Legal IT Innovators Group - www.litig.org

Legal IT AI Due Diligence Questionnaire
May 2024

1. Technical and Product-Related Questions

1.1. How does the AI enhance your product?
1.2. How does your AI work in practice? What underlying technologies do you use?
1.3. How can I tell what data is real and what is algorithmic?
1.4. Can the AI model be customized for our specific needs? Who would do this and if it were you what would the costs/SLA Look like?
1.5. Is there a kill switch/do we have to leverage your AI if we don't want to?
1.6. How do you ensure the quality and accuracy of outputs generated by the AI?
1.7. What is your liability and insurance position in relation to inaccurate content, breach of copyright/IP and/or any other liability due to the use of your AI?
1.8. How will you supervise the outputs your system creates with AI?
1.9. Which AI models do you use and what data repositories do they mine?
1.10. Do your AI models have access to internet content (live or otherwise)?
1.11. How do you guard against model poisoning or prompt injection attacks?

2. Security and Compliance Questions

2.1. How do you handle data security and privacy in relation to AI? Do you leverage an abuse monitoring exception?
2.2. What security standards do your AI capabilities comply with?
2.3. Do you comply with IS0 42001? What steps are you taking in this regard?
2.4. Please confirm you will not apply AI to our or our client's data without our explicit consent?
2.5. What measures are in place to prevent the AI from generating harmful or inappropriate content?
2.6. Can the system explain how decisions or outputs were generated showing all the relevant steps it goes through?
2.7. When using AI do you intermingle any of our client's data with any other client's data? – or our Data with any of your other client's data? Can we put ethical walls around any data set?
2.8. Please confirm none of our client's data or our data is used to educate any LLM/your AI and is not consumed within it?
2.9. What Risk Management Strategies do you apply to ensure your AI outputs are as accurate as possible?
2.10. If we wanted to ensure any AI outputs are as accurate as possible what practical steps would you recommend we take?
2.11. Where and how is data transferred/processed by your AI?
2.12. Is data stored for any period of time following processing by your AI?

3. Integration and Support Questions

3.1. How does your AI integrate with your wider product, our existing systems and workflows?
3.2. Can we access data and documents in your systems to apply our own AI to (and export the same if needed)? In particular Azure AI and Copilot?

3.3. What type of support and training do you offer for users to effectively use the AI-enhanced features?
3.4. To what extent can we supervise or run reports on how our users are using AI?
3.5. What steps do you take to do this internally?
3.6. How do you manage updates and improvements to the AI model? How will the same be communicated?
3.7. What support will you provide for the AI aspects of your product?
3.8. How do you deal with model releases and inform us of changes? Do we have the right to delay if we are for example in the middle of a project and we want consistency?

4. Ethical and Social Impact Questions

4.1. How do you address ethical considerations and bias related to the use of AI? How does your system mitigate these risks?
4.2. If the outputs of your AI are illegal, unethical, discriminatory or breach anyone's IP or law in the wider sense how will you ensure we are immune from the effects? Also how will you communicate and rectify this?
4.3. What limitations does your AI have? Please try to be specific.
4.4. What steps do you take to minimize the energy consumption of your AI?

5. Financial and Contractual Questions

5.1. Is your AI included within current pricing?
5.2. What if we are unhappy with the outputs of your AI and/or the effects on our organisation?
5.3. How scalable is your AI?
5.4. Will it impact on system performance?
5.5. What are the terms of service, especially regarding AI-generated content ownership and liability?
5.6. What are the conditions for contract termination or service discontinuation?

6. Regulatory risk under the EU AI Act (AIA)

If your answer to any of these questions is 'yes', then you should seek legal advice if your AI or any output from it is going to be used in the EU.

6.1. **Could your AI be used for any purpose that will be prohibited in the EU (as listed in Article 5 of the AIA)?** These prohibitions cover certain AI systems that:

- Deploy subliminal, manipulative, or deceptive techniques.
- Exploit vulnerabilities related to age, disability or socio-economic circumstances.
- Assess or predict the likelihood of a natural person committing a criminal offence.
- Create or expand facial recognition databases by scraping the internet or CCTV.
- Infer emotions of natural persons in a work or education setting.
- Categorise individuals by inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation).
- Use 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement (save for certain specified purposes).

6.2. **Is your AI specifically intended to be used as a product or part of a product subject to EU product safety legislation (as listed in Annex I of the AIA)?** This is unlikely to include any legal technologies.

6.3. **Is your AI specifically intended to be used for any high-risk purposes under the AIA (as listed in Annex III of the AIA)?** These include certain AI systems that:

6.3.1. Use biometric data, such as facial images, fingerprints or iris scans.
6.3.2. Are used as safety components in critical digital and physical infrastructure.

6.3.3. Are used to assess or monitor students in education and vocational training.

6.3.4. Are used for recruitment, employment and worker management.

6.3.5. Are used to manage access to essential private and public services and benefits.

6.3.6. Are used for various law enforcement purposes by law enforcement agencies.

6.3.7. Are used for migration, asylum and border control by public authorities.

6.3.8. Are used by judicial authorities or in a similar way in alternative dispute resolution to research, interpret and apply facts and law.

6.3.9. Are used to influence the outcome of elections or referenda.

6.4. **Is your AI a general-purpose AI model that is capable of competently completing a wide range of different tasks?** This does not apply where your AI uses third-party models. Examples of general-purpose AI models include:

6.4.1. Large language models (LLMs).

6.4.2. Text-to-image or text-to-video models.

6.4.3. Large vision models.

6.4.4. Multimodal modals.

6.5. **Can your AI interact directly with natural persons (e.g. is it a chatbot)?** If so, they will need to be informed that they are interacting with an AI unless it is obvious.

6.6. **Can your AI generate or manipulate text which is published with the purpose of informing the public on matters of public interest?** If so, the artificial generation or manipulation of the content will need to be disclosed (unless there is human review and editorial responsibility).

6.7. **Can your AI generate synthetic audio, image, video or text content?** If so, the output will need to be marked in a machine-readable format and detectable as artificially generated or manipulated.

6.8. **Can your AI recognise individuals' emotions or categorise them based on biometric data?** If so, they will need to be informed that they are being exposed to the system (and you also need to comply with the GDPR).

6.9. **Could your AI generate so-called 'deep fakes' (i.e. convincing but fake image, audio or video content)?** If so, the artificial generation or manipulation of the content will need to be disclosed.

NOTE: The questions within section 6 relate to suppliers of legal tech specifically. When looking at different areas of tech then there may be other questions to consider and raise.

Disclaimer: For the avoidance of doubt all views, recommendations, policies and content in this document are provided free of charge, on an informal and non-binding basis and neither Litig Limited, it's officers, nor any shareholder or delegate shall have any responsibility or liability whatsoever for any direct or consequential loss or damage arising from the use of, or reliance on such views, recommendations, policies or content.