REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE

Euroopa Liidu AI määrus ja tehisintellekti reguleerimine

Henrik Trasberg

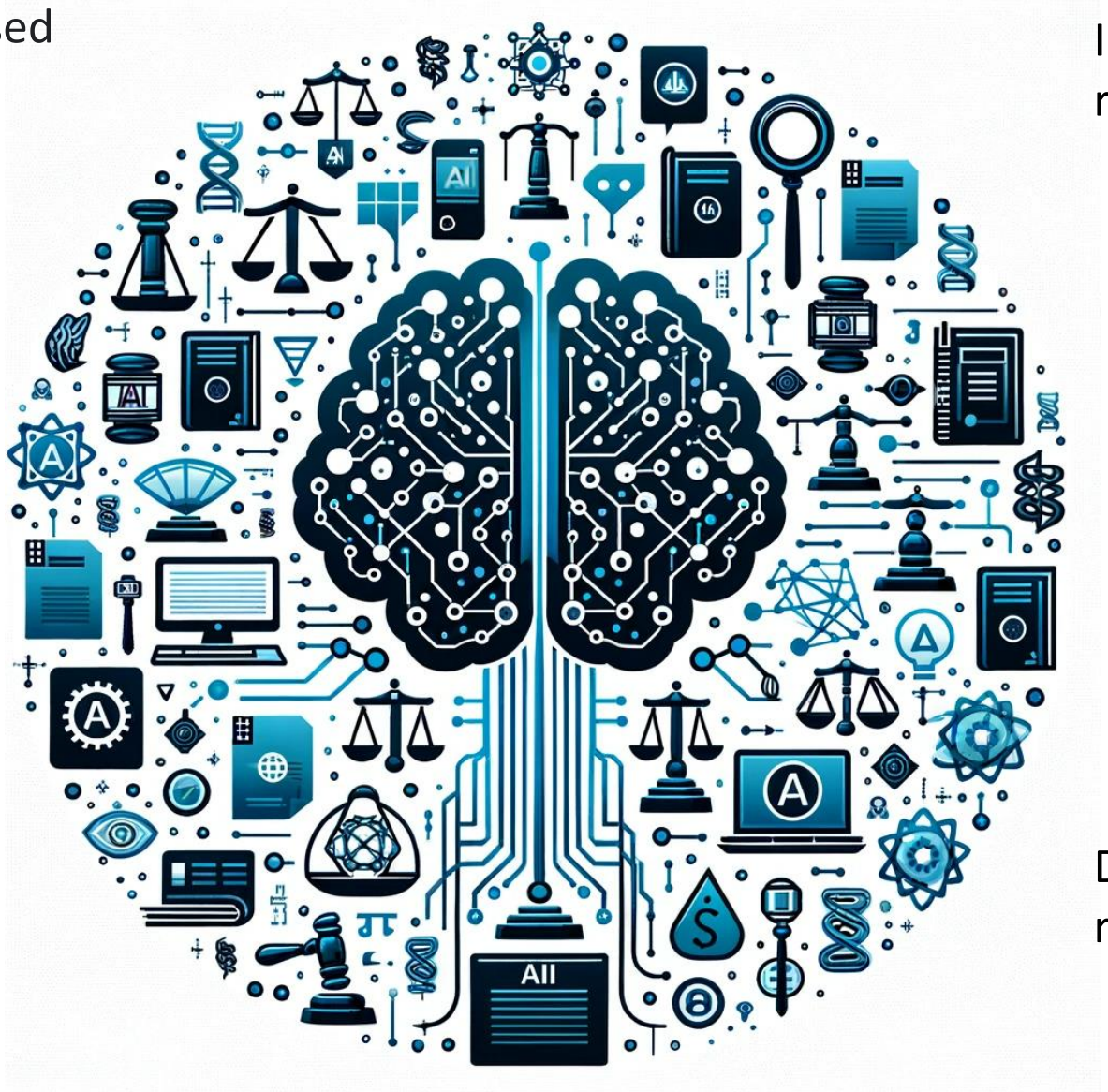
Uute tehnoloogiate ja digitaliseerimise õigusnõunik

Justiitsministeerium

Põhiõigused ja -vabadused

Isikuandmete kaitse regulatsioonid

Võlaõigus



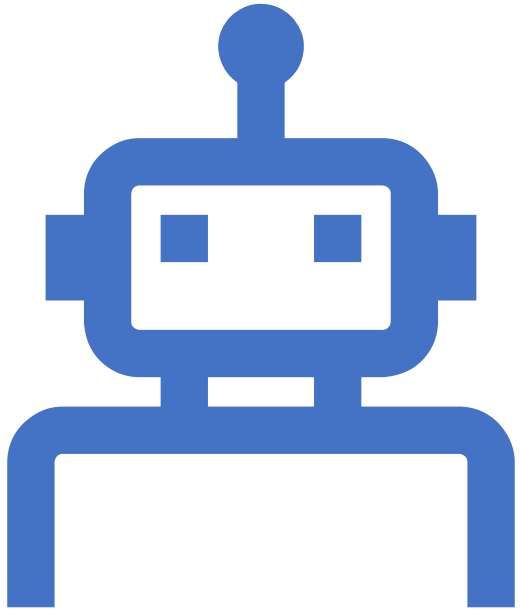
Intellektuaalomandiõigused

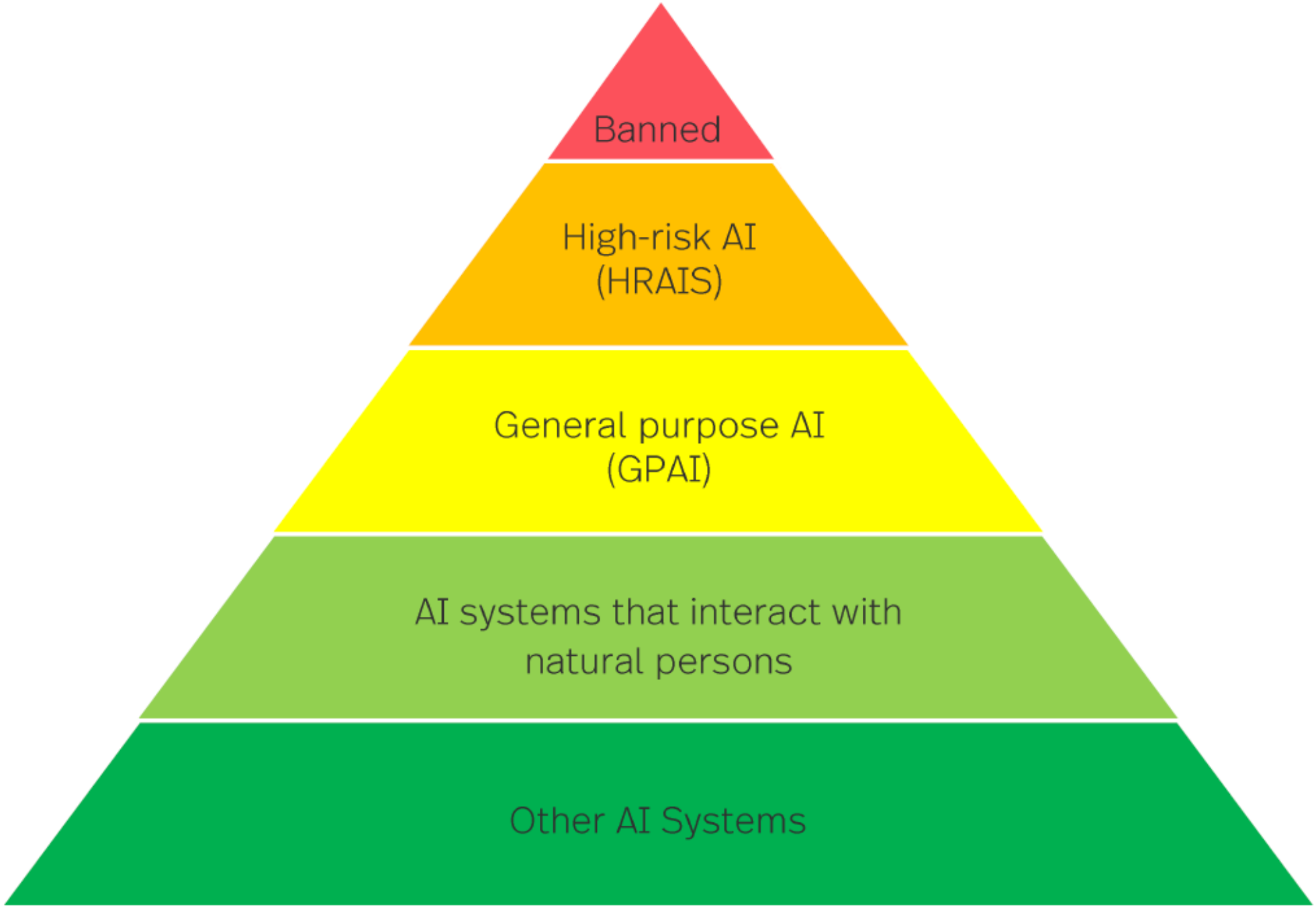
Kriminaalõigus

Digiplatvormide regulatsioon

AI definitsioon

„A machine-based system designed to **operate with varying levels of autonomy** and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.“




Banned
High-risk AI
(HRAIS)
General purpose AI
(GPAI)
AI systems that interact with
natural persons
Other AI Systems

Tehisintellekti **keelatud** kasutusjuhud

1. **Sotsiaalne hindamine** (*social scoring*)
2. **Inimeste haavatavuste ärakasutamine,** alalävisele tajule suunatud võtete kasutamine kahju tekitamiseks
3. Õiguskaitseasutuste poolt **reaalajas biomeetriline kaugtuvastamine avalikus kohas**
4. Füüsiliste isikute **biomeetriline liigitamine** biomeetriliste andmete alusel, **et tuletada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi või seksuaalset sättumust**
5. **Individuaalne ennetav politseitegevus** *(predictive policing)*
6. **Emotsioonituvastus töökohal ja haridusasutustes,** välja arvatud meditsiinilistel või ohutusega seotud põhjustel (nt pilootide väsimustaseme jälgimine)
7. Internetist või videosalvestistest näokujutiste **ulatuslik valimatu allalaadimine** andmebaaside loomiseks või laiendamiseks

Kõrge riskiga kasutusjuhud

1) AI süsteemid, mida kasutatakse toodetes, mis kuuluvad ELi tooteohutust käsitlevate õigusaktide alla. See hõlmab **mänguasju, lennundust, autosid, meditsiiniseadmeid** jm.

2) Kõrge riskiga valdkondadesse kuuluvad süsteemid, nt:

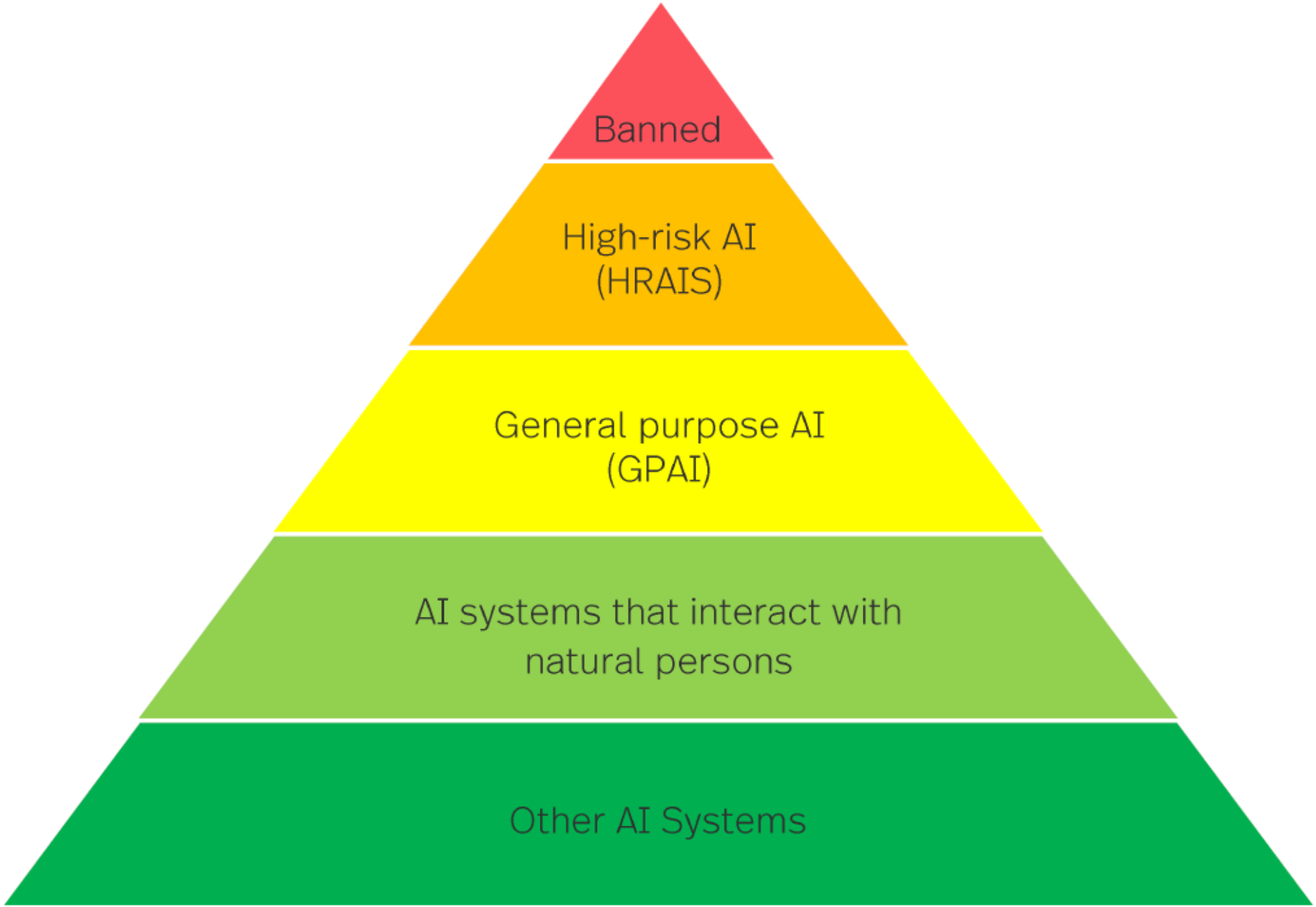
- Teatavad **kriitilise tähtsusega taristud**, näiteks maanteeliikluse ning vee-, gaasi-, kütte- ja elektrivarustuse valdkonnas;
- **haridus ja kutseõpe**, nt õpitulemuste hindamine, õppeprotsessi juhtimine ja pettuse seire;
- **tööhõive, töötajate juhtimine** ja füüsilisest isikust ettevõtjana tegutsemise võimaldamine, nt suunatud töökuulutuste avaldamine, tööle kandideerimise taotluste analüüsimine ja filtreerimine ning kandidaatide hindamine;
- **juurdepääs olulistele era- ja avalikele teenustele** ja hüvedele (nt tervishoid), füüsiliste isikute **krediidivõimelisuse hindamine** ning elu- ja tervisekindlustusega seotud riskihindamine ja hinnakujundus;
- teatavad süsteemid, mida kasutatakse **õiguskaitse**, **piirikontrolli**, **õigusemõistmise** ja **demokraatlike protsesside valdkonnas**;
- **hädaabikõnede hindamine ja liigitamine**;
- **biomeetrilise** tuvastamise, liigitamise ja emotsioonituvastuse süsteemid (väljaspool keelatud kategooriaid)

Kõrge riskiga AI süsteemi pakkuja kohustused

- **Riski- ja kvaliteedijuhtimissüsteemi** kasutuselevõtmine võimalike ohtude hindamiseks ja maandamiseks ning tagamaks süsteemi piisav täpsus ja stabiilsus
- **Treeningandmete** asjakohase kvaliteedi tagamine
- **Läbipaistvuse** tagamine süsteemi rakendaja jaoks (selleks, et kasutajad saaksid tõlgendada süsteemi väljundit ja seda asjakohaselt kasutada)
- **Inimjärelevalve** tagamine („kasutades muu hulgas asjakohaseid inimene-masin kasutajaliideseid, et füüsilised isikud saaksid teha tehisintellektisüsteemi kasutamise ajal selle üle reaalset järelevalvet“)
- AI süsteemi toimimise **logimine**
- Tehnilise **dokumentatsiooni** koostamine
- Asjakohase **küberturvalisuse** taseme tagamine
- **Vastavushindamise** tegemine ja AI süsteemi **registreerimine**

Kõrge riskiga AI süsteemi **rakendaja** (*deployer*) kohustused

- Tagada kooskõla **kasutusjuhendiga**
- Tagada **sisendandmete kvaliteet** ja asjakohasus
- Juhul, kui süsteemi toimimist kontrollib rakendaja, tagada asjakohane **inimjärelevalve**
- Avaliku sektori (ning pangandus ja kindlustusvaldkonna) süsteemides **põhiõiguste mõjuhinnang**
- Teatud juhtudel süsteemi kasutuse **logimine**
- Tagada **inimese** (nt teenuse kliendi või töötaja) **teavitamine**, kui tema suhtes tehakse otsus kõrge riskiga AI süsteemi kasutades


Banned
High-risk AI
(HRAIS)
General purpose AI
(GPAI)
AI systems that interact with
natural persons
Other AI Systems

Üldotstarbeline tehisintellekt

- **Üldotstarbelise** tehisintellektiga kaasnevad kohustused:
  - Tehniline dokumentatsioon
  - Kohustus anda *downstream* ettevõtetele infot süsteemi toimimisest
  - *Copyright policy*
  - Ülevaade autoriõigusega kaitstud materjali kasutamisest süsteemi treenimisel

- **Süsteemse riskiga üldotstarbelised mudelid** (esialgu 10^{25} FLOPSi):
  - süsteemsete riskide hindamise ja maandamise kohustus

Süsteemid, millega kaasneb läbipaistvuskohustus

- Inimest tuleb teavitada kui:
  1) ta suhtleb **juturobotiga**
  2) avaldatakse AI-ga loodud **süvavõltsing**
  3) AI teostab tema suhtes **biomeetrilist kategoriseerimist**
  4) AI tuvastab tema **emotsioone**

- Generatiivse AI pakkujate kohustus tagada nende süsteemiga loodud sünteetilise audio, video, piltide ja teksti (vesi)märgistamine.

Kohustuste **tõhusa kohaldamise** tagamine

- **Kohustuste konkretiseerimine** läbi standardite ja tegevusjuhiste.
- Tehisintellekti **liivakast**, sh testimine päriselu tingimustes
- **Innovatsiooni edendamine**: rahastusmeetmed, ligipääs EL-i arvutusvõimsusele

Millal hakkab AI määrus kehtima?

- AI määruse vastuvõtmine: 2024. a kevad

- Kohustused hakkavad asutuste jaoks kehtima:
  - **Keelatud AI:** 6 kuud pärast määruse vastuvõtmist
  - **Üldotstarbelised AI süsteemid**: 1 aasta pärast vastuvõtmist
  - **Läbipaistvuskohustused**: 2 aastat
  - **Suure riskiga AI süsteemide kohustused**: 2 aastat (toodete osas, mis on reguleeritud ELi tooteohutuse regulatsiooniga – 3 aastat)

Järelevalve

- Riiklik **turujärelevalveasutus**
- EL Komisjoni juurde luuakse **AI Office**. Seda nõustab **nõuandefoorum**, mis esindab sidusrühmi, sh tööstusharu, idufirmasid, kodanikuühiskonda ja akadeemiat
- **AI Nõukogu** (*AI Board*)

Andmepõhine riik

Kujundada Eestist läbi andmete väärindamise ja targa kasutamise juhtiva andmemajanduse ja avaliku halduse kvaliteediga riik maailmas

Inimeste heaolu

Avaliku halduse kvaliteet

Ettevõtete tootlikkus

Andmepõhine riigikorraldus ja majandus

Eesti riigikorraldus ja majandus on oma toimimises andmepõhine ja tagatud on selle kestlik areng – Eesti on maailma suurima andmemajanduse osakaaluga riik

Krativäeline riik ja ühiskond

Nii erasektor kui ka riigikorraldus on tehisintellekti poolt rikastatud – Eesti on juhtiv tehisintellekti rakendaja maailmas

Usaldusväärsus ja inimkeskne tehisintellekt ning andmekorraldus

Andmekorraldus ja tehisintellekti kasutamine riigis on inimkeskne ja usaldusväärne - sh personaalse riigi lahendused on turvalised, tagavad inimeste õiguste kaitse ning säilib usaldus Eesti digiriigi suhtes

Andmete tegevuskava 2024-2025

Tehisintellekti tegevuskava 2024-2026

REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE

Tänan!

Henrik Trasberg
Henrik.trasberg@just.ee