



KPMG LLM Compliance Kit

Ensuring regulatory compliance while
harnessing Large Language Model
opportunities

Finanstilsynet

June 13th 2023, Bent Dalager KPMG NewTech



Are you considering the potential risks of using Large Language Models in your organisation?



While ChatGPT and other LLMs can help streamline and enhance company operations, it also presents **potential risks** to a company's reputation and confidential information **if not properly monitored**.



[ChatGPT Mar 14 Version](#). Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

KPMG's LLM compliance kit helps assess and monitor models, enabling organisations to ensure compliance and enhance productivity



Assessment & quick stabilization

Get in control of LLM

Identification of issues & start monitoring and logging

1

Define and implement LLM compliance

Specific guidelines & principles

Implementation of guidelines

2

Communicate and train LLM capabilities

Ethical guidelines & education

Enhancing productivity and continuous compliance

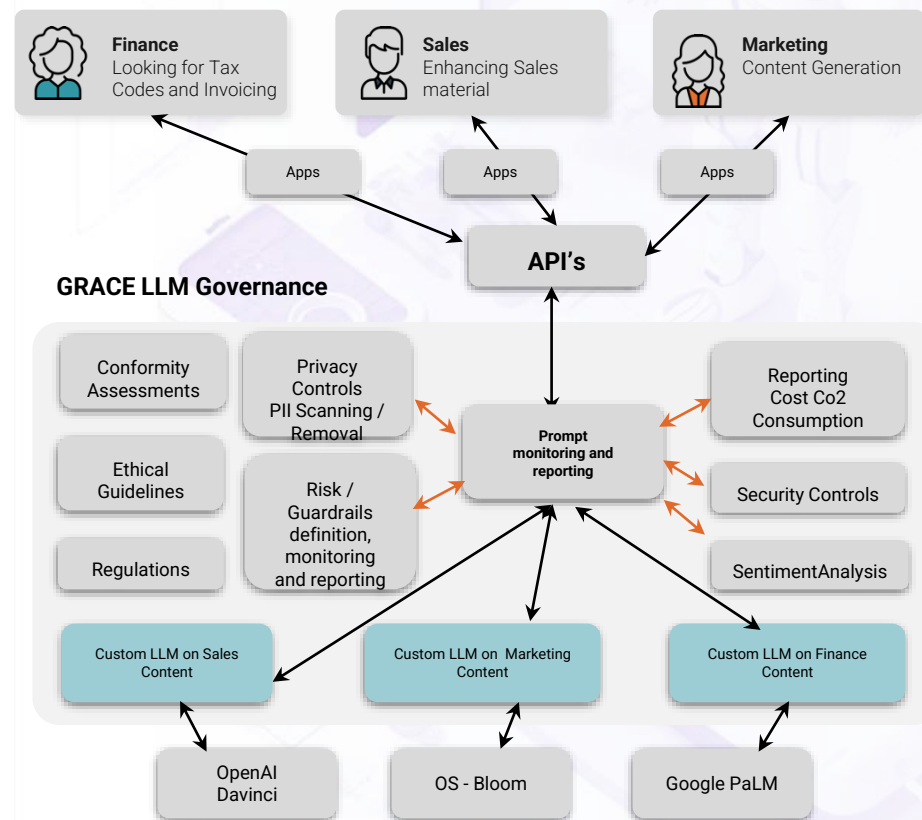
3

The LLM compliance filter enables overview and better compliance

The Grace platform enables:

- Logging
- Prompt Engineering
- Privacy controls
- Implementation of company code of conduct
- Implementation of AI ethical guidelines
- Implementation of AI and GDPR regulation

Step 1: Quick implementation of the LLM filter using a standard compliance set-up



Define and implement Governance and compliance frameworks for LLM

An AI Governance framework entails a **systematic approach to compliance** of AI models and systems to ensure that they align with ethical and legal standards general as well as company defined

AI ACT
(EU)

AI and DP Risk
(UK)

Data Ethics
Framework
(UK)

GDPR
(EU)

CAPAI
(EU)

EIOPA
(EU)

The Danish AI Pledge

AI-based solutions must be created with the best interest of society in mind

AI-based solutions must not be developed to create addictions, generate conflict, suppression or manipulation of behavior or opinion. AI solutions must be designed and integrated to optimise long-term sustainability. Furthermore, the notions of sustainability should include both economic, social and environmental aspects.

Knowledge about AI should be made available to everyone

Developers, decision makers, authorities, investors, designers and others that work with AI must take responsibility for spreading knowledge about artificial intelligence so that everyone will understand the opportunities and challenges that the technology creates.

AI solutions must be transparent in both function and design

It must be possible for a third party to audit the recommendations and decisions that AI models generate and make. The models must be transparent and it should be documented how the solutions work and generate results.

AI solutions must be tried and tested to withstand systematic and well-informed attacks

As AI solutions spread across all parts of our society managing and optimising a multitude of processes, they will become an increasing target for hackers and other bad actors. Therefore, security around AI solutions must be high and must be considered at the time when the solutions are designed, developed, tested and maintained.

Bias in AI solutions must be documented

The bias contained in AI solutions and the data that models learn from must be documented. This includes biases based on race, gender or socioeconomic status. The use of AI should work to eliminate all known forms of biases.

When AI is used to make decisions in life-and-death situations, the guidelines for these decisions must be discussed and documented in advance

AI solutions should focus on strengthening human judgement and not act on their own behalf when considering questions related to human life and death. This is for example relevant in situation where AI is used in weapons systems or medical services. In instances where the AI-based solutions will have to make a life-or-death decision on its own, for example when being implemented in a self-driving car, the lines along which it makes its decision should be discussed and documented.

When designing and developing AI-based solutions, information asymmetry between the parties involved must be addressed

Companies and public authorities should be extra aware when leveraging AI in situations that are characterised by asymmetric information, meaning situations where one party holds more data and thereby has more knowledge than his or her opponent, as these situations hold an inherently increased risk of misuse of power.

Examples of ethical/reg. considerations when using LLMs

Confidential data sharing with BigTech and other entities

Samsung Case

Risk of perpetuating biases and discrimination

Discriminating analysis/language

Breach of EU bank regulation

EU bank directives

Misleading models in production due to insufficient governance

Absence of control & competence

Issue with discerning facts from fakes

Model hallucinations and drifting

Unethical and illegal utilization of AI

Cambridge Analytica Case

Breach of GDPR regulation

Entry of personal information

Breach of company code of conduct

Language, behaviour et al

And many more

...

Step 2: Define and implement company LLM Compliance

Training in compliance and effective LLM use

Training in effective use of LLMs (using ChatGPT as an outset) :

- ✓ Communication and training in company specific standards and ethical guidelines for LMM usage
- ✓ Training in how to maximize productivity through use of LLM (ChatGPT)

Examples on the following slides

Communication and Training topics (examples)

Communicate and train LLM capabilities

3

Company AI ethical guidelines

Regulation and compliance

Ie. AIA, GDPR etc for LLM use

Company specific code of conduct

Language, values,...

Prompt engineering

How to maximize output

Writing and learning using LLMs

Revolutionizing learning and working

Coding, testing etc with LLM's

Special module

LLM interacting with other tools

AI can accomplish complex tasks with minimal human expertise

LLM for Legal, HR,...

Special modules

And more

...

Step 3: Communication and training in LLM compliance and effective LLM use

The implementation time varies based on ambition level

From a quick minimum approach with only one module to a comprehensive custom approach with all modules.

Assessment & quick stabilization

Get in control of LLM

Identification of issues & start monitoring and logging

1

Define and implement LLM compliance

Specific guidelines & principles

Implementation of guidelines

2

Communicate and train LLM capabilities

Ethical guidelines & education

Enhancing productivity and continuous compliance

3

***Excl. any internal approval process **Very dependent on communication and training approach and org. size**



Podcast: Tech Talk KPMG

<https://kpmgdenmark.smh.re/jQ> or any podcast app



KPMG

Contact: Bent Dalager

Partner & Nordic Head of NewTech



T: +45 53 75 30 00
Mail: bent.dalager@kpmg.com



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2023 KPMG P/S, a Danish limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Confidential