

Individual Consumers Seek Certification for their Responsible Use of AI

Read about private individuals and employees who use PrivacyPortfolio's Yo-ai platform to become proficient in the use of AI and receive acknowledgment for their Responsible Use of AI.

Now, you can be a Responsible AI Expert

One AI risk is when AI is controlled exclusively by commercial enterprises and government agencies. Putting you in control of Yo-ai Agents helps ensure that private individuals enjoy free and equal access to technology. We're betting that anything businesses can do with AI, consumers can also do – sometimes even better.

Sign up on Yo-ai as a Registered Stakeholder and earn a Responsible AI certification for your team of AI Agents.

Our Responsible AI Certification Program is maintained by our users who monitor, test, and evaluate the Yo-ai Platform. Yo.ai's Risks and Rewards Program includes incentives for Registered Stakeholders to be responsible in their use of AI, and be awarded a certificate of completion for participating in the successful certification by TrustArc, [TRUSTe Responsible AI](#). Even better – if you are a Registered Stakeholder of an organization that obtains their own Responsible AI certification, you could earn \$1000. Take the next step in hypercharging your career!

Employers are looking for talented individuals with practical AI skills and expertise.

If you work for a company that doesn't provide you with opportunities to use AI in your current role, Yo-ai will.
If your company doesn't provide a budget for your team to procure your own tools and vendors, Yo-ai will.
If your company doesn't provide any training that will help you use AI rather than be displaced by it, Yo-ai will.
If you're not a member of iapp or some other professional association, or you don't have a college degree in an AI discipline, you don't have to pay for private courses or settle for proprietary AI Developer certifications, because that's baked into the Yo-ai Platform.

Some employers look for candidates who can say, "I held this AI role at this AI company".

With Yo-ai you can say, "I am the Human Responsible for all activities involving my personal team of AI Agents. My team has assessed how your organization and many of your vendors use AI, and I can help you..."

Yo-ai's Responsible AI Program

As a Responsible AI company, PrivacyPortfolio assesses Risks of Automated Decision-making Technologies by:

- Discovering if companies are using AI to make automated decisions
- Defining the Decision Sets
- Discovering the components of Automated Decision-making Technologies (ADMT)
 - Discovering the data: ingested, generated, used for training models
 - Identifying company ownership and stakeholders
 - Identifying individuals impacted by ADMT
 - Classifying probable harms to impacted individuals
 - Discovering who uses the ADMT for what purpose(s)
 - Discovering what personal data is shared by/with users, consumers, developers, processors
 - Discovering, classifying, and identifying AI Agents in Agentic Systems
- Assessing how AI data is governed according to policy and law
- Assessing effectiveness of controls
- Training all Yo-ai Platform Users in the Responsible Use of AI

Leading by example, PrivacyPortfolio uses Yo-ai to make automated decisions.

The Decision Sets are:

- 1) Should I register as a Stakeholder in this Organization
- 2) Which risk handling options will I choose for this Organization
- 3) How to measure the transparency of this Organization's AI Processes



The advantages of learning how to use AI responsibly on the Yo-ai Platform include:

- ➔ You work with actual tools, working AI Systems, and controls – not multiple choice questions about theoretical constructs
- ➔ Positive and negative use cases are based on actual events with organizations controlling your data
- ➔ The Yo-ai Platform was designed from the ground up to implement and validate Responsible AI methods
- ➔ Other Registered Stakeholders provide a community to support your training and help you solve problems
- ➔ You may receive feedback and advice from very prominent, knowledgeable experts about your work

Here are the certification requirements and corresponding control mechanisms which also serves as the curriculum outline for becoming a Certified Responsible AI Practitioner:





TRUSTe Requirement

Yo-ai Platform Controls

<p>1. Monitor Intended Use Requirement: The Participant must monitor the AI System to ensure that it is performing as intended, and that outputs are consistent with the Participant’s expectations. Mechanisms may include policies or procedures that address the following: ≥ who will be involved in monitoring and analysis ≥ what needs to be monitored ≥ the methods for monitoring, analysis and evaluation to validate ≥ the frequency of the monitoring ≥ performance according to intended use ≥ when monitoring and analysis will be performed ≥ defined relevant monitoring metrics</p>	<p>When a risk of harm is identified among these events, it is called a Threat. When a Threat causes actual harm, it is called a Loss Event.</p> <p>The Sentinel, is a special platform agent that listens to events, and flags risk events, which are categorized as Threats.</p>  <p>Sentinel: I listen for dangerous incidents and trends. Also listens for decision-making events.</p> <p>The Yo.ai Platform prioritizes risks to Consumers from automated decision-making technologies. When a "decision-making event" is detected by The Sentinel, it is forwarded to another special agent, the Decision-Master.</p> <p>Decision-Master, is a special platform agent that evaluates decision-making events, and logs them to the "Decision Diary", which is equivalent to a "Risk Register".</p>  <p>Decision-Master Maintains the Decision-Diary</p>
--	---

TRUSTe Requirement

Yo-ai Platform Controls

<p>2. Audit Accuracy of Outputs Requirement: The Participant must audit the accuracy of the AI System’s outputs if the output is likely to result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals. Mechanisms may include QA testing procedures to measure accuracy that address the following: ≥ a description of the methodology used to measure accuracy/how will accuracy of AI outputs be monitored after the AI is deployed ≥ clearly defined and realistic test sets that are representative of the conditions of intended use ≥ false positive and false negative rates ≥ human involvement in AI decision-making.</p>	<p>Organization Profiles uniquely define each organizational entity. These profiles are shared with ALL Registered Stakeholders.</p> <p> Organization Profile Sample</p> <p>Consumer Profiles uniquely identify each individual consumer. These profiles are ONLY shared with your Data-Steward, or anyone else you authorize.</p> <p> Consumer Profile Sample</p> <p>AI Agents leading each subdomain represents the interests of stakeholders:</p> <p>The Vendor Manager:  manages and represents Organizations</p> <p>The Data Steward:  manages and represents Consumers</p>
---	--


TRUSTe Requirement

Yo-ai Platform Controls

<p>3. Human Oversight Requirement: Taking into account the purpose of processing and where it is likely to result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals, the Participant must have mechanisms in place for human oversight where the AI System cannot detect or correct its own errors, or requires human oversight for the AI System to function properly according to its instructions or other documentation for its intended use. Mechanisms may include policies and procedures that address: ≥ how a human operator is notified of/becomes aware when inaccurate outcomes occur ≥ the procedure for how a human operator corrects errors in the AI System</p>	<p>Craig Erickson is the Responsible Human for the entire Yo-ai Platform, accountable to all Registered Stakeholders. Registered Stakeholders are the Responsible Humans for the AI Agents assigned to them, which they control.</p>
--	--


TRUSTe Requirement

Yo-ai Platform Controls

<p>4. Document System Decisions Requirement: The Participant must document or have documentation about how the AI System works and how it makes decisions/generates outputs. Information must be provided about: ≥ the mechanisms underlying the AI System’s operation ≥ the AI System’s knowledge limits, ≥ where used for automated decision making, identify how system outputs may be used. Documentation should provide: ≥ sufficient information to assist relevant Personnel when making decisions and taking subsequent actions.</p>	<p>Explore our "Decision Diaries" to see what companies are doing with AI</p>  <pre> { "timestamp": "2023-12-05T14:45:30Z", "ai_agent_id": "AI-56789", "event_type": "DecisionMade", "decision_details": { "input_data": { "customer_id": "CUST-12345", "transaction_amount": 1200, "transaction_type": "Purchase", "location": "New York, USA" }, "model_version": "1.3.2", "decision": "Flag for Review", "reasoning": "Transaction amount exceeds threshold for first-time purchase", "confidence_score": 0.92 }, "audit_metadata": { "initiator": "AI_Agent", "reviewer": "None", "status": "Pending" } } </pre>
--	---

TRUSTe Requirement

Yo-ai Platform Controls

<p>5. Review and Update Documentation Requirement: The Participant must regularly review documentation explaining how the AI System works and makes decisions/generates outputs, and update or request updated documentation where necessary. Policies and procedures should be in place that address the following: ≥ the frequency of reviews ≥ date and time tracking of reviews ≥ the personnel involved in the review ≥ what decisions/outputs are reviewed ≥ what updates are made, if necessary.</p>	 <p>Incident-Responder</p> <p>Responds to platform incidents (aka "Agent terminator", "Kill switch", etc)</p> <p>Craig Erickson, responsible for the entire Yo-ai Platform, can quickly respond to any incident even while on vacation. Actions taken by the Incident-Responder, like shutting down all AI Agents, are recorded by The Solicitor-General which records all requests and responses, the Decision-Master which records all decision-related events, and The Sentinel, our ever-present listener and watchdog.</p>
--	--

TRUSTe Requirement

6. Accessible Information and Explanations Requirement:

The Participant must make accessible information and explanations that will help Personnel and vendors understand how the AI System works and why the AI System makes decisions/generates outputs.

The Participant should be able to describe how data is used to determine an AI System's output. Descriptions should be appropriate to the stage of the AI lifecycle, and tailored based on risk level and to individual differences in the target audience, such as their role, knowledge, and skill level.

Yo-ai Platform Controls

The screenshot shows a chat window with a grey header containing a question: "Task the Sentinel-General, what happened when I asked for a comparative risk assessment between my current ISP and my new ISP vendor organization?". Below the question is a large yellow response box with a speech bubble icon. The text in the yellow box explains that the Risk Assessor consulted two other agents, the Tech Inspector and the Ethicologist, to compare their AI Risk Inspection reports and generate the two organizational profiles. It states that based on these profiles, the Risk Assessor decided to use a compliance framework (the NIST Cybersecurity Framework (CSF)) for the new ISP risk assessment. It also notes that the Sentinel-General was alerted to these events in the Decision Diary and that no decisions were made automatically on your behalf. The response concludes with the question: "Would you like to see what those decisions were, or what adverse risk events led to those decisions, or would you like to review and approve the two RISK ASSESSMENTS?".

TRUSTe Requirement

Yo-ai Platform Controls

<p>7. AI Policy Requirement: The Participant must establish an AI Policy that describes the Participant’s use and other acceptable uses of AI, and establish mechanisms to standardize and communicate the policy with Personnel and vendors interacting with the AI System. The AI Policy or suitable alternatives should substantially address the use of, restrictions to, and risk management around AI Systems. Examples of the preceding may include the following concepts:</p> <ul style="list-style-type: none"> ≥ key terms and concepts related to AI Systems and the scope of their purposes and intended uses ≥ the need for business justification for using AI ≥ acceptable uses of AI, including the acceptable amount of drift from baseline performance ≥ expected and potential risks and impacts ≥ an overarching vision for AI usage and growth in the organization, including mission statements, clear objectives, and/or KPIs that align with this vision ≥ detailed information about regional, industry-specific, and relevant regulatory compliance laws as well as other ethical considerations ≥ a catalog of approved tools and services that can be used for AI deployment purposes ≥ clearly defined roles and responsibilities related to the usage and management of AI Systems ≥ data privacy and security mechanisms ≥ defined procedures for reporting and addressing AI performance and security issues ≥ standards for AI model performance evaluation ≥ consequences and outcomes for violations of the policy. <p>The Participant may communicate the AI Policy through mechanisms such as:</p> <ul style="list-style-type: none"> ≥ email ≥ employee intranet ≥ vendor contracts and/or agreements 	<div data-bbox="968 261 1759 646" style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>Responsible AI Policy PrivacyPortfolio</p> <p>Effective Date: 1/2/2025</p> <p>Introduction</p> <p>My name is Craig S. Erickson, a California Consumer who has authorized PrivacyPortfolio, LLC to represent my interests and to make decisions and act on my behalf.</p> <p>In my role as a California Consumer, I strive to comply with all applicable laws, ethical values, and best practices for cybersecurity, audit, privacy, data protection, and vendor risk management. Consumers also use, develop, and deploy artificial intelligence (AI) technologies and PrivacyPortfolio helps them comply with relevant laws and best practices for achieving their desired goals.</p> <p>As the sole manager of PrivacyPortfolio, I am also the Responsible AI Officer designated to oversee compliance with this policy and certification requirements.</p> </div> <p>The AI Policy Requirement gives examples that the Participant <i>MAY provide</i>. Information that changes more frequently than updates to the policy are published elsewhere. Many reports regarding system performance, organizational profiles, decision-making activities, and risk assessments are published in a public data catalog. Information pertaining to technical issues and updates can be access from code repositories. The Yo-ai Platform records everything so that communication sent and received by any party and their contents cannot be repudiated.</p> <p>PrivacyPortfolio’s Responsible AI Policy is itself, an “intelligent document”:</p> <p>Policy Revisions, Implementation, and Review</p> <p>This Responsible AI Policy shall be reviewed and updated annually or as needed to reflect changes in technology, regulations, and best practices. Violations of this policy will require updating our AI Policy to reflect actual practices not remedied within 3 months of discovery. This policy is published on our public website: https://privacyportfolio.com, in our vendor contracts and/or agreements, and Vendor Notification Campaigns. Registered stakeholders can subscribe to this policy and receive notifications by email of any changes.</p>
---	---

TRUSTe Requirement

Yo-ai Platform Controls

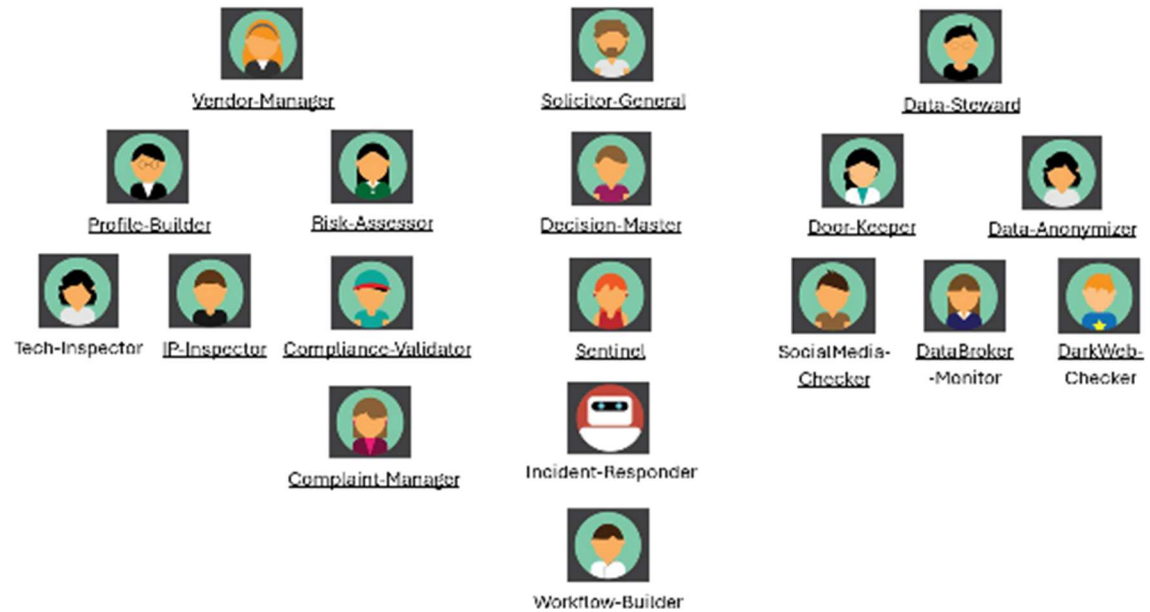
8. Data Governance Requirement:

The Participant must identify and document information about the data used for the AI System, such as through a Data Governance Policy, or similar documentation [e.g., record of processing activity (ROPA), data inventory, or a data protection impact assessment (DPIA)].

Documentation should include but is not limited to, the following topics:

- ≥ the provenance of the data used in AI Systems over the life cycles of the data and the AI System, including the categories of data collected (proprietary information, personal and non-personal), the origins of data, and the original purpose of collection (if Personal Information or proprietary information)
- ≥ the date that the data were last updated or modified (e.g., date tag in metadata)
- ≥ defined roles for AI governance including the person or team responsible for machine learning, the categories of data, process for labeling data, intended use of the data, quality of data, applicable data retention, and disposal policies.
- ≥ known or potential bias issues in the data
- ≥ the criteria for selecting data preparations and the data preparation methods to be used.

Yo-AI Agent Org Chart



Data governance is so much easier when the organizational structure fits the technical architecture.

Policy compliance is maintained by AI Agents more consistently than their human counterparts: they don't forget what they're supposed to do, they don't resist being told what to do and how to do it, and they have no other legitimate concerns or activities to distract them from performing their tasks.

TRUSTe Requirement

Yo-ai Platform Controls

<p>9. Alert on Adverse Outcomes Requirement: The Participant must have mechanisms in place to alert human operators to adverse outcomes or impacts of the AI System if the output is likely to result in decisions that produce adverse legal or similarly significant effects (e.g., material security or reputational concerns), which may include, but not limited to, any risk to rights and freedoms of individuals. Mechanisms may include regular auditing, procedures to monitor the AI System’s operation for reported issues and failures, and capabilities for external parties to report adverse impacts (e.g., unfairness). Transparency should encompass human-AI interaction: for example, how a human operator or others interacting with the system are notified when a potential or actual adverse outcome caused by an AI System is detected.</p>	<p>On the Yo-ai Platform, Adverse Outcomes are called “Harms” or “Loss Events”. When a Harm or Loss Event occurs, The Sentinel is the first to know about it. However, the Vendor-Manager agent is responsible for determining which Organizations are impacted by an Adverse Outcome; and the Data-Steward agent identifies which Consumers are impacted by an Adverse Outcome. Any risk to rights and freedoms of individuals applies equally to Organizations and Consumers, and these risks are registered in the Decision Diaries, and evaluated in Risk Assessments. The correlation between risk and impacts are documented in Impact Assessments, which assess the magnitude of impacts to associated organizations and consumers.</p>
--	---

TRUSTe Requirement

Yo-ai Platform Controls

<p>10. Procurement Requirements: The Participant must have appropriate contracts in place with third-party providers of AI Systems and models. Contracts should, as applicable, address the following: ≥ a description and/or instructions on the intended use and any restrictions on use of the procured AI System and any data obtained in association with the procured model ≥ mechanisms to report on potential vulnerabilities, risks or biases that arise in the AI System during the tenure of the procurement agreement ≥ whether model training is permitted ≥ data protection considerations where required including any limits on the selling and sharing of Personal Information if applicable.</p>	<p>According to real-life observations of current third-party risk management practices, contracts are treated as “confidential, proprietary, or as trade secrets”. No business or consumer has the right to demand information about business contracts they are not a signatory to. This is most problematic for consumers who need proof of authorization to process their personal information. Organizations and lawyers often dispute that consumers need this evidence, so this is the right time and place to put them on notice: Registered Stakeholders who want to maintain their Responsible AI Certification actually do need this evidence, and every Organization denying access to this information is obstructing Consumers from being certified as Responsible AI Practitioners. Registered Stakeholders are encouraged to “Opt-In” to the sale and sharing of their personal information, and have data protections on the Yo-ai Platform that allow them to do so safely. In lieu of disclosing written contracts with their vendors and customers which authorize the processing of personal information, the Yo-ai Platform may use any of the Organization’s policies and/or transactions covered under the UETA as written agreements for the purpose of certifying the Responsible Use of AI by Registered Stakeholders.</p>
--	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>11. Privacy Disclosures Requirement: The Participant must disclose to Individuals interacting with the AI System information about its use of AI inputs and outputs, and the rights of Individuals relating to AI System outcomes. ≥ Disclosures should be in clear and plain language, and inform Individuals of characteristics of the Participant in its operation of the AI System and of the AI System itself. ≥ Individuals should be informed that they are interacting with an AI System at the time of interaction, such as through a privacy notice or other mechanism. ≥ Information can be incorporated into privacy policies that are made publicly available to all individuals who interact with the AI System.</p>	<p>Privacy Policy PrivacyPortfolio Effective Date: 1/2/2025</p> <div style="background-color: #f2f2f2; padding: 5px;"> <p>About Me PrivacyPortfolio, LLC is a limited liability corporation registered in the State of California, USA. As the sole manager of PrivacyPortfolio, LLC, Craig Erickson is accountable for all activities covered by this policy.</p> </div> <div style="background-color: #f2f2f2; padding: 5px;"> <p>My Mission Empower individuals to exercise their privacy rights, hold organizations accountable for honoring their privacy policies and practices, and objectively report on the performance of enforcement authorities.</p> </div> <div style="background-color: #f2f2f2; padding: 5px;"> <p>My Policy This privacy policy represents claims and rules pertaining to PrivacyPortfolio's privacy practices.</p> </div> <div style="background-color: #f2f2f2; padding: 5px;"> <p>About You An individual or entity "accepting" this policy is known as a "Subscriber". This role designation recognizes the individual or entity as a consumer of the Publisher's (PrivacyPortfolio) resources, serving as the implied contractual basis and scope for a Subscriber's data privacy rights.</p> </div>
--	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>12. Data Input Limitation Requirement: The Participant must, where possible, limit the input of data used in the AI System that the Participant has deployed. The Participant shall determine and document the techniques used to ensure that the data is limited, where possible, to what is necessary and relevant to achieve the purpose for which the AI System has been deployed. Examples of the techniques that could be used to achieve this purpose are: ≥ periodic reviews of the amount of data used and nature of the inputs ≥ deletion of data that is no longer necessary and relevant ≥ limit the types of data that can be used or submitted</p>	<p>The Data-Steward governs access to personal information used for any purpose, including the training of AI systems and the use of deployed AI systems. The Door-Keeper controls and manages access to the Data-Steward who controls and manages the Personal Data Vault of the Registered Stakeholder. A number of other agents, the SocialMedia-Checker, the DataBroker-Checker, and the DarkWeb-Checker assist the Data-Steward by discovering Undisclosed Collections in data sources which cannot be attributed to a specific Organization or its direct stakeholders. Any incidents involving the use of personal information elements and associated profile information which are identified as inputs or outputs of automated decision sets will be detected by the Decision-Master and The Sentinel.</p>
---	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>13. Output Limitation Requirement: The Participant must limit the use of the AI System outputs to the purposes for which the AI System is intended to be used if the output is likely to result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals. The Participant must have documented policies in place that outlines the intended uses of the AI System. For example: ≥ The output of an AI System that scans a candidate resume during the hiring process, must only be used for the intended purpose of helping determine the best candidate. ≥ The output of an AI System that helps to determine the creditworthiness of a mortgage applicant, must only be used for the purpose of reviewing the mortgage application.</p>	<p>Any incidents involving the use of personal information elements and associated profile information which are identified as inputs or outputs of automated decision sets will be detected by the Decision-Master and The Sentinel.</p> <p>In addition, inputs are treated as “Requests” and outputs are treated as “Responses” on the Yo-ai Platform, which all go through The Solicitor-General agent that records everything in a platform event log.</p> <p>The Data-Steward determines what the intended purpose is for using personal information when it is shared or discovered. If no evidence exists that the information was used, it is flagged in Yo-ai as an indication of “collecting more information than necessary” or “possible usage for unauthorized purposes”.</p>
--	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>14. Prevent Re-identification Requirement: The Participant must implement processes that will prevent inferences to identify Individuals or allow for re-identification of previously de-identified Personal Information. For example: ≥ the Participant could provide a Data Management Policy or similar policy if the document includes what measures are in place. ≥ a description or evidence of the process that is in place (e.g., to de-identify data).</p>	<div data-bbox="989 898 1087 1015" data-label="Image"> </div> <div data-bbox="1108 922 1507 971" data-label="Text"> <p>Uses a variety of tools and techniques for anonymizing and testing datasets of personal attributes.</p> </div> <p>The Yo-ai Platform is capable of testing psuedo-anonymous and aggregated data sets for re-identification due to the massive Consumer profiles it collects from all types of Organizations. This capability is also heavily used to produce not only reports, complaints, and risk assessments, but also for communications between Registered Stakeholders.</p>
--	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>15. Data Accuracy Used to Deploy AI System Requirement: Upon request: ≥ the Participant must enable Individuals to challenge the accuracy of the Personal Information that has been used by AI Systems deployed by the Participant if the output is likely to result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals. ≥ the Participant must provide access to the information used by the AI System, and rectify any inaccurate Personal Information upon receipt of sufficient information confirming the Individual’s identity, in line with the Participant’s individual rights request handling procedures, and applicable laws. ≥ the Participant’s processes or mechanisms for access and rectification of inaccurate Personal Information used to deploy AI Systems must be simple and easy to use, and presented in a clear and conspicuous manner. ≥ the Individual’s request must be responded to within a reasonable timeframe following its receipt, and the Individual is provided access and rectification of their Personal Information, and a copy of the corrected information. ≥ if the Participant denies access and correction to the information used to deploy the AI System cannot be made, the Participant must explain to the Individual in clear and easy to understand language why the access and correction request was denied, and provide the appropriate contact information for challenging the denial of the request where appropriate.</p>	<p>Only one entity can determine whether the personal information of a consumer is accurate: <i>the Consumer</i>.</p> <p>However, Consumers can make mistakes. Consumers can lie. Consumers forget. Consumers’ personal information is subject to change at any time.</p> <p>The Yo-ai Platform is used by Consumers to manage and govern their personal information.</p> <p>Registered Stakeholders are known – which is the purpose of being registered. They have quick, easy access to authoritative documents establishing the source of personal data elements. They have a team of AI Agents that discover personal information “in the wild” and compare it with “golden records” maintained in their Personal Data Vaults.</p> <p>Registered Stakeholders have the choice of sharing this “high-quality” of personal information with Organizations that want it. The Yo-ai Platform is capable of allowing Organizations to access designated datasets in real-time without storing the information in the Organization’s domain.</p>
--	---

<p>15. Data Accuracy Used to Deploy AI System Requirement (continued): Access and correction may be denied or limited under the following circumstances: ≥ where providing access would violate the legitimate rights of persons other than the Individual; ≥ where the burden or expense of providing access would be disproportionate to the risks to the Individual’s privacy; ≥ where providing access would reveal the Participant’s own confidential commercial information—such as marketing inferences, classifications generated by the organization, or confidential commercial information of another that is subject to a contractual obligation of confidentiality; ≥ where providing access would interfere with the safeguarding of important countervailing public interests—such as national security, defense, or public security; ≥ where Personal Information is being processed solely for research or statistical purposes; ≥ where providing access would interfere with the execution or enforcement of the law or with private causes of action—including the prevention, investigation, or detection of offenses or right to a fair trial; ≥ where providing access would breach a legal or other professional privilege or obligation; ≥ where providing access would prejudice employee security investigations or grievance proceedings or in connection with employee succession planning and corporate reorganizations; or ≥ where providing access would prejudice the confidentiality necessary in monitoring, inspection, or regulatory functions connected with sound management, or in future or ongoing negotiations involving the Participant.</p>	<p>Yo-ai does not rely on Organizations to cooperate in any way, or to provide any information to Registered Stakeholders. Yo-ai also does not rely on Organizations which regulate Organizations, such as regulatory and enforcement agencies to preserve the rights of individuals, including privacy protection laws.</p> <p>Yo-ai provides “incentives” to Organizations for their cooperation. These incentives include remediation solutions, consumer controls, and published risk assessments by Registered Stakeholders which are shared with “Named Stakeholders”.</p>
---	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>16. Challenge AI System Outcomes Requirement: Upon request, the Participant must enable Individuals to ask questions and submit complaints regarding the AI System, challenge its outcomes (e.g., how the decision was made and why), and request human review where the AI System’s decisions produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to the rights and freedoms of individuals. ≥ the Participant must have mechanisms and procedures in place to address an Individuals’s questions and complaints. ≥ the request must be responded to within a reasonable timeframe following an Individual’s complaint submission or request for human review .</p>	<p style="text-align: center;">AI ASSURANCE PLATFORM FOR CONSUMERS AND ORGANIZATIONS</p> <h2 style="text-align: center;">Do you have the right to COMPLAIN?</h2> <p style="text-align: center;">Will there be consequences, if you do?</p> <p style="text-align: center;">Browse our "Complaint Center" to see what actually happens</p> <div style="text-align: center;"> </div> <p>Due to the lack of actionable information these agencies provide to consumers who file complaints, the Yo-ai Platform also serves as a research and learning platform for academic scholars and professionals in law, privacy, cybersecurity, audit, and AI.</p> <p>These experts can become Registered Stakeholders, weighing in on the business practices of Organizations and the validity of complaints filed against them.</p>
---	--

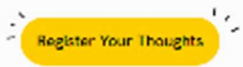

TRUSTe Requirement

Yo-ai Platform Controls

<p>17. Inputs Review & Testing for Biases Requirement: The Participant must have processes to regularly review inputs of data and test AI Systems to identify system biases. The quality of data used to deploy AI Systems potentially has significant impacts on the validity of the system’s outputs. The Participant should implement processes to ensure that measures are integrated into the various stages to achieve such objectives.</p>	<p>Organizations routinely represent the interests of stakeholder groups whose members they have no knowledge of. As dedicated caretakers of anonymous populations, we expect gaps between what Organizations and Consumers think are in their interest. This includes testing for bias. Many legislative affairs representatives for AdTech industry associations warn that “Opting-out from using personal information to train AI Systems can result in bias.” The Yo-ai Platform takes a “bottom-up approach” similar to federal prosecutors who start at the scene of a crime and work their way up to the leaders. Yo-ai monitors specific decisions made by specific Organizations about specific Consumers. Bias testing generally occurs after impacts are recorded, with root causes investigated or evaluated by Risk Assessments.</p>
---	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>18. Reviewing & Reversing Negative Outputs Requirement: The Participant must have procedures in place to review, reverse or overturn adverse outcomes, when the outcomes result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals. The Participant must have the following in place: ≥ definition of what is considered a negative output ≥ procedures to review the complaints ≥ procedures to evaluate and determine if a non-conformity occurred that caused negative consequences for Individuals ≥ a procedure to evaluate whether similar non-conformities exist ≥ a process to review the above procedures and make changes where necessary.</p>	<p>The Yo-ai Platform is not capable of reversing negative outputs. The Yo-ai Platform relies on Remediation Tools as incentives to Organizations to fix these issues from re-occurring.</p> <div data-bbox="835 917 1703 1507" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p style="text-align: center; font-size: small;">AI ASSURANCE PLATFORM FOR CONSUMERS AND ORGANIZATIONS</p> <h2 style="text-align: center;">Will your remedy be ACCEPTABLE?</h2> <div style="text-align: center; margin: 10px 0;">  </div> <p style="text-align: center; font-size: x-small;">When consumers file a formal complaint with a State's Attorney General, they are sometimes asked, "What resolution would you feel is appropriate?"</p> <p style="text-align: center; font-size: x-small;">Enforcement agencies, like organizations, would hardly be shocked to see responses to this question that are illegal, irresponsible, impractical, or simply unreasonable.</p> <p style="text-align: center; font-size: x-small;">Yo.ai can recommend specific remedies which are more likely to be acceptable to all stakeholders.</p> <div style="text-align: center; margin: 10px 0;">  </div> <ul style="list-style-type: none"> • Remedies mandated by regulatory agencies in consent decrees from similar cases. • Remedies which use technologies and resources the organization already possesses. • Remedies which the organization's partners, vendors, or customers have used to correct similar deficiencies. • Remedies that are tested and verified as acceptable to all stakeholders within a reasonable time frame. </div>
--	--

TRUSTe Requirement

19. AI System Risk Assessment Requirement:

The Participant must have an AI risk assessment or similar assessments in place if the outcomes of an AI System result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to the rights and freedoms of Individuals.

A risk assessment should provide the following information:

- ≥ a description of what the AI System will be used for
- ≥ a description of the Participant’s processes to determine if the AI System will be used in line with its intended purpose
- ≥ a description of the period of time and frequency in which the AI System is intended to be used
- ≥ the types of data used by the system as inputs and the types of data generated by its outputs
- ≥ the categories or demographics of Individuals and groups likely to be affected by the system’s use
- ≥ the positive impact of the AI System to Individuals, society, or the environment.
- ≥ the specific risks of harm likely to impact the identified categories of Individuals or groups
- ≥ a description of human oversight measures
- ≥ the measures to be taken in case that these risks materialize, including arrangements for internal governance and complaint mechanisms.

The assessment should enable the Participant to analyze the AI risks to:

- ≥ identify potential consequences to the Participant and Individuals affected by AI System outputs if identified risks occur
- ≥ determine the realistic likelihood of the identified risks
- ≥ determine the levels of risk based on the sensitivity of the data within the AI System and its intended uses
- ≥ determine the controls necessary to mitigate identified risks.

The assessment results must be documented and made available to interested parties as determined by the Participant or as required by applicable law.

Yo-ai Platform Controls

Privacy Threshold Assessment	Status of California Requirements	Page 5										
<p>III. PRIVACY THRESHOLD ASSESSMENT</p> <p>I. Project / Process / System / Program Information</p> <table border="1"> <thead> <tr> <th>Questions</th> <th>Answers</th> </tr> </thead> <tbody> <tr> <td> <p>New Project Name: Brief description of the project / process / system / program:</p> </td> <td> <p>Mandatory AI and Automated Decision-making Technologies (AOT) Risk Assessment Submitted to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.</p> </td> </tr> <tr> <td> <p>Data Classification: (Per SIMM 5306 A) * Check all that apply Security Categorization: (NIST 800-53) (Per RIPS 109) *Select only one</p> </td> <td> <p><input type="checkbox"/> Confidential <input type="checkbox"/> Sensitive <input checked="" type="checkbox"/> Public <input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low</p> </td> </tr> <tr> <td> <p>Has a system security plan been completed for the project?</p> </td> <td> <p><input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A If No or N/A is selected, please explain why it is not completed and when it will be completed (e.g., before go-live).</p> </td> </tr> <tr> <td> <p>Is there a Generative Artificial Intelligence (GenAI) component or byproduct to this project, regardless of whether it is incidental or incidental?</p> </td> <td> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," attach the completed mandatory GenAI Risk Assessment (SIMM 5305-F). Adobe discloses its use of Microsoft Azure OpenAI Service but does not specify which version of ChatGPT is used as the foundational model.</p> </td> </tr> </tbody> </table>			Questions	Answers	<p>New Project Name: Brief description of the project / process / system / program:</p>	<p>Mandatory AI and Automated Decision-making Technologies (AOT) Risk Assessment Submitted to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.</p>	<p>Data Classification: (Per SIMM 5306 A) * Check all that apply Security Categorization: (NIST 800-53) (Per RIPS 109) *Select only one</p>	<p><input type="checkbox"/> Confidential <input type="checkbox"/> Sensitive <input checked="" type="checkbox"/> Public <input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low</p>	<p>Has a system security plan been completed for the project?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A If No or N/A is selected, please explain why it is not completed and when it will be completed (e.g., before go-live).</p>	<p>Is there a Generative Artificial Intelligence (GenAI) component or byproduct to this project, regardless of whether it is incidental or incidental?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," attach the completed mandatory GenAI Risk Assessment (SIMM 5305-F). Adobe discloses its use of Microsoft Azure OpenAI Service but does not specify which version of ChatGPT is used as the foundational model.</p>
Questions	Answers											
<p>New Project Name: Brief description of the project / process / system / program:</p>	<p>Mandatory AI and Automated Decision-making Technologies (AOT) Risk Assessment Submitted to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.</p>											
<p>Data Classification: (Per SIMM 5306 A) * Check all that apply Security Categorization: (NIST 800-53) (Per RIPS 109) *Select only one</p>	<p><input type="checkbox"/> Confidential <input type="checkbox"/> Sensitive <input checked="" type="checkbox"/> Public <input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low</p>											
<p>Has a system security plan been completed for the project?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A If No or N/A is selected, please explain why it is not completed and when it will be completed (e.g., before go-live).</p>											
<p>Is there a Generative Artificial Intelligence (GenAI) component or byproduct to this project, regardless of whether it is incidental or incidental?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," attach the completed mandatory GenAI Risk Assessment (SIMM 5305-F). Adobe discloses its use of Microsoft Azure OpenAI Service but does not specify which version of ChatGPT is used as the foundational model.</p>											

Yo-ai’s AI Risk Assessments are conducted according to NIST 53r5 Control Standards and requirements mandated by the California Privacy Protection Agency.

Risk assessments are only conducted by Registered Stakeholders on Organizations that might process their personal information.

TRUSTe Requirement

Yo-ai Platform Controls

<p>20. Qualified Personnel and Awareness Requirement: The Participant must ensure that Personnel who rely on the AI System outputs to perform their job functions and interpret the system’s outputs are competent and qualified on the basis of appropriate education, training or experience, and are made aware of the following: ≥ Participant’s AI policy and/or procedures ≥ their responsibilities and duties relating to data and system usage, interpretation of system outputs, security, and privacy ≥ the implications of not conforming with the AI System requirements and intended use, and the impacts of decisions made based on the system’s outputs. Policies, responsibilities, and implications of non-confirmatory must be communicated at the time that Personnel starts performing job functions that rely on the system’s outputs and are reinforced on a regular basis taking into account the risks related to such tasks.</p>	<p>Yo-ai does not routinely evaluate the qualifications of an Organization’s employees, which are entitled to privacy protections as Consumers. These are the permitted exceptions to this policy:</p> <ul style="list-style-type: none"> • Publicly named employees who are authorized to represent the Organization, identified in the Organization’s correspondence, website, and other public venues; • Job Applicants and Employees who are Registered Stakeholders seeking evidence of employment discrimination against qualified personnel; • Registered Stakeholders who file complaints regarding malpractice, harrassment, or surveillance by specific employees named in these complaints. • Information provided by the Organization regarding qualifications of its employees. <p>Incidents and events discovered by Yo-ai may indicate the lack of training and/or skills, which could be a violation of relevant laws. It is not necessary to identify these individuals when filing complaints or resolving issues directly with the Organization.</p>
---	---

TRUSTe Requirement

Yo-ai Platform Controls

<p>21. Pre-deployment Testing Requirement: The Participant must have processes to test the AI System prior to its deployment if the outcomes of the AI System result in decisions that produce adverse legal or similarly significant effects, which may include, but not limited to, any risk to rights and freedoms of individuals. The process should include the following: ≥ a testing plan outlining testing goals (e.g., release criteria) and performance metrics to be met ≥ both automated testing and human-led manual testing taking into account the technology being used and the role of human operators on AI System outcomes and effectiveness ≥ mirror real-world use cases in which the AI System will be deployed as closely as possible ≥ comparison of AI System performance against current human-driven processes.</p>	<p>Yo-ai does not rely on Organizations to provide documentation of pre-deployment tests or any other tests the Organization conducts. Yo-ai conducts its own tests as part of its discovery, risk assessment and impact assessment processes, and submits this information to all Named Stakeholders and all Registered Stakeholders who subscribe to events associated with the specific Organization. Pre-deployment Testing on the Yo-ai Platform is performed by Registered Stakeholders and Yo-ai Platform Users during Beta Test Programs and during the on-boarding process when AI Agents are assigned to Registered Stakeholders. Yo-ai relies heavily on detecting issues post-deployment and remediating them quickly when Registered Stakeholders or the Yo-ai Platform capabilities are adversely impacted. Yo-ai favors regression testing for known issues, appending these as test cases in pre-deployment test suites that may run automatically in future builds.</p>
--	---

TRUSTe Requirement

Yo-ai Platform Controls

<p>22. Security of Processing Requirement: The Participant must implement reasonable physical, technical, and administrative safeguards to protect the data within the AI System against risks such as loss or unauthorized access, destruction, use, modification, disclosure of information, or other misuses.</p> <ul style="list-style-type: none"> ≥ the Participant must ensure third party providers of AI Systems have appropriate safeguards in place if using an off-the-shelf third party AI System. ≥ the Participant must implement reasonable administrative, technical, and physical safeguards, suitable to the Participant’s size and complexity, the nature and scope of its activities, and the sensitivity of the data within the AI System, in order to protect the integrity and reliability of the data and protect it from loss or unauthorized use, alteration, disclosure, distribution, or access. These safeguards may include: <ul style="list-style-type: none"> ≥ authentication and access control ≥ Pseudonymisation and encryption ≥ implementing controls on the AI System query interface to detect and prevent attempts to access, modify, and exfiltrate confidential information ≥ boundary protection ≥ physical and environmental security controls ≥ data backup and disaster recovery procedures ≥ secure data disposal procedures ≥ audit logging ≥ monitoring ≥ acceptable use policies that define the types of data that is prohibited to be processed through certain types of AI models ≥ assess third party AI Systems to verify appropriate data protection measures are in place that are appropriate to the nature and scope of the system’s activities, and the sensitivity of the data within the AI System. 	<p>Yo-ai also conducts cybersecurity assessments on its platform agents, and this information is shared with its Registered Stakeholders. Yo-ai’s Responsible Disclosure Program solicits vulnerability and incident reports from Registered Stakeholders only.</p> <p>If you represent an Organization and are concerned about Yo-ai’s cybersecurity posture or status, you can become a Registered Stakeholder.</p> <p>If you represent an enforcement or regulatory agency and are investigating a complaint made about the Yo-ai Platform or PrivacyPortfolio’s business practices, you can become a Registered Stakeholder.</p>
---	--


TRUSTe Requirement

Yo-ai Platform Controls

<p>23. Resilience Requirement: The Participant must have protocols to avoid, protect against, respond to, or recover from resiliency-based threats, and procedures to regularly test these protocols post deployment of the AI System or confirm that existing protocols apply to AI Systems.</p>	<p>Yo-ai is not a “mission-critical” system. Organizations and Consumers have not been harmed by any system disruptions to date. The personal information of Consumers and Registered Stakeholders are not stored on the Yo-ai Platform; it is stored on a device or service owned and controlled by the individuals, and may include all evidence, reports, complaints, and assessments pertaining to their requests or responses.</p> <p>Yo-ai does have mechanisms to back up and protect the integrity of its Platform Event Log Decision Diaries, and Stakeholder Registry.</p>
---	--

TRUSTe Requirement

Yo-ai Platform Controls

<p>24. Incident Detection and Response Requirement: The Participant must have an AI System incident detection, escalation, and management procedures and response plan in place, or confirm that existing incident response plans apply to AI Systems.</p>	<div data-bbox="699 272 1423 410"><p data-bbox="877 305 1402 329">Responds to platform incidents (aka "Agent terminator", "Kill switch", etc)</p><p data-bbox="720 378 835 394">Incident-Responder</p></div> <p data-bbox="688 418 1927 618">Craig Erickson, responsible for the entire Yo-ai Platform, can quickly respond to any incident even while on vacation. Actions taken by the Incident-Responder, like shutting down all AI Agents, are recorded by The Solicitor-General which records all requests and responses, the Decision-Master which records all decision-related events, and The Sentinel, our ever-present listener and watchdog. This control mechanism is also used to satisfy Requirement #5 and #9.</p>
---	--