally (i.e. customisation of open source; reduce scope)

Example: https://edpb.edps.europa.eu/europe-day-2021
(open source content management system for interactive story telling)

# Possible Obligations to Assess Software Alternatives



# European Data Protection Regulation (2018/1725) on Assessing Software Alternatives

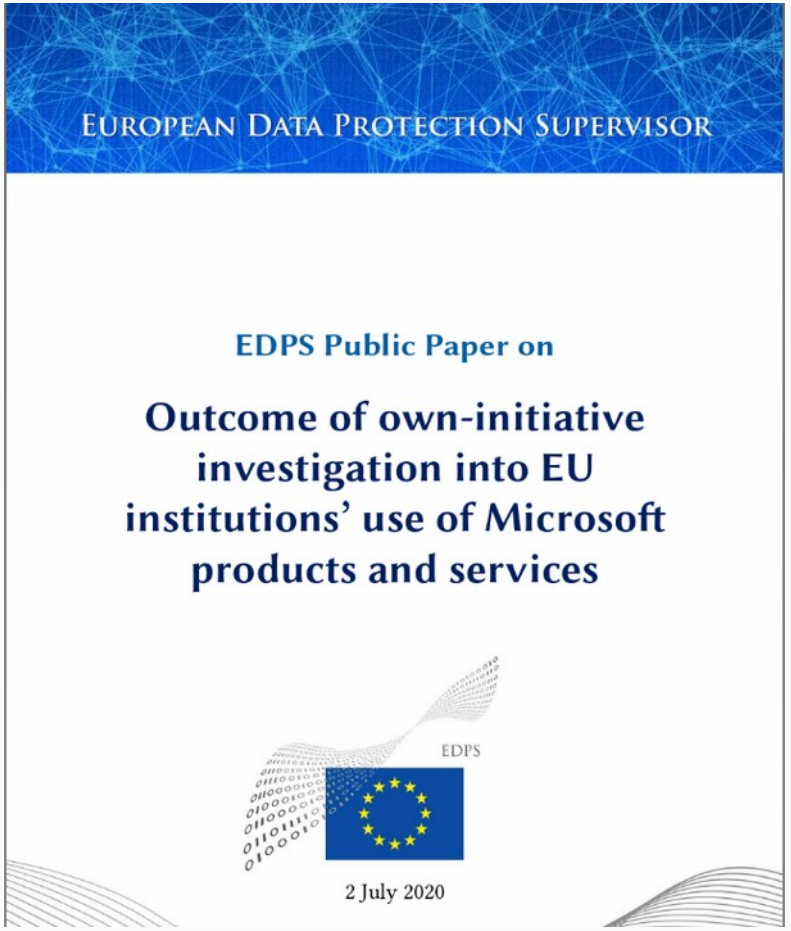
- There is no direct obligation to assess and use software alternatives.
- Though there are a number of indirect pointers:
  - Art 4(1)(c) on *data minimisation*
  - Art 26(1) on ‘taking into account [...] the risks of varying likelihood [...] the controller shall implement appropriate technical [...] measures [...] and be able to demonstrate that processing is [compliant]’
  - Art 27(1) on *data protection by design and by default* and *state of the art*
- A lack of digital sovereignty to negotiate appropriate safeguards from large-scale vendor presents a long-term risk that controllers must consider. (keywords: vendor lock-in, exit-strategy, business-continuity)

# EDPS on Assessing Software Alternatives

**Conclusion from EDPS investigation into EUI use of Microsoft products**

'The EDPS advises organisations not to consider engaging any processor (or sub-processor) that is not willing to provide sufficient guarantees to implement appropriate technical and organisational measures [...]. **To comply with the principle of data protection by design and by default, organisations should verify** both when processing is planned and during the processing, **if no other alternative software solutions allow for higher privacy safeguards**.' (para 140)

Link:
https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html#conclusion



# Court of Auditors on Assessing Software Alternatives

- 2007 Annual Report of German Federal Court of Auditors (p 233): Public administrations usually migrate to newer software versions within the same range of offers without consideration of alternative or open source software.
- March 2021: Mecklenburg-Vorpommern DPA and Court of Auditors in Germany demand from local government to act immediately and employ alternative software if data transfers in e.g. Microsoft products cannot be prevented. CoA spokesperson considers use of Microsoft products neither legally compliant nor economically viable.
- EDPS invited on a short notice the European Court of Auditors to this workshop, but their legal service could not accommodate the invitation; EDPS is open to consider synergies with the CoA on developing procurement best practices for large-scale cloud software providers

# Thank you! Questions?

# Used Images

- Illustrations from https://undraw.co (custom open source license):
  ‘text files’, ‘social ideas’, ‘questions’, ‘building websites’, ‘live collaboration’, ‘sorting thoughts’, ‘split testing’
- Pictures from https://unsplash.com (custom open source license)
  - Cliff https://unsplash.com/photos/l4MwmH8QIxk
- Fonts and Emojis
  - Fira Sans using the Open Font License (OFL)
  - FontAwesome 5 (Free) using the Open Font License (OFL)

# Backup

# Enforcement Today for Risks of Tomorrow 😟

# Cognative Bias and Future Forecast

- '**Present bias** is the tendency to rather settle for a smaller present reward than to wait for a larger future reward, in a trade-off situation' (wikipedia)
  - Profit from Office 365/teams now, deal with risks later
- '**Escalation of commitment** is a human behavior pattern in which an individual or group facing increasingly negative outcomes from a decision, action, or investment nevertheless continues the behavior instead of altering course.' (wikipedia)
- Slow acquisition of dependence feels less severe
- Analogy: climate change
- **Have law enforcement authorities the mandate to stop sleepwalkers before they reach the cliff?**

# Schrems-II and International Data Transfers

"We have asked **EU institutions and bodies to analyse the legality of data transfers to the US** and to act in accordance with the accountability principle. We will be providing them with some guidance on how conducting transfer impact assessments soon but it is clear that **the decision of whether or not a transfer should be continued, suspended or discontinued correspond to them**. To the extent that this would help, data controllers can **renegotiate their contracts** with their service providers or to find new ones that can ensure compliance with the law."

From the conference

CPDP 2021

Leonardo CERVERA NAVAS,
EDPS Director