

# Software Alternatives to Large-Scale Providers

Workshop #2

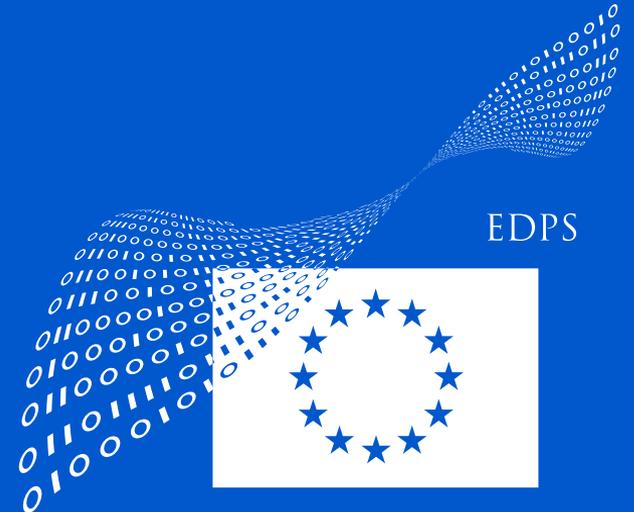
49<sup>th</sup> EDPS-DPO Meeting

June 4<sup>th</sup>, 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 RITSCHHEL ( <a href="#">Carl Duisberg Centren</a> , DPO)
50 min	Discussion 	

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

# EDPS IT Today

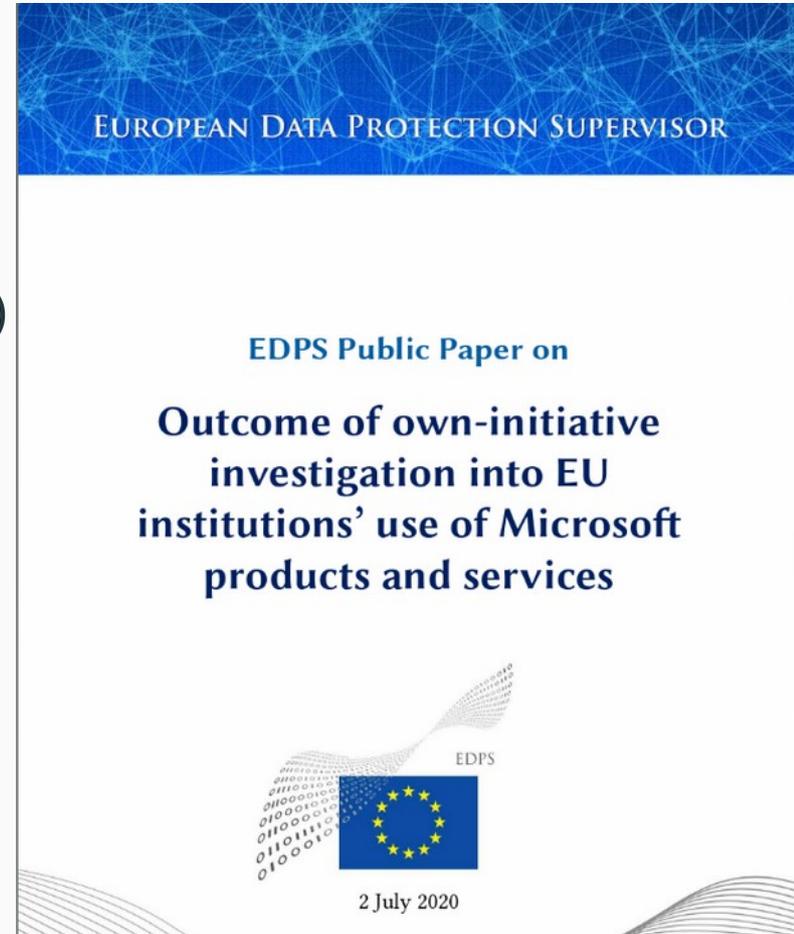


## Also the EDPS depends on software from large-scale providers

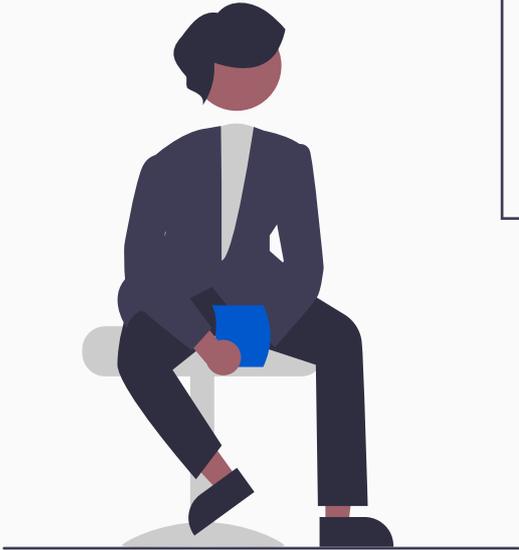
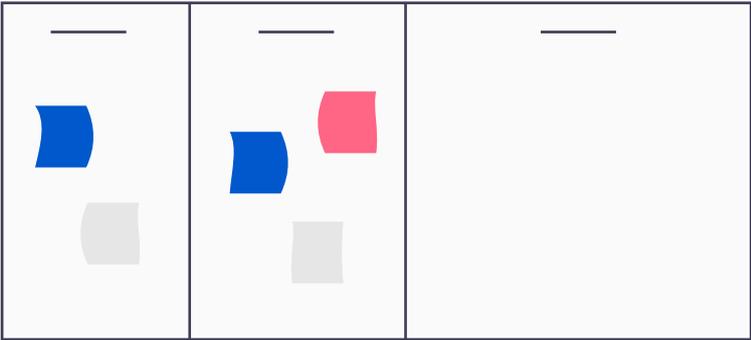
- Twitter 
- LinkedIn 
- Youtube 
- Microsoft Office 2016  (dominant use)
- Microsoft OneDrive/Sharepoint   
(early access via EP provided EDPS IT accounts/devices)

# 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



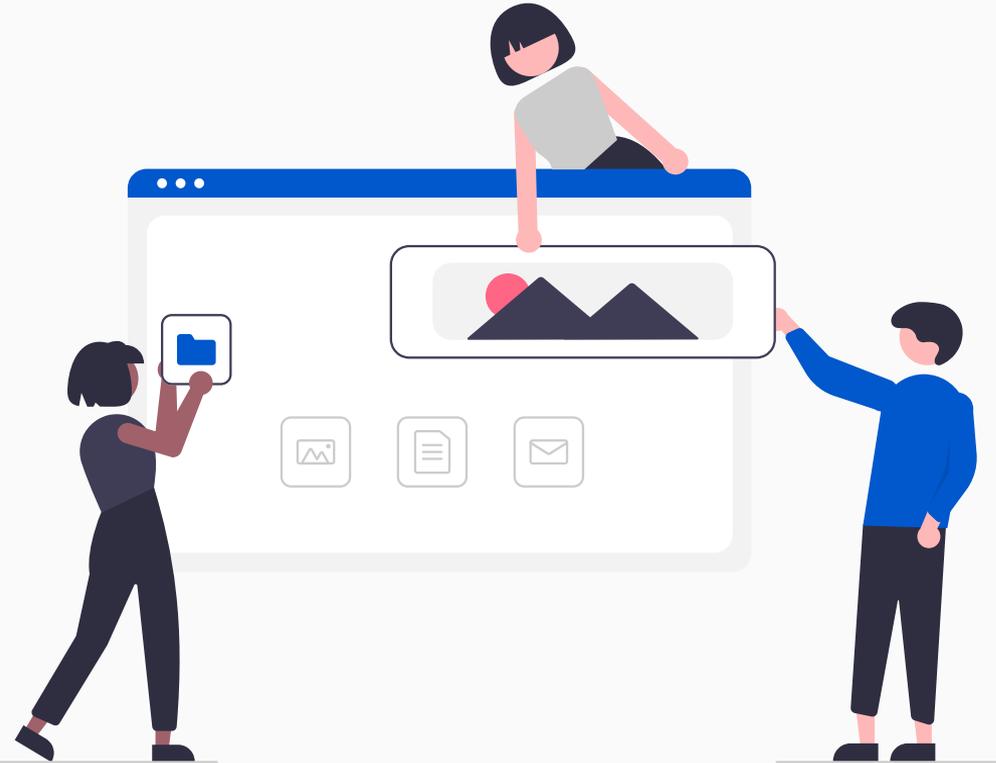
## EDPS Strategy for 2020-2024

“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 Initiatives

- 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<sup>th</sup> EDPS-DPO meeting)

# EDPS IT Tomorrow ?



- 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://chaos.social/@echo_pbreyer),  
<https://mastodon.social/@RegierungBW>,  
<https://bawue.social/explore>

## **Peertube** (Youtube)

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

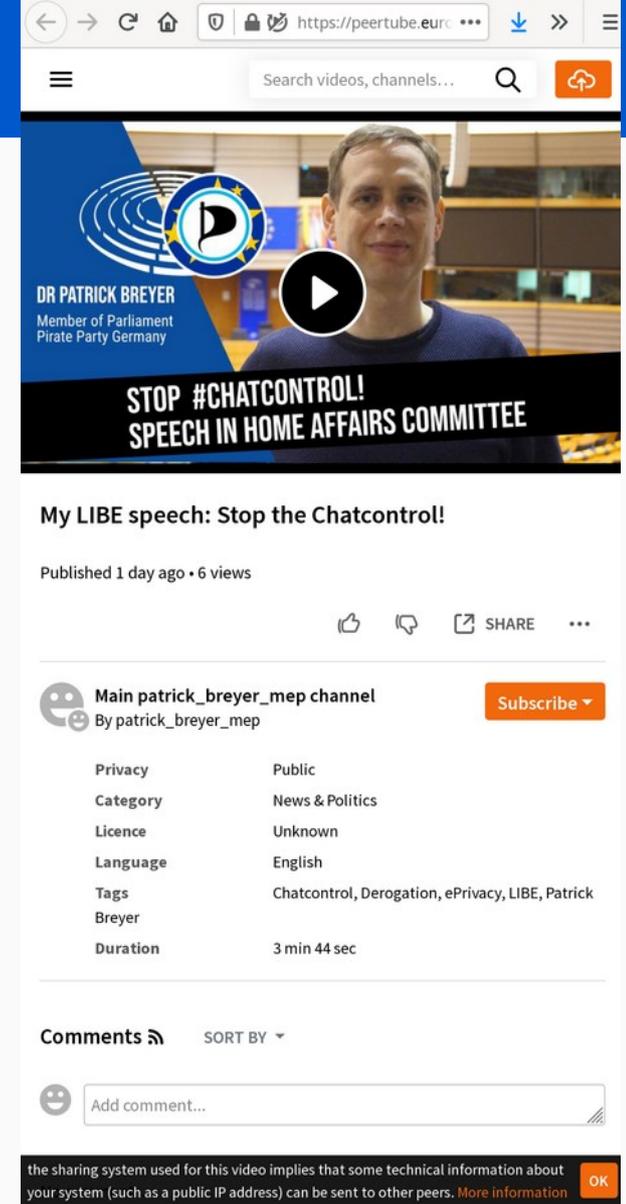
# Quick glimpse into Mastodon @m

- 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

The screenshot shows a Mastodon profile page for Patrick Breyer (@echo\_pbreyer@chaos.social). The profile header features a yellow background with a 'PIRATES' logo on the left and a portrait of Patrick Breyer on the right. Text on the right side of the header reads 'DR. PATRICK BREYER', 'DIGITAL EXPERTISE', and 'IN THE EUROPEAN PARLIAMENT'. Below the header, the profile statistics are displayed: 2.31K Toots, 17 Following, and 937 Followers. A 'Follow' button is visible on the right. The main content area shows a toot from Patrick Breyer, dated 13h, with the text: 'Erinnerung! Wir suchen neue Crewmitglieder! Du möchtest den Arbeitsalltag eines Europaabgeordneten kennenlernen? Du kennst dich mit Öffentlichkeitsarbeit und Social Media aus? Du sprichst fließend Englisch? Dann bewirb dich jetzt! patrick-breyer.de/?p=595320'. Below the toot is a recruitment poster for the 'EUROPEAN PIRATE PARTY' with the text: 'JOIN THE PIRATE CREW!', 'SUCHT: PRAKTIKAN/IN IM BEREICH PR & VERWALTUNG', 'TRAUM: APRIL - JULI 2021', 'WERBUNGSFRIST: 08. MÄRZ 2021', and 'BEWIRB DICH JETZT!'. The right sidebar contains a bio for Dr. Patrick Breyer, stating he is a digital freedom fighter and MEP for the European Pirate Party, with a link to his homepage (patrick-breyer.de) and a 'Joined May 2019' date. Below the bio is a Mastodon logo and a link to 'chaos.social - a Fediverse instance for & by the Chaos community'. At the bottom right, there is a 'TRENDING NOW' section for the hashtag #kde, with 13 people talking.

# 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?)



The screenshot shows a Peertube video player interface. At the top, there's a browser address bar with the URL 'https://peertube.eur...'. Below it is a search bar with the text 'Search videos, channels...'. The video player itself shows a video thumbnail with a play button. The video title is 'My LIBE speech: Stop the Chatcontrol!'. Below the title, it says 'Published 1 day ago • 6 views'. There are icons for like, comment, and share. The channel name is 'Main patrick\_breyer\_mep channel' with a 'Subscribe' button. Below the channel name, there's a table of video metadata:

Privacy	Public
Category	News & Politics
Licence	Unknown
Language	English
Tags	Chatcontrol, Derogation, ePrivacy, LIBE, Patrick Breyer
Duration	3 min 44 sec

At the bottom, there's a 'Comments' section with a 'SORT BY' dropdown and a text input field for adding a comment. A small disclaimer at the very bottom states: 'the sharing system used for this video implies that some technical information about your system (such as a public IP address) can be sent to other peers. More information'.

# 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

the most popular self-hosted collaboration solution for tens of millions of users  
at thousands of organizations across the globe



SIEMENS



DEGES



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

The screenshot displays a web browser window with the address `https://cloud.riemann.cc/apps/files/?dir=/tmp&fileid=284`. The main content area shows a document editor for a file named "letter-reference.odt". The document is a letter from Wojciech Rafał Wiewiórowski, Supervisor of the European Data Protection Supervisor, to Mr Roberto VIOLA, Director-General of DG CNECT, European Commission. The letter discusses the monitoring of COVID-19 spread and the need for a coordinated European approach to data protection.

The document content includes:

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI  
SUPERVISOR

Mr Roberto VIOLA  
Director-General  
DG CNECT  
European Commission

EDPS ref.	EDPS case	Date
<u>WRW/V.C/mj/D(2020)0724</u>	C2020-0337	04 May 2020

**Monitoring spread of COVID-19**

Dear Mr Viola,

Thank you for consulting the EDPS on the monitoring of the spread of the COVID-19 outbreak. It is indeed a matter of great urgency.

Firstly, let me underline that data protection rules' currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics. I am aware of the discussions taking place in some Member States with telecommunications providers with the objective of using such data to track the spread of the COVID-19 outbreak, and call in help from above. The prophet Brian.

I share and support your call for an urgent establishment of a coordinated European approach to handle the emergency in the most efficient, effective and compliant way possible. There is a clear need to act at the European level now.

On the basis of the information provided in your letter and in absence of a more specific data model, please find below some elements for your consideration:

The right sidebar shows the document's style and character settings, and a paragraph of text. The bottom sidebar shows the activity log for the document, listing several download events via public link and one sharing event.

Activity log for "letter-reference.odt":

- Downloaded via public link (a month ago)
- Downloaded via public link (a month ago)
- Downloaded via public link (a month ago)
- You changed letter-reference.odt (2 months ago)
- Shared as public link (2 months ago)
- Downloaded via public link (2 months ago)
- Downloaded via public link (4 months ago)

Page 1 of 3 | 845 words, 5,333 characters | Insert mode: inactive | Standard selection | English (UK)

## 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.	<p>Does your organisation have a personal data breach management process?</p> <p>If yes, please briefly describe it in the "Comment" field and provide us a copy of this procedure.</p>
1.10.	<p>Will the EDPS's data be separated from other clients (other instance on same machine/other virtual machine/other physical machine) and/or encrypted?</p> <p>If yes, please provide more details in the "Comment" field.</p>
1.11.	<p>Does your organisation offer automatic data/document deletion after a certain period?</p> <p>If yes, please provide more details in the "Comment" field.</p>
1.12.	<p>Can data be destroyed in a secure way after the retention period was reached and/or when the contract ends?</p> <p>If yes, please provide more details in the "Comment" field.</p>
1.13.	<p>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?</p> <p>If yes, please provide more details in the "Comment" field.</p>

## 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)

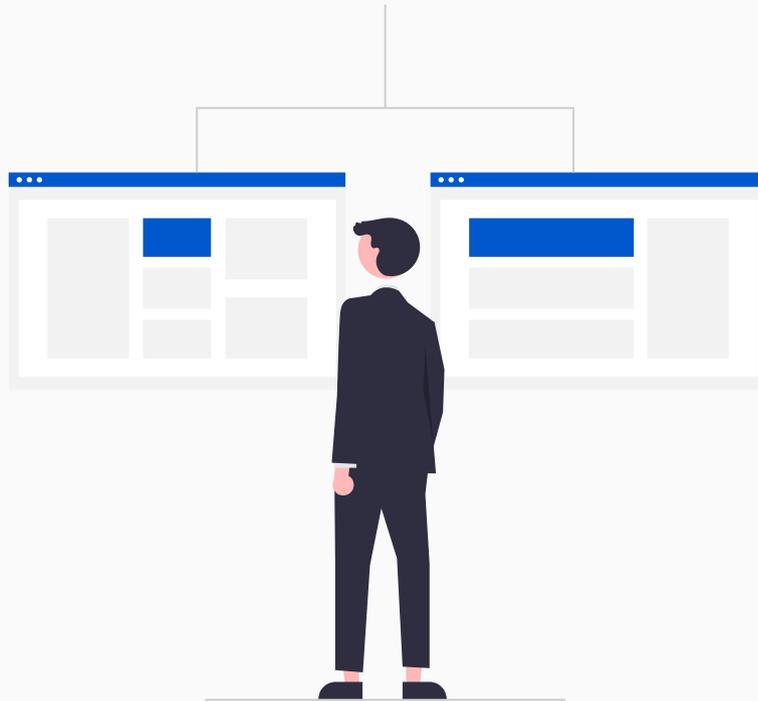
## Risk Management

- 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

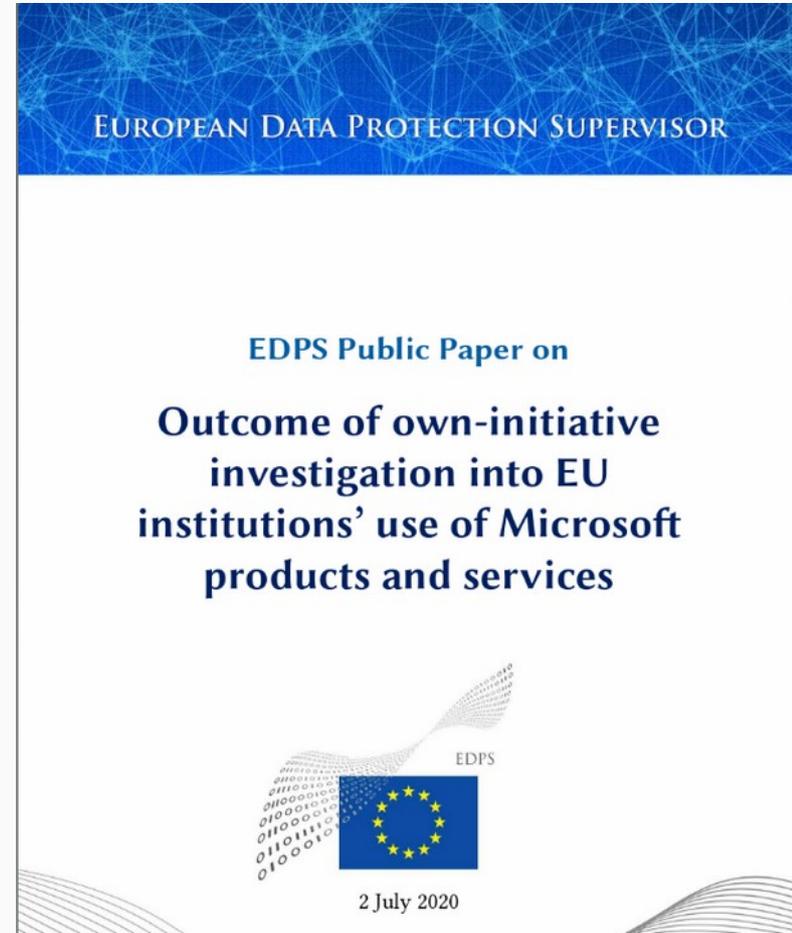
- There is no direct obligation to assess and use software alternatives.
- Though there are a number of indirect pointers:
  - Art 4(1)(c) on *data minimisation*
  - Art 26(1) on ‘taking into account [...] the risks of varying likelihood [...] the controller shall implement appropriate technical [...] 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)

## 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:

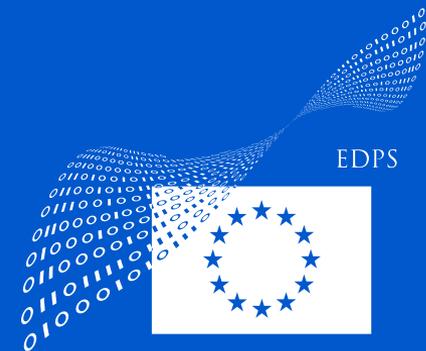
[https://edps.europa.eu/sites/edp/files/publication/20-07-02\\_edps\\_euis\\_microsoft\\_contract\\_investigation\\_en.html#conclusion](https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html#conclusion)



# 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/l4MwmH8QlXk>
- Fonts and Emojis
  - Fira Sans using the [Open Font License \(OFL\)](#)
  - FontAwesome 5 (Free) using the [Open Font License \(OFL\)](#)

# Backup

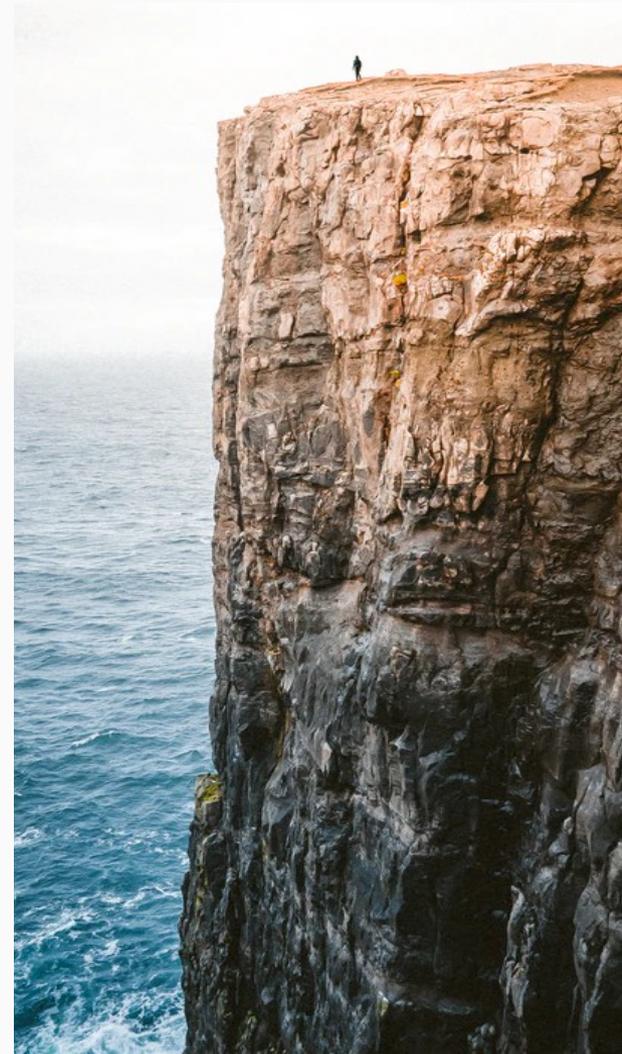


# Enforcement Today for Risks of Tomorrow 🙄



# Cognitive 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?**



“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