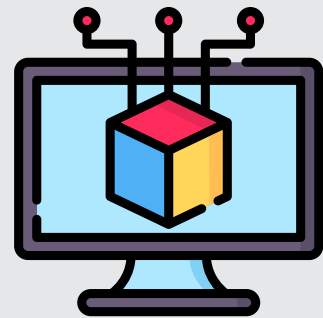


AI DEPLOYMENT CHECKLIST

CONSIDERATIONS FOR PILOTS

CONSIDERATIONS FOR PILOTING A SOFTWARE APPLICATION:

- Clearing the security review process
- Dedicated technology resources to make the application available
- Identified user group with capacity and incentive to test the application
- Clarification as to whether the application will be used for work product or tested on templates or form materials



IF THE PILOT WILL INVOLVE LEGAL WORK PRODUCT, ALSO CONFIRM THE FOLLOWING:

- User inputs are not used to train the underlying model (including PII or confidential information)
- If user inputs are used, they are deidentified to remove PII
- Uploaded documents are stored separately from the LLM model
- Sessions are cleared after a time identified by the user



TECHNICAL VETTING CRITERIA FOR GAI AND LLMS



DATA

- Is the data right for the use case?
- Has it been gathered with consent or license?
- Is it comprehensive or are there gaps in the data?
- Does it include biases that will undermine the reliability of conclusions?
- How often is the data warehouse updated?



ALGORITHMS

- Has the application been tested/vetted for your use case?
- Does the application provide reference material to enable verification of results?
- How often does the algorithm produce hallucinations?
- What alternative programming is incorporated to reduce/correct hallucinations?



PROCESSING

- Is personal or client information retained or deidentified?
- Are user inputs used to train the underlying model?
- Are sessions cleared after usage?
- Where does processing occur – locally, in the cloud, or on a vendor server?

NEGOTIATING AI VENDOR AGREEMENTS

- Clients should review potential AI vendors through their usual vendor diligence process, including with respect to IT and InfoSec
- You must understand the particular engagement and service/technology being provided (e.g., custom development, model-as-a-service, etc.)
 - Consider updates, support, maintenance, etc.
- Restrict the vendor's data processing rights where applicable
 - Review data use agreements, data processing agreements, data licensing agreements, etc., with AI-related issues in mind
 - Consider whether it is appropriate for the client's input data to be used as training data to improve the model
- Obtain commitments that the vendor will provide all information necessary to fulfill applicable legal obligations (e.g., notice and transparency obligations)
- Review and negotiate the representations/warranties, risk and liability terms with AI-specific issues in mind, including with respect to IP infringement, compliance, etc.

ALABAMA • FLORIDA • GEORGIA • LOUISIANA • MARYLAND • MISSISSIPPI • NORTH CAROLINA • SOUTH CAROLINA • TENNESSEE • TEXAS • VIRGINIA • WASHINGTON, D.C.

www.bakerdonelson.com