Responsible and Ethical AI

Governing Principles for the Use of AI in Verint Products

June 2024

VERINT.

VERINT

Table of Contents

VERINT

Introduction

As a provider of Customer Experience (CX) Automation offerings that incorporate artificial intelligence (AI), Verint is committed to ensuring its solutions not only deliver significant ROI to our customers but also leverage AI in an ethical, responsible manner. The Verint Open Platform is architected with data and AI at its core, with best-of-breed applications and AI-powered bots that automate a broad range of functions impacting the cost and quality of CX. This document highlights our AI strategy, the principles we follow as we execute on that strategy, and the processes, controls, and guidelines we have put into place to guide our use of AI.

Verint AI Strategy

Verint Da Vinci™ AI is core to the Verint Open Platform and powers the applications our customers use every day. To keep pace with the rapid innovation in the AI industry, Verint's AI model development is an open approach that strategy incorporates both proprietary and third-party models. Our open approach to AI means customers can be confident in an investment in Verint Da Vinci AI for the long term.

Verint Da Vinci AI maximizes impact by injecting AI directly into business workflows, putting AI at the fingertips of our customers. By injecting AI directly into business workflows, users of our solutions can:

- Convert unstructured data to intelligence and action.
- Use machine learning to improve business processes.
- Detect anomalies in data and take appropriate action.
- Identify trends and opportunities with predictive modeling.

We have infused Verint Da Vinci AI into a growing team of specialized bots, each of which is built to use AI to do one thing and to do it well. Our bots live in the Verint Open Platform and are deployed for use both in the platform as well as with Verint solutions implemented in other clouds. Customers can generally choose to deploy any or all our bots with their Verint solutions. Each bot works to augment our customers' human workforces and enhance CX automation, such as by:

- Summarizing interactions.
- Removing after-call work efforts.
- Responding to customer inquiries in self-service and deflecting contacts.
- Automatically scoring quality evaluations across interactions.
- Forecasting future customer interaction demand across channels.

Our AI models are trained on public, open source, licensed, synthetic, anonymous, and de-identified data sets generated from the Verint Engagement Data Hub to make smarter and faster decisions. These trained AI models are not publicly accessible, no customer data is actually incorporated into enhancements or new offerings, and these models are only available for use by our customers.

Engagement data may consist of:

- Interaction data across channels
- Experience data from both customers and employees.
- Workforce performance data

The Verint Open Platform has unique capabilities to harmonize these diverse data types from multiple applications into a cohesive whole. The AI models within Verint Da Vinci can also be further trained on an

organization's specific data to improve their ability to provide better insight and enhance CX automation. When such additional training occurs, those uniquely trained AI models are available for use only by that specific organization.

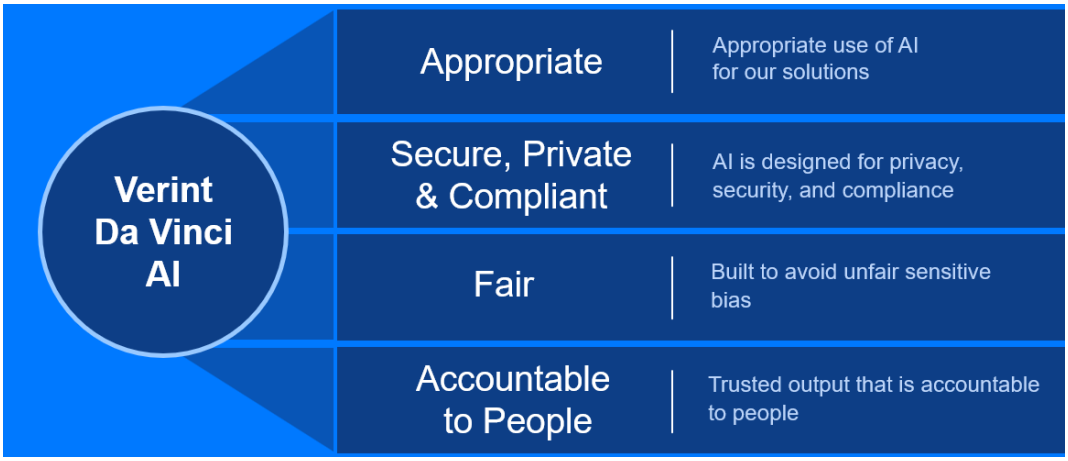
Verint Da Vinci AI services and models are built in Verint Labs, in combination with data from the Engagement Data Hub within the bounds of the Verint Open Platform. Verint Labs are secure, controlled environments managed by a team of data and AI scientists actively collaborating with customers on specific projects, with the infrastructure to securely incorporate tools and algorithms from partners, external research organizations, and universities. This team drives the research-to-product pipeline of Verint Da Vinci and the Verint Open Platform by focusing on improving our AI and machine learning capabilities.

Guiding Principles for AI

AI is integral to the Verint Open Platform and powers the applications our customers use every day. Verint realizes that advanced technologies like AI can raise important challenges that must be addressed clearly, thoughtfully, and directly. The principles that guide our use of AI in our offerings include:

- Deploying AI only for appropriate uses.
- Using AI securely and in compliance with privacy and other regulations.
- Working to ensure AI operates in a fair and safe manner.
- Designing AI to be controlled and accountable to people.

These principles inform our commitment to developing AI technology responsibly and ethically. They are incorporated into our company culture and are ingrained in the processes used to deliver the technologies and solutions we provide our customers.



Appropriate: Using AI appropriately for our solutions

Verint works to limit potentially harmful applications as we design and deploy AI technologies. We review the AI technologies we deploy, their use cases, and the related risks. Verint also evaluates how the AI technology will scale across billions of interactions and global deployments to help ensure the AI technology we offer can provide the value we intend.

Secure, Private, and Compliant

AI technologies are often exposed to large amounts of personal data, raising issues related to data privacy and security. Verint designs and develops AI technologies using research and development best practices.

Verint works to develop its AI systems in compliance with applicable laws and regulations and designs such systems in a manner that allows compliant use by customers. This includes respecting third-party intellectual property rights in the design and development process.

Verint also supports the adoption of data protection, compliance, and privacy regulations to address risks associated with AI, as well as the implementation of safe data handling practices, and undertakes annual policy reviews and updates to keep pace with changes.

Fair: Building AI to avoid unfair sensitive bias

AI algorithms and datasets can reflect and/or reinforce unfair sensitive biases. Verint understands that distinguishing fair from unfair biases is not always simple and may differ across cultures and societies. We seek to avoid the use of our AI solutions resulting in unjust impacts on people, particularly those related to sensitive characteristics such as race, ethnicity, gender, nationality, income, sexual orientation, disability, age, and political or religious belief.

Accountable to People: Delivering trusted output that is accountable to people

The AI technologies and use cases Verint offers provide appropriate opportunities for assessments, relevant transparent explanations, and value. Our AI technologies are subject to appropriate human direction and control. This helps to manage risks related to ethical use cases, unintended consequences, and transparency, and provides mechanisms to help alleviate misinformation and manipulation.

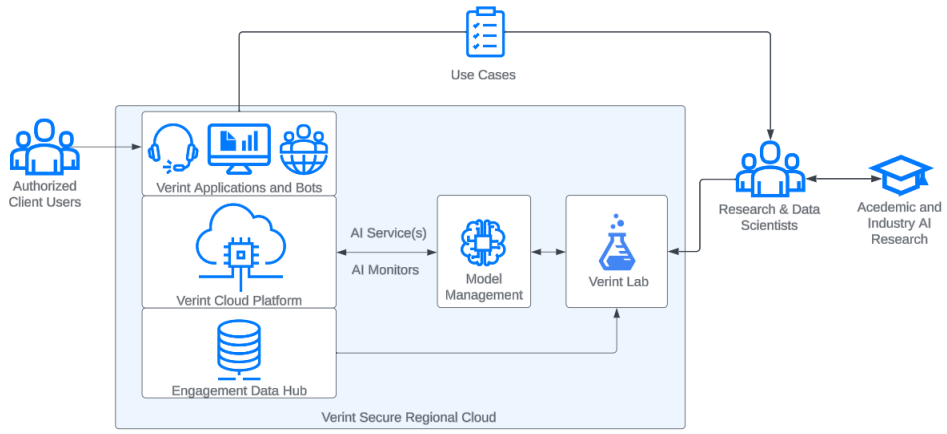
Processes and Controls

Verint has established and maintains standard practices across its research, engineering, development, and operational activities when AI is being offered in a solution, including:

- Development and deployment practices in accordance with compliance standards.
- Model management and data use and sourcing rules.
- Risk assessments built into processes and reviewed by compliance teams.
- Model monitoring.
- Support through our Verint Connect forums.

Development and Deployment Practices

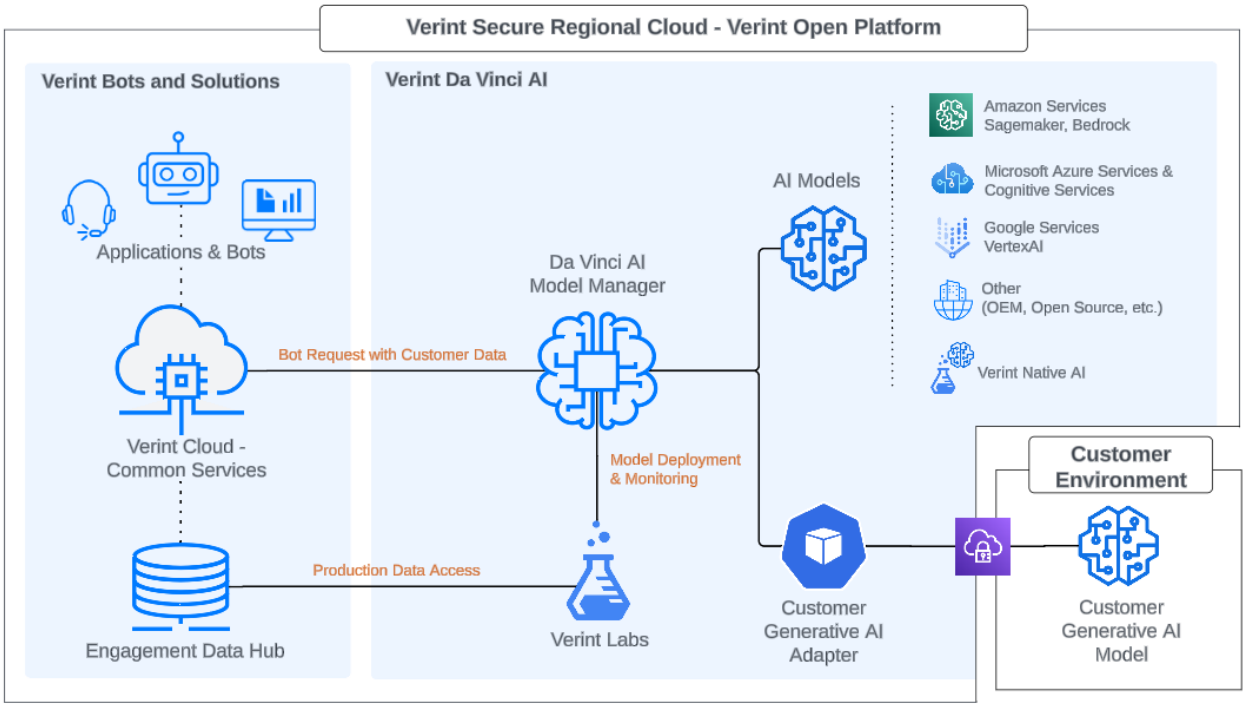
Verint's AI capabilities are developed and reside within the Verint Open Platform. The Verint Open Platform includes secure regional cloud environments wherein Verint maintains industry-standard security practices (https://www.verint.com/verint-cloud-security-and-compliance/) that follows applicable guidelines set forth by PCI, GDPR, ISO, SOC2, and HIPAA, as examples. Verint has implemented and maintains appropriate technical and organizational measures intended to protect personal data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction. Our security practices govern assets and data within our control, as well as our operating environments.



Verint AI Model Management: Data Use Sourcing Rules

Verint has also established practices for building, deploying, and managing AI models and data use restrictions:

- Customer data does not leave the Verint secure regional cloud environment when using our AI services.
- Verint may access, process and use customer data when improving or creating enhancements or new offerings related to the SaaS Service, however, no customer data is actually incorporated into such enhancements or new offerings.
- Verint's AI provision in its Master Service Agreement (MSA) makes clear:
    - Inputs and outputs are confidential information of our customer
    - Without a customer's written consent, Verint will not directly train AI models with customer data



Note that third-party AI services operate within the Verint Secure Regional Cloud environments. These services run in a private, not public, configuration. The services are fully controlled by Verint and do not permit the training of those third-party AI models using customer data, or provide access to inputs and outputs by those third parties.

AI Considerations and Guidelines

Verint has established a framework of considerations and guidelines for key factors that are involved in the development, deployment, and use of AI technologies. The framework addresses some common questions about how AI impacts these solutions. For example, is the service meant only to provide information for humans to act on, or is it meant for making automated decisions? How explainable are the model's predictions? Does the implementation provide any means to understand why the engine made the prediction it did? Is AI used in a way that can impact human employment or pay? Verint seeks to address these considerations across our solution offerings, as discussed above, and evaluates them from the following perspectives:

Transparency

Lack of transparency in AI systems, particularly in deep learning models, is a pressing issue. This opaqueness obscures the decision-making processes and underlying logic of these technologies. To help provide insight into those opaque areas, we seek to provide the context and scope of the information that the underlying algorithms and processes are using. This includes:

- Display transparency: Provides a real-time understanding of the task being performed by the AI, and of the actions the AI system is taking.
- Explainability: Provides information in a backward-looking manner on the logic, process, factors, or reasoning upon which the system's actions or recommendations are based.

Ethical Decision Making

Instilling ethical values in AI systems, especially in decision-making contexts with significant consequences, presents a considerable challenge. Researchers and developers must prioritize the ethical implications of AI technologies to avoid negative societal impacts.

We seek to address this by:

- Performing an AI ethics review for new projects as part of the research scope and definition process. The AI ethics review process explores the possible harms that can be caused by normal use of the AI: with high quality results; with incorrect or low-quality results; how the technology could be misapplied; and how the AI can correctly or incorrectly learn as it is used. The Verint ethics review includes the following questions and a discussion of how each issue may be mitigated:
    - What possible harms exist when the technology is being used as intended and functioning correctly?
    - What possible harm exists when the technology is being used as intended but giving incorrect results?
    - What possible harms exist following from potential misuse of the technology?
    - If the system learns from user input once deployed:
        - What checks and limitations are intended with respect to system learning?
        - Does that learning incorporate any customer specific data?
        - Is the learning applicable to the offering generally, or only at the tenant level?

Bias and Discrimination

AI systems can inadvertently perpetuate or amplify societal sensitive biases due to biased training data or algorithmic design. To minimize discrimination and ensure fairness, it is crucial to invest in the development of unbiased algorithms and diverse training data sets.

We seek to address this by:

- Being aware of commonly known biases that may be present in AI systems, such as data bias, algorithmic bias, and confirmation bias.
- Periodically reviewing, evaluating, and addressing AI-generated outputs during the development process for potential biases and inaccuracies.
- Addressing bias or accuracy issues reported through our Incident Management System as a bug/defect.
- Using AI systems provided by vendors with transparent methodologies and documentation to better understand their decision-making processes.
- Documenting and communicating any identified biases and mitigation efforts.

Privacy Concerns

AI technologies often collect and analyze large amounts of personal data, raising issues related to data privacy and security. To mitigate privacy risks, we endeavor to adhere to safe data handling practices.

We seek to address this by:

- Complying with privacy and other laws applicable to Verint as a provider of AI.
- Adhering to Verint's Code of Conduct, Global Information Security Policy, and privacy policies when accessing and processing personal data.
- Complying with our contractual obligations concerning the handling of customer data, including with respect to personal data.
- Using secure and data privacy linked environments, such as Verint Labs, to research, develop, and test AI systems or services.

Security Risks

As AI technologies become increasingly sophisticated, the security risks associated with their use and the potential for misuse also increase. Hackers and malicious actors can harness the power of AI to develop more advanced cyberattacks, bypass security measures, and exploit vulnerabilities in systems.

We seek to address this by:

- Adhering to Verint's internal AI Use Policy, these guidelines, and our Global Information Security Policy when using and developing AI systems.
- Using secure and data privacy linked environments, such as Verint Labs, to research, develop, and test AI systems or services.

Legal and Regulatory Considerations

New legal frameworks and regulations are being adopted around the world to address the unique issues arising from AI technologies, including allocation of responsibilities, liabilities, and intellectual property rights. Legal systems are evolving to keep pace with technological advancements and protect the rights of individuals and businesses.

The rights and laws that may apply to Verint offerings include:

- Data protection and privacy laws.
- Intellectual property laws.

- Laws applicable to employment, the protection of protected classes, or other human interest related laws and regulations.
- Laws regulating the use of AI itself.

We seek to address this by:

- Developing AI systems designed to be in compliance with applicable laws and regulations and designing such systems in a manner that allows compliant use by customers.
- Respecting third-party intellectual property rights in the design and development process.
- Adhering to Verint's internal AI Use Policy and these guidelines when developing AI services or systems that are used by our customers.
- Monitoring and reviewing applicable updates to legal and regulatory requirements and best practices.

Misinformation and Manipulation

AI-generated content, such as deepfakes, contributes to the spread of false information and the manipulation of public opinion. Efforts to detect and combat AI-generated misinformation are critical in preserving the integrity of information in the digital age. Data from individuals (such as customers of our customers) may be collected and fed into AI services for further enrichment or automation and often includes the type of information (i.e., personal sensitive information, voice audio recordings, pictures, account information, etc.) that can be used by malicious actors to falsely represent an individual. Scrutinizing the security of each AI service we use—as well as ensuring the AI service does not act on behalf of or represent itself as the consumer—are core focuses for us.

We seek to address them by:

- Ensuring the data inputs going into an AI service are protected, and there are safeguards to prevent interception or use by third parties for alternative purposes.
- Ensuring the AI service does not act on behalf of or represent itself as the consumer.

Unintended Consequences

AI systems, due to their complexity and lack of constant human oversight, might exhibit unexpected behaviors or make decisions with unforeseen consequences. This unpredictability can result in outcomes that negatively impact individuals, businesses, or society. Robust testing, validation, and monitoring processes can help developers and researchers identify and fix these types of issues before they escalate.

We seek to address this by:

- Designing AI models used in the service to provide explanations displayed to the human decision maker.
- Including in product documentation descriptions of the AI models used with the Verint Open Platform.
- Establishing a development approval process that requires review of how AI capabilities are combined with other Verint functionality, and how the AI will be adopted within the Verint offerings to restrict further development use cases without required approvals.

Model Monitoring

The Verint Open Platform provides capabilities to both actively (i.e., continually observe and analyze) and passively (i.e., issues reported through our standard support tickets) monitor AI services deployed for

customers in regional clouds around the world. Model monitoring serves as a measure to maintain the health, efficiency, and effectiveness of AI applications or bots.

Passive Monitoring

Verint provides a mechanism for clients, partners, and Verint employees (i.e., professional services team members working on behalf of clients) to submit support tickets about application or bot behaviors that are unexpected or should be investigated. Verint's support organization will coordinate with the appropriate product, engineering, and research teams behind the scenes to address the issue or to answer a question.

Active Monitoring

Active model monitors may be put in place as part of the core project definition across engineering/architecture, research, and development depending on the use case. Each application or bot that deploys AI can monitor performance and incorporate enhancements back into the core model, provide additional training data, perform additional model training events, or implement other remediation tasks to address problems identified by the monitor.

Support for AI

Verint Connect is the Verint extranet for customers and partners and is the primary support mechanism for these constituents to contact Verint, ask questions, find information, report problems, and receive training materials. If any question, issue, or problem with an AI component of a Verint solution is encountered, it can be reported through Verint Connect with the appropriate severity rating for a response by Verint.