



Central European Institute of Technology
BRNO | CZECH REPUBLIC

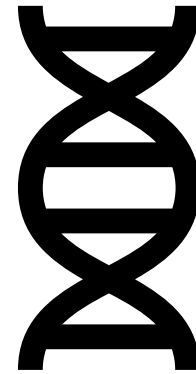


Agentic AI and sensitive data

ELIXIR IMPACT Webinar: Discover Agentic AI in Life Sciences

Vojtech Bystry
vojtech.bystry@ceitec.muni.cz

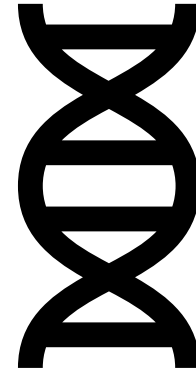
Sensitive
data



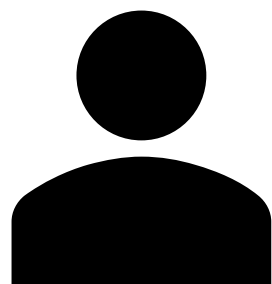
GCTAG..

TRE/SPE

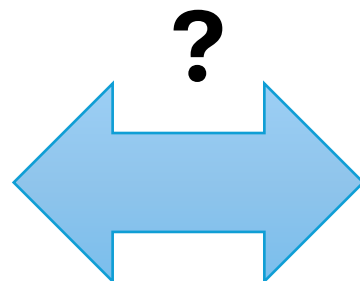
Sensitive
data



GCTAG..

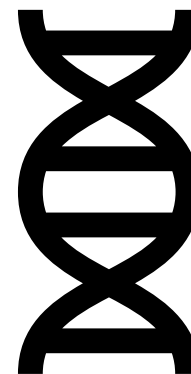


Researcher



TRE

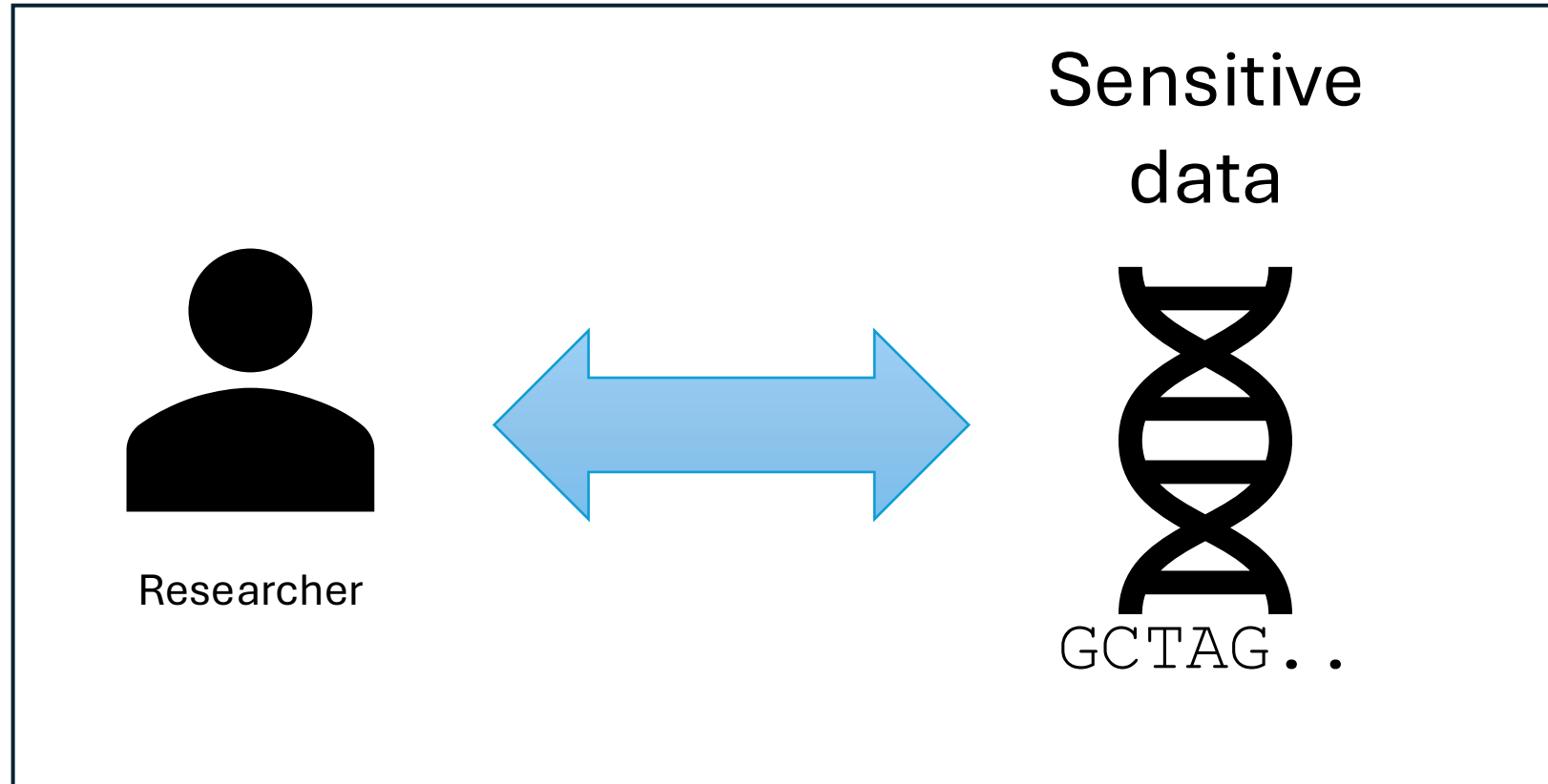
Sensitive
data



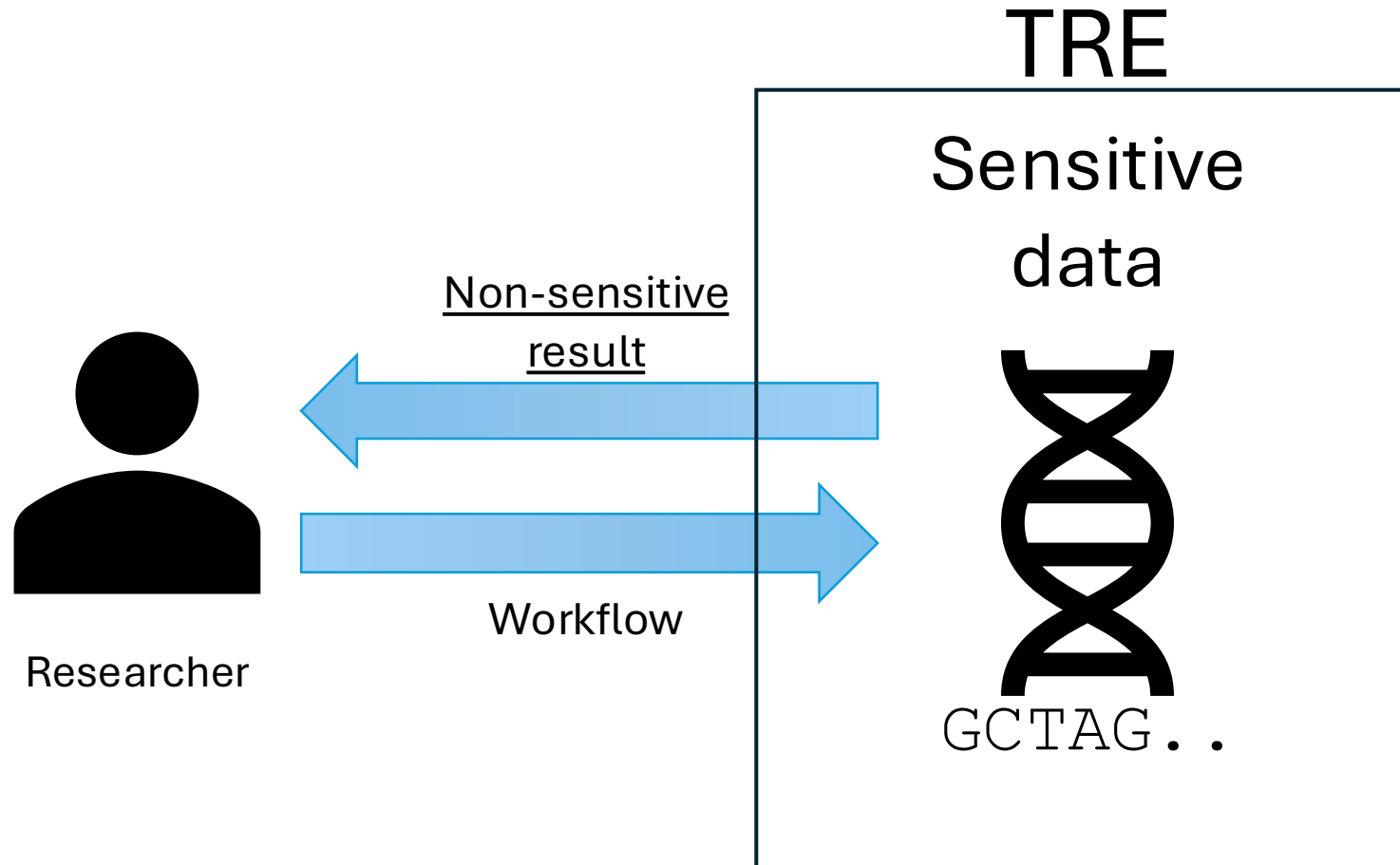
GCTAG..

Interactive work with the data

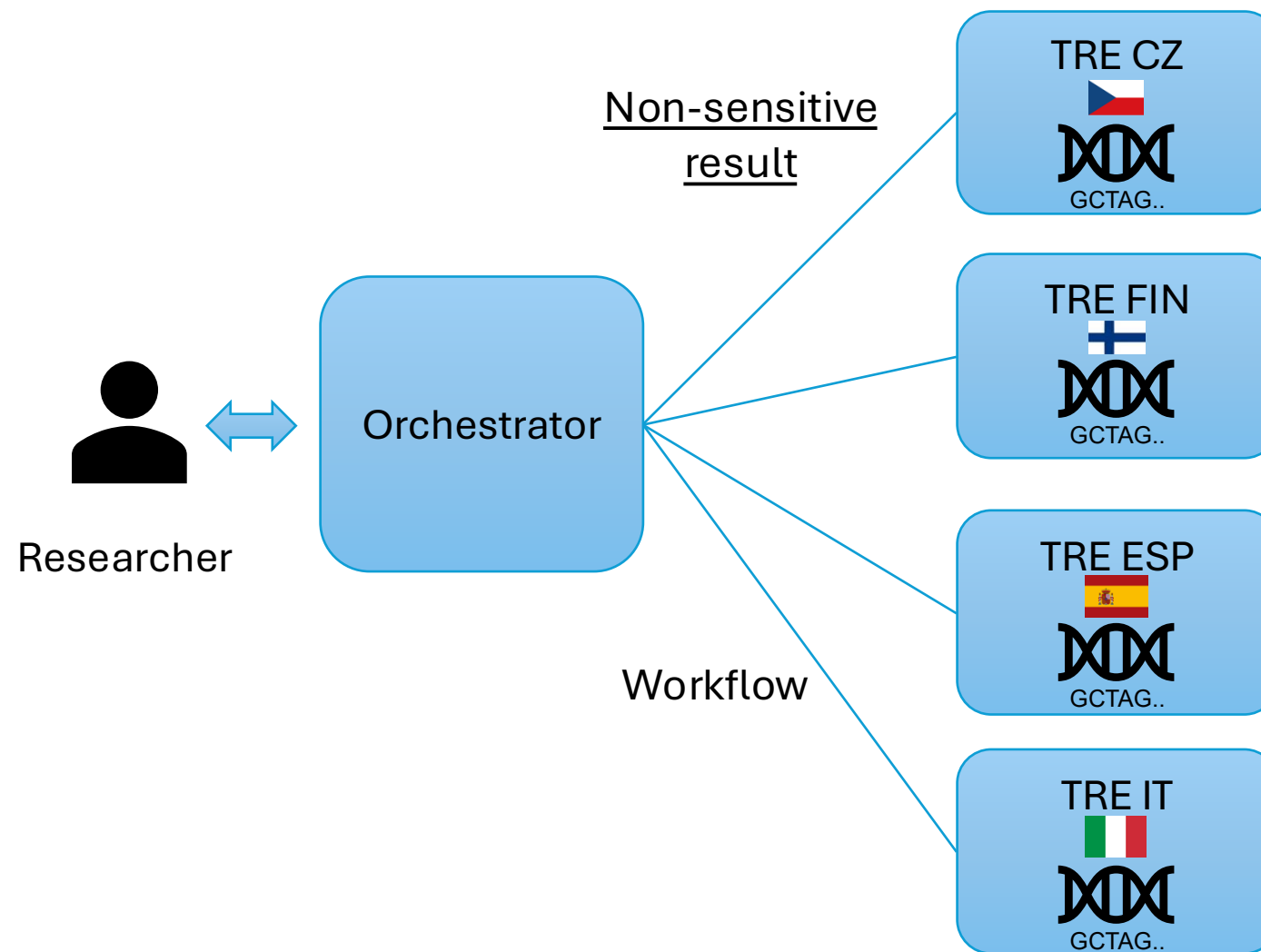
TRE



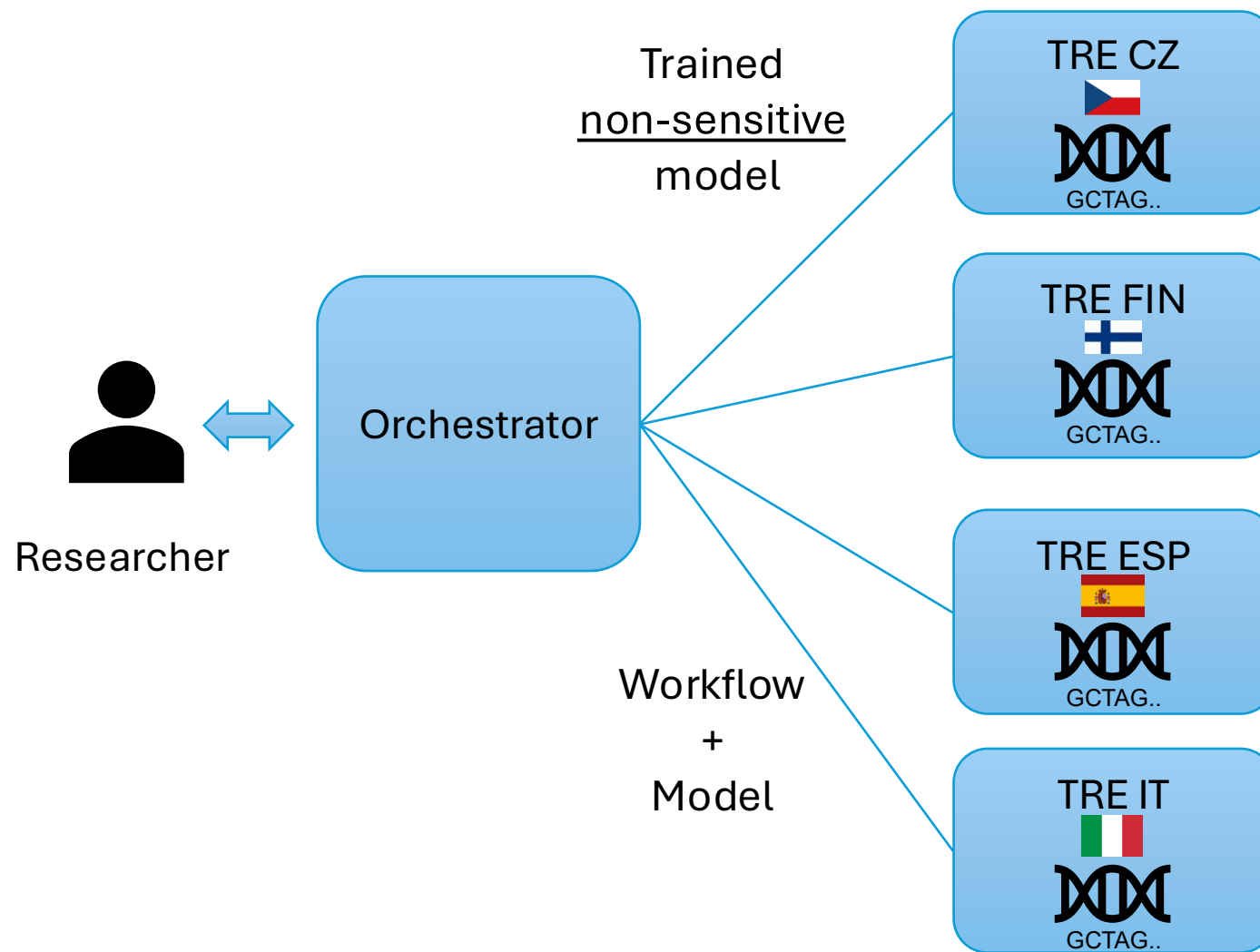
Task/Analysis/Workflow execution

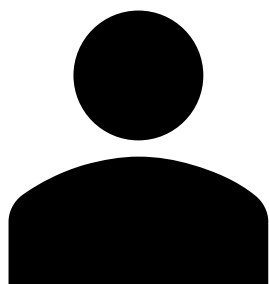


Federated Analysis

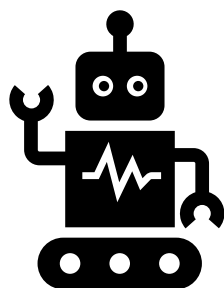


Federated Learning





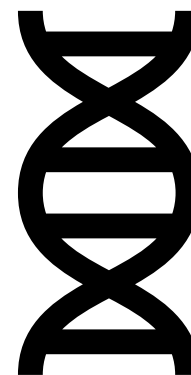
Researcher



AI Agent

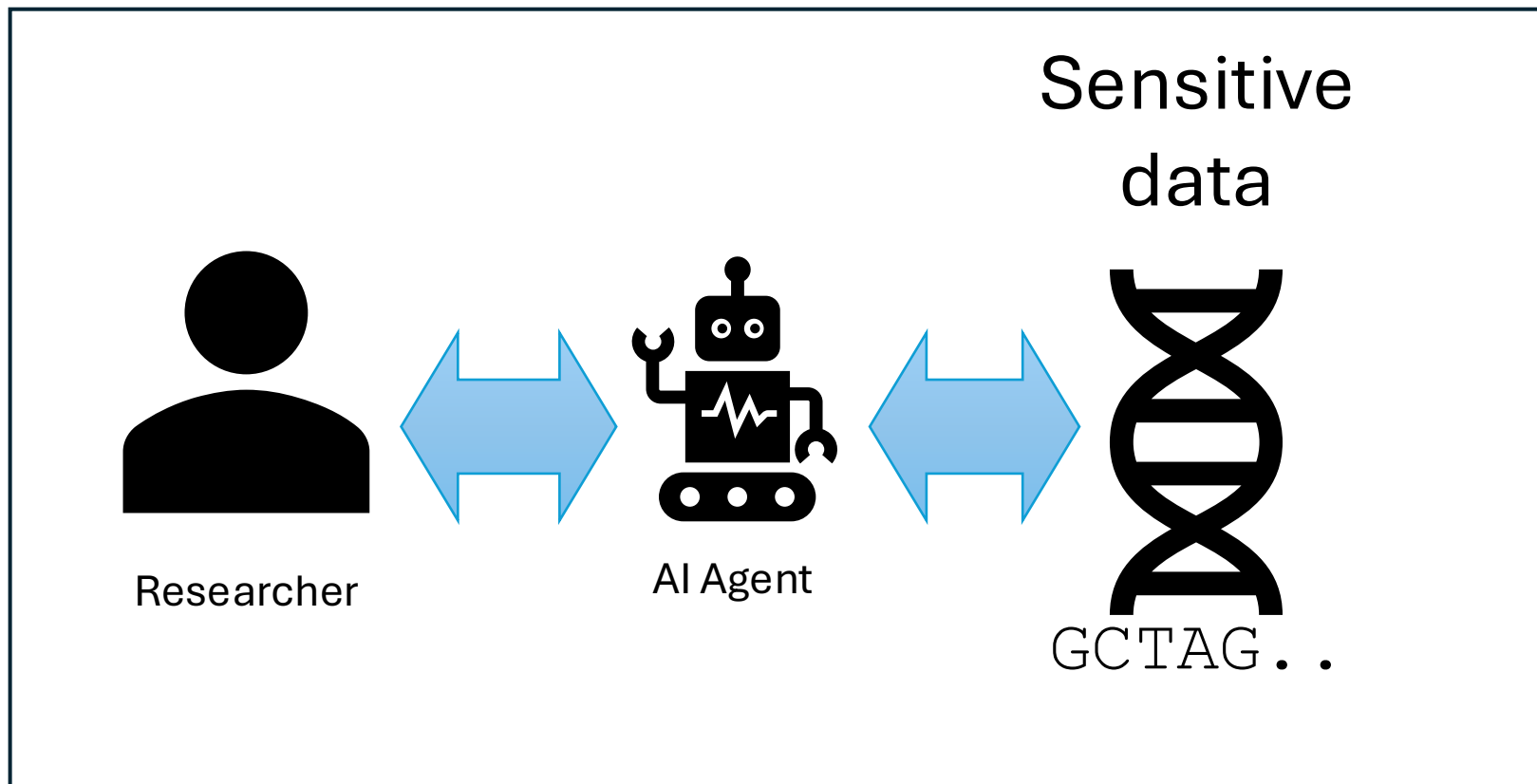
TRE

Sensitive
data



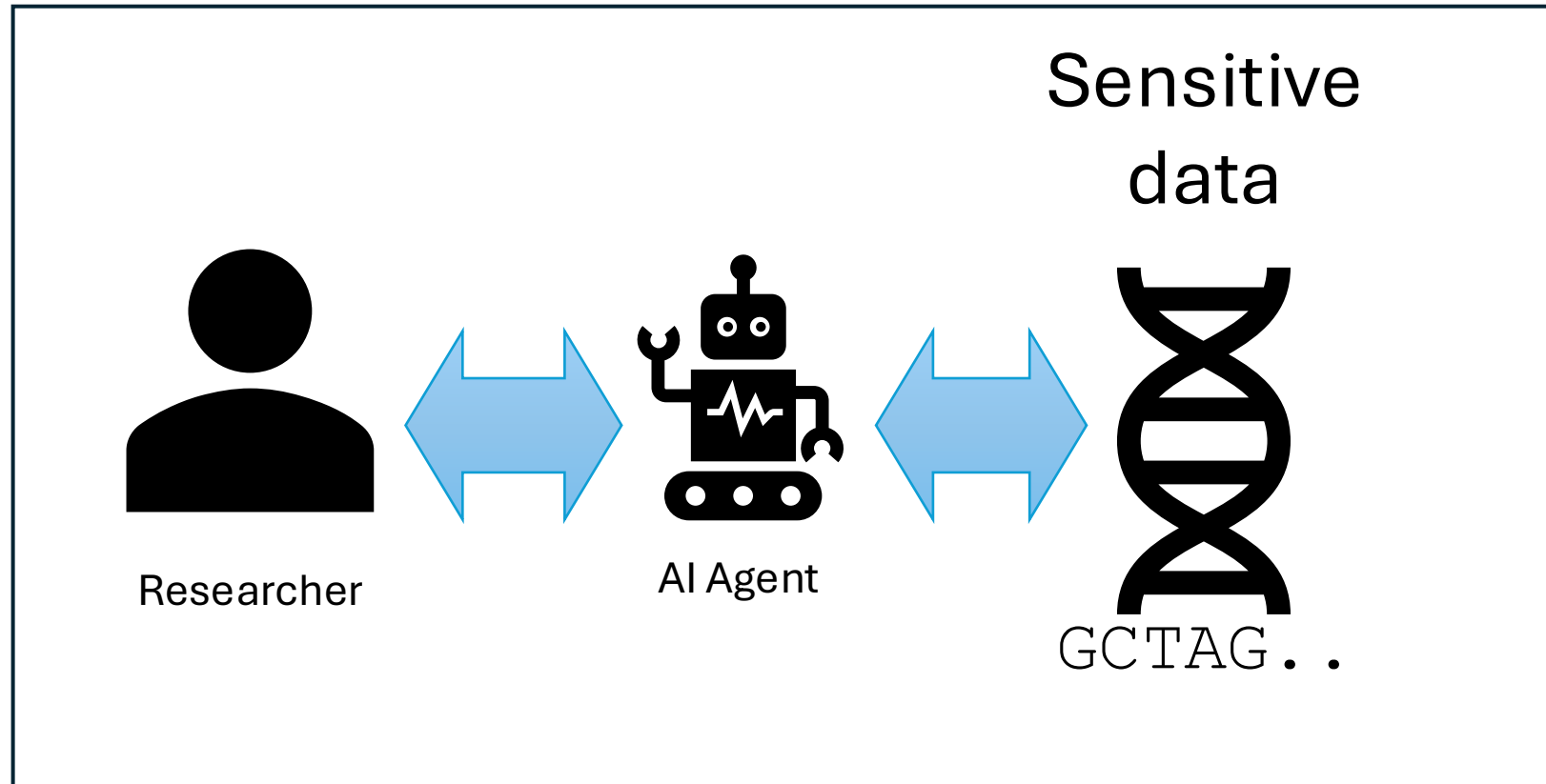
GCTAG..

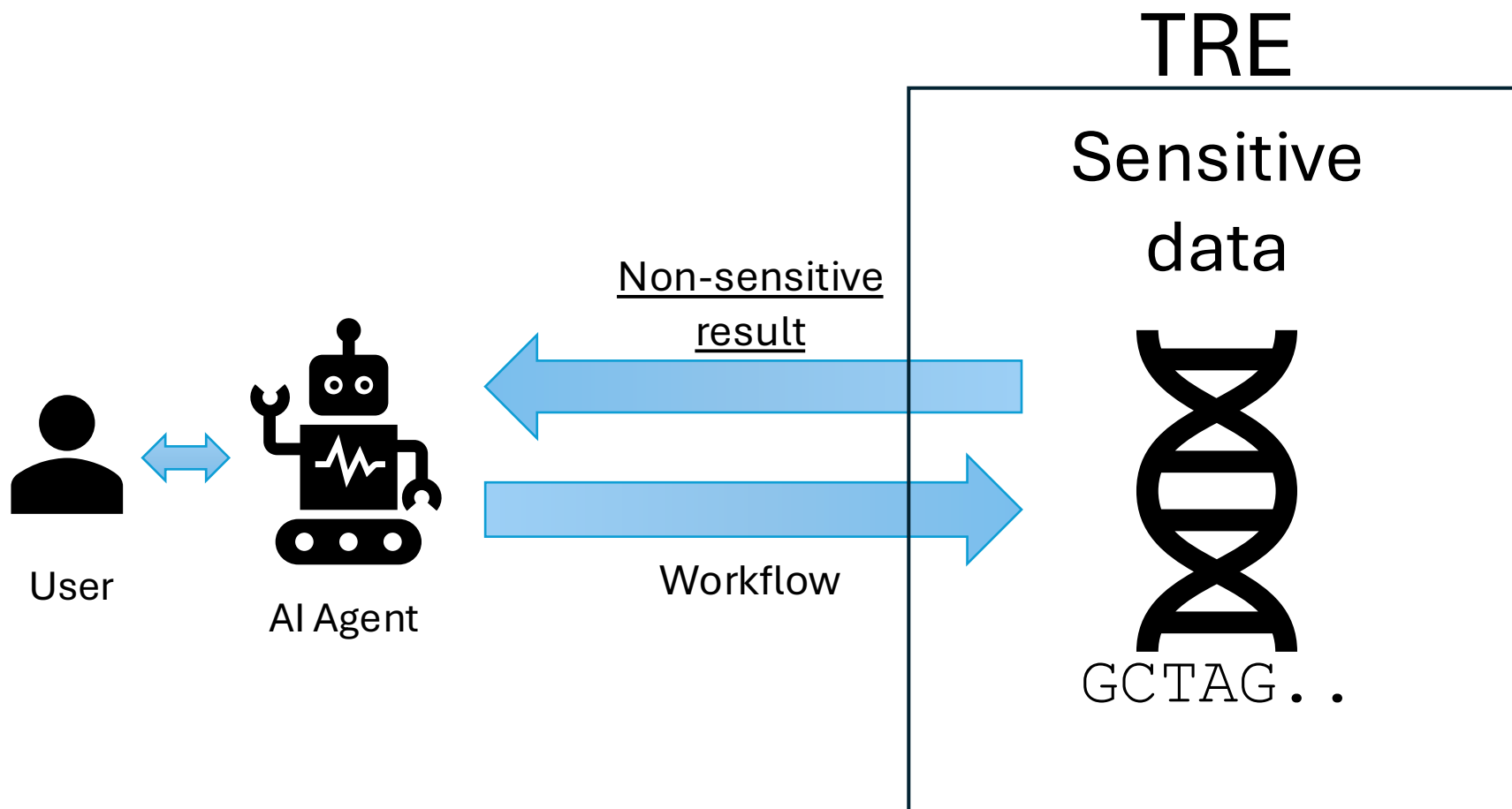
TRE

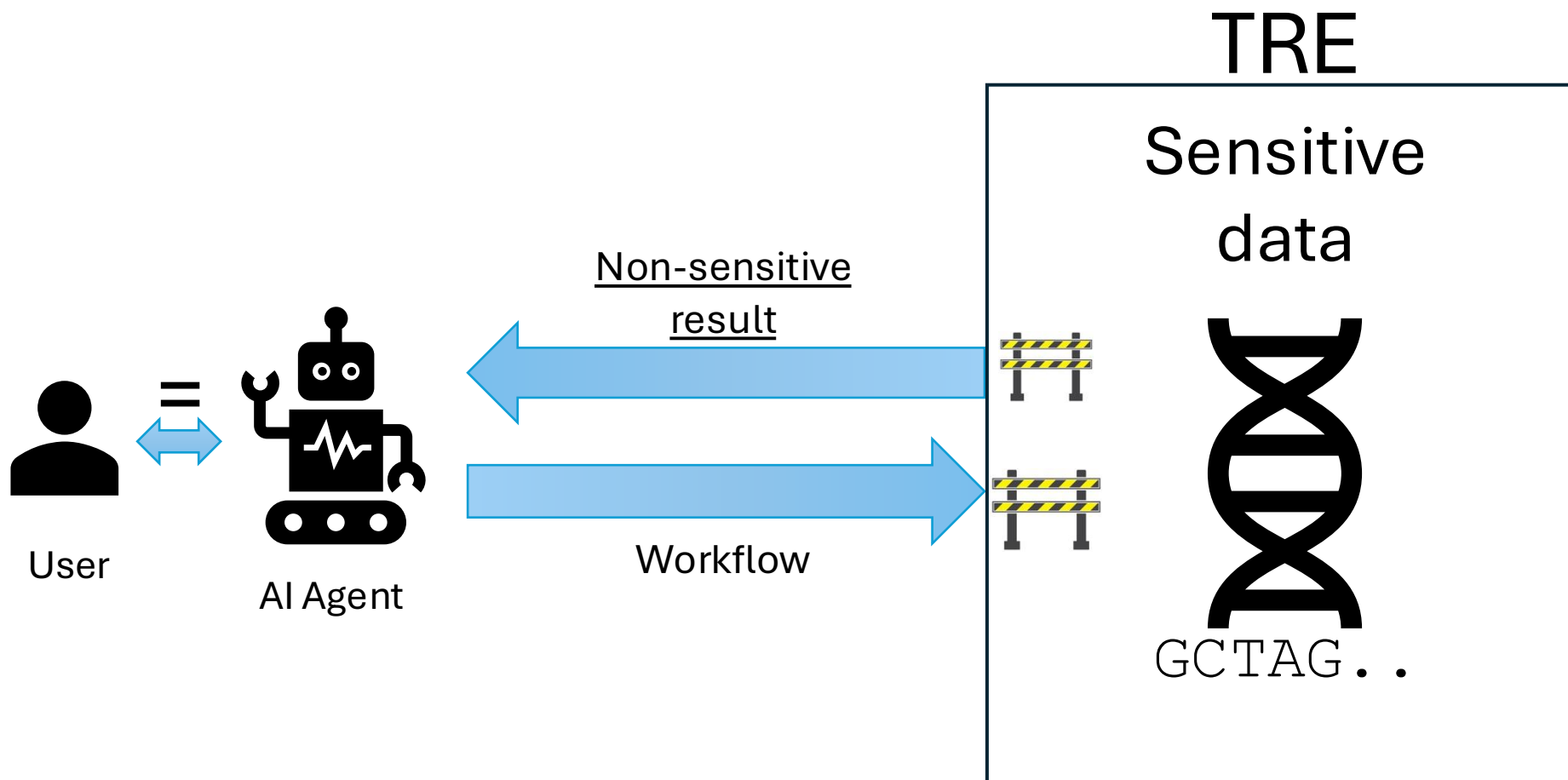


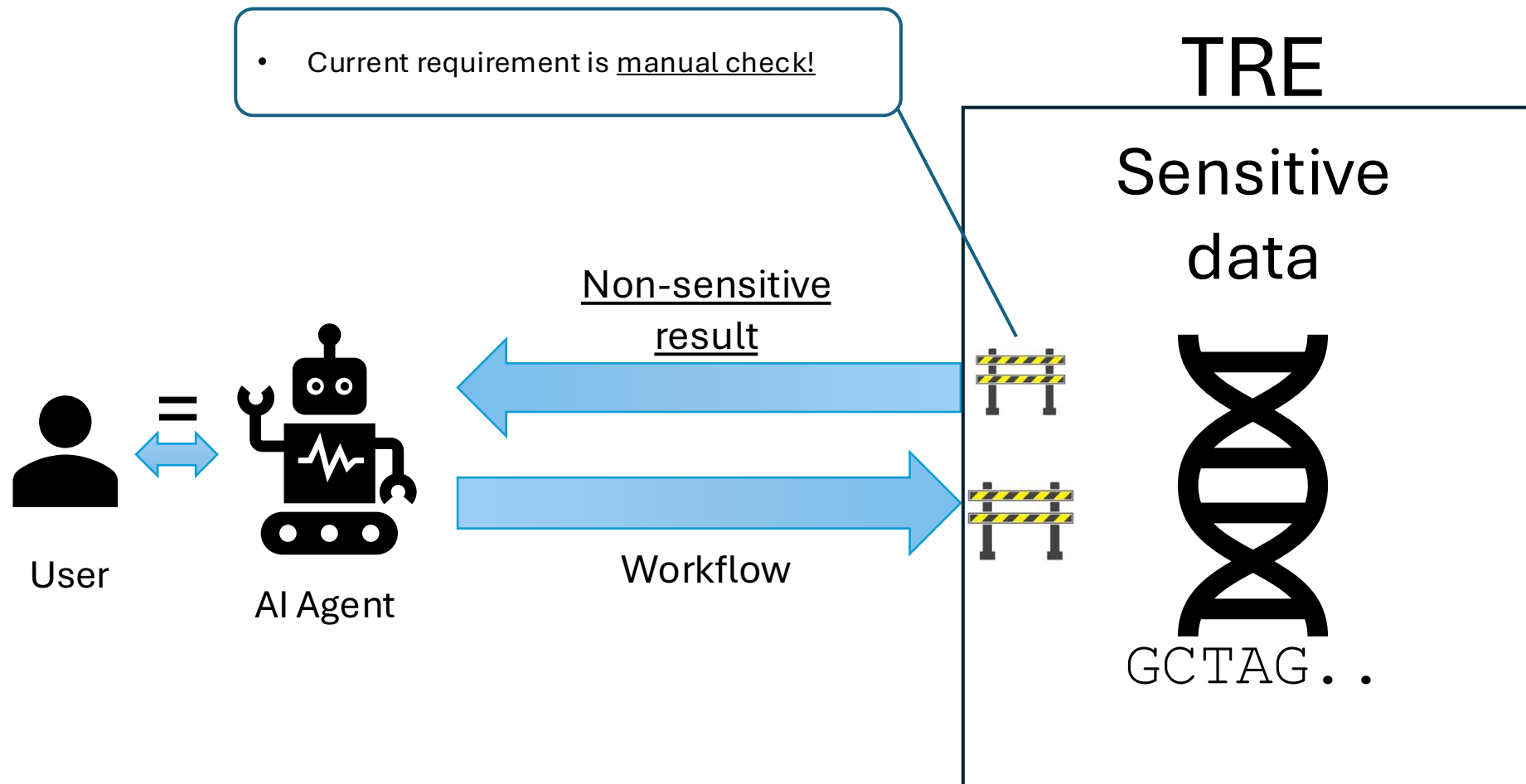
- Open weight models only
- High requirements on TRE – (GPU, Security)

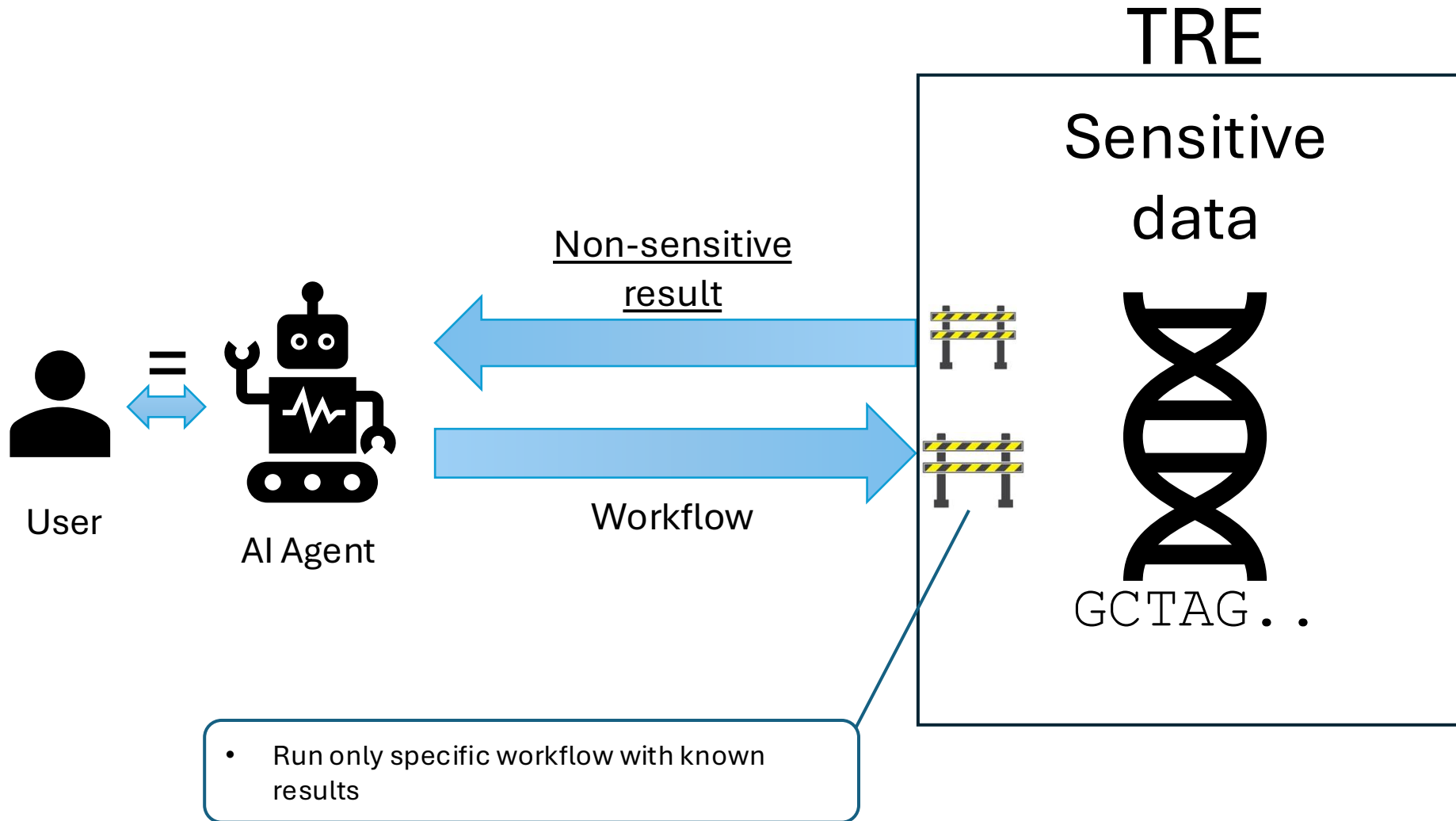
TRE



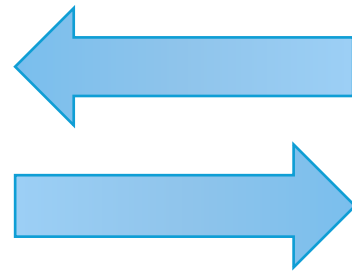
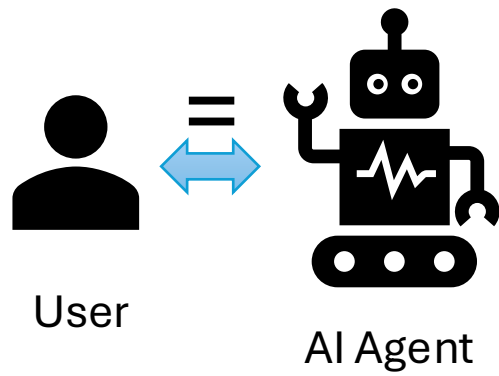








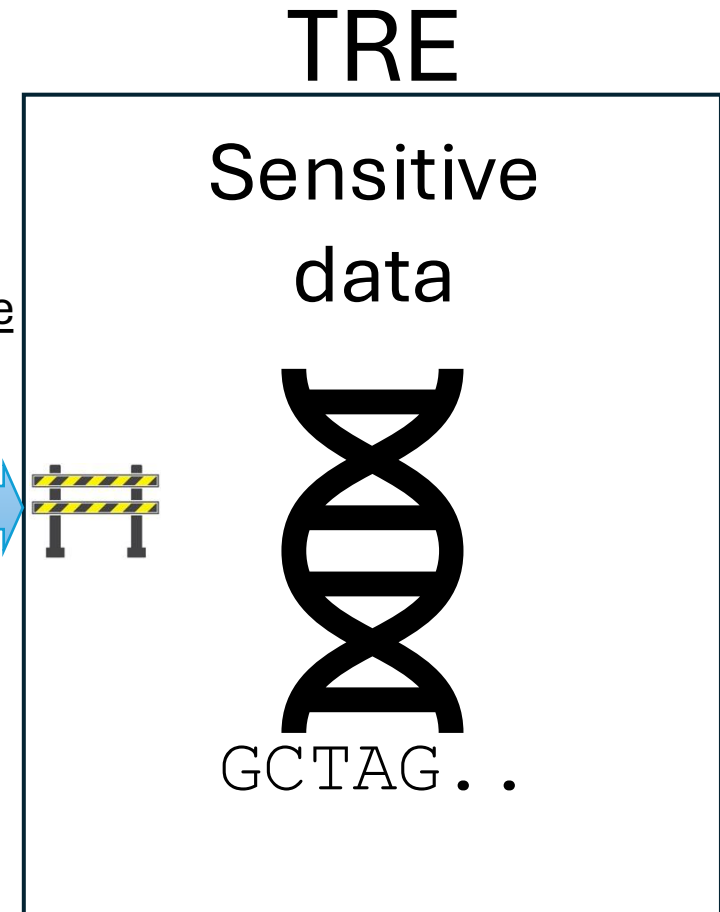
- Require authentication token (LS AAI)
- Allow only pre-approved tasks



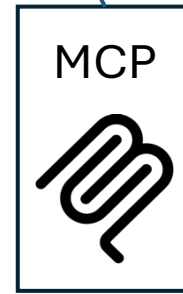
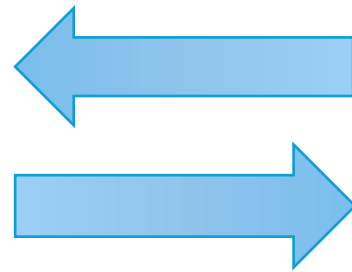
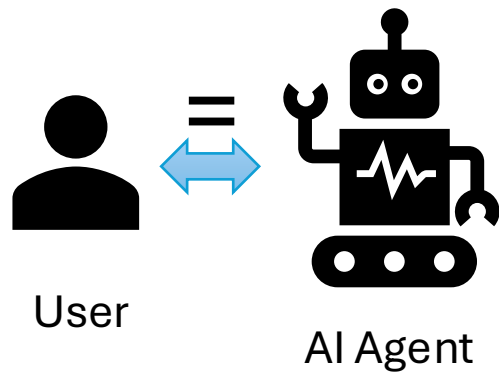
Non-sensitive
result



Workflow

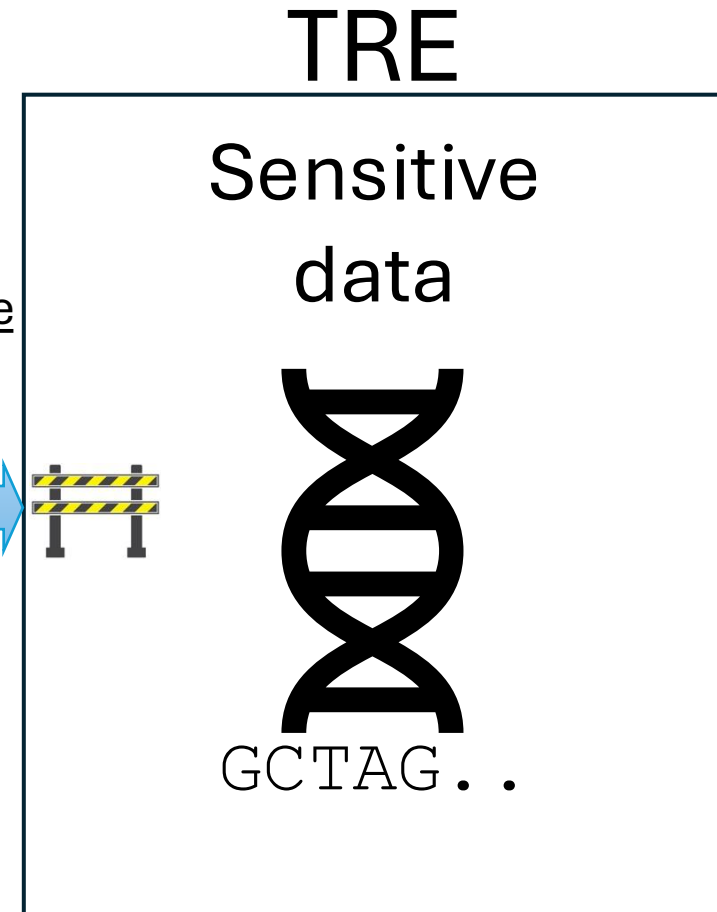


- Require authentication token (LS AAI)
- Allow only pre-approved tasks

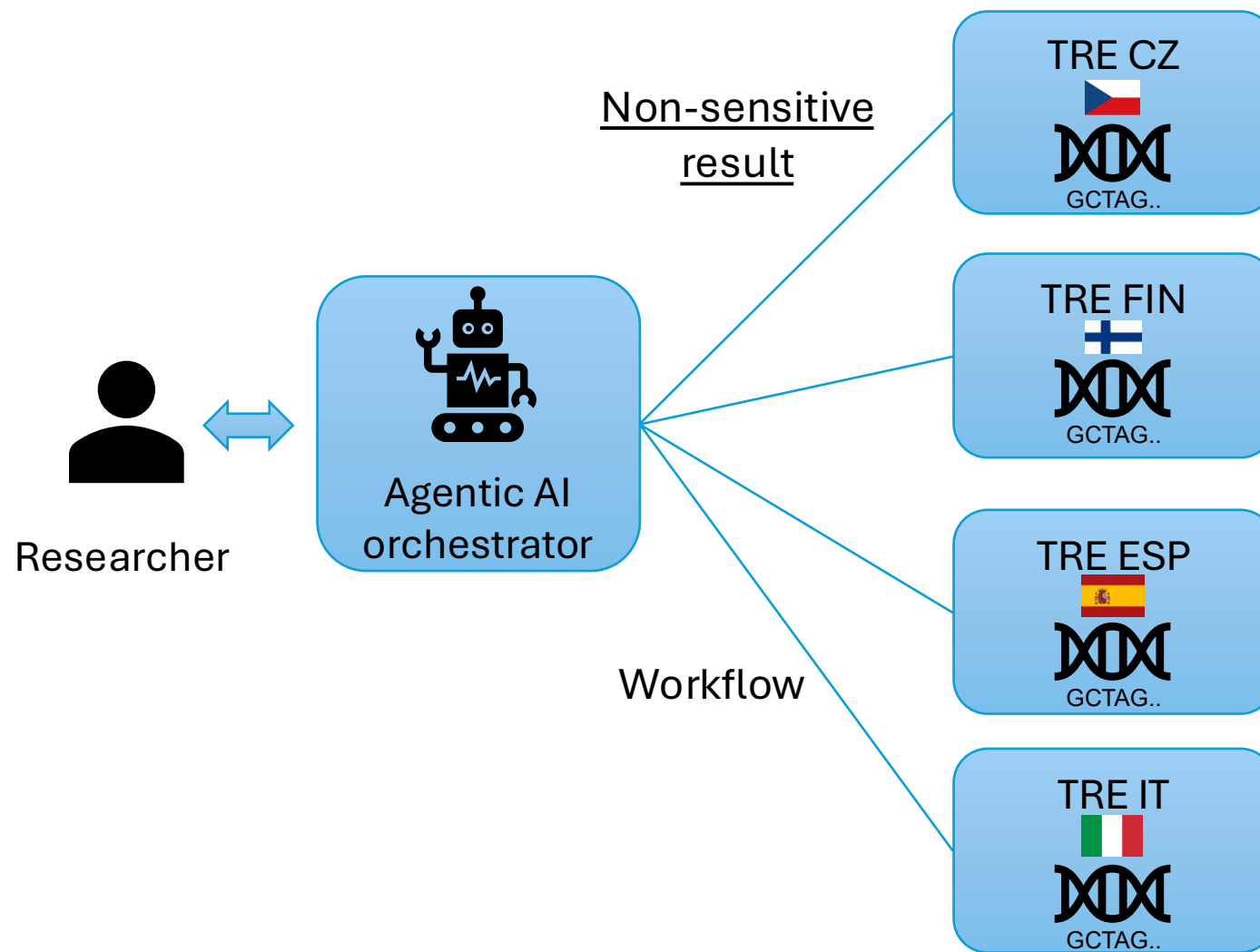


Non-sensitive
result

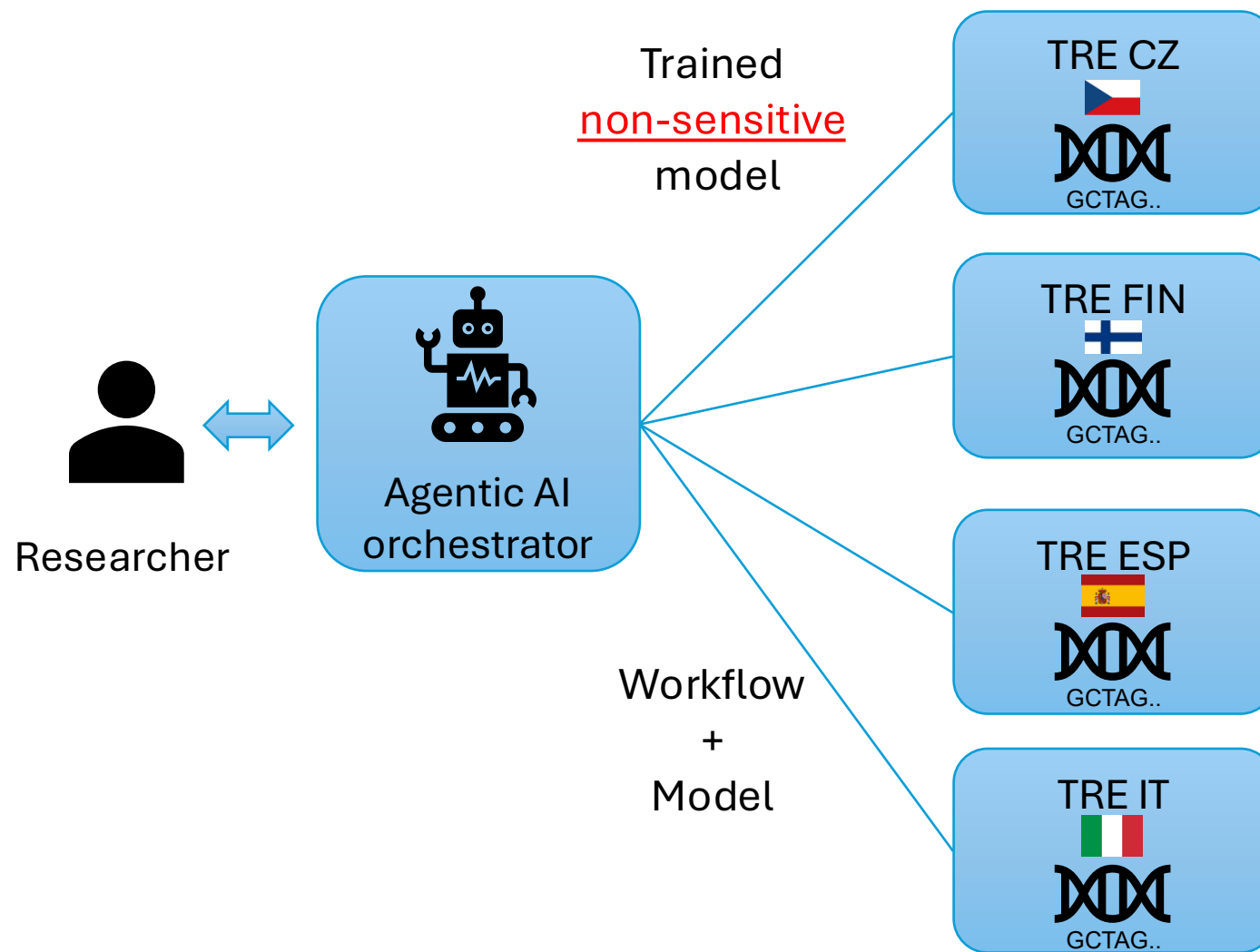
Workflow

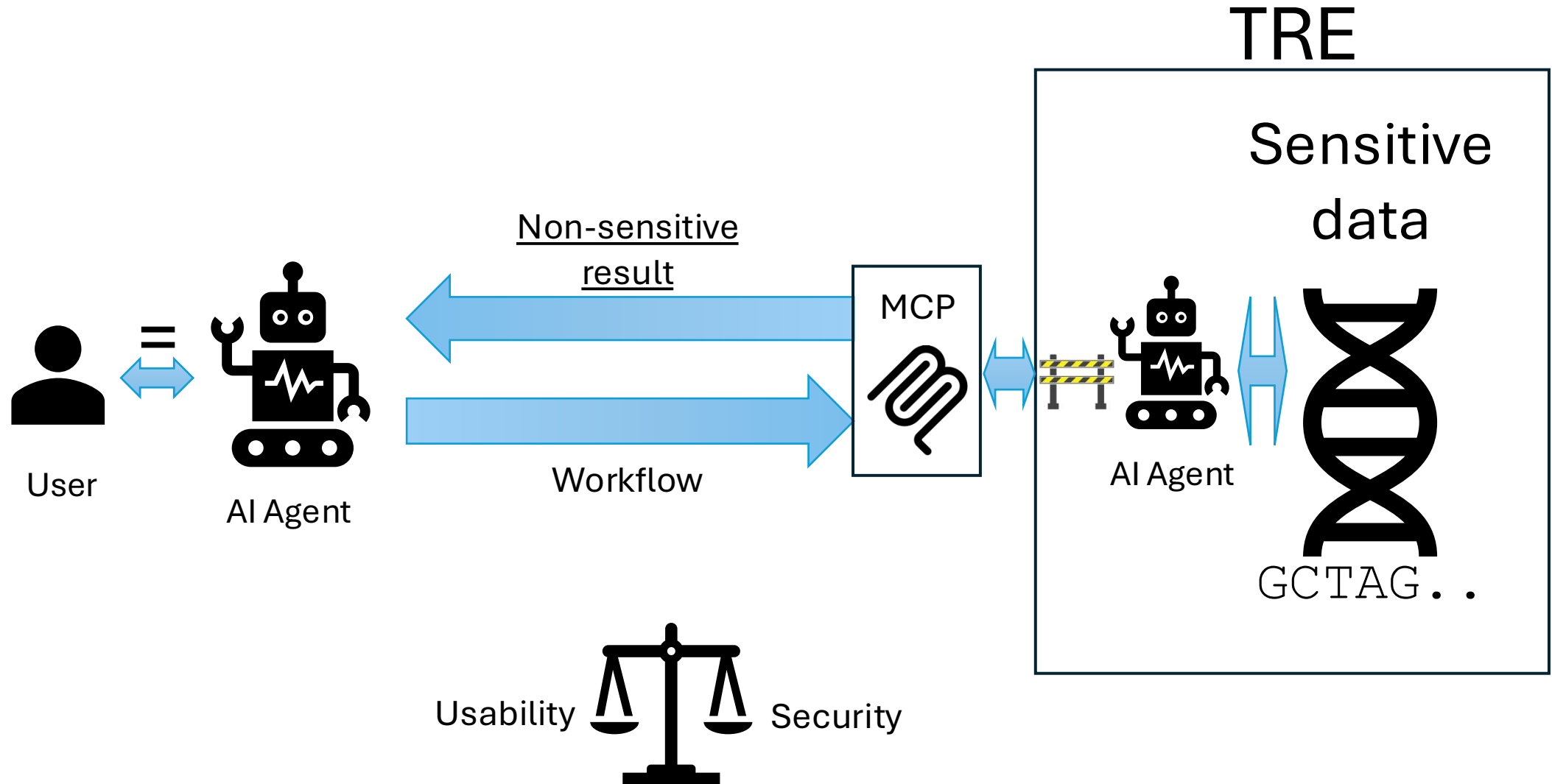


Federated Analysis



Federated Learning





Agentic AI and sensitive data

- Agentic AI runned locally inside TRE
- Agentic AI runned as orchestrator of workflow in TRE (Federated analysis/learning)
- Training of AI models on sensitive data in TRE ("Federated learning") – currently not possible



CEITEC



@CEITEC_Brno

Thank you for your
attention.

vojtech.bystry@ceitec.muni.cz

