Report

Organization: **KYP.ai GmbH**

https://kyp.ai/

Publication date: Apr 22, 2025, 09:01 AM PDT

Reporting period: 2025

Section 1 - Risk identification and evaluation

a. How does your organization define and/or classify different types of risks related to AI, such as unreasonable risks?

AI Risk Definition

KYP.ai adheres to the risk definitions formulated by the NIST AI RMF. This framework defines risk as a composite measure of the probability of an event occurring and the magnitude of its consequences.

Unreasonable Risks are those specific to AI that cannot be adequately controlled or mitigated through available technical or governance measures. These include:

- Risks to Fundamental Rights and Dignity
- Uncontrollable or Unpredictable Systems
- Discriminatory or Harmful Bias
- Deceptive or Manipulative Systems
- Dual-Use Technologies with Severe Misuse Potential

Predictable Risks are those specific to AI that can be adequately controlled or mitigated through available technical or governance measures. These include:

- Data-Related Risks
- Model-Related Risks
- Security-Related Risks
- Operational Risks
- Human-AI Interaction Risks
- Ethical and Social Risks

Each of these risks has sub-categories.

Both unreasonable and predictable risks are classified as threats (negative) and opportunities (positive), with appropriate risk mitigation plans such as:

- Threats: Eliminate, mitigate, outsource, or acceptance
- Opportunities: Explore, venture, observe, or quit

These risks are subject to bi-annual assessment and are included in the company risk register.

b. What practices does your organization use to identify and evaluate risks such as vulnerabilities, incidents, emerging risks and misuse, throughout the AI lifecycle?

Risk Identification

We emphasize preventive and proactive measures, integrating risk assessment into the planning and development stages. New software features are evaluated for potential vulnerabilities, incidents, emerging risks, and misuse.

Risk Evaluation

Risk evaluation is continuous throughout the software's lifecycle and the organization's operations, conducted bi-annually as outlined above.

c. Describe how your organization conducts testing (e.g., red-teaming) to evaluate the model's/system's fitness for moving beyond the development stage?

• Beyond the development stage: Application penetration testing is performed on new software versions using top pen testing tools like Burp Suite before it is released to customers.

• Additional penetration testing: Infrastructure components (e.g., cloud servers) hosting KYP.ai software undergo penetration testing before releasing a new cloud server environment to customers.

• Regular assessments: Regular penetration tests and asset configuration reviews are conducted on components and tools used for source code development (internal KYP.ai infrastructure).All the above - supported with ongoing contributory testing with internal representatives - KYP.ai in-house solution (exact copy of software provided to customers) to test both technical and non-technical impact of user and organizational experience.

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

Yes

e. Are quantitative and/or qualitative risk evaluation metrics used and if yes, with what caveats? Does your organization make vulnerability and incident reporting mechanisms accessible to a diverse set of stakeholders? Does your organization have incentive programs for the responsible disclosure of risks, incidents and vulnerabilities?

- Delphi Method used for GenAI Ris Assessment (KYP.ai Product) and Third-Party Risk Assessment (Third Party - AI vendors).
- KYP.ai Operational risks – quantitative evaluation matrix for negative (threats) and positive (opportunities) risks.
- Monte Carlo risk analysis – used to assess new KYP.ai Product features and reassessment of existing features.

---

f. Is external independent expertise leveraged for the identification, assessment, and evaluation of risks and if yes, how? Does your organization have mechanisms to receive reports of risks, incidents or vulnerabilities by third parties?

Yes, on different levels:

- external consultation with privacy lawyers.
- external audits – 2023&2024 EU GDPR legal audit.
- external audit - 2024& 2025 – SOC2 attestation.
- targeted 2025 & 2026 – external technical validation;

---

g. Does your organization contribute to the development of and/or use international technical standards or best practices for the identification, assessment, and evaluation of risks?

Yes:

- contribution to pilot reporting framework on Code of Conduct in 2024 (OECD.AI).
- EDPB stakeholder meetings on EU GDPR for AIs – 2024.

further strenghtening of presence expected in 2025 and 2026.

Use of international technical standards:

- KYP.ai single control framework – one control addressing requirements of many frameworks/standards/laws

Such as: SOC2, ISO 42001, ISO 27001, HIPAA, EU GDPR, US Privacy Laws, PCI DSS, NIST AI RMF, DORA, ITIL, COBIT5

h. How does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks, in particular systemic risks?

- ongoing feedback from customers.
- regular assessment of applicable sector – specific regulations and frameworks.
- product risks – regular GenAI risk reviews.
- bi-annual operational risks – reviews with Heads of Business Units with further re-assessment by Founders Team.
- risks categories are divided into threats (negative) and opportunities (positive) with appropriate risk mitigation/exploration plan.
- engage in active observation and research on the relevant topic, incorporating feedback from competent authorities and international organizations, such as think tanks.

Any further comments and for implementation documentation

Supplementary information re: section 1d above (reports):

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

• Reports received from vendors providing cloud infrastructure for SaaS services through configured alerts.

• Reports received from the source code producer (Java). Monitoring AI incidents via sources such as the OECD AI Incidents Monitor (AIM), social media, data protection authorities, and other competent authorities, including recommendations for remediation.

• Active participation in workshops and seminars related to AI technology development.

• Proactive engagement in forums and social media discussions about AI risks, and involvement in global projects addressing these topics.

Section 2 - Risk management and information security

a. What steps does your organization take to address risks and vulnerabilities across the AI lifecycle?

During the design and planning phase:

• Each initiative resulting in the design and development of a new business or security feature is assessed for potential risks to customers and end-users.

During the development phase:

• Ongoing testing of source code using SonarQube and SonarLint.

• Quality Analysis (QA) involving a combination of automated and manual tests.

Prior to deployment:

• Penetration testing is performed on the newly designed software version.

• Penetration testing is conducted on the newly designed cloud server built for the customer (for SaaS services).

b. How do testing measures inform actions to address identified risks?

• Each test results in follow-up review actions, leading to remediation efforts scheduled for resolution by the DevSecOps team. Subsequently, re-testing is conducted to ensure the issues have been resolved.

• If an identified vulnerability is deemed a threat to customer or end-user privacy and security, it is communicated to the customer's dedicated security team (as per contractual arrangements along with guidance and recommendations for resolution).

c. When does testing take place in secure environments, if at all, and if it does, how?

• in a dedicated DevOPS environment – during design phase, planning and development stage.

• in a dedicated sandbox environment – during software pre-deployment stage.

• for newly built cloud server – pentesting performed in pre-production environment before it is released to the customer.

• ongoing end user testing performed on KYP.ai in-house solution – installed on KYP.ai personnel devices (exact copy of the solution offered to customers), performed in a dedicated internal production or on-premises environment (both hosted in internal KYP.ai environment).

---

d. How does your organization promote data quality and mitigate risks of harmful bias, including in training and data collection processes?

External:

• advising customers on data integrity and quality risks that need to be addressed before implementing AI solutions.

• customers determine the data they process and their retention periods (including during the PoC stage) using various data anonymization and access management controls.

• maintaining open communication with KYP.ai's compliance function, available to customers and end users for any queries regarding data collection.

Internal:

• conducting regular end-user testing on KYP.ai's in-house solution (an exact copy of the customer-facing solution) to early detect and address any inadvertent data collection, quasi-identifiers, or deceptive patterns.

---

e. How does your organization protect intellectual property, including copyright-protected content?

Set of policies and agreements signed with prospective customers, onboard customers, own personnel and vendors:

• non-disclosure agreements.

• data Protection and Information Security Policy for KYP.ai personnel members.

• data protection clauses and Data Protection Agreements with vendors and customers.

• confidentiality clauses in contracts with KYP.ai personnel and third parties (customers, vendors, prospects).

• third party management – assessment of AI features and AI tools used for internal KYP.ai use including assessment of content protection controls.

• only pre-approved software with a valid KYP.ai business license may be used for work internally within KYP.ai organization.

• customers determine what data is collected and processed through KYP.ai software installed on their end-user devices.

f. How does your organization protect privacy? How does your organization guard against systems divulging confidential or sensitive data?

Contract Level:

• Establishing privacy protection clauses and data protection agreements with customers and vendors.

Product Level:

• Implementing a privacy-by-design concept.

• Incorporating complex features that allow customized privacy controls, including anonymization.

• Conducting ongoing testing of KYP.ai's in-house solution (an exact copy of the customer-facing solution) by end users to detect privacy issues early.

Organization Level:

• Enforcing strict access control to KYP.ai's internal environment and customer environments.

Source Code and Software Development Stage:

• Performing manual and automated testing (including penetration testing) on software to identify and address any privacy issues.

g. How does your organization implement AI-specific information security practices pertaining to operational and cyber/physical security?

- i. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?
- ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights? What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?
- iii. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?
- iv. How often are security measures reviewed?
- v. Does your organization have an insider threat detection program?

i.How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?

a. On Product Level (KYP.ai Software):

• Unique AI Threats: Specific threats related to the AI model, including AI-specific threat landscapes and actors.

• Third-Party Threats: Risks associated with components and third-party software used in AI development, such as Java libraries.

• AI Development Lifecycle Vulnerabilities: Continuous source code review and protection (using tools like SonarLint and SonarQube), and application penetration testing.

• AI-Related Data Security Controls: Measures for data retention, processing, and privacy.

• AI-Specific Monitoring: Security alerts and monitoring.

b. On an organizational level:

• AI-SaaS Related Controls: Internal and customer cloud infrastructure security, including vulnerability detection, SIEM alerts monitoring, Crowdsec, and penetration testing.

• AI On-Premises Solutions: Comprehensive security and data protection controls for solutions hosted entirely within the customer's infrastructure.

• Risk Management: Emphasis on operational risks for each business unit and their convergence.

Policies are created for these processes, followed by the establishment of operational procedures to ensure transparency in operations.

ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights?

Customers have full control over the types of data, including proprietary data, that are collected and processed through the KYP.ai Connect App and KYP.ai Platform. The solution includes features to prevent the processing of personal or business confidential data, such as anonymization, disabling screenshot collection, and categorizing applications as private or productive (by default, apps are classified as neutral).

At the organizational level, KYP.ai prohibits the processing of intellectual property, trade secrets, personal data, and confidential business data. Sufficient preventive measures are in place, including legally binding policies and security protocols applied to the KYP.ai network and onboarded AI systems.

What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?

On Product level (KYP.ai ConnectApp and KYP.ai Platform): By default, no personal data or business confidential data is processed or stored. External AI engines do not process any personal identifiable information (PII). All sensitive data processing is confined to the KYP.ai Platform, which is hosted on customer infrastructure.

Organizational level: Access to the development environment is enforced through multiple layers of security, including MFA and 3FA for critical resources. Environments are separated into testing and production, with dedicated environments for customers. The change management process involves different levels of approval, ensuring source code protection and review. Network traffic is monitored using solutions such as Crowdsec.

iii. What is your organization's vulnerability management process?

On Product level (KYP.ai ConnectApp and KYP.ai Platform):

• Source Code Monitoring: Continuous monitoring of source code using SonarQube and SonarLint to detect vulnerabilities.

• Application Penetration Testing: Conducted on new software versions to identify potential security issues.

• Vulnerability Remediation: Actions taken to address detected vulnerabilities.

Organizational level:

• Infrastructure Monitoring: Continuous monitoring of internal infrastructure through the company's SIEM.

• Infrastructure Penetration Testing: Performed on newly built servers for customers before release.

• Periodic Penetration Testing: Regular testing of the internal KYP.ai environment.

• Alert Monitoring: Ongoing monitoring of alerts from third-party cloud infrastructure.

Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?

• Yes, Customer and Partner Communication: Informing customers and partners about detected vulnerabilities and recommending remediation actions.

iv. How often are security measures reviewed?

On an ongoing basis accompanied with periodical formal manual reviews such as identity and access management, vulnerability scanning reviews.

v. Does your organization have an insider threat detection program?

Yes, this is addressed in our HR policies. Conduct at work is continuously evaluated with ongoing feedback. Additionally, an internal whistleblower line is available 24/7 for reporting any issues without fear of retaliation.

h. How does your organization address vulnerabilities, incidents, emerging risks?

On multiple levels:

Continuous Market Analysis:

Regularly conducting market analysis to stay updated on industry trends and customer needs, ensuring compliance with evolving legal standards.

Themed Discussions with Prospective Customers:

Engage in themed discussions with prospective customers during the engagement and onboarding stages, focusing on security, risk, and compliance from both technological and legal perspectives. This includes understanding and adhering to regulations such as EU GDPR, SOC2, CCPA, and HIPAA, ISO 42001

Regular Source Code Protection Reviews:

Perform ongoing reviews of source code protection using tools like SonarQube and SonarLint during the development process, ensuring compliance with legal requirements for data security and privacy.

Comprehensive Testing Before Deployment:

Combine manual and automated tests before deploying new software versions or developed functionalities to ensure they meet legal standards for security and compliance.

Ongoing End-User Testing:

Conduct continuous end-user testing at the organizational level using in-house solutions to identify new risks, perceived bugs, or patterns that may impact privacy or information security. This helps ensure ongoing compliance with legal requirements and mitigates potential legal risks.

Any further comments and for implementation documentation

N/A

Section 3 - Transparency reporting on advanced AI systems

a. Does your organization publish clear and understandable reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems?

- i. How often are such reports usually updated?
- ii. How are new significant releases reflected in such reports?
- iii. Which of the following information is included in your organization's publicly available documentation: details and results of the evaluations conducted for potential safety, security, and societal risks including risks to the enjoyment of human rights; assessments of the model's or system's effects and risks to safety and society (such as those related to harmful bias, discrimination, threats to protection of privacy or personal data, fairness); results of red-teaming or other testing conducted to evaluate the model's/system's fitness for moving beyond the development stage; capacities of a model/system and significant limitations in performance with implications for appropriate use domains; other technical documentation and instructions for use if relevant.

<u>i. Yes, InfoSec documentation:</u>

• Platform Architecture Document: Updated quarterly.

• Server Installation Details for SaaS Solutions: Continuously updated.

• Application Installation Details for On-Premises Solutions: Continuously updated.

• Customer Contracts: Includes detailed and customized technical information such as installation procedures, Service Level Agreements, service requirements, and previously agreed compliance terms and conditions.

• New Document Releases: Delivered directly to new customers by the dedicated Customer Success team.

• Software Releases/Upgrades: Scheduled according to the customer's plan.

<u>iii and iv. Significant releases information is included in the above-mentioned information:</u>

– added/updated information specifying new features of the product, upgrade of the software how does it relates to data protection and security, helping to do due diligence DPIA.

iv. The following information is included:

- Potential Safety, Security, and Societal Risks:

Evaluations conducted for risks including enjoyment of human rights:

Documentation: Responsible use of KYP.ai Connect App and KYP.ai Platform

GenAI Risk Assessment -KYP.ai Connect App and KYP.ai Platform

- Model/System Effects and Risks:

Assessments of effects and risks to safety and society, such as harmful bias, discrimination, threats to privacy or personal data, fairness.

Documentation: KYP.ai Platform Architecture

KYP.ai GenAI Risk Assessment for KYP.ai platform and KYP.ai ConnectApp

Responsible Use of AI Policy

- Red-Teaming and Testing Results:

Results of red-teaming or other testing to evaluate the model's/system's fitness for moving beyond the development stage.

Documentation:

KYP.ai Application pentests (and cloud environment - servers - pentests for SaaS type solution)

- Model/System Capacities and Limitations:

Capacities of a model/system and significant limitations in performance with implications for appropriate use domains.

Documentation:

KYP.ai Platform Architecture

- Technical Documentation and Instructions:

Other relevant technical documentation and instructions for use.

Documentation:

KYP.ai Platform Architecture

KYP.ai Server Installation Documentation

KYP.ai Application Installation Documentation

Contract with appendencies - Data Protection Agreement, SLA, Technical installation plans

Please note these documents are available on request.

b. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?

• InfoSec documents including outcome of risks and impact evaluation can be provided upon request during the discovery call.

• The privacy notice is publicly accessible on the KYP.ai website.

• Although KYP.ai operates within the private sector and serves private sector customers, documents can be made available upon request from public companies or bodies.

c. Does your organization disclose privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?

• A consent form will appear before launching the KYP.ai ConnectApp and KYP.ai Platform on an end-user device.

• The privacy policy displayed on the end-user's desktop can be fully customized to align with the customer's own privacy policies.

• This can be addressed within the employment contract (as an annex), through a consent form for informational purposes, or both.

KYP.ai privacy notice - available to public: Privacy notice - KYP.ai | Productivity Intelligence Platform

d. Does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?

- With KYP.ai Platform 360, customers have full control over the data used to train the platform
- They can adjust the settings at any stage to add or eliminate types of data.
- The AI features of KYP.ai Platform do not store or process any personal or business data unless the customer chooses to do so.

e. Does your organization demonstrate transparency related to advanced AI systems through any other methods?

- End users, including both customers and KYP.ai organization members (using the in-house solution identical to the customer version), can view the data processed about them through their individual dashboard, accessible 24/7.
- Customers can request an audit of the KYP.ai system at any time.
- Penetration tests of the application and cloud instance built for customers are provided during engagement, onboarding, and on an ad-hoc basis.

Any further comments and for implementation documentation

N/A

Section 4 - Organizational governance, incident management and transparency

a. How has AI risk management been embedded in your organization governance framework? When and under what circumstances are policies updated?

On Product Level:

Risk Assessment of new product features during plan and design stage, ongoing GenAI Risk Assessment performed at least bi-annually.

On KYP.ai Organization Level:

Ongoing Operational Risks Assessment – performed at least bi-annually with Heads of Business units and Founders Team.

Third Party Management process:

Vendor due diligence process includes risk assessment of use of AI Product or AI features of that product (identification and verification of third-party risk);

Sales process:

Advising customers on both technological and non-technological risks of KYP.ai Product.

---

b. Are relevant staff trained on your organization's governance policies and risk management practices? If so, how?

- Each new personnel member of organization must write and confirm understanding of KYP.ai Global Policy of Information Security and Data Protection.
- EU GDPR & Data Protection online training – must be completed within first 30 days of cooperation and then renewed on annual basis.
- Agreements with personnel contain clauses related to information protection and data security.
- Ongoing regular awareness sessions for all personnel members.

---

c. Does your organization communicate its risk management policies and practices with users and/or the public? If so, how?

- KYP.ai Security and Compliance policies (including risk management practices) addressed within Info Security documentation provided to prospective customers.
- Info Sessions for customers to discuss risk and compliance concerns, areas.
- Regular external audits performed on group companies including risk management and reporting.

d. Are steps taken to address reported incidents documented and maintained internally? If so, how?

- Established incident management process and an internal KYP.ai Incident Management and Data Protection Team.
- Each safety incident must be reported immediately to this team for prompt resolution.
- Data protection incidents must be reported within 72 hours to this team and the Intragroup Data Protection Officer. If a data breach is suspected or confirmed, it must also be reported to the relevant data protection authorities and the customer's data protection officer/security team.
- Incidents are documented on incident logs and tracked for resolution.

e. How does your organization share relevant information about vulnerabilities, incidents, emerging risks, and misuse with others?

- Post factum - with customers – according to agreed terms of service – as soon as vulnerability is detected and requires remediation, immediately upon discovery of incident.
- Prevention and risk advisory - for emerging risks and potential misuse (i.e. micromanagement of individuals instead of process mining)

f. Does your organization share information, as appropriate, with relevant other stakeholders regarding advanced AI system incidents? If so, how? Does your organization share and report incident-related information publicly?

• Yes, during the engagement and onboarding stages with prospective customers, we advise them about potential risks related to advanced AI system incidents.

• These risks are discussed in dedicated meetings focused on security, privacy, and technical installation, where we provide guidance on how to prevent such risks for both SaaS and on-premises solutions.

• In case of detection of vulnerability with high or critical risk to customers network security – all customers using versions of software impacted are notified about the issue along with advising them on necessary remediation actions according to terms specified in agreements with customers.

• In the event of data protection and security incidents, the Intracompany Data Protection Officer is involved in investigating and assessing the impact on data subjects. The incident is reported to relevant data protection authorities within 72 hours of detection or suspicion.

g. How does your organization share research and best practices on addressing or managing risk?

• During the engagement and onboarding stages, we hold dedicated meetings with the legal, compliance/security team, or privacy officer to discuss best practices based on KYP.ai's in-house solutions and observations within the organization.

• Each customer is advised to determine the categories of applications to be monitored using KYP.ai software, whether productive or private—to address data minimization.

h. Does your organization use international technical standards or best practices for AI risk management and governance policies?

Yes, on many different levels:

• Internal policies and procedures are grounded in the principles of ISO 27001, ISO 42001, SOC2, EU AI Act, EU GDPR, US Privacy laws, NIST AI RMF, ITIL, COBIT 5, and HIPAA, OWASP ZAP.

• KYP.ai holds SOC2 Type1 accreditation, with Type 2 accreditation targeted - August 2025.

• For SaaS solutions, only global cloud service providers that comply with these standards and laws are utilized.

Any further comments and for implementation documentation

N/A

Section 5 - Content authentication & provenance mechanisms

a. What mechanisms, if any, does your organization put in place to allow users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?

• Before launching the application, a pop-up requests consent for data collection.

• Customers are advised to hold information sessions and consult with their organization to ensure responsible AI use.

• End-users have 24/7 access to a dashboard showing their collected data and always can opt out from collection.

b. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems? If yes, how? Does your organization use international technical standards or best practices when developing or implementing content provenance?

For KYP.ai ConnectApp:

• Customers determine the content processed through the KYP.ai ConnectApp.

• Metadata, which includes information such as creation date, author, and modification history, is embedded in the content and can be viewed through individual dashboard and admin console (organization level).

• Within the KYP.ai organization -policies are enforced to ensure that only authorized AI systems are used, preventing the processing of unauthorized content.

• Anonymization and masking controls - can be customized according to customers own policies and procedures in this area.

Any further comments and for implementation documentation

N/A

Section 6 - Research & investment to advance AI safety & mitigate societal risks

a. How does your organization advance research and investment related to the following: security, safety, bias and disinformation, fairness, explainability and interpretability, transparency, robustness, and/or trustworthiness of advanced AI systems?

- we continuously observe industry trends by actively participating in initiatives hosted by OECD.AI, stakeholder meetings with the European Data Protection Board (EDPB), and customer-organized workshops.
- we also monitor the needs of both prospective and onboarded customers.
- additionally, KYP.ai follows recommendations issued by competent authorities regarding the security and development of advanced AI systems.

---

b. How does your organization collaborate on and invest in research to advance the state of content authentication and provenance?

- **Collaboration:** We share best practices with customers based on the use and ongoing testing of the KYP.ai in-house solution to identify potential patterns where content authentication and provenance rules may be violated. These observations can be shared during collaborations in global initiatives hosted by OECD.AI, stakeholder meetings with the European Data Protection Board (EDPB), and customer-organized workshops.
- **Customer Control:** Customers installing KYP.ai software within their organization have full control and decision-making authority over what data is collected and processed from end-user devices.
- **Additional Features:** The KYP.ai Connect App and Platform offer additional features to ensure data is anonymized and that no unwanted content is inadvertently collected or processed.

---

c. Does your organization participate in projects, collaborations, and investments in research that support the advancement of AI safety, security, and trustworthiness, as well as risk evaluation and mitigation tools?

- Yes, we are continuously researching projects and exploring collaboration opportunities for pilot projects related to AI safety and compliance. We actively participate in events, meetings, and workshops organized by key industry stakeholders such as the European Data Protection Board (EDPB) and OECD.AI, as well as other initiatives within the AI industry.

- We also plan our own initiatives in collaboration with the AI industry in 2025 and 2026;

d. What research or investment is your organization pursuing to minimize socio-economic and/or environmental risks from AI?

- Process mining and deep tech research on costs optimization for private sector (BPO sector, financial, commercial) - micro scale - cooperation with customers and customers tailored solutions in this area.

Any further comments and for implementation documentation

N/A

Section 7 - Advancing human and global interests

a. What research or investment is your organization pursuing to maximize socio-economic and environmental benefits from AI? Please provide examples.

Investment in AIs and AgenticAIs:

We are investing in the development of AIs and AgenticAIs to drive product innovation and enhance customer organizational growth - micro scale according to customers demand.

Ongoing Research:

Our ongoing research spans multiple domains, including human resources, law and compliance, and business development. This research is conducted in partnership with SMEs in these fields, following FTM practices.

b. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities, limitations and impacts of advanced AI systems? Please provide examples.

- AI literacy training planned for 2025.
- Ongoing awareness regarding use of AI systems.
- Internal testing of KYP.ai in-house solution to increase awareness about developed software.
- Dedicated internal channel and initiatives regarding education about AIs and its impact on workforce.
- Dedicated workshops and sessions for customers, partners and prospective customers on nature, capabilities of KYP.ai Productivity 360 Platform.

c. Does your organization prioritize AI projects for responsible stewardship of trustworthy and human-centric AI in support of the UN Sustainable Development Goals? Please provide examples.

Yes, Included in KYP.ai ESG policy and Global Partner Code of Conduct:

- People
- Modern Slavery and Forced Labour
- Children's Rights
- Working Hours and Leave
- Wages and Benefits
- Non-Discrimination and Fair Treatment
- Freedom of Association and Collective Bargaining
- Health Safety and Well-being
- Resources
- Responsible Sourcing of Materials and Minerals
- Responsible Circular Economy and Waste Management
- Water Management
- Substances of Concern
- Climate
- Energy Consumption
- Business Ethics
- Business Integrity
- Confidentiality and Intellectual Property Rights
- Fair Competition
- Data Privacy
- Information Security
- Principles of Responsible Use of AI

d. Does your organization collaborate with civil society and community groups to identify and develop AI solutions in support of the UN Sustainable Development Goals and to address the world's greatest challenges? Please provide examples.

Strategic Activities for 2025

In 2025, we plan to strategically advance initiatives, including AI-ESG Convergence, aligning with the UN Sustainable Development Goals as a benchmark.

Commitment to ESG Principles

Since 2025, KYP.ai has embedded these principles in our Code of Conduct with vendors and partners, emphasizing support for green energy and green AI as core elements of our ESG policy.

Global Impact

By delivering solutions to customers in developing countries, KYP.ai fosters community growth, business development, and local economic advancement within the global supply chain.

Any further comments and for implementation documentation

N/A