



Safeguarding Your Digital Life

Personal Data & Device Protection in the AI Era

Dr Tymoteusz Miller

University of Szczecin

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development





The AI Revolution: A Double-Edged Sword

Unprecedented Convenience

AI is deeply embedded in daily life — offering personalisation, automation, and efficiency at every turn.

Significant New Risks

That same integration introduces serious vulnerabilities to personal data and device security.

Every Interaction Counts

From chatbots to smart devices, each AI interaction can potentially expose sensitive information.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

The Growing Threat Landscape



Data Leakage

Sensitive PII and PHI can be inadvertently shared with AI services during routine interactions.

Profile Building

AI providers log user data over time, creating detailed profiles that can be exploited or sold.

Prompt Injection

Malicious actors manipulate AI systems to extract sensitive information from unsuspecting users.

Training Data Risks

Personal data used in AI training sets can cause compliance failures and biased model outputs.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

Real-World Risks: When Data Leaves Your Device

73%

Risk Unaware

of employees admit to pasting sensitive data into AI chatbots without realising the risk.

→ Health Data Exposure

A user asking an AI about medical conditions — "I have type 2 diabetes..." — inadvertently shares protected health information.

→ Financial Details at Risk

Pasting credit card numbers or financial records into AI prompts can lead to direct exposure of sensitive account data.

→ Compromised API Keys

Sharing API keys for debugging purposes can result in full account compromise and unauthorised system access.

❏ All examples sourced from PiiBlock research into real-world AI prompt data leakage incidents.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

The Solution: Privacy-First AI



On-Device Processing

Keeping data and AI models local to your device ensures sensitive information never leaves your control.



Real-Time Anonymisation

Tools that detect and mask sensitive data *before* it is sent to AI services, preserving privacy by default.



Privacy Proxies

Middleware that scrubs PII from prompts, ensuring your identity is never exposed to AI providers.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

Innovative Solutions in Action

Sinaptic.AI

Browser extensions providing real-time PII detection and network interception, with all data processed entirely on-device.

Umbrai

An on-device AI privacy app that anonymises sensitive data and ensures full GDPR compliance for EU businesses.

PiiBlock / PrivacyShield

A free, open-source browser extension that masks personal data before it reaches AI chatbots — zero server-side processing.



Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

Decentralised & Self-Sovereign AI

Vora Aegis

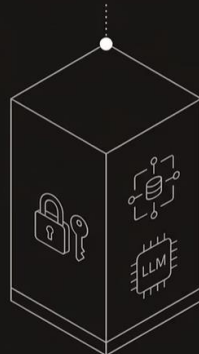
Self-hosted solution prioritizing offline secrets and a security-first approach.



Self-hosted solution prioritizing offline secrets and a security-first approach.

PIN AI

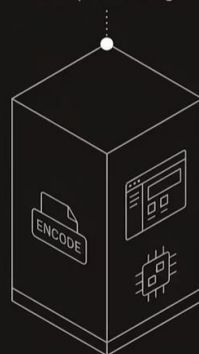
Utilizes cryptographic security, off-chain computation, and on-device LLMs.



Utilizes cryptographic security, off-chain computation, and on-device LLMs.

Thinkspan

An end-to-end encrypted personal command centre with on-device data processing.



An end-to-end encrypted personal command centre with on-device data processing.

A new generation of tools is placing AI control firmly back in the hands of the individual — removing reliance on centralised cloud providers entirely.

- **Vora Aegis:** Self-hosted AI with a security-first approach, keeping all secrets offline.
- **PIN AI:** Combines cryptographic security with private off-chain computation and on-device language models.
- **Thinkspan:** An end-to-end encrypted super app powering a private AI assistant with fully local data processing.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

Key Features of Modern Data Protection Tools



Local Processing

All sensitive data analysis occurs directly on the user's device — no cloud upload required.



Real-Time Detection & Masking

Instant identification and anonymisation of PII and PHI before any data is transmitted.



Visual Feedback

Sensitive data is highlighted in-context, actively educating users about what they are sharing.



Custom Rules & Control

Users can define their own exclusions, whitelist services, and manage data access granularly.



Compliance & Audit Trails

Built-in support for GDPR and other regulatory frameworks, with full logging for accountability.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development



THE ROAD AHEAD

The Future is Private

The landscape is shifting decisively towards user-controlled, private AI interactions. Centralised data harvesting is no longer an inevitable trade-off.

On-device processing and robust anonymisation are the twin pillars of **digital sovereignty** — enabling individuals and organisations to harness the full power of AI without surrendering their personal data.

- ❑ Adopting privacy-first tools is not a compromise on capability — it is an upgrade in control.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development



Take Control of Your Digital Footprint

01

Explore Privacy Tools

Investigate privacy-enhancing browser extensions such as PiiBlock and Sinaptic.AI.

02

Choose Private-by-Design AI

Prioritise AI services that offer on-device processing or robust, verifiable data protection policies.

03

Stay Informed

Continuously update your knowledge of AI privacy risks, emerging threats, and best practices.

Your data is your own. Protect it.

Erasmus+ Cooperation partnerships in higher education, 2024-1-PL01-KA220-HED-000250324, WP3. Skills and competencies development

