

AITHYRA

AI Training

**Empowering Innovation,
Responsibly**

Welcome to AITHYRA's mandatory AI training.



Our goal: To empower you to use powerful AI tools confidently, ethically, and securely.



This training will cover our Acceptable Use Policy, your responsibilities, and give you and overview about the current tools.

The Opportunity and the Responsibility



The Opportunity: AITHYRA provides cutting-edge AI tools (OpenWebUI, models from OpenAI, Google, Anthropic, etc.) to accelerate scientific and administrative work.



The Responsibility: As an Austrian research institute, our use of AI is governed by strict EU regulations:

EU AI Act: Regulates AI systems based on risk.

GDPR: Protects all personal data.

NIS2: Sets high cybersecurity standards.



Compliance is a shared responsibility, and this training is a mandatory and documented requirement under the EU AI Act.

The 6 Core Principles of AI Use



Use the Right Tool for Your Data.



You are the Pilot, Not the Passenger.



Uphold Absolute Research & Academic Integrity.



Innovate Sustainably.



Respect IP and Foster Our Entrepreneurial Culture.



Assess High-Risk Innovation (EU AI Act).

Principle #1: Use the Right Tool for Your Data

Data Classification is Your First Step

- Our primary tool is "AITHYRA Chat," which offers access to on-premises and external API models.
- AITHYRA has enterprise agreements with external providers (Google, OpenAI, etc.) ensuring your data is NOT used for their model training.
- However, you **must** classify your data and choose the appropriate model location.

Data Sensitivity Level	Permitted Model Location	Key Action
Public / Non-sensitive	On-premises or External API	No restrictions
Internal (non-sensitive)	On-premises or External API	No restrictions
Personal Data (GDPR)	On-premises preferred	Anonymize data; Consult DPO if external API is needed
Special Categories (Health, HR)	On-premises ONLY	Mandatory anonymization; DPO approval required for any exception

Principle #2 & #3: Your Accountability & Research Integrity

You Are Responsible for Your Work

- **You are the Pilot:** AI tools can (will!) make mistakes ("hallucinate"). You are ultimately responsible for the accuracy, quality, and integrity of any work you produce with AI assistance.
 - Always review and verify AI-generated text, code, or data before use.
 - This aligns with the AI Act's requirement for meaningful human oversight.
- **Uphold Research Integrity:**
 - **No Plagiarism:** Presenting AI-generated content as your own original thought is plagiarism.
 - **Disclose & Cite:** You must transparently disclose which AI tools were used in publications and reports. Cite the models and software as you would any other scientific instrument.
 - **Ensure Reproducibility:** Keep records of prompts and model versions to allow for verification.

Principle #4: Innovate Sustainably

Be Efficient with Our Resources

- AITHYRA is committed to Green IT and responsible resource management.
- **Choose Efficient Models:** Don't use a massive external model to proofread an email when a smaller, or an on-premises model is sufficient. Document the use of larger models in your project records.
- **Minimize Waste:** Write efficient code to minimize computational waste on our HPC resources. We track the carbon footprint of compute/AI workloads.

Principle #5: Respect IP & Foster Entrepreneurial Culture

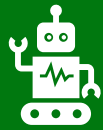
- **Ownership of Output:** generally, work created with AI tools during employment belongs to AITHYRA under your employment agreement.
- **Innovation Strategy:** We strongly encourage an entrepreneurial culture and spin-offs.
- **Start-Up Guidance:** If you are planning a start-up based on AI-assisted work, you **must** consult Academic Affairs early to clarify IP rights and transfer possibilities.

Principle #6: Assessing High-Risk Innovation (EU AI Act)

Consult Before You Build

- The EU AI Act places strict requirements on "high-risk" AI systems.
- **What is High-Risk?** Systems used in areas like medical diagnostics, recruitment, employee evaluation, or controlling critical lab infrastructure.
- **Your Obligation:** If you are **developing a novel AI system** for a high-risk area, you **must consult** with IT/Scientific Computing and Academic Affairs early in the process to ensure compliance.
- This does not apply to the general use of AITHYRA's existing, approved tools for research.

Practical Compliance in Your Daily Work



Data Protection Impact Assessments (DPIA): A DPIA is mandatory before deploying any AI system likely to pose a high risk to individuals' rights, such as those used for profiling or automated decisions.



Data Minimization: Only process data that is strictly necessary. Anonymize or pseudonymize data whenever possible, especially for high-risk or sensitive datasets.



Cybersecurity & Incident Reporting: Report any suspected AI errors, bias, security incidents, or data breaches immediately. Under NIS2, significant incidents must be reported to authorities within 24 hours.

Support & Proposing New Tools

We're Here to Help

- **Your Support System:**
 - For technical questions or policy clarifications, contact IT/Scientific Computing.
 - For questions on personal data, GDPR, and DPIAs, consult the **Data Protection Officer (DPO)**.
- For high-risk projects or ethical concerns, involve the **Ethics Committee** and **Academic Affairs**.
- **Evolving Our Toolkit:** If you find a new tool that could benefit AITHYRA, propose it to IT/Scientific Computing for evaluation and integration.

Let's Practice!

Scenario 1: The Health Data Dilemma

Scenario:

A scientist is analyzing anonymized patient survey data for a research paper. The data contains sensitive health information. She finds that an external API model from one of our partners gives much better results than the on-premises models available in "AITHYRA Chat."

What should they do next?

- **(A)** Go ahead and use the external API. The data is anonymized, so it's safe.
- **(B)** Use the on-premises model even if the results are worse, because the policy is absolute.
- **(C)** Consult with the Data Protection Officer (DPO) to review the case, confirm the necessity, and ensure all compliance measures are met *before* using the external API.
- **(D)** Email the IT department to ask for their opinion.

The Correct Answer is (C): Consult with the Data Protection Officer (DPO).

Why?

- **Principle #1: Use the Right Tool for Your Data.** The policy states that for highly sensitive information like health data, you **must prioritize on-premises models**.
- An exception is possible if external models are required for performance, but this requires a formal consultation process.
- The DPO is the designated expert to assess GDPR compliance, evaluate the risks, and approve the exception, ensuring it is documented correctly. Anonymization is a great first step, but it doesn't bypass the need for consultation with this type of data.

Let's Practice!

Scenario 2: The Postdoc and the Publication

Scenario:

A postdoc, uses an AI model via "AITHYRA Chat" to generate a first draft of his literature review and to polish the grammar of his entire manuscript. He edits the generated text heavily for accuracy and flow. In his final manuscript submitted for publication, he doesn't mention the AI tool.

Question for the Audience:

Is their action compliant with AITHYRA policy?

(Show of hands: Yes or No)

The Answer is: NO, this is not compliant.

Why?

Principle #3: Uphold Absolute Research & Academic Integrity.

- **Attribution is Mandatory:** Presenting AI-generated content as your own original thought without attribution is considered plagiarism.
- **Disclosure is Required:** The policy is explicit: "In publications and reports, you must transparently disclose which AI tools were used and for what purpose".
- **How to Comply:** The postdoc should add a sentence in his methods or acknowledgments section, such as: *"Manuscript text was edited for clarity and grammar using Claude 3 Opus via AITHYRA Chat."*

Let's Practice!

Scenario 3: The High-Risk Idea

Scenario:

HR & IT are excited about building a new, internal AI tool. The tool's purpose is to screen student applications for AITHYRA's summer internship program by automatically ranking candidates based on their CVs.

Question for the Audience:

What is the team's FIRST and MOST IMPORTANT step, according to AITHYRA policy?

The First Step: Consult with DPO/ IT/Scientific Computing/Academic Affairs.

Why?

Principle #6: Assess High-Risk Innovation (EU AI Act).

- This is not general use of an existing tool; it is the **development of a novel AI system**.
- The use case—**recruitment**—is explicitly defined as a "high-risk" area under the EU AI Act.
- Therefore, the team **must consult** with the designated governance bodies *early in the process* to ensure a full risk assessment and compliance plan is in place before they begin development.

Quickfire Round: Who Do You Call?

Match the situation to the correct AITHYRA contact point.

Your Situation...	Who do you call? (DPO, IT/SciComp, Academic Affairs)
1. "I need to process a dataset with personal data and I'm unsure about the right model."	DPO
2. "I found an amazing new AI tool online that would be great for my team."	IT / Scientific Computing (to propose it)
3. "My research has led to a great idea for a start-up company."	Academic Affairs
4. "I suspect an AI model is producing biased results in my analysis."	IT / SciComp (for technical issues) and the DPO / Ethics Committee (for bias/risk)

01

You Are Responsible: Always verify AI outputs. You are the final authority.

02

Classify Your Data First: This determines which tool you can use.

03

On-Premises for Sensitive Data: Prioritize on-premises models for personal and sensitive data. Consult the DPO for exceptions.

04

Disclose and Cite: Be transparent about your use of AI in all research outputs.

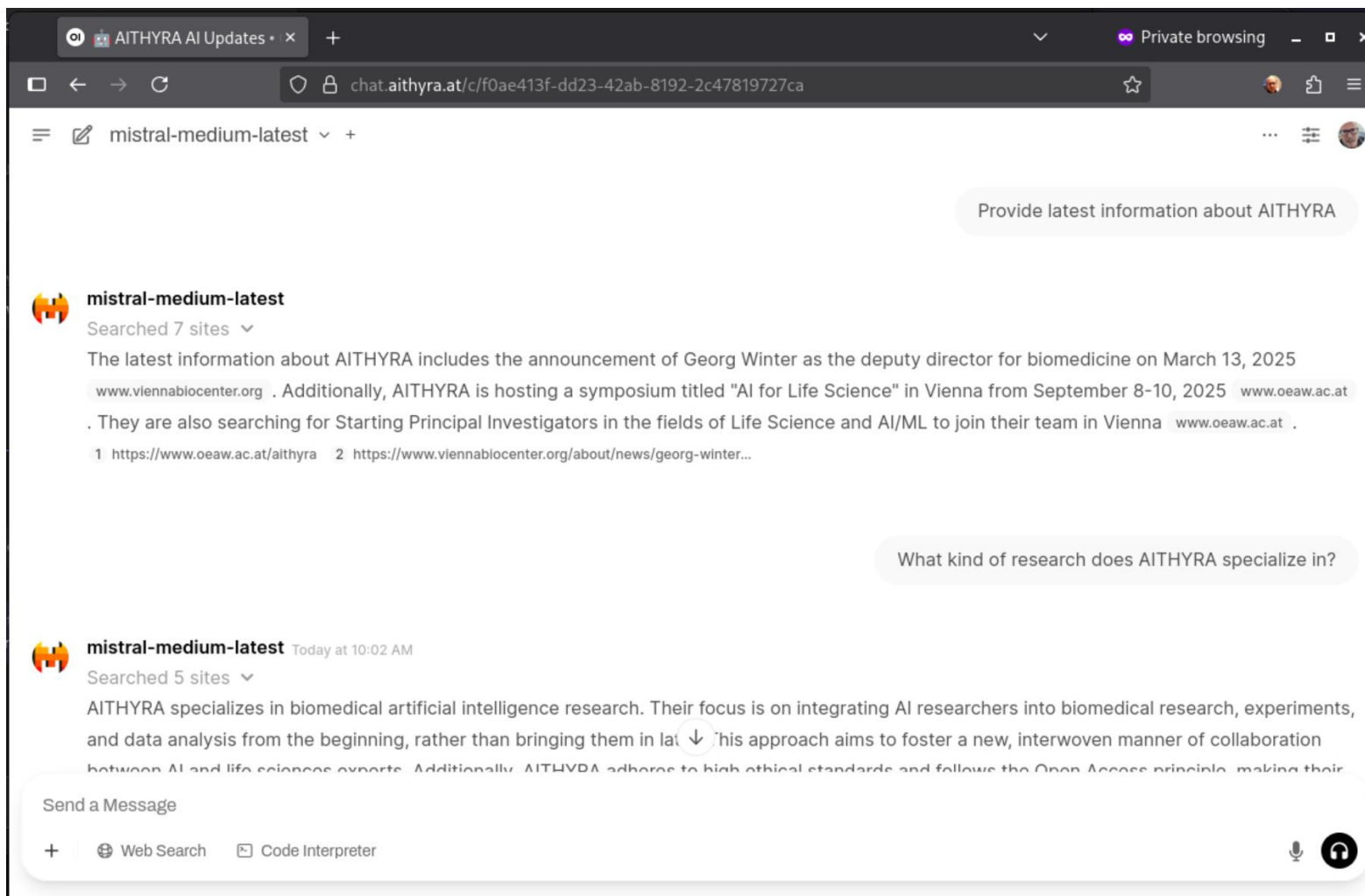
05

When in Doubt, Ask: Consult with IT, the DPO, or Academic Affairs before starting a high-risk project or when handling sensitive data.

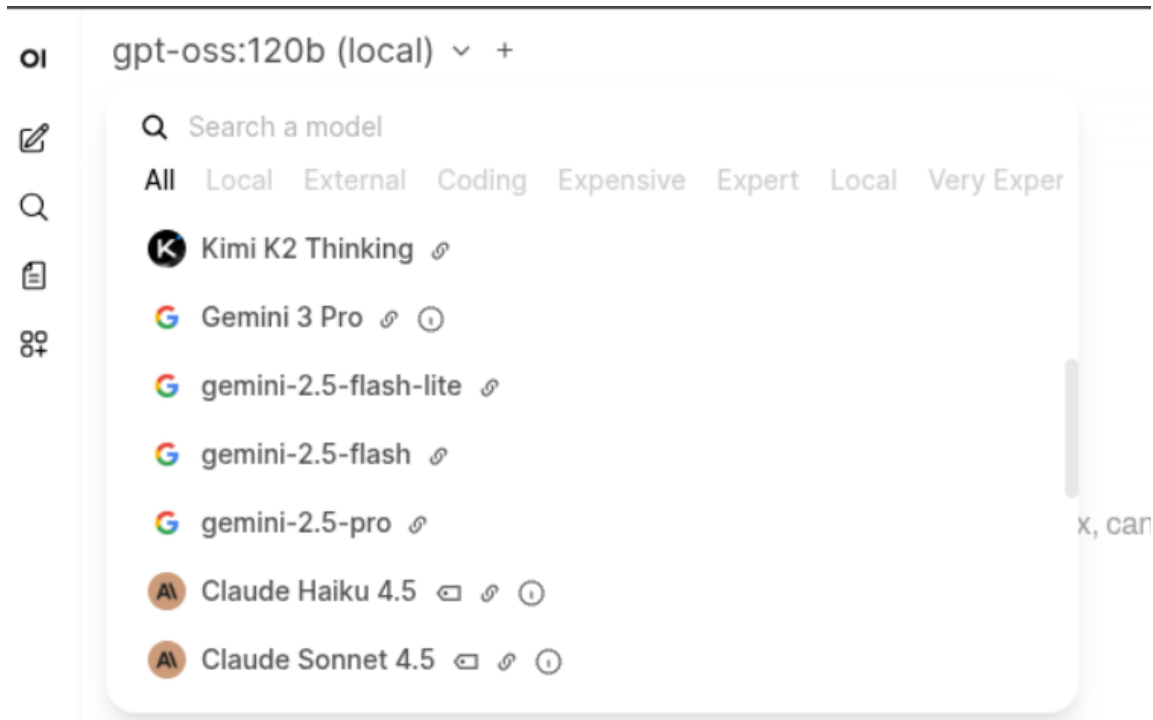
Our Tools:

AITHYRA Chat

<https://chat.aithyra.at>



So many models.



Current Model Selection

- **Recommended Default:**
 - **gpt-oss** (Locally run - Fast, secure, zero data leakage).
- **Advanced External Models:**
 - **Gemini 3 Pro** (Google)
 - **GPT-5.1 & GPT-5.1 Chat latest** (OpenAI)
 - **Claude Sonnet 4.5** (Anthropic)
 - **Kimi K2 Thinking**
- **Other Available Models:**
 - **Mistral / Magistral**
 - **DeepSeek**
 - **Qwen3-VL** (also local)
 - **Grok**
- **Image Models**
 - GPT Image
 - Nano Banana (Gemini)

Which model to use?

Efficiency & Use Cases

- **Standard Tasks (Default):**
 - ***Use:*** gpt-oss or **GPT-5.1 Chat latest**
 - ***Tasks:*** Grammar checks, translations, summaries, simple code questions.
- **Complex Tasks:**
 - ***Use:*** **Gemini 3 Pro, GPT-5.1, Claude Sonnet 4.5, Kimi K2 Thinking**
 - ***Tasks:*** Policy drafting, large document summaries, complex code-bases, full program logic

Tip: Try different models to see which handles your specific scientific context best.

Prompts you could try

- **Refinement:** "Check this for grammar and clarity and suggest simpler phrasing for complex sentences."
- **Data Extraction:** "Take this offer text and provide positions in a table with columns: product number, name, price."
- **Meeting Admin:** "Summarize this transcript into: 1. Key Decisions, 2. Action Items (with owners), 3. Open Questions."
- **Process Drafting:** "Draft a Purchase-to-Pay process compliant with Austrian Bundesvergabegesetz and create a mermaid diagram."
- **New Scientific Examples:**
 - *Coding:* "Analyze this Python script for memory inefficiencies regarding large genomic datasets and suggest optimizations."
 - *Literature:* "Summarize the methodology section of the attached PDF and highlight any potential limitations mentioned by the authors."



What else is possible?

- Creating images
- Storing/Creating "Knowledge"
- Search the Web
- Share Chats with other members of AITHYRA
- See inline Web-Previews
- Run/install the chat on your cell phone
- And more:

<https://docs.openwebui.com/features/>

When to be careful?

Uploading documents: "Focused Retrieval" vs. "Full document".

Hallucinations / Wrong information / Biases

Avoid decision making!

Provide context!

Models usually provide better results when prompted in English.

Don't use created code without checking first!

GPT Researcher. Next Level.

<https://gptr.aithyra.at/>

Say Goodbye to Hours of Research

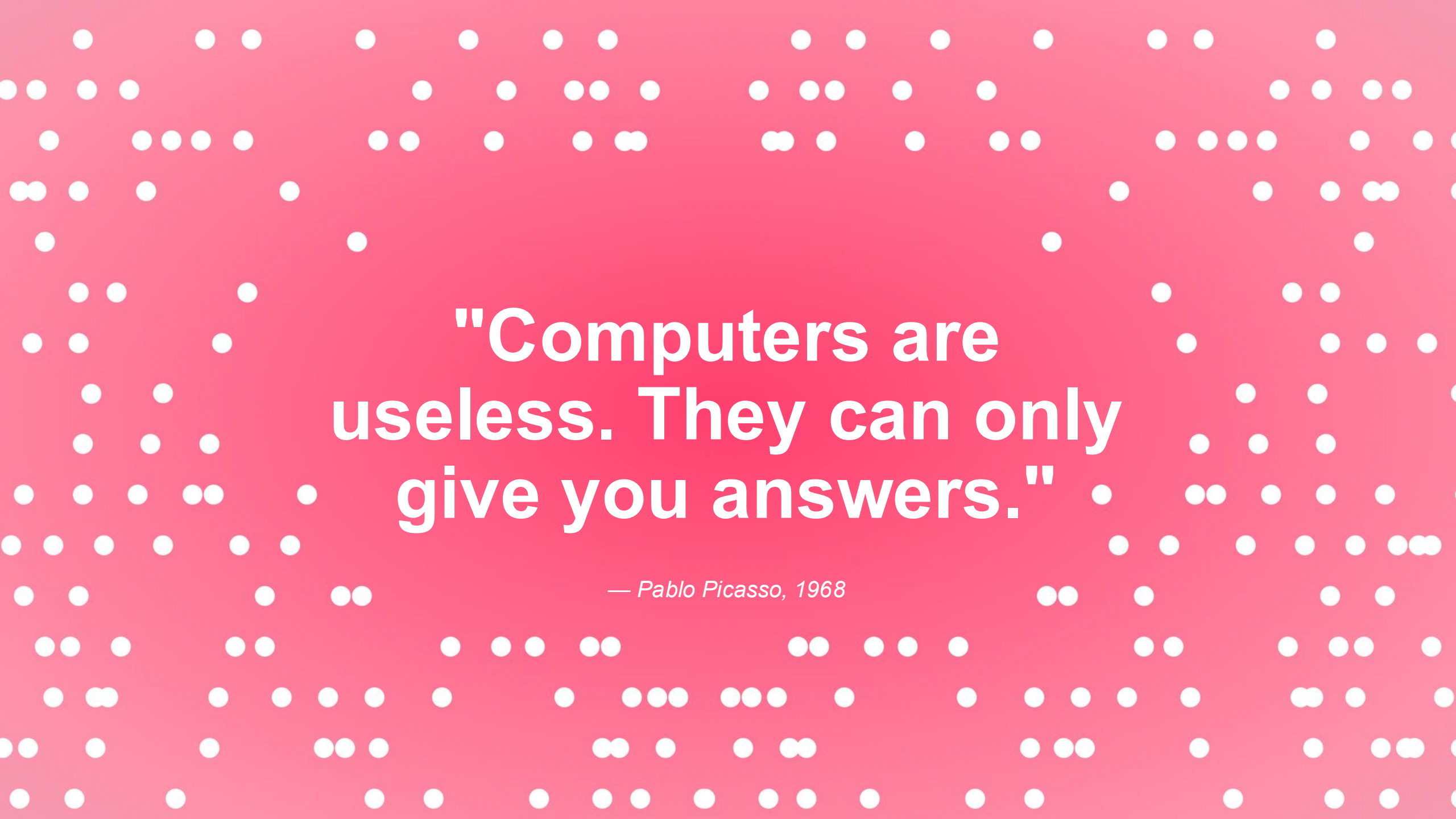
Say Hello to **GPT Researcher**, your AI mate for rapid insights and comprehensive research. GPT Researcher takes care of everything from accurate source gathering and organization of research results to generation of customized reports with citations.

Start
Researching

The background is a solid orange color. It is decorated with various white geometric shapes, including circles of different sizes and horizontal bars of different lengths, some of which are rounded at the ends. These shapes are scattered across the frame, creating a modern, abstract pattern.

**"AI won't replace
humans — but humans
with AI will replace
humans without AI."**

— Karim Lakhani, Harvard Business School, 2023

The background is a solid pink color with a pattern of white dots of varying sizes scattered across it. The dots are arranged in a way that suggests a digital or pixelated aesthetic.

**"Computers are
useless. They can only
give you answers."**

— Pablo Picasso, 1968

The image features a central teal background with a gradient. Scattered across the background are numerous white dots and short horizontal lines, creating a dynamic, abstract pattern. The dots are of varying sizes and are arranged in some cases into small groups or clusters. The lines are also of varying lengths and are positioned at different angles. The overall effect is a modern, minimalist aesthetic.

AITHYRA