



# **Management of Entrustable Professional Activities for Medical Training at UA**

## **APSEI - WORK 4**

**Tomás Brás - 112665**

**Carolina Silva - 113475**

**Afonso Ferreira - 113480**

**Ricardo Antunes - 115243**

**Carlos Soto - 123551**



# Table Of Contents

**01** Context

**02** Commercial Ecosystem

**03** Property and Patent

**04** Open Source Software

**05** Cybersecurity

**06** How to recover from an attack

**07** Privacy Protection

**08** Ethical Aspects

**09** Artificial Intelligence

**10** Hyperscalers

**11** Network Effect



# 1. CONTEXT

PAÍS

## Universidade de Aveiro vai abrir curso de Medicina

A atual proposta envolve ensino na UA e orientação tutorial clínica em três Unidades Locais de Saúde, designadamente a ULS Região de Aveiro, a ULS Entre-Douro-e-Vouga e a ULS Gaia/Espinho, no âmbito do Centro Académico Clínico Egas Moniz Health Alliance.

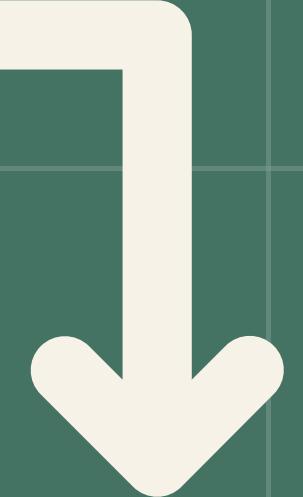
New Medicine course at UA



Constant evolution  
of students



Evaluation on paper



**EVALMED**  
Integrated digital  
system for managing  
Etrustable Professional  
Activities (EPA)



## PROBLEM

- Too much information on a single sheet of paper
- Difficult organization between student and tutor
- Lack of feedback and statistics

# 2. Commercial Ecosystem



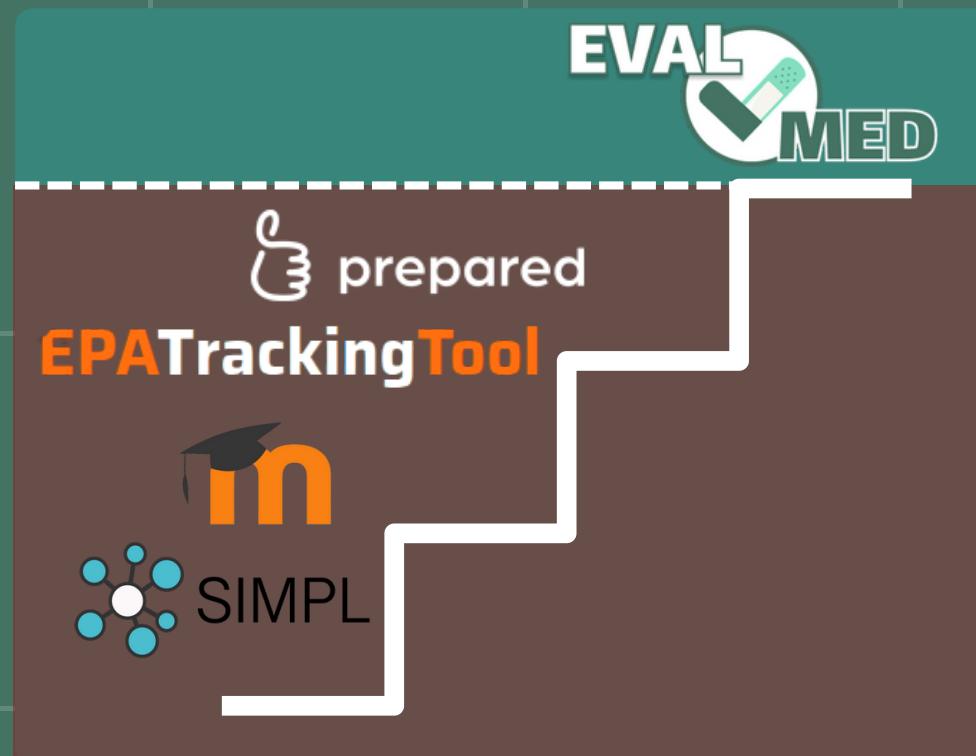
## Ed Tech Ecosystem

Software License  
**agreements** with other  
educational institutions



## Infrastructure

- Software currently hosted on a IEETA VM
- Move to cloud infrastructure (Google Cloud)



## Competitive Differentiators

- Yearly editions
- Send feedback
- Push notifications



## Scalability & Growth

- Economy of scale
- Reusable codebase
- Network effects

### 3. Intellectual Property & Registered Brand Aspects

Intellectual Property protects the assets that differentiate EvalMed from other similar products



Protecting these assets makes the product more impactful in a large scale

**Trade Name**

**EVALMED**

**Logo & Visual Identity**



**UX Design**



**Source code**

EPA / EvalMed / [Edit](#)

Marshmallow1119 Merge branch 'develop' into bug/frontend/improvements\_frontend\_all

Name

- ..
- backend
- frontend
- mongo-init
- uploads/profile-images

# Investigation of Current Patents

## Espacenet

The screenshot shows the Espacenet patent search interface. The top navigation bar includes the logo, a search bar labeled "Entrustable Professional Activities", and various search filters like "Advanced search", "Filters", and "Popup tips". The main content area displays 9 results found, with each result listing a patent number, publication date, assignee, earliest priority date, earliest publication date, and a brief abstract. The abstracts mention "professional activities" and "professional".

9 results found

Result	Patent Number	Publication Date	Assignee	Earliest Priority Date	Earliest Publication Date	Abstract Excerpt
1.	CN109978402A	2019-07-05	AFFILIATED RUIJIN HOSPITAL NORTH CAMPUS SHANGHAI JIAOTONG UNI...	2019-04-04	2019-07-05	... the following beneficial effects that the evaluation requirements of theories and practices are met by using trusted professional activities (EPAs); the work-based assessment should be concentrated on the trusted professional activities (EPA) and the general capabilities, on one hand... clinically, has good adhesion with clinical practice activities, and has very strong evaluation capability ...
2.	US2024249831A1	2024-07-25	FIREFLY LAB LLC [US]	2021-10-08	2023-04-13	... utilize performance evaluations obtained from evaluator healthcare professionals for a target healthcare professional and matched peer group, and can be...
3.	US11145407B1	2021-10-12	FIREFLY LAB LLC [US]	2019-04-22	2021-10-12	... or optimizing performance tracking of a medical professional.
4.	CN113887998A (B)	2022-01-04	GUANGZHOU XIANGSHI ENG CONSULTATION CO LTD	2021-10-18	2022-01-04	The invention relates to a project cost consultation intelligent work order management method, system and equipment and storage medium, and the method comprises the steps of: dividing a cost consultation service into a plurality of project work orders when a splitting

# Investigation of Current Patents

USPTO

An official website of the United States government [Here's how you know](#)

**uspto**

Search www.uspto.gov

Home Help

www.uspto.gov Entrustable Professional Activities Search

Narrow your search results

Reset all

Include results from:

Web pages  
 Documents

Apply

Show only content from these topics:

Patents guidance  
 Trademarks guidance

[View more](#)

Viewing 1-15 of 62 results

**Living with intention**

<https://www.uspto.gov/learning-and-resources/journeys-innovation/field-stories/living-intention>

... courtesy of Duane Sander) Like Kurtenbach, Sander struggled to find time for sports and other activities outside the farm, where caring for animals and crops was a team effort 24 hours a day, seven days a week. His opportunity to play football would need to wait until high school. For Kurtenbach, 1951...

**Microsoft PowerPoint - Slides NO NOTES for Advanced Patent Law Institute 2017**

[https://www.uspto.gov/sites/default/files/documents/Advanced\\_Patent\\_Law\\_Institute\\_2017\\_Slides.pdf](https://www.uspto.gov/sites/default/files/documents/Advanced_Patent_Law_Institute_2017_Slides.pdf)

... 37 C.F.R. § 11.18(c)(1). - Order noted that behavior was outside of the ordinary standard of professional obligation and client's interests. - Aggravating factor: has not accepted responsibility or shown remorse for remarks. - Suspended from practice before USPTO for 6 months. 18 Dishonesty, Fraud, ...

**a guide to protecting and enforcing IP rights in China**

[https://www.uspto.gov/sites/default/files/documents/China\\_IPToolkit\\_FINAL.pdf](https://www.uspto.gov/sites/default/files/documents/China_IPToolkit_FINAL.pdf)

a guide to protecting and enforcing IP rights in China

**Comments Related Electronic Submission of Applications for**

<https://www.uspto.gov/patents/laws/comments-public/comments-related-electronic-submission-applications>

...and with the exception of extremely inactive art, the PTO should ensure that classified files in active arts remain available to the public. At a minimum, paper files, corresponding to those removed from the Examiners' search areas, should remain available to users of the Public Search Room. Although...

**FY 2022 AGENCY FINANCIAL REPORT**

[https://www.uspto.gov/sites/default/files/documents/USPTO FY22AFR.pdf](https://www.uspto.gov/sites/default/files/documents/USPTOFY22AFR.pdf)

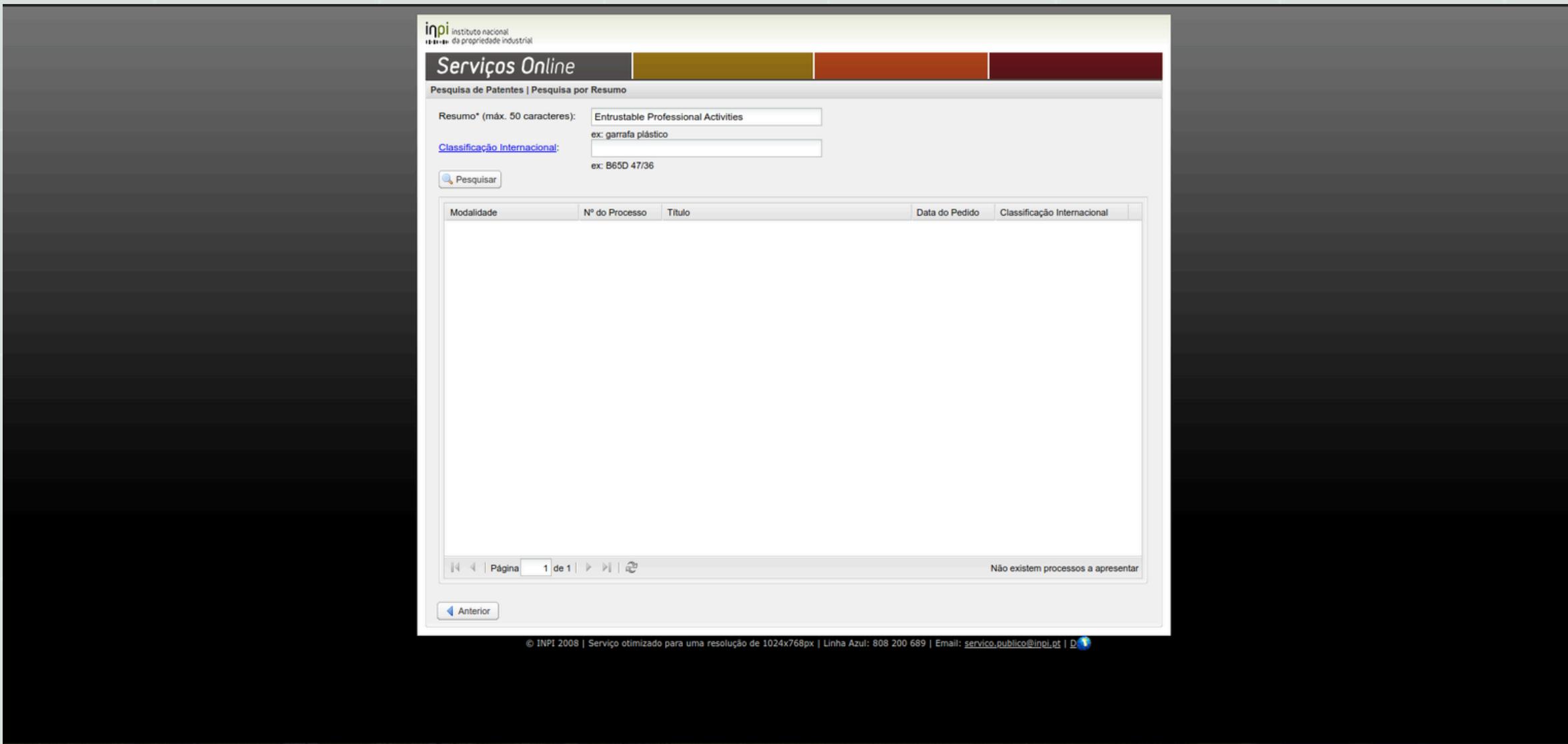
... business lines — the patent program and the trademark program — bolstered by inclusive innovation activities and mission support services. The

Look up specific intellectual property information:

[Search for a patent](#)  
[Search for a trademark](#)  
[Search the Copyright Office's public catalog](#)

# Investigation of Current Patents

INPI Portugal



# Method for discovering patents

Visit reliable patent filing websites



Implement automatic technology watch strategy



Conduct effective manual search



## 4. Analysis of OSS Usage

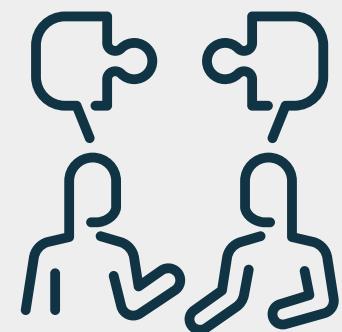


**open source  
initiative®**

# Limitations of OSS Usage

- **License compatibility issues**

Different dependencies in our project present different, potentially incompatible licenses, which needs to be addressed



- **In-viability of turning our project into OSS**

Our commercialization plan does not allow for our project to become OSS, so we must avoid typical copyleft licensed software



**Result: Analysis of licenses used by dependencies is vital to avoid forcing our codebase from becoming OSS**

# Analysis of OSS Licenses

## Frontend Dependencies

- **MIT License**

Highly-permissible, allows for use without any restrictions on any project with no liability

- **Apache 2.0**

Excludes our project as Derivative Work on the grounds that our product merely calls API's for the Works

- **CC-BY-4.0**

Allows for free use of the Work as well as it is visibly credited in our project

- **Hippocratic-2.1**

Allows for free use of the Work as long as it follows Human Rights Principles

# Analysis of OSS Licenses

## Backend Dependencies

- **MIT License**

Highly-permissible, allows for use without any restrictions on any project with no liability

- **EPL 2.0 / GPL2 w/ CPE / EDL 1.0**

GPL2 is a copyleft license which would force us to go OSS but the exception allows for use of this Work as long as all licenses of other Works are explicated

- **Apache 2.0**

Excludes our project as Derivative Work on the grounds that our product merely calls API's for the Works

- **The GNU General Public License, v2 with Universal FOSS Exception, v1.0 (MySQL)**

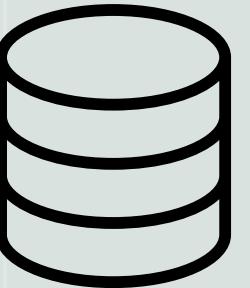
**Obligates Derivative Work (which includes our project in the license's definition) to also have this license, and forces software with this license to be OSS**



# Precautions to take

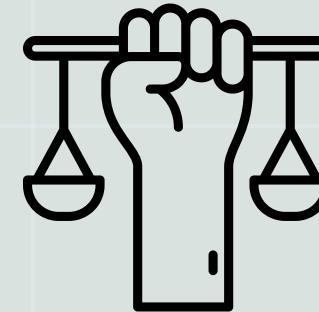
- **Replace MySQL dependency with another DB**

The PostgreSQL connector is protected by an MIT-like license (PostgreSQL license)



- **Follow Human Rights Principles**

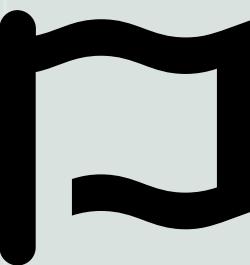
Don't become a terrorist organization?



- **Credit Font Awesome clearly on our work**
- **Reference all licenses in other dependencies as per the GPL 2.0 w/ classpath exception**

Insert a disclaimer in our home page crediting Font Awesome and our uses of their software

Retain a list of licenses per dependency

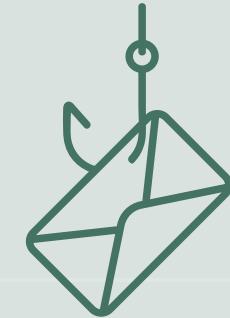


## 5. What cybersecurity problems would the project have to overcome?

### Authentication Threats

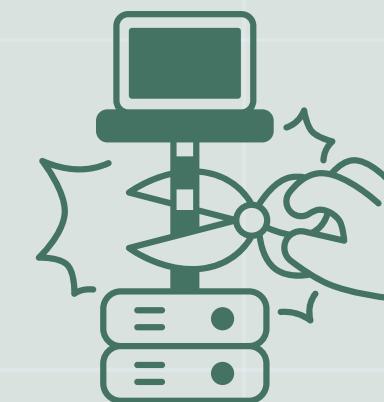
#### Phishing

Fake OTP login pages  
Fake university IdP



#### Man-In-The-Middle

An attacker intercepts data transmitted between the client and the server



### DataBase risks

#### SQL injection

When user input is directly included in SQL or JPA queries without proper validation or sanitization, attackers can inject malicious code into the database queries.



# What cybersecurity problems would the project have to overcome?

## Distributed Denial of Service

A DDoS attack overwhelms the system with traffic from multiple compromised devices (often part of a botnet).

### Common attack vectors

Massive API calls

- File uploads/downloads
- Flooding application endpoints

## Frontend Dependencies

### Supply Chain Attacks

Malicious code injected into a widely used package or build pipeline (CI/CD).

### Lack of Continuous Updates

Exposure to known vulnerabilities with available fixes.  
Implement automated dependency monitoring tools (e.g., Dependabot, Snyk)



# What cybersecurity legislation would we have to follow?

- **General Data Protection Regulation (GDPR – Regulation (EU) 2016/679)**

1. Mandatory for all entities processing personal data of EU citizens

Portugal - Law No. 58/2019: Enforces GDPR locally. Supervisory Authority: CNPD



- **NIS2 Directive (EU Directive 2022/2555)**

1. The primary goal is to ensure a robust cybersecurity posture, capable of preventing, detecting, and effectively responding to cybersecurity incidents

- **Cybersecurity Act (EU Regulation 2019/881)**

1. The goal is to increase trust and security within the European cyberspace.



- **Cyber Solidarity Act (Effective from Feb 4, 2025)**

- **Cyber Resilience Act (CRA – Effective from Dec 10, 2024)**

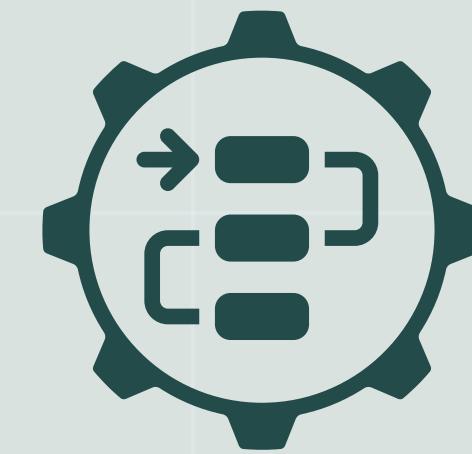
# In detail, how would we implement our cybersecurity measures?



**Multi-Factor Authentication**



**Injection Attack Prevention**



**Dependency Management**



**Intrusion Detection and Prevention**



**DDoS Protection**



**CI/CD and Supply Chain Security**

# 6. What processes would we implement if we have to recover from an attack?



- **Disaster Recovery Plan (DRP)**

While not fully containerized, the platform uses logical module separation and Docker Compose for reliable system restoration, with future plans for greater resilience through service decoupling.

- **Data Backup and Redundancy**

The platform uses both relational (MySQL) and document-based (MongoDB) databases, which must be subject to daily automated backups using tools such as mysqldump, mongodump, or cloud-native solutions (e.g., AWS or GCP).

- **Recovery and Orchestration**

Services can be quickly restored using Docker or Kubernetes, with minimal impact through modular recovery.

- **Scalability and Future Infrastructure Planning**

As usage grows, adopting NGINX for reverse proxying and AWS Auto Scaling will be key to improving resilience, availability, and performance under variable workloads.

- **Incident Response Plan (IRP)**

EvalMed maintains an Incident Response Plan (IRP) with clear roles, GDPR compliant breach notification procedures, and defined RTO/RPO for each module.

In case of a major incident, transparent communication with each of universities.

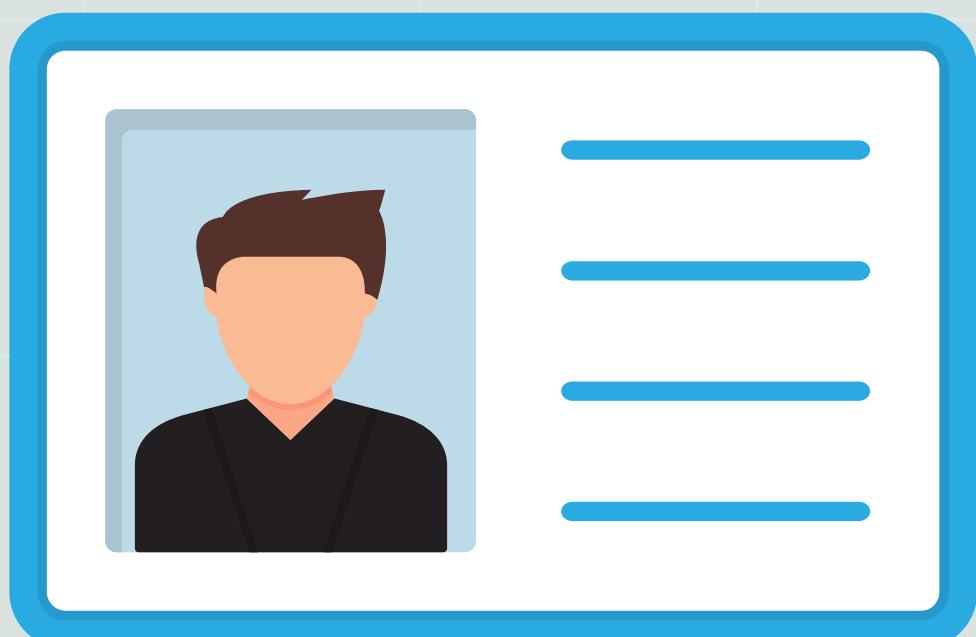
# 7. Privacy Protection

## Current Private Information Storage Policy

### Currently:

- We store PII in our DB relative to university credentials

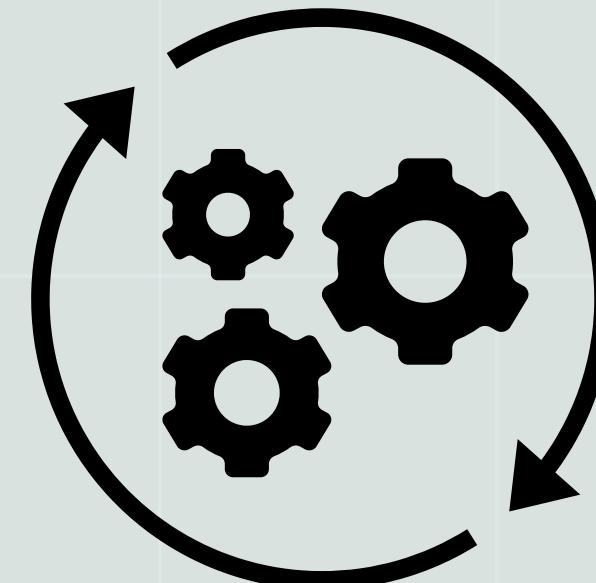
Name, Email, Profile Image



### Future Solution:

- Private Data Could Be Inserted Manually or Automatically

Manual Insertion by Admin vs Automatic Integration with University processes (data is always stored there)



# Current Private Information Storage Policy

**PROBLEM:** Storing the information makes us liable for private data leaks and requires a lot of mechanisms to follow GDPR laws

**SOLUTION:** Change business strategy to enforce automatic integration with University so that we don't store private information

## WE BECOME A DATA PROCESSOR

Our clients are the Data Controllers

Business Model followed by similar platforms like Moodle



# Technical Impact on Our Project

- **Anonymisation of information**

Evaluation Reports, calendarization and procedure information would all still need to be stored in our DBs

- **Initial Generation of Anonymous Identifiers**

Initial generation of random IDs for everyone and every course would need to be an automated and protected process

- **Logging of all processed information**

GDPR requires logging of all processed private information to be maintained

- **Fetching Private Information**

Changing our business model implicates changing the way we access private information within our product

- **Encryption of Profile Pictures**

While associated with a random ID, profile pictures can still be considered private information, therefore must be encrypted

# Other Responsibilities

- **Processing Security Audits**

Security of processing needs to be assured by both the Data Controller and the Data Processor



- **Processes to Notify Data Breaches**

According to GDPR we must be able to notify the Data Controller should a leak occur



- **Processing Legal Requests**

We are not responsible for deleting private data, we can redirect requests to the data controller



## 8. Ethical Aspects & Compliance Regulation

### Transparency & Accountability

The AI should be clear and reviewable

If we explain how it works and how to be used → User Trust

### Data Privacy & GDPR

- Handles sensitive student/tutor data correctly
- Requires informed consent & data minimization
- Application should be used for educational use

### Academic Specific Ethical Aspects:

Each university has its own set of regulations and ethical aspects that need to be followed, so it's required to insure that the platform is in compliance with all of them and evaluation methods

### Consent on usage of data for model training:

Even though the data is anonymous, it is ethically and legally necessary to obtain explicit user consent before using any form of educational or interaction data for training machine learning models.



# 9. AI Integration: Current and Future Applications

**Are there AI aspects in our project? What are they?**

Yes. EvalMed integrates and plans to expand AI features to enhance the assessment process in the new medical course.

- **Current AI Functionality:**

- Voice-to-text transcription using Automatic Speech Recognition (ASR) for tutor and student self-assessments.

- **Planned AI Features:**

- Intelligent feedback support using Large Language Models (LLMs) to suggest draft comments based on historical evaluation data (strengths, challenges, clinical context).
- Institutional analytics: Generation of anonymized, aggregated performance reports (by EPA, activity, year) to support pedagogical decisions.



# Data Challenges and Mitigation Strategies

What problems would we have in terms of data? What must we avoid to acquire data adequately?

- **Cold Start & Representation Bias**

- Limited initial dataset due to new program.
- Lack of feedback could prevent the dataset from growing and evolving
- Students / Tutors might not want to have their data used to train models
- **Mitigation:** Broad platform adoption, usage monitoring, corrective strategies.

- **Speech Data Challenges**

- ASR may struggle with accents and diverse speech patterns so we need to ensure our external AI recognizes a magnitude of languages correctly

- **Operational Risks**

- Incomplete evaluations, sync errors, unvalidated changes to forms.
- Mitigation: Data validation rules, strict version control, robust sync mechanisms.

- **Privacy and Consent (GDPR)**

- Videos of the students doing evaluations need to be anonymized
- Users need to consent for their data to be used to train these models

# 10. HYPERSCALERS

**Why Migrate from Academic Hosting?**

**Current State:** IEETA VM (limited scalability, reliability)

**Goal:** Prepare for production-level deployment and AI-powered features

**Benefits of Hyperscalers (AWS, GCP)**

- Elastic compute & storage
- Global data centers (low latency)
- Integrated AI, monitoring, and security tools
- High availability and disaster recovery options
- Isolated instances per organization



**Legal & Ethical Considerations**

**GDPR Compliance:**

- Data must remain within the EEA or protected under EU standards
- Use of anonymized data reduces compliance risk

# 11. Network Effects

## Positive Network Effects to Boost EvalMed's Success

**What kind of network effects could we explore?**

### User Growth = Data Quality

- More students, tutors, and institutions → richer, more diverse datasets → better AI performance (context, nuance, personalization).



### Learning Communities

- Peer review, comments, and asynchronous discussions foster a culture of shared knowledge and continuous improvement.



### Cross-Institutional Adoption

- Enables EPA evaluation standardization → tracking skills over time and between institutions.
- Opens up benchmarking, accreditation support, and public policy use.



### System Integration & Stickiness

- Seamless fit with existing LMS, OTT, and institutional login systems → smoother adoption, less resistance.



### Prestige Adoption = Trust Signal

- Early use by leading institutions builds credibility, encouraging others to follow — crucial in conservative academic environments.



# Risks of Negative Network Effects & How to Prevent Them

## What negative network effects must we avoid?

### Data & Notification Overload

- More users = risk of irrelevant notifications or noisy, low-quality data.  
→ Use smart notifications and quality control mechanisms.

### Participation Imbalance

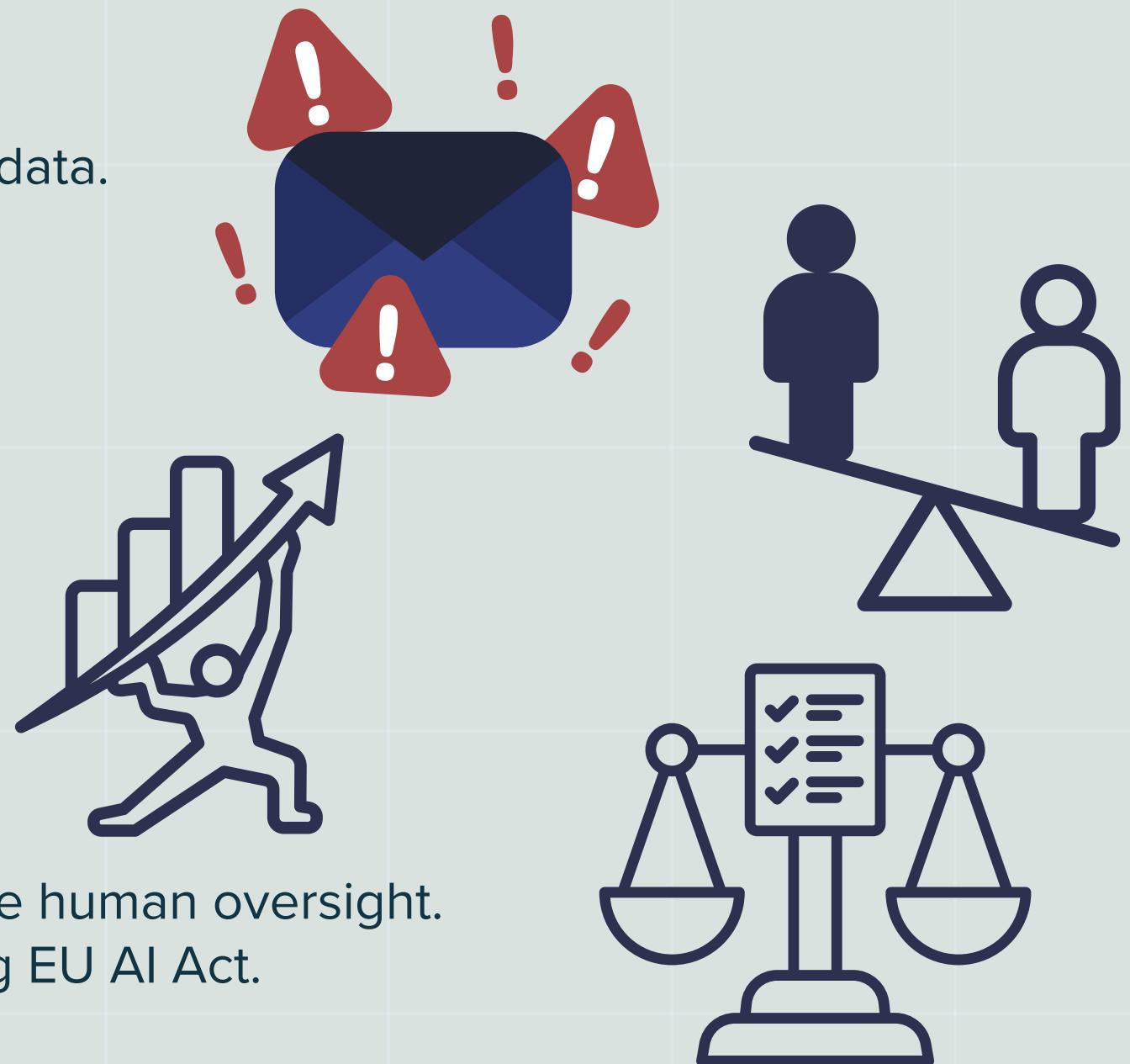
- Over-reliance on a few users or institutions may bias data.  
→ Promote equitable engagement and monitor usage patterns.

### Scalability & Security Challenges

- More institutions = greater strain on infrastructure.  
→ Adopt modular, cloud-agnostic architecture; prioritize security.

### Legal and Ethical Risks

- Scaling must respect GDPR, ensure explainable AI, and preserve human oversight.  
→ Ensure compliance and transparency, aligned with the upcoming EU AI Act.





EVALMED



deti

universidade de aveiro  
departamento de eletrónica,  
telecomunicações e informática

# Thank you!

**APSEI - Trabalho 4**

**Does anyone have any questions?**

**Tomás Brás - 112665**

**Carolina Silva - 113475**

**Afonso Ferreira - 113480**

**Ricardo Antunes - 115243**

**Carlos Soto - 123551**