



CryptPad

Recent Advances in Privacy and Collaboration

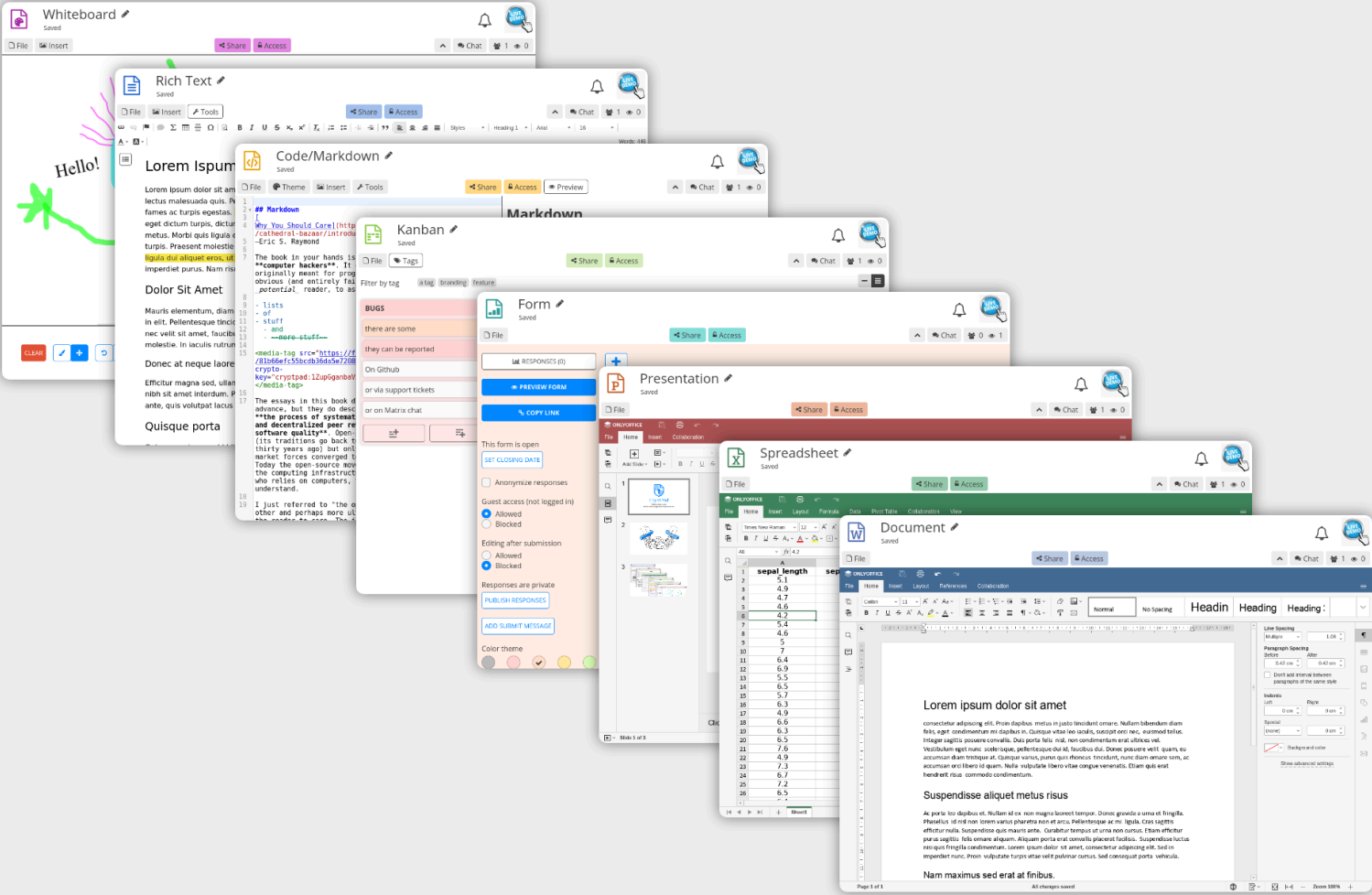
Fabrice Mouhartem

February 1st, 2025

@FOSDEM 2025

Introduction

CryptPad



What is CryptPad?

- **Online collaborative office suite**

What is CryptPad?

- **Online collaborative office suite**
- End-to-end encrypted real-time collaboration
- Born at XWiki 10 years ago 🎂

What is CryptPad?

- **Online collaborative office suite**
- End-to-end encrypted real-time collaboration
- Born at XWiki 10 years ago 🎂
- Free and Open-Source Software (AGPLv3)
- Project website:
 - <https://cryptpad.org/>
- Flagship instance:
 - <https://cryptpad.fr/>



The screenshot shows the Noyb website header with navigation links: News, Our work, Exercise your rights!, Support us!, About us, and GDPRhub. The article title is "Microsoft violates children's privacy - but blames your local school". The byline is "Data Subject Rights / 04 June 2024". The text discusses how schools in the EU have implemented digital services, but big tech companies like Microsoft have violated children's data protection rights by blaming schools as the "controller" for their data.

noyb

News Our work Exercise your rights! Support us! About us GDPRhub

Home > News >

Microsoft violates children's privacy - but blames your local school

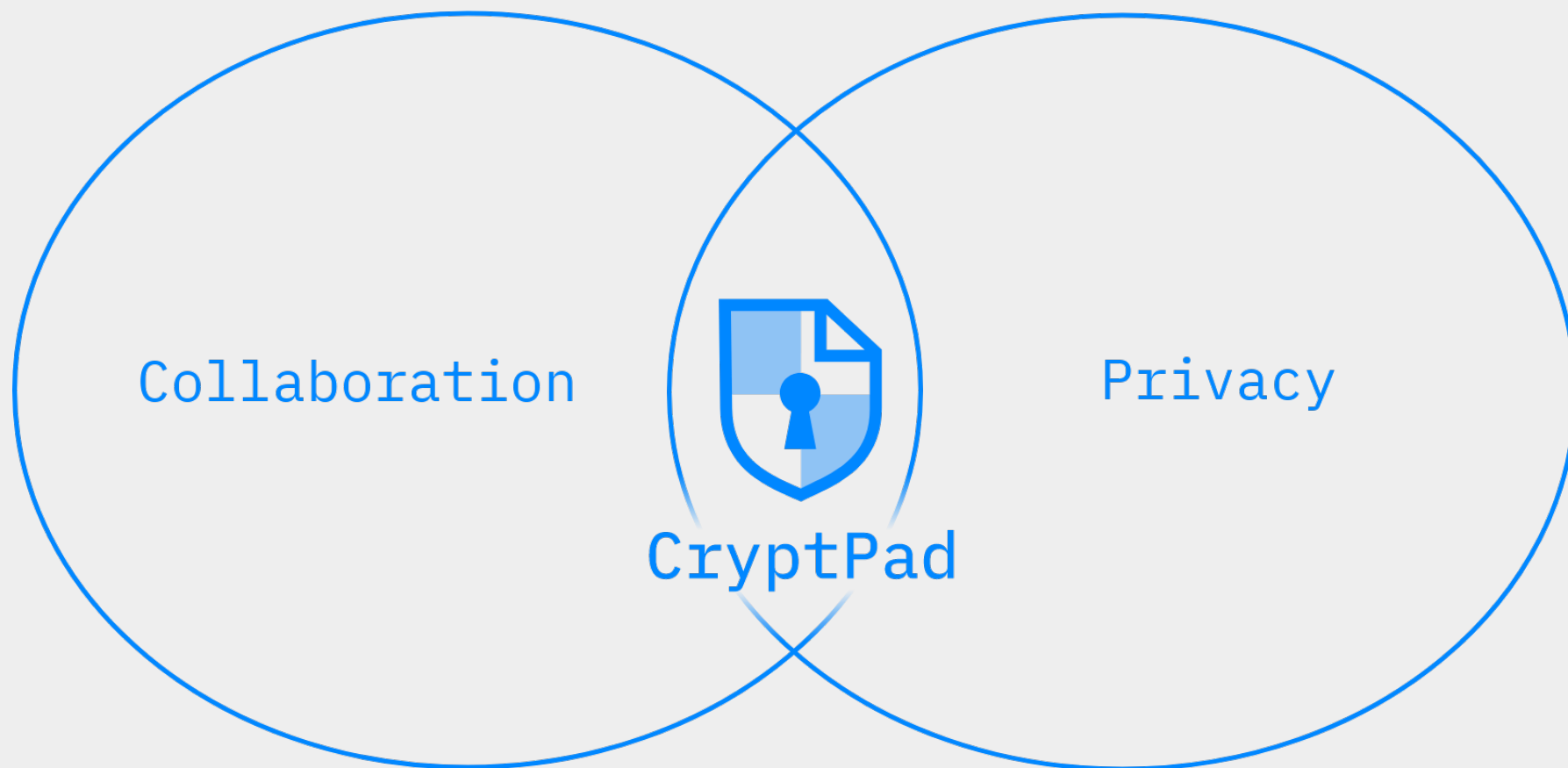
Data Subject Rights / 04 June 2024

In the wake of the pandemic, schools in the European Union have increasingly begun to implement digital services for online learning. While these modernisation efforts are a welcome development, a small number of big tech companies immediately tried to dominate the space - often with the intention of getting children used to their systems and creating a new generation of future "loyal" customers. One of them is Microsoft, whose 365 Education services violate children's data protection rights. When pupils wanted to exercise their GDPR rights, Microsoft said schools were the "controller" for their data. However, the schools have no control over the systems.



<https://noyb.eu/en/microsoft-violates-childrens-privacy-blames-your-local-school>

You can have both



Yes, you can have both

CryptPad development

- Development and issue management on **GitHub**
- Lead by the CryptPad Team

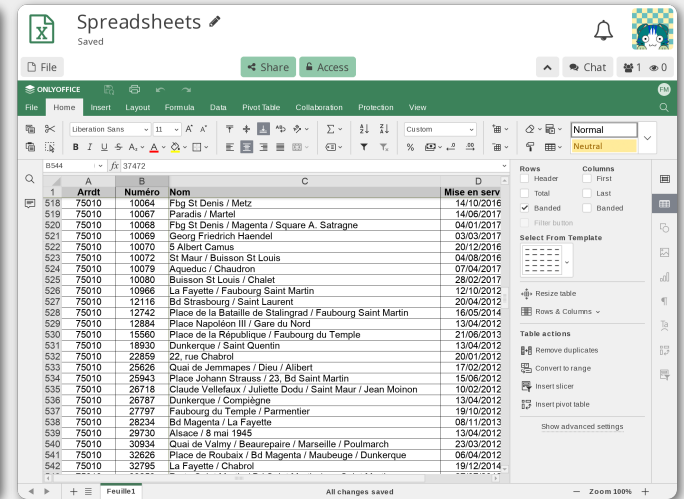
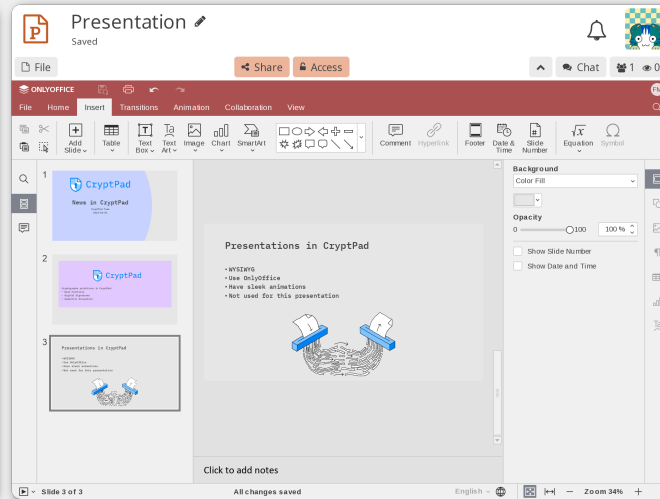
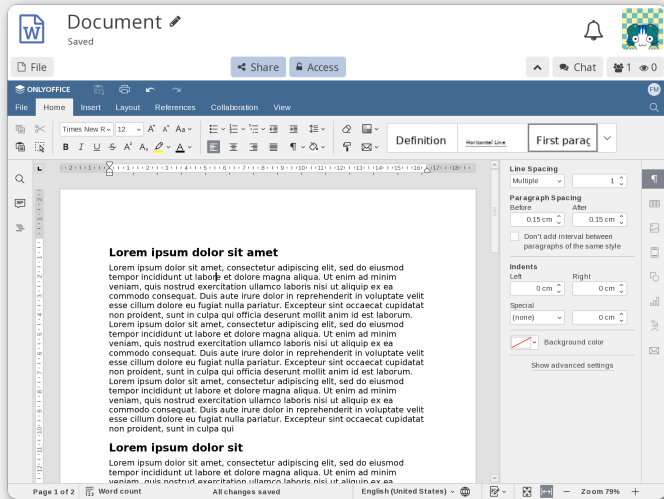
CryptPad development

- Development and issue management on **GitHub**
- Lead by the CryptPad Team
- Quaterly releases
 - Move to calendar versioning in 2024
 - YYYY.MM.minor

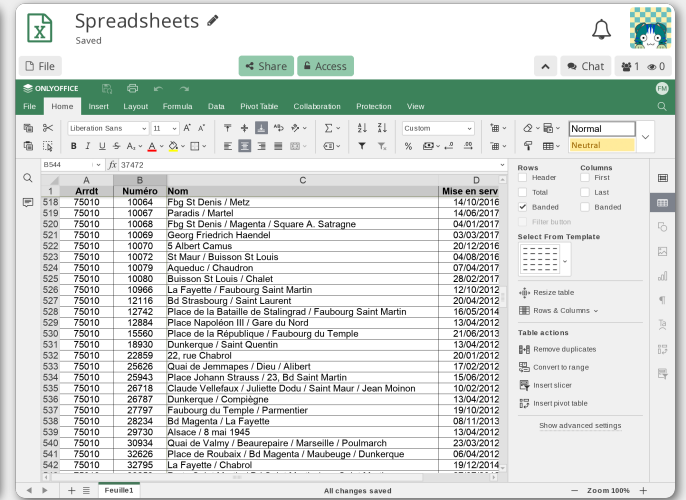
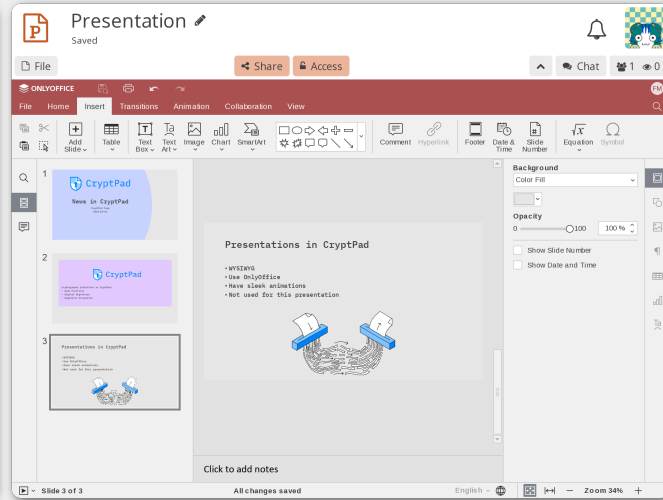
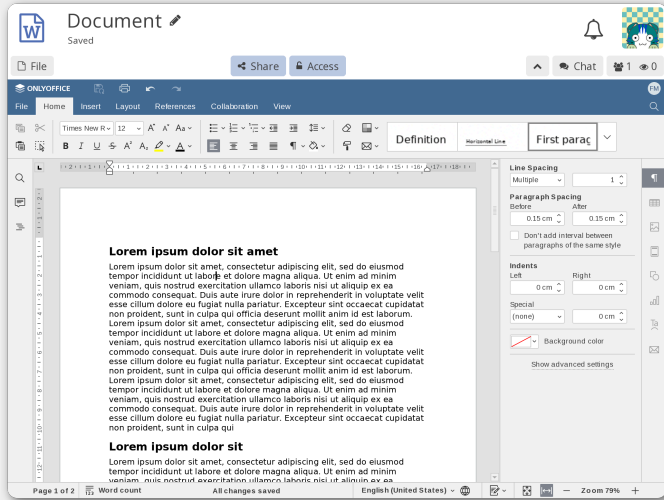
CryptPad development

- Development and issue management on **GitHub**
- Lead by the CryptPad Team
- Quaterly releases
 - Move to calendar versioning in 2024
 - YYYY.MM.minor
- Support
 - Internal support system
 - GitHub issues
 - Community forum
 - Matrix space

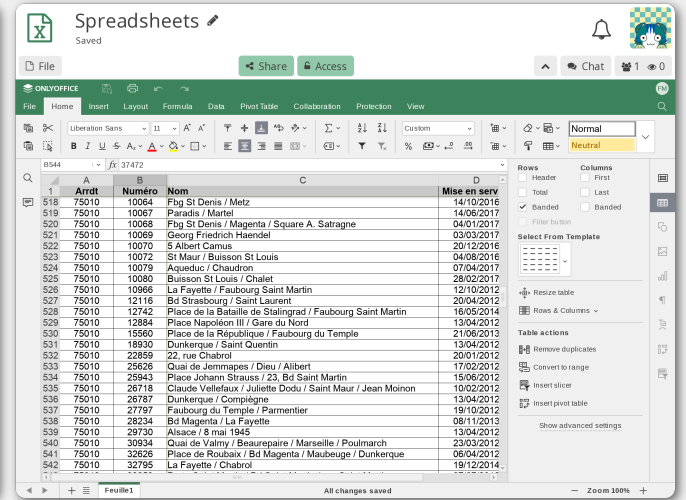
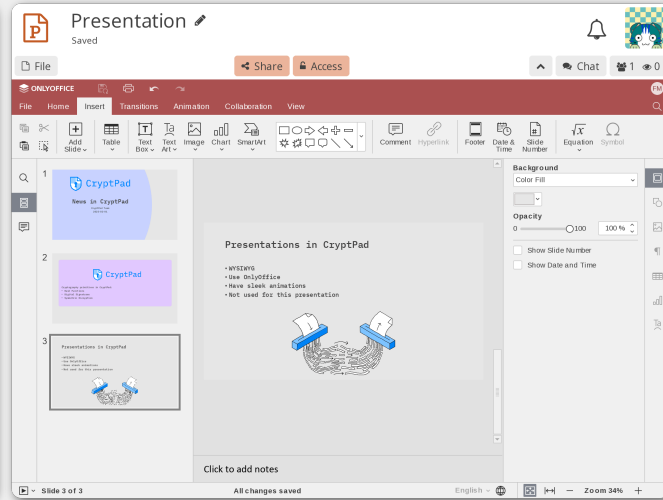
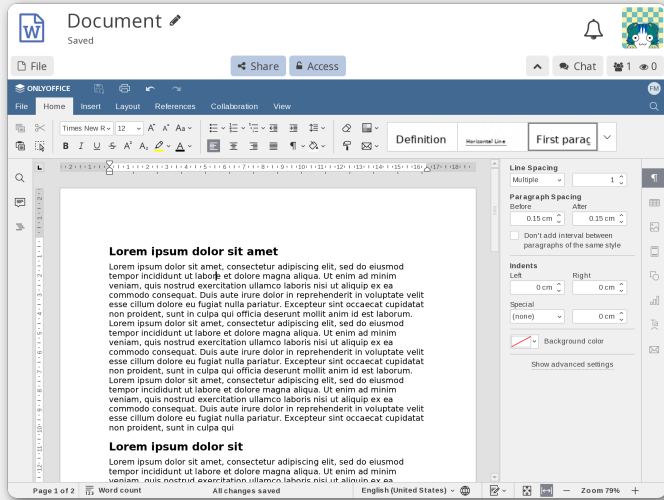
CryptPad changes in 2024



- Apps for most Office tasks
 - Spreadsheets
 - WYSIWYG word processor
 - Presentations



- Apps for most Office tasks
 - Spreadsheets
 - WYSIWYG word processor
 - Presentations
- News in 2024
 - Improved stability



- Apps for most Office tasks
 - Spreadsheets
 - WYSIWYG word processor
 - Presentations
- News in 2024
 - Improved stability
- Next steps
 - Upgrade to OnlyOffice v8



Track progress

- *Web Content Accessibility Guidelines* (WCAG) 2.1 AA compliance




Track progress

- *Web Content Accessibility Guidelines (WCAG) 2.1 AA compliance*


Current focuses

- Keyboard Navigation
- Focus Indicators
- Responsive Design

Quickscans

- Accessibility scans done in August 2024 by 
- Target: WCAG 2.2 AA for apps and drive

Quickscans

- Accessibility scans done in August 2024 by 
- Target: WCAG 2.2 AA for apps and drive
- Issues in the report are labelled in GitHub

Summary on CryptPad's apps audit

The suite is quite accessible already. In some parts it is obvious that effort has been put into making the apps accessible. There is also some room for improvement. Most of the issues come down to insufficient contrast, lack of labeling and parts that are still unreachable by keyboard.



Track progress

Goal

Enhancing UI responsiveness for an improved mobile experience

- All elements are easily accessible and visible
- Optimized scaling of interactive elements for mobile devices
 - E.g., tables, menus, forms, ...

Sodium plugin



- <https://github.com/crytpad/crytpad-sodium-plugin>
- Easily replace crypto library for performance reasons
- Legacy TweetNaCl.js kept for simplicity on small instances

Sodium plugin



- <https://github.com/crytpad/crytpad-sodium-plugin>
- Easily replace crypto library for performance reasons
- Legacy TweetNaCl.js kept for simplicity on small instances
- Tutorial blogpost
 - <https://blog.crytpad.org/2024/10/03/tutorial-sodium-plugin/>

Monitoring plugin



- <https://github.com/cryptpad/cryptpad-monitoring-plugin>
- Monitoring usage data for Prometheus/Grafana

SSO plugin



- <https://github.com/cryptpad/sso>
- Allow the use of single-sign-on (SSO) systems (one or more)
 - OIDC
 - SAML
- Important for organization
- SSO login restriction

Scalable Server prototype



- <https://github.com/crytpad/scalable-server>
- Distributed CryptPad server
- Independent prototype
- Exploratory phase
 - Encouraging results

End-to-End tests

✓ pad_anon.spec.js	
✗ pad - export (.doc)	3.5m
pad_anon.spec.js:220	
✗ pad - export (md)	3.5m
pad_anon.spec.js:259	
✓ pad - comment	10.9s
pad_anon.spec.js:27	
✓ pad - create and open snapshot	30.2s
pad_anon.spec.js:49	
✓ pad - history (previous version)	10.9s
pad_anon.spec.js:90	
✓ pad - toggle tools	10.5s
pad_anon.spec.js:107	
✓ pad - import file	23.7s
pad_anon.spec.js:130	
✓ pad - make a copy	20.8s
pad_anon.spec.js:154	
✓ pad - export (html)	11.1s
pad_anon.spec.js:181	
✓ pad - share at a moment in history	34.8s
pad_anon.spec.js:292	
✓ drive_anon.spec.js	
✗ drive - anon - user menu - donate	3.5m
drive_anon.spec.js:20	
✓ drive - anon - user menu - settings	7.9s

End-to-End tests

- <https://github.com/cryptpad/e2e-test-suite>
- Use of Playwright for automated testing locally
 - Integration with Browserstack for more plateforms
 - @axe-core framework for accessibility testing
- ≈300 tests to check for breaking changes before release

End-to-End tests

- <https://github.com/cryptpad/e2e-test-suite>
- Use of Playwright for automated testing locally
 - Integration with Browserstack for more platforms
 - @axe-core framework for accessibility testing
- ≈ 300 tests to check for breaking changes before release
- Some bugs were discovered via automated testing
- On our side:
 - Dedicated test instance for releases

- Client-side API
 - To integrate a CryptPad instance into external platforms

Goal:

Use CryptPad as an E2EE editor without data persistence

CryptPad.fr

- We faced low QoS issues at the beginning of 2024...

- We faced low QoS issues at the beginning of 2024...
- CryptPad.fr resources
 - More RAM and CPU allocated to backend

- We faced low QoS issues at the beginning of 2024...
- CryptPad.fr resources
 - More RAM and CPU allocated to backend
- ZFS Migration
 - Full database migrated to a new machine, replacing BTRFS
 - Data access is much faster



Try CryptPad Cloud

Test drive your own instance of CryptPad. Keep it with a subscription plan if it fits your needs

Your CryptPad Cloud URL

`https:// demonname .cryptpad.cloud`

Please share some information to understand your needs and keep in touch:

First name

Crypt

Last name

Pad

- Cloud Demo & Paid Instances
 - Explore CryptPad Cloud Features
 - Use the form¹ on our website to create a demo instance
 - Customize Your Own Instance
 - Integrated with instance onboarding for a seamless setup
 - CryptPad Cloud Instance Management
 - Manage your own instance with help of our support team

¹<https://cryptpad.org/try-cloud/>

Usage statistics

Data	2023	2024	Δ
Monthly Registrations	5,000	6,505	+30%
Monthly Pad Activity	814,369	1,001,535	+23%
Monthly Unique IP addresses	178,442	213,438	+20%

Usage statistics

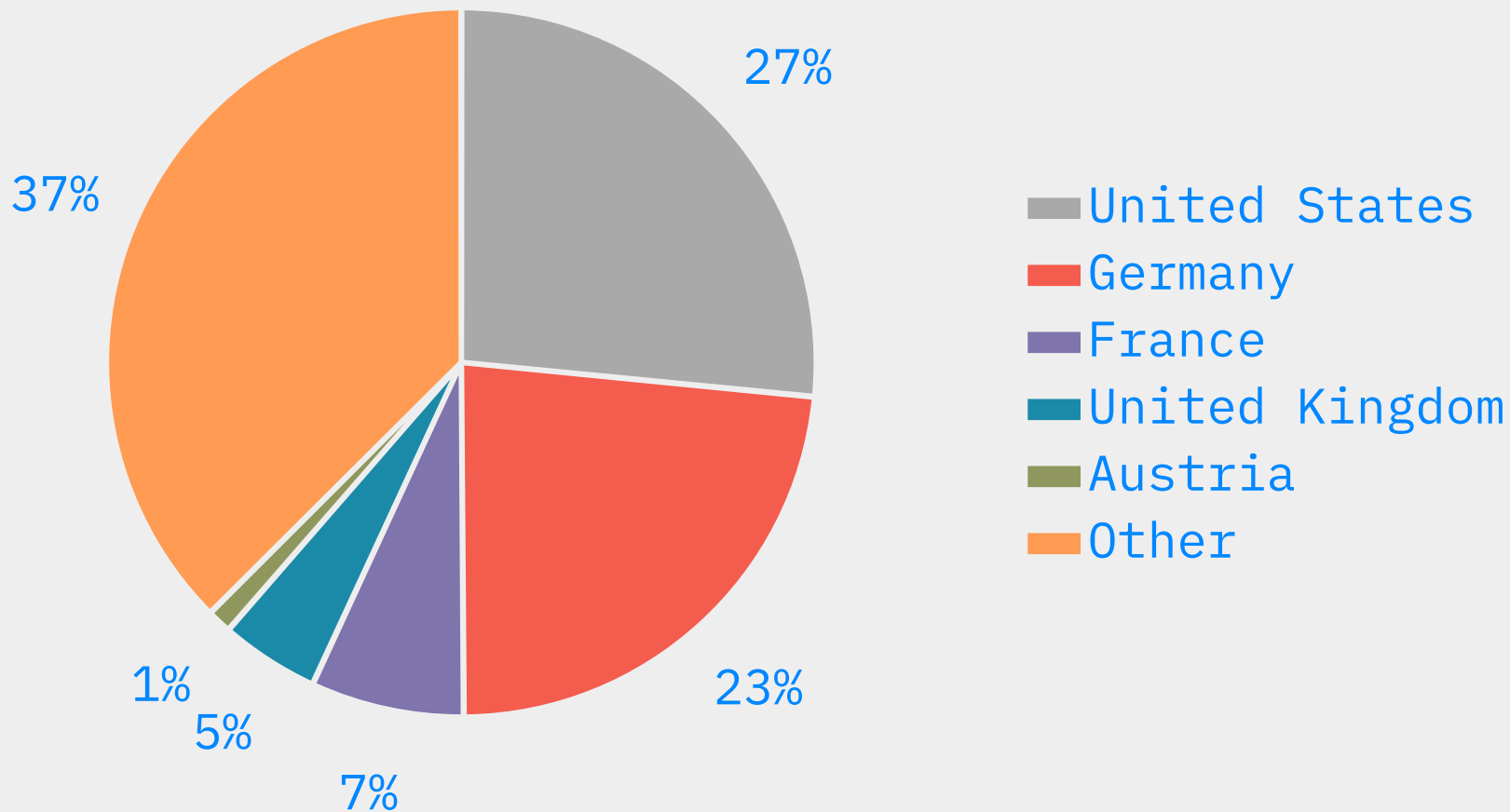


Figure 1: 2024 total usage per country



- Transparent management:
 - ▶ <https://blog.cryptpad.org/2025/01/28/CryptPad-Funding-Status-January-2025/>



- Transparent management:
 - <https://blog.cryptpad.org/2025/01/28/CryptPad-Funding-Status-January-2025/>
- Medium term financing with research projects



- Transparent management:
 - <https://blog.cryptpad.org/2025/01/28/CryptPad-Funding-Status-January-2025/>
- Medium term financing with research projects
- Sustainability is not achieved yet
 - Individual subscriptions: $\approx 1,000$
- Need for more independent revenue stream



open collective



Conclusion

Conclusion

- CryptPad project:
 - Progress on multiple fronts
 - Both UX/UI and backend improvements
 - New plugins for the CryptPad ecosystem
- CryptPad product:
 - Growth for CryptPad.fr
 - CryptPad Cloud ☁



Roadmap

- Works on post-quantum integration this summer
- Continue the effort on accessibility and mobile usage
- Focus on quality of life improvements and feature requests
- Replacement of CKEditor4 for Richtext edition
- OnlyOffice upgrade



CryptPad

- David – CryptPad Team Lead
- Andreea – Junior Developer
- Daria – Junior Developer
- Diana – Junior Developer
- Fabrice – R&D Engineer
- Mathilde – Deployment Engineer,
Community & Support
- Wolfgang – R&D Engineer
- Yann – Privacy Engineer
- Zuzanna – Software Dev Engineer
- Ludovic – XWiki CEO

Thank you for your attention



Question time

Stay in touch:

- Blog: <https://blog.cryptpad.org/>
- Mastodon: <https://fosstodon.org/@cryptpad>
- Community forum: <https://forum.cryptpad.org/>
- FOSDEM: **K1-B-3** stand