OECD AI Transparency Report

Organization: By My Side Labs (KOR) **Reporting Period:** Q4 2026 **Published:** November 10, 2026

Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Application developer (/provider)

> **If any of the fields above are selected, please indicate your organization size:**
>
> Micro enterprise: fewer than 10 employees

Section 1 – Risk Identification and Evaluation

1. How does your organization define and/or classify different types of risks related to AI?[1]

- Maintain an internal taxonomy, classification system, and/or set of risk area definitions
- Other (please specify): Japan's Principles-Code for generative AI (listed No. 4 on the Cabinet Office list, 26 Oct 2026); Google Play and Apple App Store policies; our Acceptable Use Policy (https://byve.bymysidelabs.com/en/acceptable-use)

> **How does your organization define thresholds at which severe risks, unless adequately mitigated, may be considered "unreasonable"? Please describe the framework(s) most relevant to your organization's role and context. If your organisation does not use formal thresholds, you may describe instead the policies, decision criteria, or governance processes you apply when assessing severe AI risks. You may also describe: • Specific examples of contexts in which your models or systems could, in your assessment, pose unreasonable or intolerable risk; • How mitigations are graduated by capability or propensity level; • How your organisation considers the specificities of different AI technologies, such as generative AI and agentic AI, including any specific risk assessment or governance mechanisms applied to agentic AI capabilities.**
>
> We do not develop models. Our risk boundary is the type of app a user asks BYVE AI to build. Requests are refused before generation if they fall into our prohibited categories: illegal gambling, pornography or adult services, child sexual exploitation, malware or account theft, voice phishing and fraud, forgery of identity or official documents, non-consensual deepfakes, extremist propaganda, and promotion of self-harm or suicide methods. Requests that would help evade Google Play or App Store rules, or collect, track or send personal data without consent, are also refused. Generated apps run on the user's own device inside a sandboxed WebView, can reach only an allowlist of reviewed servers,

> and can use phone features and online data only through capabilities we approve. Sensitive actions such as SMS and email only open a composer; the user must press send.

2. Both before and after deployment, what practices does your organization use to identify and evaluate vulnerabilities, incidents, emerging risks and misuse throughout the AI system lifecycle?

- Internal red teaming[3]
- Internal benchmarks, standard metrics (e.g., frequency, severity scores)
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Incident reports, including reports shared by other organizations
- Automated monitoring / remote status reporting (e.g., telemetry pipelines, automated alerts when risk thresholds are breached)
- Multilingual and cross-cultural evaluation, including collaboration with local ecosystems (e.g., national AI institutes, language-specific evaluation consortia) for under-represented languages and cultural contexts (please specify): BYVE AI is offered in 80+ languages; we review failures and refusals by language and fix language-specific issues.

> **Please briefly describe your organization's decision-making process for deploying an AI model or system including: who has decision authority; what evidence and criteria are required (e.g., performance, safety/security, robustness, fairness, privacy, compliance, independent external testing, evaluation, validation and verification (TEVV) or assurance); contextual caveats or limitations required in interpreting risk evaluation metric results; what approvals/sign-offs are needed; and what safeguards (e.g., mitigations, monitoring, or phased release) must be in place to move into deployment.**
>
> By My Side Labs is run by one person, the representative, who has sole decision authority. A change ships only after automated test suites pass, it is checked on real Android and iOS devices, and server changes are staged and verified before promotion. Risky behaviour can be switched off on the server without an app update, and every release keeps a rollback path.

> **Following deployment, how do you use incident reports — including those shared by other organizations — to identify emerging issues, update risk assessments, and trigger corrective actions.**
>
> Failures and policy refusals are logged and monitored automatically. User reports arrive through the in-app inquiry form and mark@bymysidelabs.com. Each confirmed issue gets a root-cause fix, affected users are refunded tokens automatically when a server or provider error is confirmed, and we notify them in their language.

3. Does your organization have mechanisms to receive and/or share reports of risks, incidents or vulnerabilities by/with third parties?

Yes, receiving only

> **If yes, please indicate which stakeholders reporting mechanisms may be accessible to, recognising specifics will depend on the nature of the report and risk level. For each, indicate whether access is on a standing basis (Always), activated based on context (Ad hoc/as relevant), or not currently accessible.**

	Always	Ad hoc / as relevant	Not currently accessible
Relevant employees (security, legal/compliance, etc.)			□
Public authorities (e.g., public reporting offices for security incidents or data breaches)		□	
Supervisory authorities (e.g., data protection authorities)		□	
Industry partners or industry fora			□
Users (end users, enterprise customers, developers using APIs)	□		
Business customers / deploying organizations (if different from “users”)			□
Supply-chain partners (cloud, data providers, etc.): *Model providers (OpenAI, DeepSeek, Alibaba Cloud, Z.ai) and Cloudflare*		□	
Academia / researchers			□
Independent auditors			□
Standards bodies / multi-stakeholder initiatives (OECD.AI, ISO/IEC, IEEE, etc.)			□
Specific civil society organizations			□
Media / general public (people or communities indirectly impacted)	□		
Other			

Please describe how your organisation determines when and how reporting mechanisms are made accessible to different stakeholders (e.g. based on legal or regulatory requirements, internal policies, or risk level). Please also provide public URLs or details on how to submit reports. If none, write “Not applicable”

Anyone can report by email to mark@bymysidelabs.com, and app users can use My Page > Support > Contact in BYVE AI. Rights holders and users can also make requests under Japan's Principles-Code as described at https://byve.bymysidelabs.com/en/ai-principle-code. Access is standing for users and the public; public and supervisory authorities are handled as relevant.

4. If your organization has programs to incentivize risk(s) disclosure, incidents and systemic vulnerabilities, please share what type of programs you use?

- Not applicable

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

Uses

> **If contributes or uses, please select all that apply:**
>
> - Industry-led best practices or codes of conduct
> - Other international or regional standards (please specify): Japan's Principles-Code for the Protection of IP and Transparency for the Appropriate Use of Generative AI (Cabinet Office of Japan)

6. Does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks that could have broad and potentially cascading socio-economic impacts? Please indicate which stakeholders you collaborate with, and whether collaboration is on a standing basis (Always-on), activated based on context (Ad hoc/as relevant), or there is no current collaboration.

	Always-on	Ad hoc / as relevant	No current collaboration
Relevant employees (security, legal/compliance, etc.)			□
Public authorities / regulators / AI safety institutes / other public sector bodies and inter-governmental coordination structures			□
Industry partners or industry fora			□
Users (end users, enterprise customers, developers using APIs)	□		
Business customers / deploying organizations (if different from “users”)			□
Supply-chain partners (cloud, data providers, etc.): *Model providers (OpenAI, DeepSeek, Alibaba Cloud, Z.ai) and Cloudflare*		□	
Academia / researchers			□
Independent auditors			□
Standards bodies / multi-stakeholder initiatives (OECD.AI; ISO/IEC; IEEE; AIID etc.)			□
Independent civil society organizations (e.g., for evaluations, audits, or policy review)			□
Media / general public (people or communities indirectly impacted)			□

	Always-on	Ad hoc / as relevant	No current collaboration
Other(s) (please add any other relevant stakeholder groups):			
Not applicable			

Please describe examples of how your organization collaborates. Examples may include: participating in multi-stakeholder or industry initiatives; partnering with academia, civil society, or the public sector; establishing internal or joint governance structures with external experts or in partnership with other efforts to share knowledge and jointly address risks.

We work directly with users through in-app inquiries, and with our model and infrastructure providers when an outage or policy issue affects users. As a one-person studio we do not currently take part in multi-stakeholder initiatives.

Any further comments and implementation documentation.

No answer provided

Section 2 – Risk Management and Information Security

7. Across the AI system lifecycle, what steps does your organization take to manage risks and vulnerabilities? Please indicate which specific practices, tools or metrics your organization uses at each lifecycle stage. You may refer to tools or metrics present in the OECD.AI Catalogue of Tools and Metrics or suggest additions. Respondents may complete only the lifecycle stages relevant to their organisation's role. Stages that do not apply may be left blank.

Plan and design

Collect and process data

Build, integrate and interpret model

Verify and validate

Deploy

Operate and monitor

Please provide a consolidated description of your organisation's approach to risk management across the AI system lifecycle, including how the practices identified above operate together and any cross-cutting governance, review or escalation processes. Please also indicate how often these practices are reviewed and what types of events trigger reviews and updates. Where relevant, please distinguish between different types of AI systems (e.g. generative or agentic AI).

Risk management is built into one release pipeline run by the representative. Each request passes a policy check, generation runs on third-party models under our instructions, the output app is checked automatically, and it runs only on the user's device in a sandbox with allowlisted network access.

Practices are reviewed after every incident, every model or provider change, and at least once a year together with our Principles-Code disclosure.

Please describe any measures used to ensure data quality and fairness across the data collection and curation stage (e.g., dataset audits, filtering training data to remove harmful content or personal information, fine-tuning on curated data, use of moderation tools, assessment of limitations to model generalisability).

We do not train or fine-tune models and do not curate training data. For data quality we rely on the model developers' published practices and disclose which models we use.

8. What security measures are used in testing AI systems?

- Isolation of staging environments (from production / operational environments)
- Restrictions on outbound Internet or API access, including a list of permitted domains or APIs
- Containment measures for prompt-injection and jailbreak attempts
- Rate limits and resource caps
- Access controls, including roles-based permissions
- Audit logging and monitoring
- Use of synthetic, anonymized, or dummy data, as appropriate

8.A. Please indicate, if relevant, the team or role responsible for overseeing secure testing and whether this responsibility is shared across multiple teams and/or functions.

The representative is responsible for secure testing; it is not shared across teams.

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

9.A. Safeguards that promote lawful data use and transparency in AI training:

- Other(s) (please specify): We do not train AI models, so training-data safeguards apply to our model providers. We publish which models we use and answer rights-holder requests under Japan's Principles-Code.

9.B. Safeguards that reduce the risk of dissemination of outputs that may infringe copyright:

- Designating clear points of contact so creators or rights holders can raise concerns about infringing outputs
- Other(s) (specify): In games, our instructions tell the AI not to use the titles, names, logos or trademarked character artwork of existing works but to replace them with original ones. Generated apps can load content only from an allowlist of sources, and our asset server returns pictures of real things only under free licences that allow commercial use, with credits. Prohibited requests are refused before generation. Details: https://byve.bymysidelabs.com/en/ai-principle-code

10. How do you protect privacy and prevent your systems from disclosing confidential or sensitive data across the AI lifecycle?

- Make information about data privacy, practices, and controls accessible to a diverse set of stakeholders

- Use security controls, including encryption at rest and in transit

> **Describe key privacy measures and data-protection standards applied.**
>
> Chats and generated apps stay on the user's device by default. Requests are sent over HTTPS to our backend and then to the model provider only to generate the app. Recovery copies of results are kept for up to 24 hours and request and token history for 365 days. To check generation quality and recover results, requests and generated results are also kept on our generation server with no fixed automatic deletion schedule while the service operates; we delete them on request with the install ID. The privacy policy is published in 80 languages.

11. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems across the AI system lifecycle? Respondents may complete the checkbox subsections in 11.A–11.D or describe their overall approach under 11.E.

> **11.A. Governance, policy and assessments**
>
> - Maintain vulnerability management processes (scanning, channels for external reporting, patching, remediation)
> - Regularly review security measures and update them in response to emerging risks, incidents, or major releases
> - These responsibilities are delegated contractually to model or infrastructure providers

> **11.B. Technical and operational controls**
>
> - Apply multi-factor authentication (MFA) and role-based access controls for advanced AI systems
> - Monitor system activity and log access to detect anomalies or misuse
> - Conduct secure AI development and/or deployment practices
> - These responsibilities are delegated contractually to model or infrastructure providers

> **11.C. Protection of sensitive or high value AI assets**
>
> - Limit access to proprietary AI assets based on role or need-to-know
> - These responsibilities are delegated contractually to model or infrastructure providers

> **11.D. Insider risk protection detections**
>
> - Other (please specify): One-person organisation; no other staff have access.

> **11.E. Please describe the main security measures your organization applies and indicate which are specific to particularly sensitive AI assets, where relevant.**
>
> API keys for AI providers are held only on our servers and never shipped in the app. App requests are checked with Google Play Integrity and Apple App Attest. The backend runs on Cloudflare Workers with rate limits, IP-based abuse limits and security alerts. Account access uses multi-factor authentication. Infrastructure and model security are also covered by our providers' controls.

12. 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?

- Internal vulnerability disclosure receipt and tracking processes
- Investigation of reported or identified risks and vulnerabilities
- Development of patches or other mitigations for confirmed risks or vulnerabilities
- Testing of patches or other mitigations

13. What post-deployment practices does your organization use to monitor and respond to vulnerabilities, incidents, emerging risks and misuse of advanced AI systems?

- Conduct post-deployment monitoring
- Perform root-cause analysis and apply lessons learned to improve future development and/or deployment practices

14. Do you develop or deploy agentic AI systems (systems that can autonomously plan/act or use tools)?[4]

Yes

> **14.A. If yes, please indicate which categories of controls your organization applies. Please select all.**
>
> - Constraints on the agent's action space (e.g., tool-use permissions, environment sandboxing, allowlists/blocklists of resources, scope limits per task)
> - Human oversight or interruptibility mechanisms (approval requirements for sensitive actions, escalation paths, interruption interfaces)
> - Logging of agent actions

Please provide any further comments and implementation documentation.

No answer provided

Section 3 – Transparency Reporting on Advanced AI Systems

15. Does your organization publish public reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems? Are these clear and understandable by non-technical audiences?

Yes

> **15.A. If yes, which of the following information is included in your organization's publicly available documentation for any of your AI products?**
>
> - Capabilities, behaviours, and limitations, including domains of appropriate and inappropriate use or indicative thresholds associated with systemic risks.
> - Technical documentation and instructions for use if relevant.
> - Plain-language or non-technical summaries

Please provide links or references showing where this information is made public.

https://byve.bymysidelabs.com/en/terms , https://byve.bymysidelabs.com/en/acceptable-use , https://byve.bymysidelabs.com/en/faq , https://byve.bymysidelabs.com/en/ai-principle-code

15.B. If yes, how often are such reports usually updated?

Other (e.g., triggered by material changes, incidents, or new risks)

16. 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?

- Public documentation

Describe how evaluation results are shared and with which stakeholders (e.g. other organizations, governments, civil society and academia, etc). You may also indicate whether non-technical or plain-language summaries are provided for broader audiences.

We have not run formal external risk evaluations. We publish our practices and limits in plain language in our policies and Principles-Code disclosure, available in many languages: https://byve.bymysidelabs.com/en/ai-principle-code

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

Yes

If yes, provide links to privacy policies or notices covering personal data, user inputs, and AI-generated outputs.

https://byve.bymysidelabs.com/en/privacy

18. How 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?

- Public documentation

Please provide links to any publicly available information.

We do not train models. Our disclosure lists the third-party models we use and points to their developers' published information: https://byve.bymysidelabs.com/en/ai-principle-code

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

Yes

If yes, describe additional method(s), including where relevant transparency measures related to AI agents

> We accepted Japan's Principles-Code for generative AI and are listed as No. 4 on the Cabinet Office list of businesses that have filed (26 October 2026): https://www.cas.go.jp/jp/seisakukaigi/titeki2/ai_principle_code/jigyousha_ichiran.html . The disclosure is published in 65 languages.

20. Does your organization publish statistical insights derived from anonymised, aggregated usage data to advance understanding of AI adoption and its economic impacts in areas including occupations and tasks by region, sector and country? To this end, do you contribute to international cooperation efforts?

No

Please estimate the total staff time and annual expenses associated with conducting compliance activities and include any further comments and implementation documentation (optional).

Handled by the representative alongside development; no separate budget.

Section 4 – Organizational Governance, Incident Management, and Transparency

21. How has AI risk management been embedded in your organization's governance framework?

- Executive oversight

> **Please describe how AI risk management is integrated into governance structures, including: which roles or bodies have advisory versus decision-making authority; which roles or bodies have final accountability for AI risk-related decisions; and how often policies are reviewed or updated (e.g., following major incidents, regulatory changes, or material updates to systems).**
>
> By My Side Labs is a one-person studio. The representative has both advisory and final decision authority over AI risk and is accountable for it. Policies are reviewed after major incidents, regulatory changes such as Japan's Principles-Code, model or provider changes, and at least once a year.

22. Are relevant staff trained on your organization's governance policies and risk management practices?

Not applicable

23. Are steps taken to address reported incidents documented and maintained internally?

Yes

> **If yes, describe how incident records are kept and used for follow-up (e.g., incident logs, root-cause analysis reports, internal tracking systems). You may indicate whether and how you define escalation thresholds for when incidents must be surfaced to senior leadership or external parties.**

> Failures, refusals and security alerts are recorded on the server. Each user-facing incident is logged with its cause, the fix, refunds or compensation given, and the notice sent to affected users. Incidents that affect many users are handled immediately by the representative.

24. Does your organization share research and best practices on addressing or managing risk?

No

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

Yes

> **If yes, please indicate which standards or frameworks apply:**
>
> - Industry-led best practices or codes of conduct
> - Other international or regional standards (please specify): Japan's Principles-Code for generative AI (Cabinet Office of Japan); Google Play and Apple App Store policies

> **If yes, describe which international technical standards or best practices your organization uses.**
>
> We follow Japan's Principles-Code for generative AI and the app store policies of Google Play and Apple. We do not currently hold ISO/IEC or NIST-based certifications.

Any further comments and implementation documentation.

No answer provided

Section 5 – Content Authentication & Provenance Mechanisms

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

- User disclosure (e.g., text notice, verbal statement, or system label)
- Documentation or FAQs explaining when and how AI is used in the system

> **Provide any additional details or context on how or when users are informed they are interacting with advanced AI systems (e.g. if such mechanisms are planned, in testing, or applied only to certain products).**
>
> BYVE AI is presented as an AI app builder in its name, store listings and onboarding. Our FAQ and policies explain that apps are generated by third-party AI models.

27. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems?

No

Any further comments and implementation documentation.

BYVE AI generates on-device apps (HTML and JavaScript), not image, audio or video files, so we do not currently apply watermarking or C2PA.

Section 6 – Research & Investment to Advance AI Safety & Mitigate Societal Risks

28. Does your organization advance research and investment in the following areas?

- System performance and outcomes (e.g. accuracy, consistency)
- Robustness or reliability

> **If yes, please describe key research or investment initiatives in the areas selected above (e.g., dedicated safety teams, funding of research programs, contributions to open-source safety tools, publishing research, partnerships and collaborative research initiatives). You may also indicate whether related outputs are publicly shared, shared with partners or within consortia or not publicly disclosed.**
>
> We run internal evaluations of generated apps on fixed request sets across many languages, measuring whether apps start without errors, whether controls work, and generation time, and we use the results to improve our generation pipeline. Results are not published.

29. Does your organization pursue research or investment related to socio-economic or environmental considerations in the development and deployment of AI?

- Socio-economic considerations (e.g., AI adoption and productivity, workforce transitions, skills development, access to AI tools)

> **If yes, please provide examples of relevant research or investment initiatives for the areas selected above.**
>
> BYVE AI lets people without coding skills build working apps in their own language for free; tokens can be earned through rewarded ads, and the app is available in 80+ languages.

Any further comments and implementation documentation.

No answer provided

Section 7 – Advancing Human and Global Interests

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

Yes

> **If yes, describe any digital literacy or training initiatives your organization supports (e.g., user education, public AI-education programs, school or university partnerships, community workshops). You may also indicate whether these efforts include or prioritise underserved or underrepresented communities.**
>
> We publish a free library of example apps with the requests that produced them, and a FAQ in many languages that explains what the AI can and cannot do.

31. Does your organization pursue AI projects that aim to deliver societal or public benefits, including through partnerships with civil society and community groups?

Yes

> **If yes, please provide examples, including any collaborations with civil society, community groups, or efforts to address broader societal challenges.**
>
> Uyaji is a free, ad-free AI agent for residents of Ulsan, South Korea, that answers everyday questions about buses, pharmacies, local services and events using official public data.

Any further comments and implementation documentation.

No answer provided