APDL

Association pour la Protection des Données au Luxembourg

28 JANUARY 2024

APDL

Association pour la Protection des Données au Luxembourg

ETHICAL AI AND EVOLUTION: DPO & CISO PERSPECTIVE

TUESDAY 28TH JANAURY 2024

MICHAEL HOFMANN

SHARIQ ARIF

PROGRAM

A word of welcome

Conference:

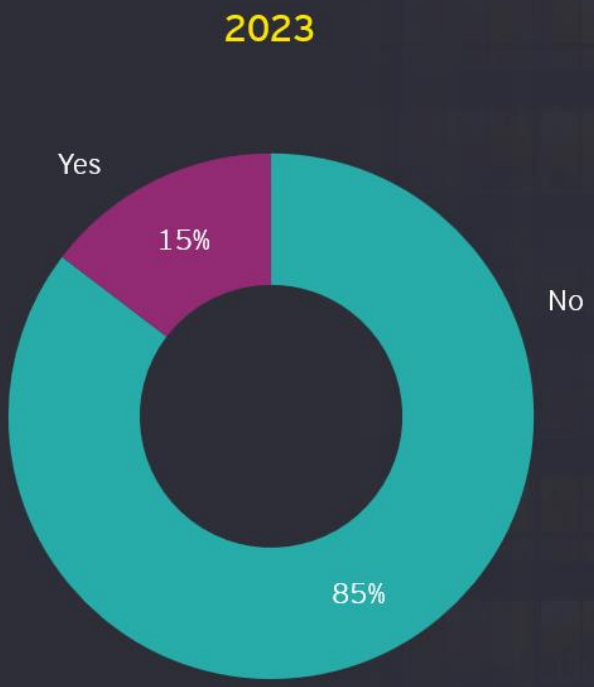
Ethical AI and Evolution

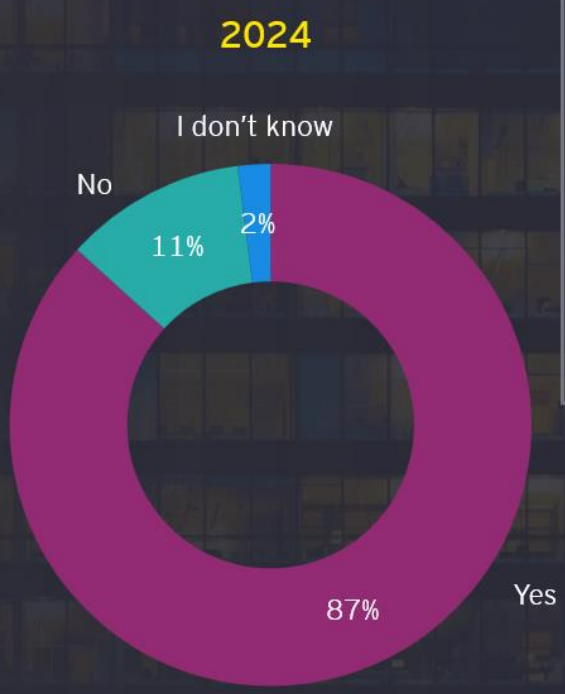
1

KEY TRENDS: STATISTICS

EXAMPLE OF CHANGE IN OPINION

Do you believe GenAI will help drive increased effectiveness and efficiencies within your tax function in the next three years?





Why now?

1. Advances in large language models and neural networks
2. Increased computing power and storage
3. Investment and Innovation

2024 EY TAX AND FINANCE OPERATIONS SURVEY
CONDUCTED ANONYMOUSLY BY OXFORD ECONOMICS

- 1,600 LEADERS (WITH MAJORITY OF CFOS AND VP TAX)
- 32 COUNTRIES

EXAMPLE OF NEWS

AFP

17 janvier 2025 09:37

Apple a temporairement retiré son service d'intelligence artificielle qui résume des faits d'actualité après une plainte de la chaîne publique britannique BBC.

Apple a désactivé, jeudi, l'un de ses **nouveaux outils d'intelligence artificielle (IA) générative, qui permet de recevoir des résumés sur l'actualité**, après des erreurs et une plainte de la BBC en décembre.

Le géant américain des smartphones a commencé à déployer, cet hiver, son système d'IA générative, "**Apple Intelligence**", deux ans après qu'OpenAI a lancé cette vague technologique avec ChatGPT, qui converse avec les utilisateurs et produit des contenus à la demande.

Essentials still are:

- **Trust**
- **Risk**
- **Context**
- **The Trusted AI Solution Lifecycle ?**

APDL
Association pour la Protection des Données au Luxembourg

2

KEY RISKS

RISKS, ETHICS AND CONTROLS

Trust, Transparency & Accuracy

- Accuracy of data inputs and output results
- Over reliance on given information without due diligence on sources.
- Transparency: explain-ability and trace-ability of outputs

Privacy, Surveillance & Security

- Data collection with unclear use; will your sensitive data be made open to the public via the next training round?
- What surveillance applications of GPT will society deem ethical?
- Privacy & Cybersecurity Concerns

Fairness & Bias

- Bias towards certain sub-groups due to public training data
- Bias in model can drive unfair outcomes in some business applications
- Toxicity in responses requires ongoing management

Legal Issues

- Potential Copyrights and IP infringement
- Liability of Use
- GDPR Compliance

3

CAN AI ENABLE THE DPO

APDL
Association pour la Protection des Données au Luxembourg

DATA PROCESSING AGREEMENTS

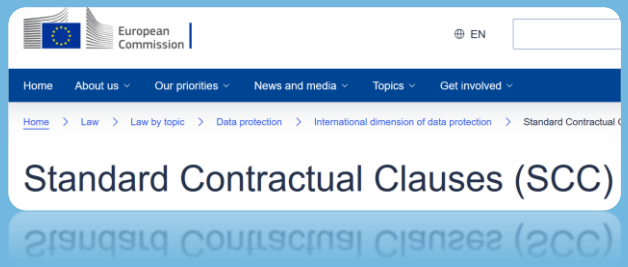
Use Case 1

APDL
Association pour la Protection des Données au Luxembourg

Read and understand the data processing agreement → Read and understand the GDPR text → Add supplementary texts that add more detail

Add supplementary texts that add more detail → Add reasoning layers for tool to effectively compare the data processing agreement with benchmark → Ask it to share inconsistencies → Keep an auditable trace

Transfer Impact Assessment (TIA): the CNIL Consults You on a Draft Guide

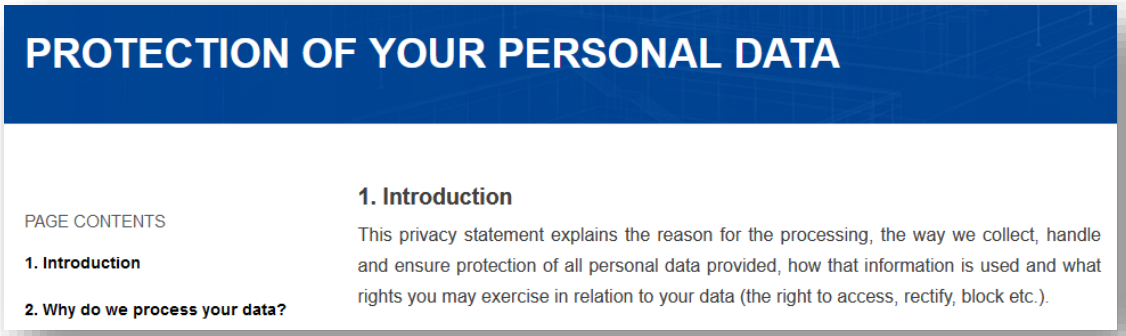


edpb
European Data Protection Board

PRIVACY STATEMENT ASSESSMENTS

Use Case 2

APDL
Association pour la Protection des Données au Luxembourg



PROTECTION OF YOUR PERSONAL DATA

PAGE CONTENTS

1. Introduction

2. Why do we process your data?

1. Introduction

This privacy statement explains the reason for the processing, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you may exercise in relation to your data (the right to access, rectify, block etc.).

Get the tool to check if a privacy statement made is correct

This is a task that can be automated and be provided to the DPO for review

The tool would need to understand the privacy statement –outline the relevant articles of the GDPR that underpin this text (esp. art. 13) and would need to benchmark against both

RECORD OF PROCESSING ACTIVITIES

Use Case 3

APDL
Association pour la Protection des Données au Luxembourg

A GenAI solution have the power to create Record of Processing activities on the basis of :

- Templates from supervisory authorities : e.g. the CNIL
- Procedures, policies within a firm that outline the core processing activities per function
- Data Processing Agreements that outline transfers of personal data
- (automatically) identified and categorized data elements.

DPO elevated to reviewer, voice of the data subject and source of guidance for the business and senior management and liaison point with the business

DATA PROTECTION IMPACT ASSESSMENTS

Use Case 4

APDL
Association pour la Protection des Données au Luxembourg

Input DPIAs frameworks

Nature of activity

Security Measures

Supporting documents to be used can be fed and interpreted by the AI agent

Record of Processing Activity

Contracts

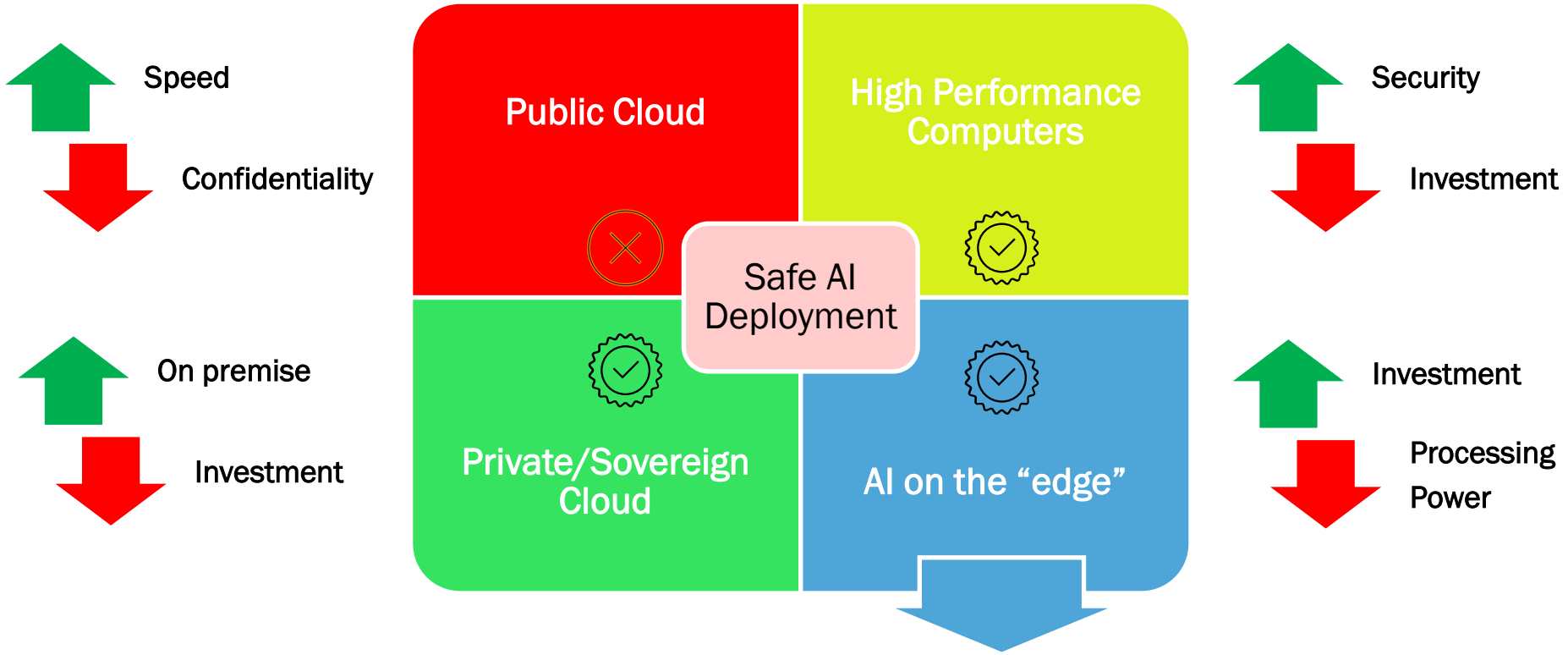
The AI solution would be able to extract the relevant fields from the company's files and prefill the relevant framework

The AI solution populates Data Protection Risk Assessment template

DPO and Controller reviews outputs and re-iterates when presented with updates

AIPD
Analyse d'impact relative à la protection des données (AIPD) 1 : la méthode

PRAGMATIC ETHICAL AI DEPLOYMENT



Data Privacy: data never leaves your premises.

Cost Efficiency: local deployment can offer than cloud services

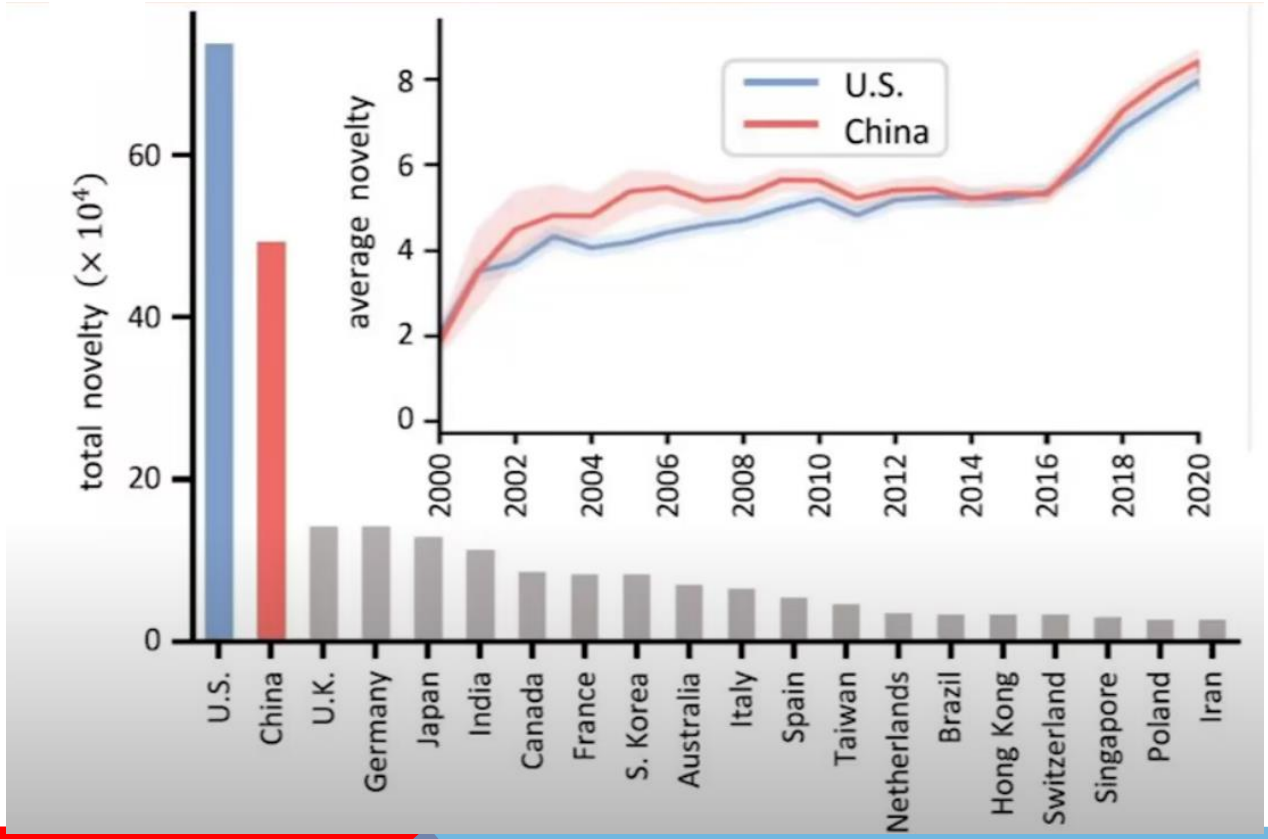
Customization: allows fine-tuning making models more relevant.

Latency Reduction: no reliance on internet-based APIs

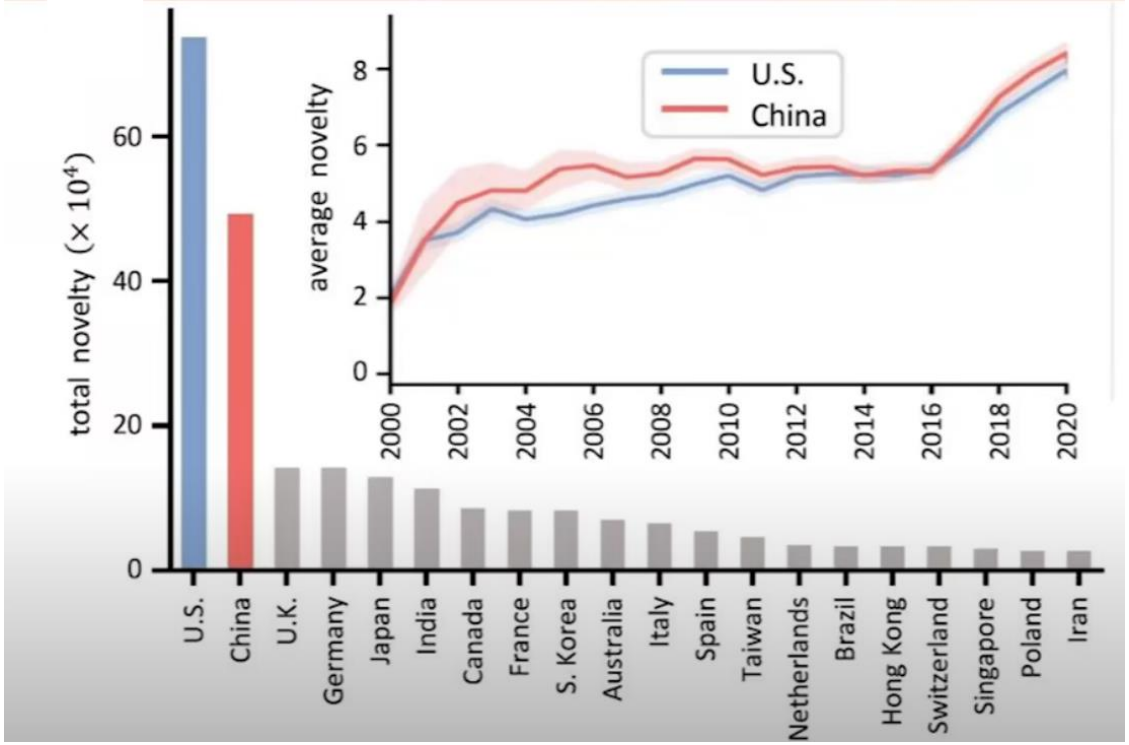
4

EVOLUTION

EVOLUTION


total novelty (× 10⁴)
0
20
40
60
U.S.
China
U.K.
Germany
Japan
India
Canada
France
S. Korea
Australia
Italy
Spain
Taiwan
Netherlands
Brazil
Hong Kong
Switzerland
Singapore
Poland
Iran
average novelty
0
2
4
6
8
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
U.S.
China

EVOLUTION



Open AI training: 5 billion USD

- Propriety model – Black Box
- Massive financing and data centers
- Most advanced chips
- Heavy energy costs

Stargate: 100 - 500 billion USD

Deepseek R1 zero

- Open source model
- AI training: 5 million USD
- Performance, Chain of Thought COT
- Cheaper, less power
- Transparency & Censorship

OpenAI o1: $60.00 per 1M output tokens
DeepSeek R1: $2.19 per 1M output tokens

US - CHINA AI BATTLE

Deepseek R1 zero is an open AI, developed in China with High Performance, Transparency and Minimal Cost

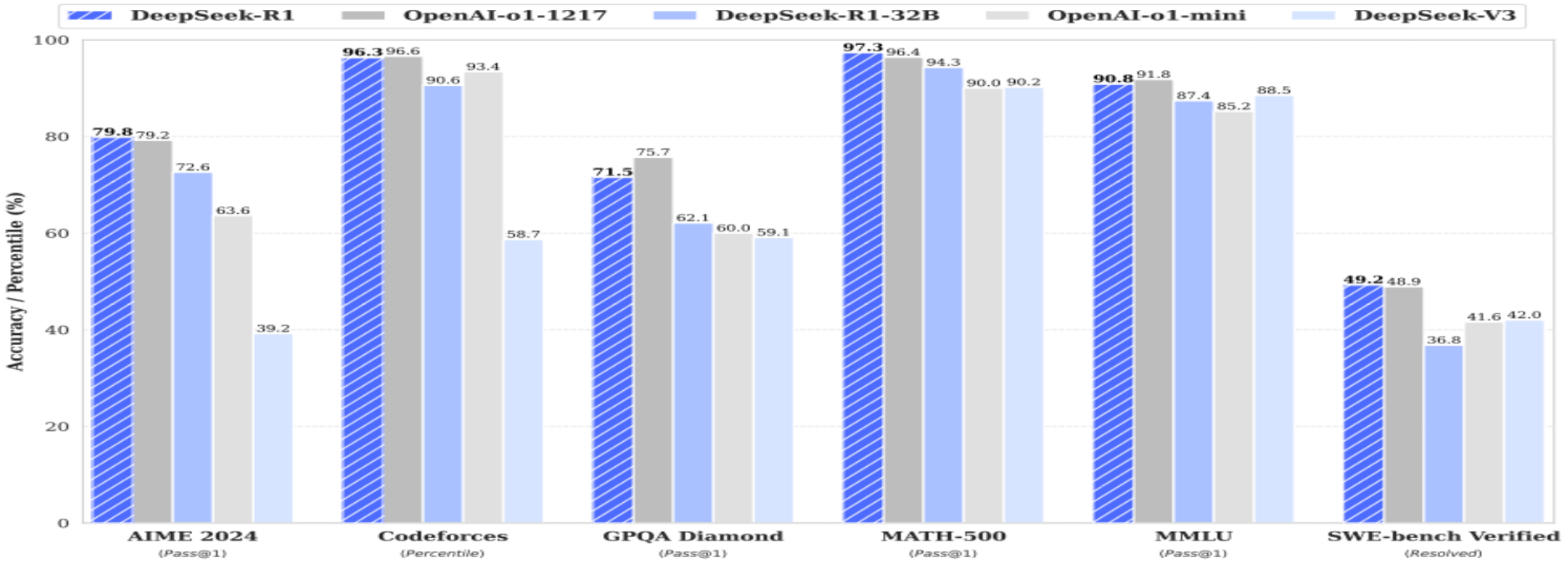
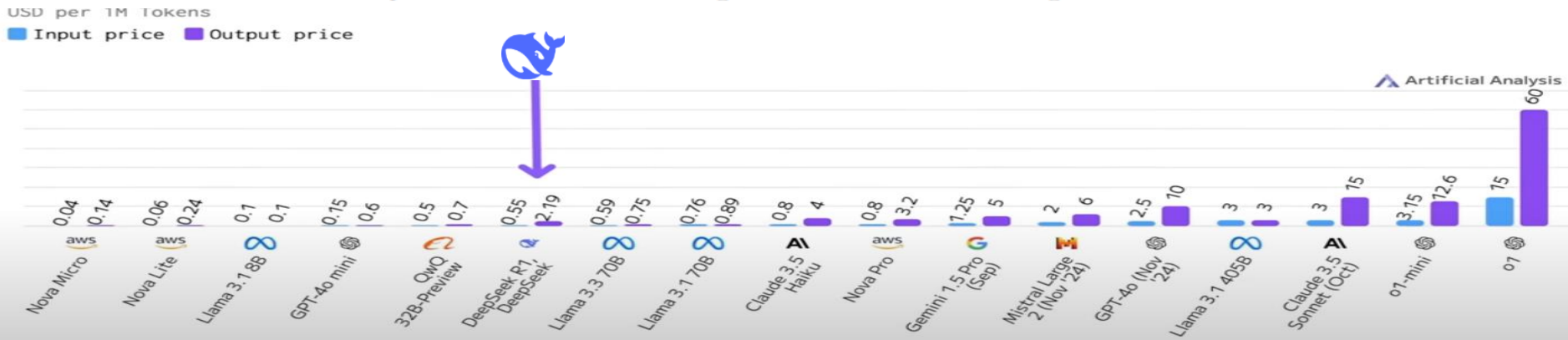


Figure 1 | Benchmark performance of DeepSeek-R1.

arXiv:2501.12948v1 [cs.CL] 22 Jan 2025



BENEFIT OF CERTIFICATION GDPR & AI

AIA Cert

AIA-Cert is a comprehensive and efficient certification scheme to assess and certify compliance with the main obligations of major AI regulations, including:

- the European Artificial Intelligence Act,
- the OECD Principles on artificial intelligence, and
- the Convention of the Council of Europe on artificial intelligence.

Developed by the European Centre for Certification and Privacy in charge of Europrivacy, the European Data Protection Seal recognized by all EU and EEA National Authorities.

➔ **Regulatory compliance with:**

- **EU AI Act**
- **OECD Principles**
- **CoE Framework Convention on AI**

aiacert.com

5

THANK YOU!

APDL
Association pour la Protection des Données au Luxembourg

Association à but non lucratif créée par et pour les professionnels de la protection des données au Luxembourg

Rejoignez-nous sur www.apdl.lu