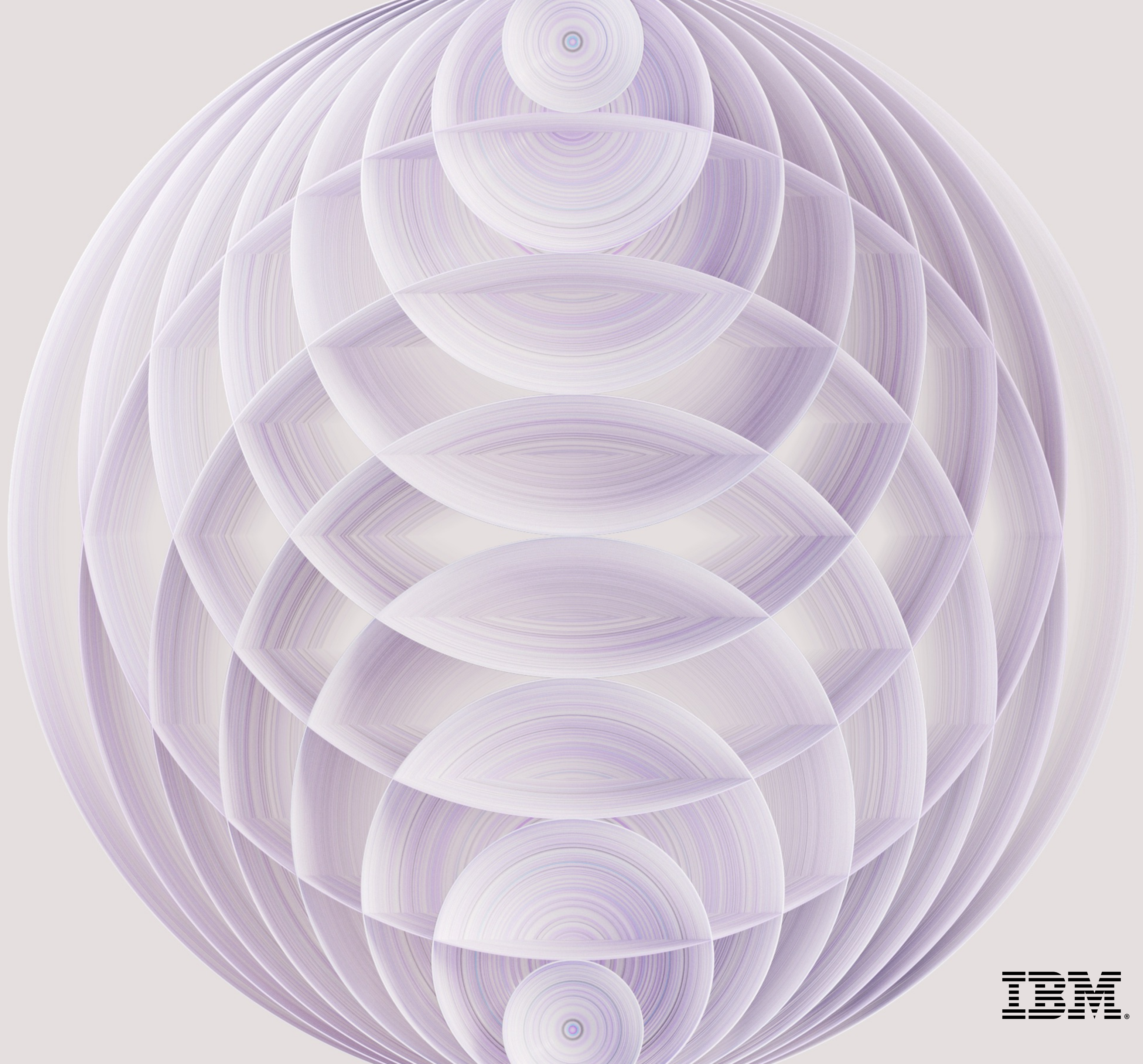


# Irányítsd az AI-t mielőtt az irányít téged!

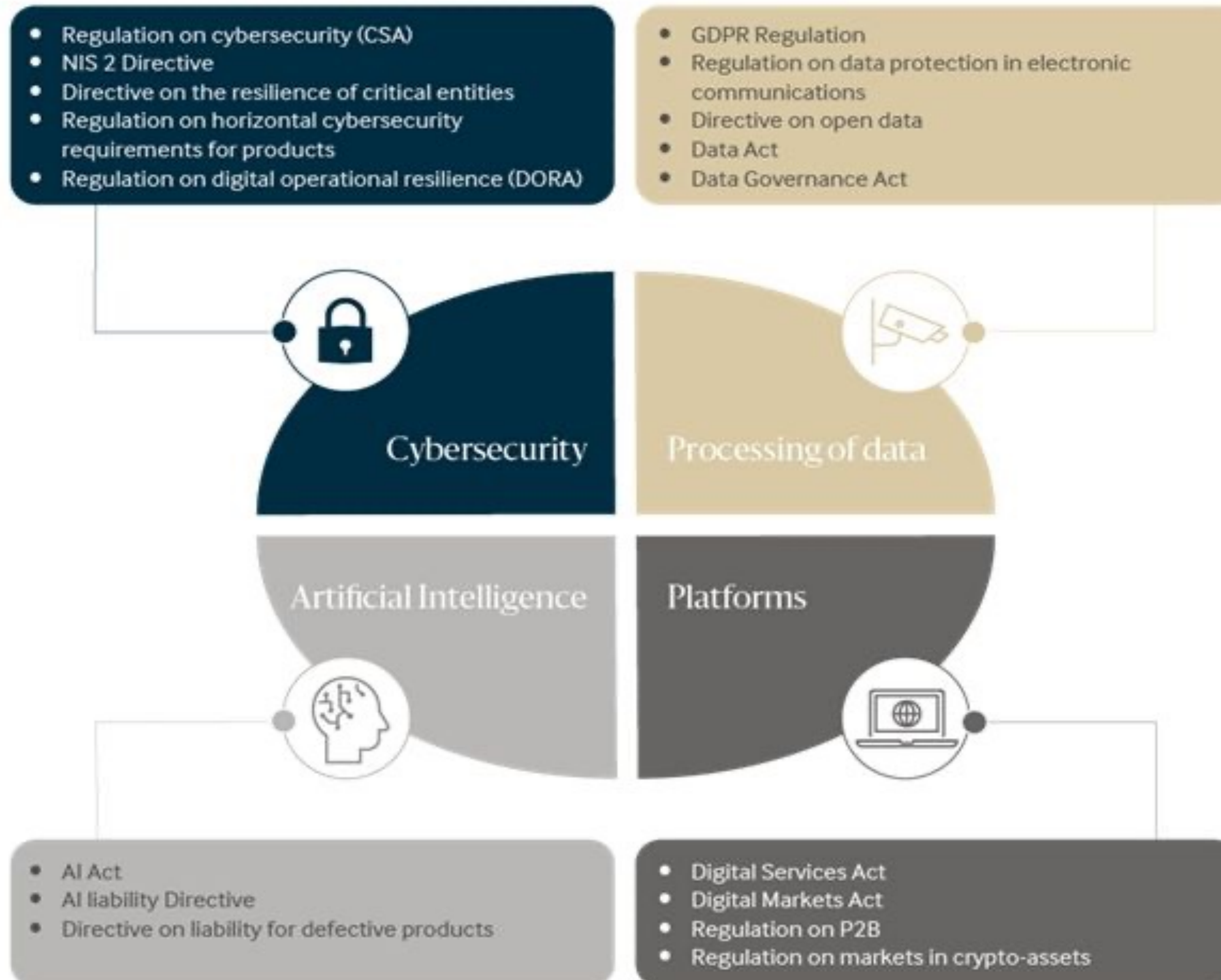
**Husztai Dániel**

[daniel.husztai1@ibm.com](mailto:daniel.husztai1@ibm.com)

**watsonx**



# Adatstratégia és szabályozások az Európai Unióban



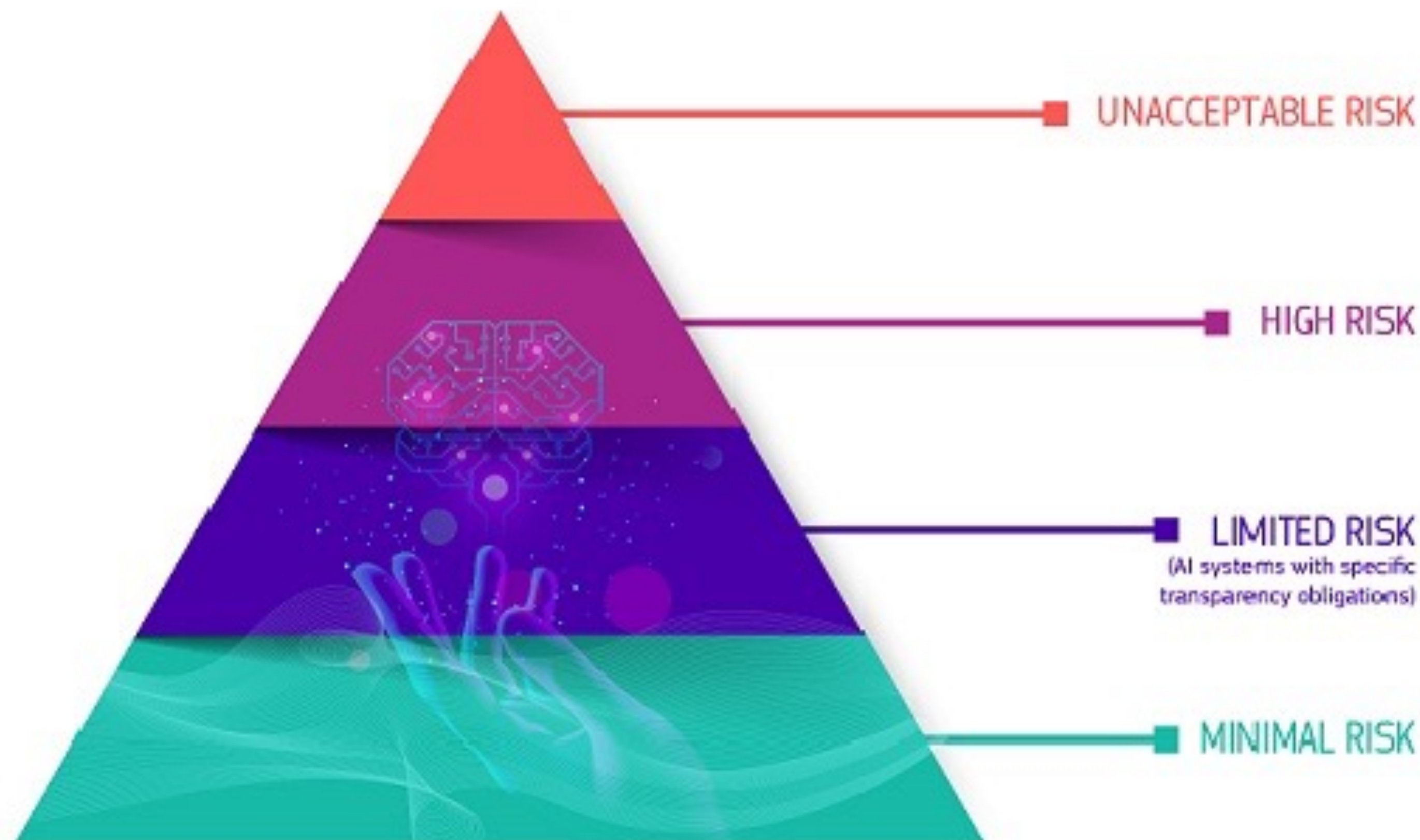
# EU AI szabályozás

## A jogszabály főbb elemei:

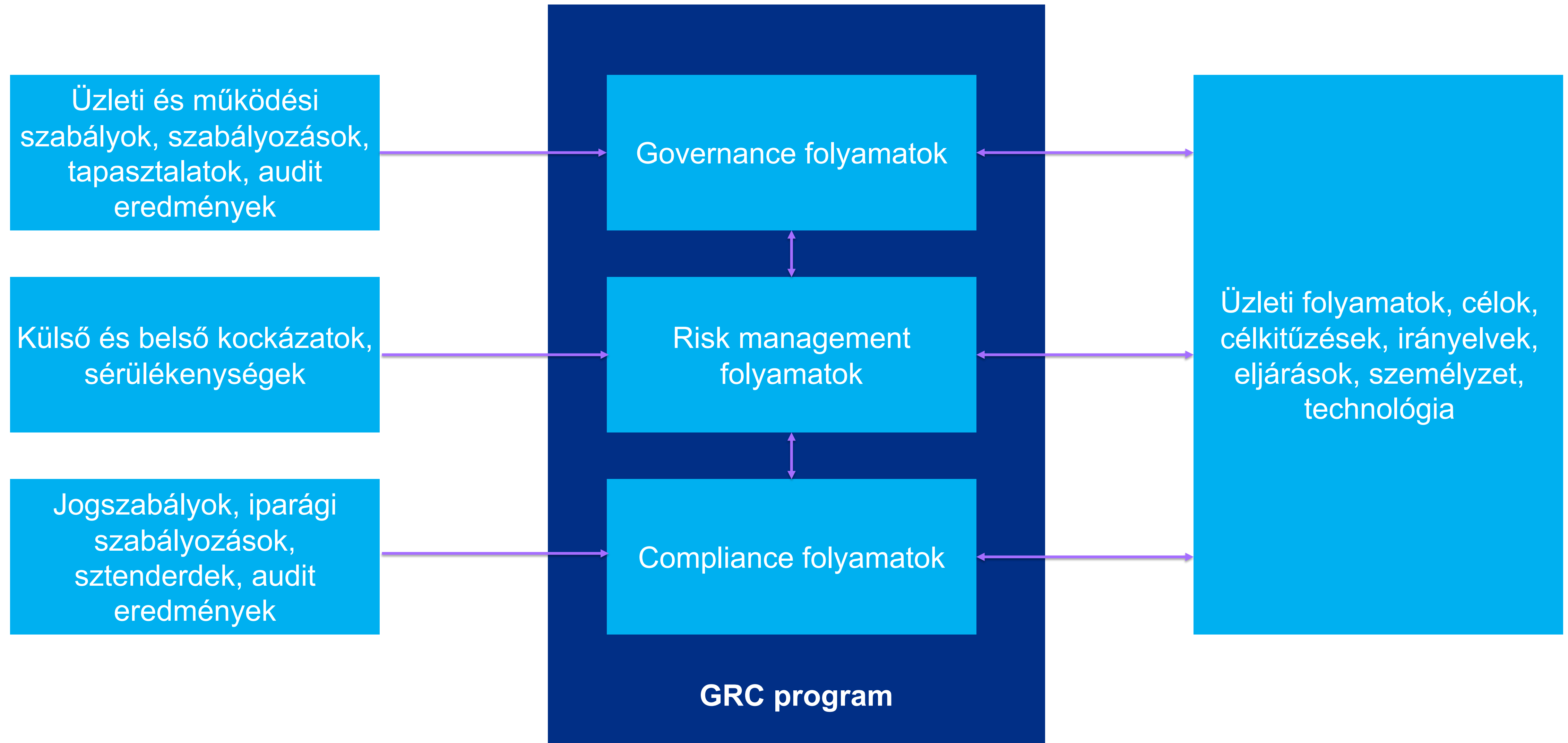
- Átláthatóság
- Emberi ellenőrzés
- Alapvető jogok védelme

## Kockázati szintek:

- Nem elfogadható
- Magas
- Korlátozott
- Minimális



# Integrált kockázatkezelés (GRC)



# Kihívások az integrált kockázatkezelésben (GRC)



Törvényi szabályozások és hatásuk kezelése



Vállalatot érintő kockázatok konzisztens nézete



GRC adatminőségi kihívások és adatsilók kezelése



Felelősségi körök kialakítása a kockázatkezelési és szabályozási megfelelés során



Váratlan, kockázatos események bekövetkeztenek csökkentése

# Mesterséges Intelligencia felügyet

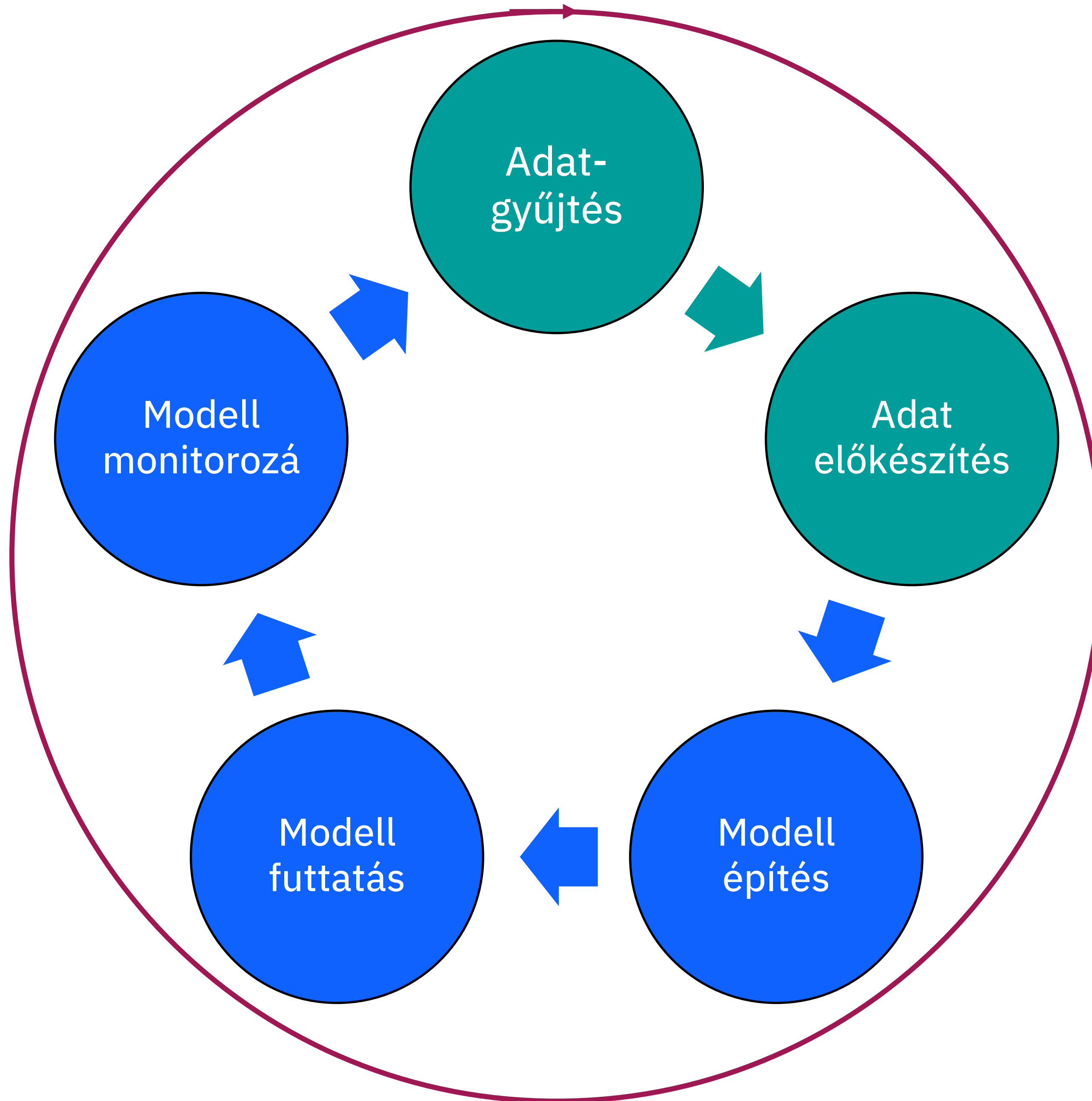


Egy szervezet mesterséges intelligencia tevékenységének irányítása, nyomon követése.

# Teljeskörű MI életciklus kezelés az IBM watsonx segítségével



# Megbízható MI



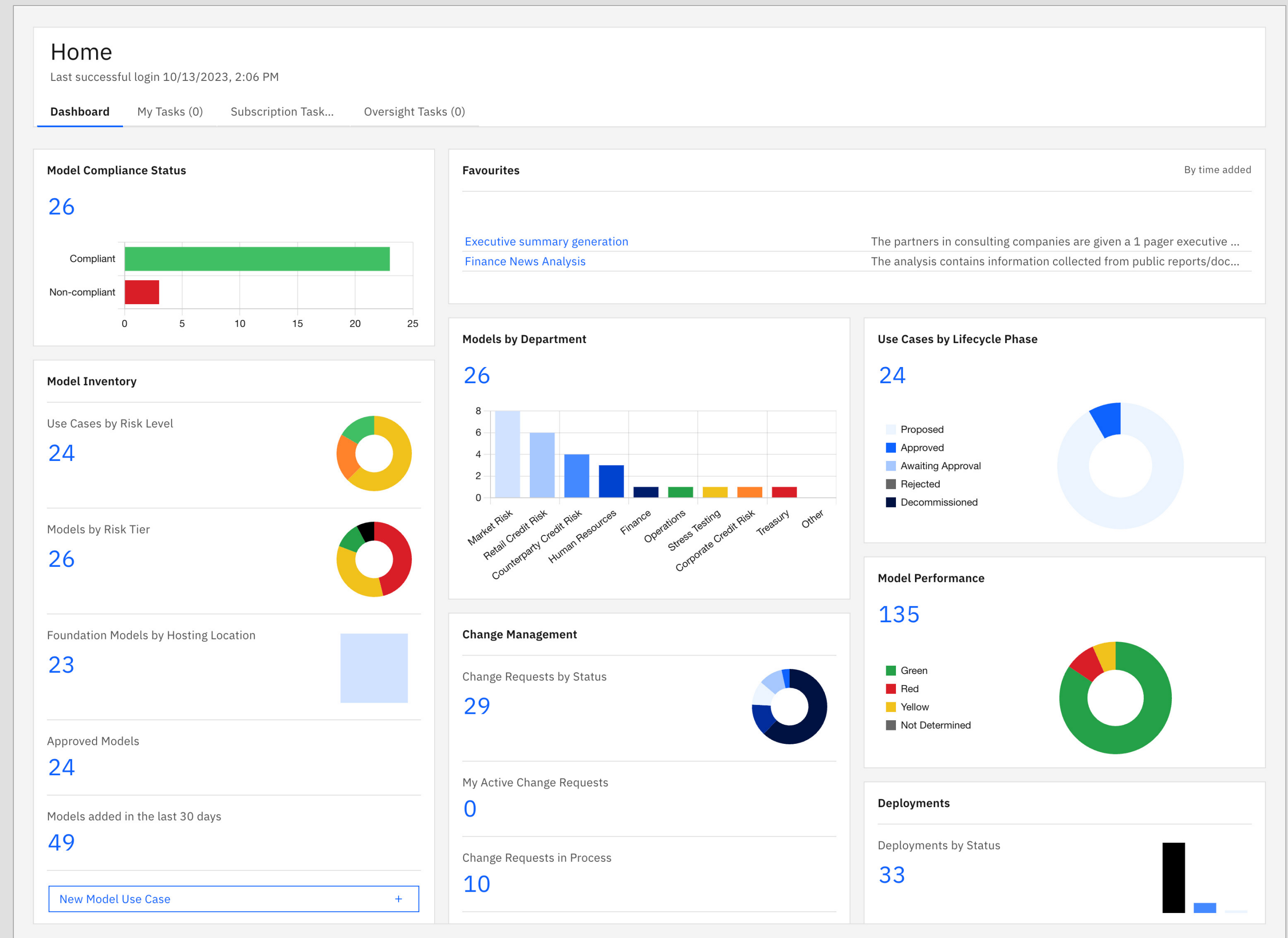
- **Adat:** Teljeskörű felügyet az adatok felett
- **Modell:** MLOps folyamat az elmagyarázhatóság és robosztusság érdekében
- **Folyamat:** Automatizálás a konzisztencia, a hatékonyság és az átláthatóság növelése érdekében



# Jogszabályi megfelelés

## EU és hazai MI szabályozások

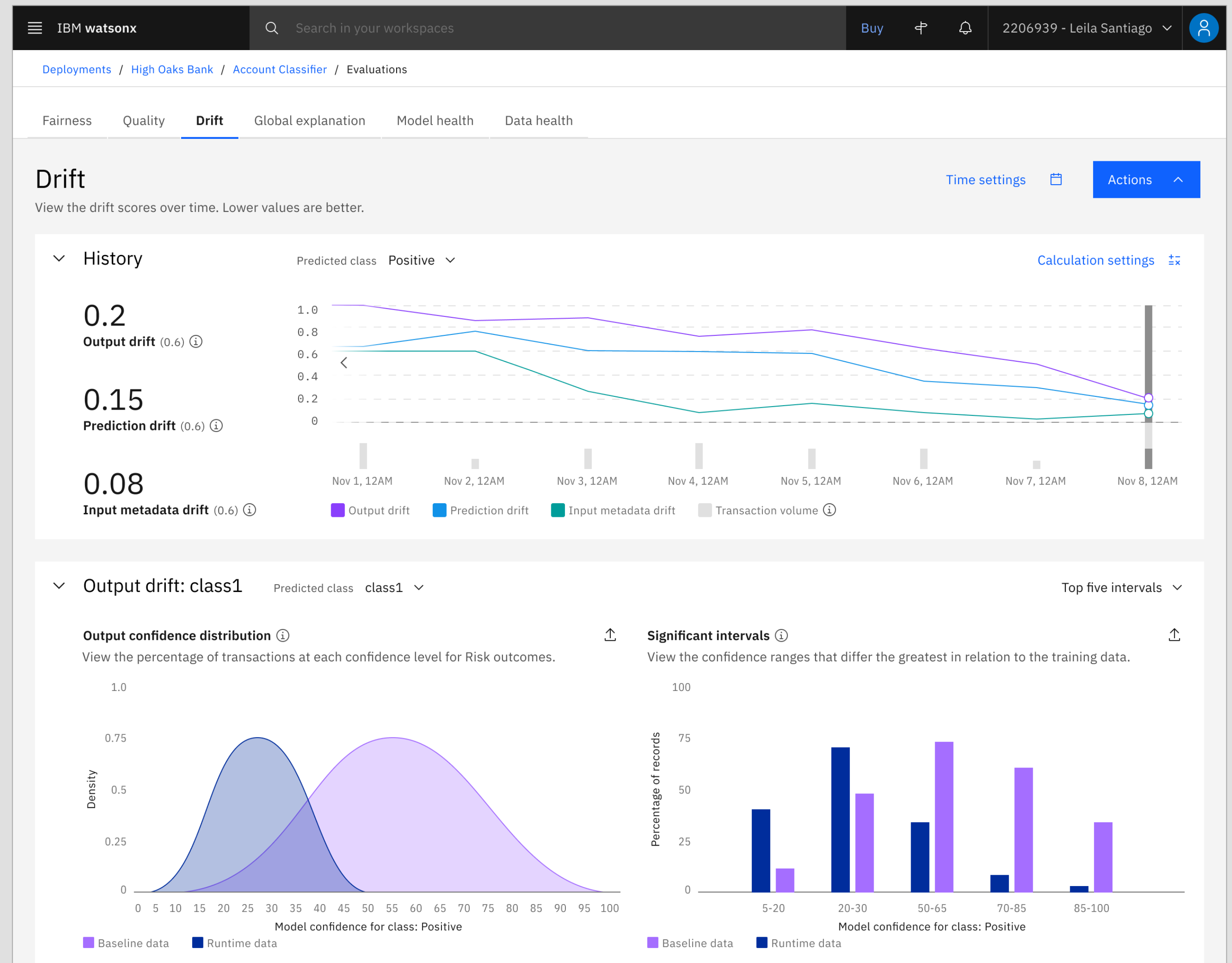
- Mesterséges intelligenciára vonatkozó szabályozások lefordítása végrehajtható irányelvekké
- Auditálás és egyéb külső MI adatszolgáltatás
- Átlátható MI folyamatok kialakítása



# Megbízható MI

## A kockázat kezelése és a hírnév védelme

- Előre beállított riasztások az MI modellek automatikus felügyeletére
- Kockázatok kezelés és jogszabályi megfelelés biztosítása
- Magyarázható modelleredmények biztosítása a vizsgálatok támogatása és a bírságok elkerülése érdekében



# Életciklus felügyelet

## MI modellek magabiztos felhasználása

- Modellek nyomon követése a teljes MI életciklus során
- Modell metaadatok automatikus rögzítése a jogszabályi megfelelés érdekében
- Modellek teljesítményének felügyelete a teljes szervezeten belül, automatikus jelentéskészítés

The screenshot displays the IBM Watsonx Governance interface. The top navigation bar includes the IBM Watsonx logo, a search bar, and user information (2206939 - Leila Santiago). The breadcrumb trail shows the path: Projects / OCCS Project / OCCS Model. A sidebar on the left lists various governance categories: Governance (selected), Foundation model, Prompt template, Prompt parameters, Evaluation (with sub-items: Develop, Test, Validate, Operate), Additional details, and Attachments. The main content area is titled 'Governance' and shows details for an AI use case named 'OCCS Crew Communication System'. The use case is approved and has a unique ID. The description states it's an advanced machine learning solution for enhancing crew communication. The approach is 'Flan-UL2-12345' and the version is '0.2.21'. A lifecycle bar at the bottom shows three stages: 01 Develop, 02 Validate (currently active), and 03 Operate.

# Bemutató

## Három szerepkör:

- Risk Manager
- Model Ops Engineer
- Data Scientist / Prompt Engineer

The screenshot displays the IBM watsonx interface for an AI Factsheet. The breadcrumb navigation shows the path: Deployments / Insurex.ai - Development / Insurance claim summarization. The left sidebar lists various asset categories, with 'Test results' selected under the 'Insurex.ai - watsonx.governance' development environment. The main content area, titled 'Generative AI Quality', features a 'Feedback' dropdown and several performance metrics, each with a red downward arrow indicating a decrease:

- Flesch Readability:** 48.46 (Scale: 0 to 206.84)
- Text quality Recall:** 0.61 (Scale: 0 to 1)
- Text quality Precision:** 0.25 (Scale: 0 to 1)
- F1 Score:** 0.33 (Scale: 0 to 1)

On the right, the 'About this asset' panel provides details for the 'Insurance claim summarization' asset, including its name, description (not provided), asset ID, and creation/modification information.

