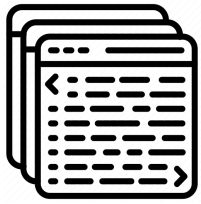
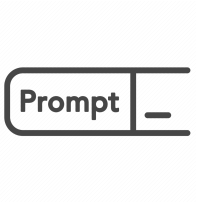
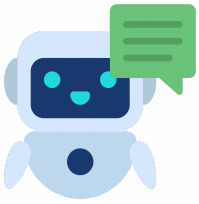
Compliance Gate AI Tool White Paper - Beta

This document outlines the general functionality of the AI tool, its use case, and potential errors. It is important that you read this document in its entirety before you use the AI tool.

Functionality







1. Collection creation >	2. User prompt >	3. Search skill >	4. LLM output
Splits up source text into searchable items	The user writes a prompt, normally a question	Selects the relevant items in the collection based on the prompt	Generates a probability based response based on the selected items **and** the prompt
Sample source text	Is CE marking required on the packaging?	ITEM 1: Article 16 - General principles of the CE marking ITEM 2: Article 17 - Rules and conditions for affixing the CE marking	Yes, the CE marking shall be affixed to the packaging where it is not possible affix it to the product.

Disclaimer

You are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of the AI tool. This AI tool uses machine learning models that generate predictions based on patterns in data. Output generated by machine learning models is probabilistic and should be evaluated for accuracy on a case by case basis, including by employing human review of such output. Output generated by the AI tool does not constitute legal advice. You must read the White Paper to better understand the functionality and limitations of the AI tool before use. You are also required to read the entirety of the Terms of Service.

User Data

We use third party services ('AI software providers') that are not owned or controlled by us and who can collect personal data from the user of the AI tool. We are not responsible for the privacy practices or the content of such Third Party Services.

Accordingly, you should refrain from inputting user prompts that contain sensitive data, such as personal information and intellectual property. Additionally, you are encouraged to read the terms and conditions and privacy policies of the AI software provider here.

Important information

How should the AI tool be used?

1. The purpose of the AI tool is to help you navigate various compliance related texts.

2. The value lies in its ability to provide somewhat coherent responses to natural language. In other words, you can write questions and receive an “answer” that might be easier to understand compared to the original source texts.

3. All generated outputs must be compared to the source text. You must not only take the selected items into consideration, but the complete source text.

What the AI tool is not

1. The AI tool does not think or have “opinions”. It cannot interpret or understand anything. It generates a response by “guessing” the next word based on mathematical probability. Think of it as a more advanced form of auto complete.

2. The AI tool is not a “truth engine”. It “blindly” generates a response based on the LLM prompt without any fact check. It can also make up false information, which is called hallucination (See LLM output: LLM hallucination).

How do you select sources?

We normally create the collections based on the original regulation or directive text. Here are two examples:

DIRECTIVE 2014/35/EU

PART 134—COUNTRY OF ORIGIN MARKING

Sometimes we need to include more than one source text in the collection. Further, we may also include official guidance pages and documents in the collection.

Recommended process

Step 1: Write your question

Step 2: Test Narrow, Medium, and Broad to see how the output changes

Step 3: Compare the output to the source items - Does it match or can you find errors?

Step 4: Compare the output to the original source text - Does it match or can you find errors?

Data

1. The AI tool does not operate as an archive or file storage service. You are solely responsible for the backup of generated outputs and other safeguards appropriate for your needs.

2. The AI tool sends the user prompt to an external data processor. Read the Privacy Policy for more details.

Terminology

Source text: Regulation, directive, or other text

Collection: Set of items created based on the source text

Source items **or** Items: Subsection of the collection, which is based on the source text

LLM: Large Language Model

User prompt: The part of the prompt written by the user (normally a question)

LLM prompt: The complete text (including user prompt, selected source items and static prompt text) sent to the LLM

Output: The “answer” generated by the LLM based on the LLM prompt

Beta Version

This AI tools is work in progress until further notice. We are working to improve the quality and consistency of the outputs. Part of this is due to us optimizing the system, but also because the underlying technology is far from perfect. Such limitations are covered in this document.

Risks Assessment

Detailed information about potential risks and system limitations are detailed under Risk Assessment. It is important that you read this part to better understand the limitations of the AI tool.

Identified Errors

See the error log at the end of this document for more information.

Terms of Services

You can read the complete Terms of Service here.

User Prompts

General examples

19 CFR Part 134 - Country of Origin Marking

Can I claim that my product is made in the USA if we repack it here, but manufacture the products in India?

What should we print on product if we buy components from China but assemble it in Mexico?

Toy Safety Directive 2009/48/EC

Does this directive cover pet toys?

Can I print the CE mark on the packaging if there is not space on the product?

Is safety testing required?

Additional instructions

You can also go beyond direct questions and request the LLM to provide additional information. Keep in mind that the quality and relevance of the output can vary.

Does this directive cover pet toys? (explain why if it does or doesn't)

Summarise what I need to include in the Declaration of Conformity in a numbered list

Questions relevant to the source text

The search skill can only find relevant source items in the collection and the LLM can only generate a relevant output if the source text has information related to the question you ask. Keep in mind that regulations/directives do not address every single scenario, detail, or comparison.

Good = Is safety testing mentioned?

Bad = Is third party laboratory testing mandatory for cotton t-shirts?

Keep in mind that questions that are unrelated can still result in an LLM generated output based on model training data - which is completely irrelevant to the source text.

Relevant Terminology

It is important to use terms that are present in the source text. The search skill may not be able to find the relevant source items if you don’t use relevant terminology.

Good = Is a Declaration of Conformity required?

Bad = What kind of paperwork do I need?

Focused questions

The LLM relies on the search skill to generate a response. The search skill in turn selects source items in the collection based on the words included in the user prompt. You can generally expect more relevant outputs when the questions are focused.

Good = Is a Declaration of Conformity required?

Output: Yes, a Declaration of Conformity is required according to Directive 2006/95/EC.

Comment: Search skill can “focus” on finding source items related to “Declaration of Conformity”.

Bad = Do I need certificates, labels and registrations?

Output: No, the source text does not mention certificates, labels or registrations.

Comment: The search skill is capped to a limited number of items, and a relevant output for a less focused question would require more items than the search skill can include. Further, LLMs generally tend to perform poorly when receiving too many words.

Technical information

1. Collection creation

a. The collection is created by scanning a designated source text. The source text normally consists of a copy of a regulation or directive text.

b. The collection consists of a certain number of items. Each item contains a part of the source text. The number of source items contained in a collection varies depending on the number of words in the source text. The structure and complexity (i.e., tables in source text) can also affect the final number of source items. Here are some examples:

- REACH Regulation (EC) 1907/2006: Around 900 source items
- Use of Bisphenol A in Varnishes and Coatings Regulation (EU) 2018/213: Around 20 items

c. Ideally, a single source item is a contextual article/clause/part of the source text, as this makes it easier for the search skill to find relevant items. However, we cannot control how the source text is broken down into individual source items that combined form a collection.

d. This is an example of an item from the Low Voltage Directive 2014/35/EU (Link):

> Rules and conditions for affixing the CE marking
>
> 1. The CE marking shall be affixed visibly, legibly and indelibly to the electrical equipment or to its data plate. Where that is not possible or not warranted on account of the nature of the electrical equipment, it shall be affixed to the packaging and to the accompanying documents.
>
> 2. The CE marking shall be affixed before the electrical equipment is placed on the market.
>
> 3. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking.

e. These items are necessary as the LLM cannot generate a relevant response based on the entire source text. It needs to receive smaller text items that are selected by the search skill.

Testing: Once the collection is created from the source text, we select 5 text segments from the start, middle, and end of the source text. We then search these 5 text segments in the collection to determine if the created collection covers the full span of the source text.

However, we cannot check that every single word from the source text was included in the collection.

2. User Prompt

a. The user writes a question in the interface. Here is an example:

> Is CE marking required on the packaging?

b. The user prompt is used in the following ways:

Search skill (Step 3): Select items from the collection that are related to the user prompt.

Large Language Model (Step 4): Generate a response based on the LLM prompt (including user prompt, selected source items and static prompt text).

3. Search skill

The search skill selects one or more items based on the user prompt. This is normally a question.

Question: Is CE marking required on the packaging?

ITEM 1:

Rules and conditions for affixing the CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the electrical equipment or to its data plate. Where that is not possible or not warranted on account of the nature of the electrical equipment, it shall be affixed to the packaging and to the accompanying documents.

2. The CE marking shall be affixed before the electrical equipment is placed on the market.

3. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking.

ITEM 2:

Article 16

General principles of the CE marking

The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

Article 17

Number of items

1. You can select the number of items to include: Narrow (1 item), Medium (2 items), and Broad (3 items).

2. Including more items means that the LLM has more information from the source text from which to generate a response. For more direct questions, narrow may be a better option. However, questions that are slightly more complex may benefit from including 2 or more items.

3. You will need to test the different options to see what generates the most informational output.

Testing: Once the collection is created from the source text, we write a prompt asks about its product scope. We then check that the selected source item belongs to the correct source text. This is to ensure that the right collection is selected by the AI tool.

4. Large Language Model (LLM)

The LLM is only applied to the final step. The LLM receives the user question and selected items as part of a single unified LLM prompt.

Example

Based on the user prompt and item examples on the previous page, the LLM might generate the following response:

> Yes, the CE marking shall be affixed to the packaging where it is not possible or not warranted to affix it to the electrical equipment or its data plate.

Option 1: Answer my question (User prompt + source items)

> Only use the following pieces of source text to answer the question. Do not try to make up an answer.
>
> [Search skill: Source items]
>
> Question: [USER PROMPT QUESTION] (reply only based on the source text above)

Option 2: Summarise from source (Summarise source items only)

The user prompt question is only used by the search skill. The LLM is only tasked with summarising the selected source items. This reduces the risk of hallucination.

> Only use the following pieces of content to create a summary:
>
> [Search skill: Source items]
>
> Summarise the source text above using bullet points

Notes

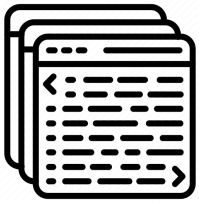
1. The static prompt text is seen in red. This means that it cannot be changed by the user. Nor is it necessary to manually input the text above.

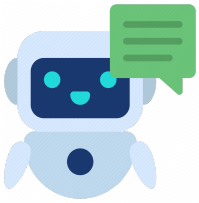
2. The purpose of the static prompt text is to instruct the LLM to only generate a response based on the selected source items and the user prompt question. This is for the sake of reducing LLM hallucination (See LLM output: LLM hallucination).

3. The static prompt text is subject to continuous optimization. Hence, you should only consider the text on the previous page as examples.

Testing: We have tested multiple prompt structures to improve the quality of the output and reduce the occurrence and extent of LLM hallucination.

Risk Assessment





1. Collection creation >	2. User prompt >	3. Search skill >	4. LLM output
Sample source text	Is CE marking required on the packaging?	ITEM 1: Article 16 - General principles of the CE marking ITEM 2: Article 17 - Rules and conditions for affixing the CE marking	Yes, the CE marking shall be affixed to the packaging where it is not possible affix it to the product.
Collection not created on the entire source text	n/a	Cannot search the complete source text	Output generated based on insufficient items
Source items are not contextual	n/a	Incomplete/partially correct items selected	Output generated based on insufficient items
	Incorrect terminology in user prompt	Cannot find the relevant parts unless you use the same or related terminology as in the source text	Output generated based on irrelevant items
	Unrelated user prompt	Cannot find any relevant items or selects random items	Output generated based on irrelevant items
		Incorrect/irrelevant source items selected	Output generated based on irrelevant items
			LLM fails to include all relevant source items
			LLM hallucination

Red text indicates the origin of the error and the **blue text** describes how it impacts the other parts of the process.

Collection creation: Collection source items not created for the full source text

This means that insufficient LLM outputs could be created as the search skill cannot find the necessary information in the source items because these were not created as part of the collection.

Collection creation: Source items are not contextual

We cannot control how the source items are divided in the collection. This means that certain articles/parts of the regulation could be split up into different items, which could result in the LLM

producing an insufficient output.

User prompt: Incorrect terminology

The search skill cannot find the relevant parts unless you use the same or related terminology as in the source text. For example, if you ask about “labeling requirements”, while the source text refers to these as “identification” or “markings” then the search skill may not find relevant items.

User prompt: Unrelated prompts

Asking questions that are unrelated to the source text can result in irrelevant and/or misleading outputs. For example, asking questions about Directive A while you have selected Directive B in the interface can have this effect.

Search skill: Cannot find any relevant items or selects random items.

LLM: Generates a random, irrelevant and/or misleading output.

Example

User prompt: Where is the moon located?

LLM: The moon is located in Earth's orbit.

As you can see above, the source text does not provide any answer to this question. But, prompts can still “force” the LLM to respond based on model training data that has no relation to the source text and its source items.

Search skill: Incorrect/irrelevant source items selected

We cannot control which source items from the collection are selected by the search skill. The LLM generates an incomplete or even incorrect output if the items are wrong (as in, not related to the user prompt) **or** if only some of the relevant items are selected.

LLM output: LLM fails to include all relevant source items

The LLM may not generate a response that takes all selected source items into consideration. This can therefore result in the output being insufficient or incorrect.

LLM output: LLM hallucination

The LLM can make up false information. You can learn more about LLM hallucination here:

https://www.techtarget.com/whatis/definition/AI-hallucination

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9939079/

https://en.wikipedia.org/wiki/Hallucination_(artificial_intelligence)

https://blogs.sw.siemens.com/verificationhorizons/2023/06/15/decoding-llm-hallucinations/

AI models changes and updates

1. Changes to the AI search skill and the LLM can impact the performance of the AI tool as a whole. Further, AI models can be replaced entirely. It is likely that we will test different LLMs in the future.

2. Technical problems cannot be ruled out either, which could result in downtime or a drastic reduction in output quality.

Languages

1. All collections are created based on English language source texts. As such, all source items in each collection are also in English.

2. We have only tested and optimized the system based on English language user prompts and LLM prompts.

3. Our tests have demonstrated that you can write user prompts in other languages, such as Chinese. However, keep in mind that the translation of the source items may impact the accuracy of the outputs.

Error log

Error	Result	Status
1. Collection creation Date: 2023-07-27 Source items are not created for the entire source text.	We estimate that 7 to 10% of the source text is missing. This means that the missing information cannot be found by the search skill. This can result in insufficient information for the LLM. This is likely due to limitations in the software used to “break down” the source text into individual items. We currently do not know when a better version of the software can be provided, and if this will fully resolve this error.	**Unresolved**