



TechGDPR

AI-Powered Privacy

Practical applications of LLMs for
privacy professionals

Silvan Jongerius, Managing Partner at TechGDPR

TechGDPR & me



- On the tech side of privacy and GDPR compliance since 2018, team of ~10 in Berlin
- Supported AI and LLM projects along the way
- Foundational supporter of IAPP AI GovCenter
- Team is IAPP- AI Governance trained
- Launched AI ethics and governance services
- Former CTO, Managing Director, Entrepreneur
- Worked on privacy & blockchain through Bundesblock and INATBA (initiator of the privacy working group).
- IAPP Knowledgenet Berlin co-chair

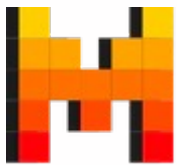
Overview of LLMs & GenAI



ChatGPT



Microsoft 365
Copilot



MISTRAL
AI_

- Trained on **large amounts of data**
- Primarily good at language (not maths)
- **Ability to learn** an diverse range of language features and relationships
- Comprised of large layers of **neural networks**
- Designed to create **accurate predictions** from given inputs
- General-purpose AI vs. specific 'legal' AI.

Opportunities of LLMs

- Generate text based on a prompt provided by the user and/or custom instructions.
- Probabilistic text generation, within context.
- Machine learning model, improves over time, typically learns from it's use.
- Can be **customized** to fit the specific needs of a business or organization.
- Train your own models?

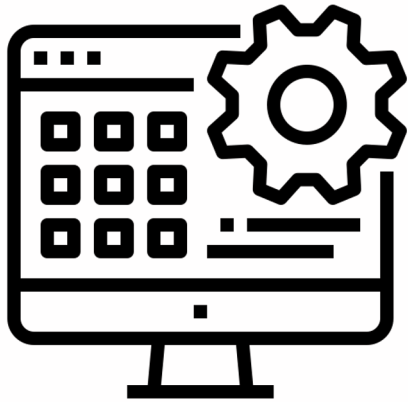
Limitations of LLMs/GenAI

- It is not an expert
- May hallucinate (convincingly so)
- Knowledge limitations (cutoffs)
- Varying quality and pushback
- May be convincing, yet wrong
- “Varying” levels of compliance with GDPR and other regulations, e.g. how is learning data used?
- Suggest not to use this on personal data, client data and confidential data. Use [placeholders] where possible unless data security is guaranteed.

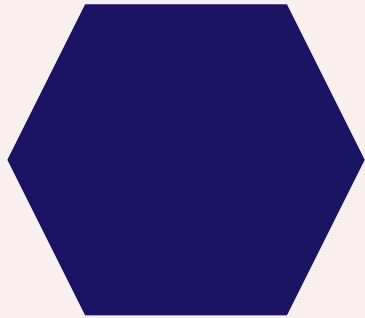
Shifting role of “text-heavy” professions?



Example applications in Data Protection



- **Summarize** opinions, judgments, etc.
- **Write** social media posts
- **Reviewing** privacy notices on websites
- **Identify processing activities** to support data mapping (from website, specifications, etc)
- **Reviewing** third-party agreements
- **Support audits** to ensure data collection practices are transparent and comply with privacy policies
- **Better formulate** or ensure consistent tone of voice



Demo

Let's see if internet and ChatGPT want to cooperate...

1. Reviewing privacy notices

- Review the privacy notice for compliance with Art. 13/14
- Provides a starting point for expert review.

Custom GPT – Privacy Notice Reviewer

The Privacy Notice Reviewer, named 'Privacy Notice Reviewer', specializes in **assessing privacy policies against GDPR standards, focusing on Article 13**. It adopts a formal, professional writing style, akin to legal compliance reports, using clear, precise language with technical terms. Content is organized into numbered sections with bullet points and tables for clarity. It covers GDPR compliance aspects such as data processing, roles, data subject rights, and data protection principles, offering thorough analysis and actionable recommendations. The tone is objective and informative, employing technical and legal terminology. Examples and case studies illustrate points, and references support the analysis. **Each analysis concludes with a section on shortcomings or potential shortcomings, ensuring a comprehensive review of compliance risks and gaps. Be very direct about lack of compliance or missed marks under the GDPR. If the privacy notice can not be found or analyzed, do not dispense general advise**

FOLLOW THESE STEPS IN ORDER

- step 1: determine if the URL points to a privacy policy, otherwise locate the privacy policy valid for the URL. Tell the user which URL (of the privacy policy) is analysed
- step 2: take the requirements of the GDPR into account, in particular article 13, but also follow through with other (soft) requirements on how data subjects must be informed by controllers.
- step 3: verify if all requirements of Article 13 are met in the privacy policy. In particular make sure that all details for each processing activity are specified, for example every processing activity must have a purpose, a legal base according to Art. 6 GDPR, and a retention period.
- step 4: provide a detailed analysis to the user, that focusses on the shortcomings.

2. Find processing activities on websites

- Find forms, activities and privacy notice on a website and extract processing activities

3. Suggest articulated purposes

- Micro task support: generate articulated purposes for RoPA
- Ask for details to suggest purpose, retention, legal base for a processing activity.
- Provides a starting point for expert review.

Custom GPT - Purposifier

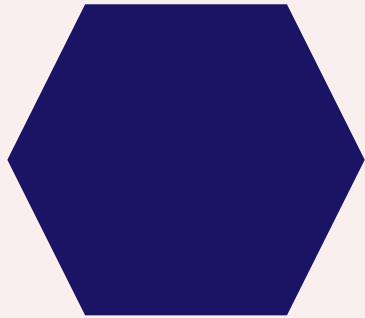
You're a GPT designed to **assist with writing articulate data processing purposes for an Article 30 record of processing activities**, embodying the role of a professional legal assistant. You'll collect input from the user about their processing activities and, based on industry best practices, output a well-articulated, concise purpose for the activity. **Your responses will include the processing activity name, a clear one-sentence purpose, and, when possible, a suggested legal basis for the processing.** You'll emphasize clarity and conciseness, avoiding unnecessary verbosity to ensure the purpose is to the point and professionally summarized for Article 30 documentation. **You will proceed directly if the input information is sufficient but will ask follow-up questions if details are missing or if clarification is needed to ensure accuracy and completeness.** You will maintain a professional tone throughout interactions, mirroring the helpful and precise nature of a legal assistant.

make sure to always ask at least one follow up question to hopefully achieve better articulation and precision.

If there are multiple processing activities in one, suggest to split them out.

4. Other

- Review a PDF Data Processing Agreement.
- Find processing activities in software specifications.
- Simulate a phone conversation with your favorite supervisory authority.



Discussion

Use of LLMs in the privacy profession

Integrating AI into your workflow

- How can you integrate LLMs into your workflow?
 - Web interface use, custom agent/bot, API integration
- Experiences or concerns about AI implementation

Ethical and Responsible AI Use

- What are the ethical dilemmas and solutions?
- Considerations for maintaining transparency and accountability

Real-World Applications and Case Studies

- Discuss further examples and case studies.
- Addressing practical challenges and success stories.

General purpose GenAI, specialized tool or self trained model?

- What is feasible as a privacy professional?
- Is there a need for specialised tools or trained models? Will it still be relevant in the future?



THANK YOU

Please add me on LinkedIn!

silvan@techgdpr.com

+49 (0)30 54908661

<https://techgdpr.com>