

Open in app ↗

 Member-only story

Things Not To Use AI For

Artificial Intelligence Red Lines

2 min read · Jan 18, 2026



Gunnar Östberg



Listen



Share



More



Image illustration of the story, made by AI.

AI is everywhere, from drafting emails to optimizing code. But you should not use AI for everything.

AI strategy and ethics experts point to clear red lines. Areas where AI should not be used at all, or only under very strict conditions. These limits are driven by legislation such as the EU AI Act, by professional standards, and by basic risk logic.

You should know which things you should never hand to AI cloud services.

Here they are.

Personal no-gos

To protect yourself and your family, never treat AI as a private vault or an oracle. It is neither.

Data you submit to cloud-based AI services may be logged, reviewed, retained, or used for model improvement, depending on the provider and settings. You lose full control the moment you prompt.

Avoid in particular:

- **Sensitive identifiers**

Social security numbers, addresses, passwords, bank card details, passports, CVs with personal data.

- **Health and mental health**

Medical advice, diagnoses, symptoms, psychotherapy, crisis support.

- **Finance and law**

Tax advice, investments, contracts, wills, loan or risk analysis.

- **Emergencies**

Fire, cardiac arrest, gas leaks. Call emergency services such as 112 or 911. Do not prompt.

- **Intimate life decisions**

Dating messages, relationship advice, emotional or facial analysis, and major life choices.

- **Photos and documents**

Images of children, medical records, and identity documents.

- **Personal economic profiling**

Detailed analysis of your own or your family's finances or tax returns.

Rule of thumb:

If you would not post it publicly on social media, do not submit it to an AI cloud service.

Use opt-out settings where available. Always cross-verify outputs.

Institutional red lines

From micro-level human decisions to macro-level societal systems.

- **Decisions with power over people**
Fully automated decisions in credit, recruitment, education, or justice without meaningful human oversight.
- **Manipulation of vulnerable groups**
Targeting children, the elderly, or people in debt through behavioral nudging or rewards.
- **Privacy at scale**
Monitoring employees, students, or citizens through large-scale data hoarding or inference.
- **Integrity and anonymity violations**
Re-identification, tracking, or profiling that breaches GDPR or equivalent protections.
- **Safety-critical systems**
Uncontrolled AI in power grids, vehicles, robots, medical devices, or industrial control systems.
- **Health and therapy**
AI acting as primary therapist or diagnostician without expert supervision.
- **Surveillance**
Mass surveillance and facial recognition, except in narrowly defined lawful cases such as counter-terrorism or child protection.
- **Democratic manipulation**
Opinion shaping, disinformation, propaganda, and election interference.

- **Critical autonomy**

Direct AI control of essential societal infrastructure without layered safeguards.

- **Existential development**

Uncontrolled advanced AI systems without alignment, monitoring, and shutdown mechanisms.

Final test

Audit for irreversibility.

If failure costs lives, liberty, or democracy, humans must retain veto power. Always.

[AI](#)[Eu Ai Act](#)[Gdpr](#)[Safety](#)[Edit profile](#)

Written by Gunnar Östberg

196 followers · 143 following

CEO Business Clarity. I write enjoyable, rewarding articles that retain their value. Please check my profile to see the various story topics!

No responses yet



Gunnar Östberg

What are your thoughts?