BRIEFING 07 · COMPLIANCE

Is your AI & sourcing stack illegal in Japan?

A reading of the two laws — APPI and the Employment Security Act — that govern candidate-sourcing in Japan, with a checklist for verifying the AI tools your company uses.

6 / 1642

FILED SERVICES IN THE #4 CATEGORY

Of 1642 services filed with MHLW, 6 are in the category that allows AI candidate aggregation without per-candidate request.

inside THIS BRIEFING

What follows, in twelve sections.

For HR directors, procurement teams, recruiting firm owners, and in-house counsel evaluating AI sourcing tools for Japan. Built from primary sources: APPI, MHLW guidance, PPC Q&A, and the public registry as of April 2026.

Sources: 個人情報保護法 (e-Gov 法令検索) · 職業安定法 (e-Gov 法令検索) · 個人情報保護委員会 Q&A · 厚生労働省「特定募集情報等提供事業概況報告書」集計結果 (令和7年6月1日時点 · 令和8年3月公表) · 優良募集情報等提供事業者認定制度 (yuryonintei.com, MHLW 委託事業 site, accessed April 2026).

01 THE NUMBER THAT MATTERS

6 of 1642.

As of June 1, 2025 — the most recent published MHLW aggregate — 1283 entities had filed as 特定募集情報等提供事業者 (Specified Recruitment Information Providers) in Japan. Among them, 1642 distinct services were registered. The four legal categories are not evenly populated. One of them is almost empty.

第1号 — job postings at employer request — has 1502 services. 第3号 — candidate information at candidate request — has 623. 第4号 — candidate information collected *without* request — has 6.

MHLW STATUS REPORT · AS OF JUNE 1, 2025 · PUBLISHED MARCH 2026

Filed services by 号 classification.

CATEGORY	DESCRIPTION	SERVICES
第1号	Job postings at employer request	1502
第2号	Job postings without employer request (aggregators)	132
第3号	Candidate information at candidate request	623
第4号	**Candidate information collected without request**	**6**

A single entity can file in multiple categories. Total services exceed total entities for that reason.

> Thousands of AI sourcing platforms describe themselves in language that, under Japanese law, sits squarely in the #4 category. Six services are filed there. Make of that what you will.

02 TWO LAWS, NOT ONE

Two regimes, not one.

Compliance discussions about AI recruiting in Japan often collapse into a single conversation about “data privacy.” The actual legal picture is two parallel regimes, each with its own regulator, registration, penalty structure, and audit cadence. A platform can comply with one and remain unlawful under the other.

LAW 1 · DATA PRIVACY

個人情報保護法
Act on the Protection of Personal Information

Regulator	PPC（個人情報保護委員会）
Scope	All personal data handling
Registration	Not required
Reach	Extraterritorial (Art. 171)
Max fine	¥100M (corporate)

LAW 2 · RECRUITING OPERATIONS

職業安定法
Employment Security Act

Regulator	MHLW · 厚生労働省
Scope	Recruiting info provision
Registration	届出 required (4 categories)
Reach	Japan-resident candidates
Penalty	6 mo. / ¥300K (Art. 65(7))

APPI governs the data — every record about an identifiable Japan-resident individual, regardless of where the operator is incorporated or where the server sits. The 職業安定法 governs the act of providing candidate information to employers — which is what every AI sourcing platform does at the moment it returns a ranked candidate list to a paying client.

Both laws apply at the same time. A platform incorporated in California, scraping LinkedIn data, processing on US-based AI infrastructure, and selling subscriptions to Tokyo recruiters needs to satisfy *both* regimes. There is no single-law shortcut.

> “If a platform’s compliance story addresses only one law, the platform has not done compliance.

03 WHAT CHANGED IN OCTOBER 2022

Crawlers, into the net.

Before October 1, 2022, the 職業安定法 covered services that acted on a direct request from a job seeker or an employer. Platforms that crawled public web data to build candidate databases — without any per-candidate sign-up — operated in a regulatory gray zone. The 2022 amendment closed that zone.

Three changes mattered for AI sourcing.

Three changes that defined the new regime.

1. The definition expanded. 募集情報等提供 was redrawn to include crawler-type platforms collecting candidate data without per-candidate request — creating the 第4号 category that many AI sourcing tools, regardless of where they were built, now sit inside.

2. A registration system was created. Any operator that collects candidate information for provision to employers must file 届出 (notification) with MHLW *before* beginning operation. Operating without filing is a criminal offense — up to 6 months' imprisonment or a ¥300,000 fine under Article 65(7), with parallel penalties applying to the corporate entity under Article 67 (両罰規定).

3. New ongoing obligations attached. Filed providers must file an annual 概況報告書 (status report); maintain 的確な表示 (accurate display) of recruiting information; respond to candidate complaints; protect personal information separately from APPI obligations; and disclose the principal factors used to rank search results — a direct nod to AI scoring platforms.

> ### The ranking-disclosure rule (Art. 43-6) — verbatim.
>
> *MHLW's Q&A on the amendment is explicit about what must and what must not be disclosed: the* ***principal factors*** *used in ranking are public-disclosure items; the underlying algorithm code and the calculation procedure that uses those factors are not. AI is not exempted. AI scoring platforms must disclose what their score is built from, even if the model itself remains proprietary.*

04 THE APPI COMPLIANCE STACK

Six categories of obligation.

APPI is not a single compliance test. It is a stack of obligations that apply at distinct points in the data lifecycle. An AI sourcing platform meets the stack only if every layer holds.

The stack, layer by layer.

LAYER	OBLIGATION	ARTICLE
Acquisition	Lawful means (適正な取得). Cannot acquire by methods that violate the source's terms.	Art. 20
Purpose	Specify purpose of use as concretely as possible; publicly disclose; do not exceed scope.	Art. 17, 18, 21
Security	Organizational, personnel, physical, technical safeguards. External-environment awareness for overseas processing.	Art. 23
Third-party provision	Consent, opt-out filing, or 委託 (entrustment) framing for each provision to a client.	Art. 27
Cross-border transfer	If data is processed in a foreign country, additional consent and disclosure obligations apply.	Art. 28
Data subject rights	Disclosure, correction, deletion, cessation of use — accessible to the candidate.	Art. 32–35

Layer 1, Article 20, is where most foreign platforms break first. APPI requires data to be acquired by "fair means." Public visibility on the source site does not by itself make the means fair. If the source platform's terms expressly prohibit automated collection, scraping is not within the "fair means" that Article 20 contemplates — regardless of whether the data is technically reachable to a logged-out browser.

04 CONT. · CROSS-BORDER PROCESSING

The foreign-processor problem.

A common defense from foreign AI platforms is that data sits on AWS Tokyo, or on Japanese servers — therefore APPI cross-border rules don't apply. The PPC has answered that defense directly.

> **PPC Q&A — verbatim translation.**
>
> *When a domestic operator entrusts the handling of personal data to a foreign third party, the operator must implement security measures based on an understanding of the personal-information-protection regime in the foreign country.* ***This obligation applies even where the personal data itself is stored on servers located within Japan.*** *(PPC General Guidelines Q&A Q10-25.)*

The implication for AI recruiting platforms: if your model runs on US-based OpenAI, Anthropic, or Google infrastructure, the operator is processing personal data through a foreign entity even if the storage layer is in Japan. The 外的環境の把握 (external-environment understanding) obligation under Article 23 attaches. So does Article 28 cross-border transfer analysis, depending on the legal characterization (entrustment vs third-party provision) of the processor relationship.

The adequacy whitelist is short.

Under Japan's adequacy framework, only the EU and the UK are recognized as equivalent to Japan's regime. The United States is not. A platform sending Japan-sourced candidate data to US infrastructure cannot rely on adequacy; it must satisfy the cross-border consent or appropriate-safeguards path under Article 28, plus the security obligations under Article 23.

"Our servers are in Japan" is not the answer when inference happens in Virginia.

05 WHERE POPULAR PLATFORMS FAIL

Four structural gaps.

Many of the AI sourcing platforms now actively sold into the Japan market — most of them built in the United States, marketed in English, and not built around either of the two laws above — share a recognizable pattern of compliance gaps. The pattern is not random; it follows from the way these platforms were architected.

Gap 1 · The data supply chain begins with scraping. Most of the "tens of millions of profiles" databases marketed by foreign AI sourcing platforms are sourced, directly or indirectly, from LinkedIn. LinkedIn's User Agreement (Section 8.2) prohibits using software, scripts, robots, crawlers, or browser plugins to scrape or copy profile data. Under APPI Article 20, data acquired in violation of the source's terms is unlikely to qualify as "fair means" (適正な取得). A US court may take a different view of whether scraping public data violates the Computer Fraud and Abuse Act — that is a US statutory question. Japanese law applies a different test, and Japanese law is what governs Japan-resident data subjects.

Gap 2 · No 特定募集情報等提供事業 filing. The MHLW filing is required *before* commencement of business. Almost no foreign-incorporated AI sourcing platforms have filed. Operating without filing is a criminal offense under Article 65(7) of the Employment Security Act. The dual-penalty provision in Article 67 means the corporate entity faces parallel liability alongside any responsible individuals.

Gap 3 · Cross-border AI processing without Article 23 / 28 compliance. The defense that "we're a US company, APPI doesn't apply" fails on Article 171 (extraterritorial application). The defense that "data is stored in Japan" fails on PPC Q10-25. What is left is the actual obligation: external-environment understanding, documented security measures, and — for genuine third-party transfer — Article 28 consent or an adequacy-equivalent framework. The US is not on the adequacy list.

Gap 4 · The cold-email model violates the Anti-Spam Act. Japan's 特定電子メール法 requires *prior opt-in consent* before commercial email is sent — the inverse of the US CAN-SPAM regime, which permits unsolicited email with an opt-out path. Platforms that supply email addresses for cold outreach to Japan-resident candidates create direct exposure for every send. The recipient's location, not the sender's, is what triggers application.

05 CONT. · THE DAISY-CHAIN PROBLEM

The opt-out shortcut that doesn’t work.

Some platforms attempt to characterize their candidate-data provision to clients under the APPI Article 27(2) opt-out mechanism — file with the PPC, publicly disclose, maintain an accessible opt-out, and provide without per-candidate consent. The 2022 APPI amendment closed this path for any data that was itself acquired through opt-out or through improper means.

> **The daisy-chain prohibition.**
>
> *Personal data acquired through the opt-out mechanism, or acquired through improper means, cannot be re-provided to a third party under another opt-out claim. The chain breaks at the second link.*

Read together with the Article 20 “fair means” requirement, the practical consequence is sharp. If the upstream data was scraped from a site whose terms prohibit scraping, the data was arguably acquired through improper means. Once that determination is on the table, the opt-out provision path is unavailable downstream — for the original scraper, for any reseller, and for any AI platform that built its database on the resold data.

This is the reason platforms in this category often quietly avoid framing their provisioning model in any specific APPI lane. There is no clean lane to occupy.

“We’re not based in Japan” is not a defense.

APPI Article 171 (formerly Article 75) applies extraterritorially to any operator handling personal information about persons in Japan in connection with providing goods or services to Japan. The data subject’s residency is what matters, not the operator’s. A San Francisco platform with paying Tokyo clients and a Japan-resident database is squarely in scope — and the PPC can issue orders and compel reports from foreign operators since 2022.

> **“Distance is not cover. The PPC’s reach follows the data subject, not the server.**

06 THE RIKUNABI PRECEDENT

The 2019 case that set the floor.

リクナビDMPフォロー remains Japan's most consequential recruiting-data enforcement action. The PPC issued a corrective recommendation (勧告) against Recruit Career in August 2019, and a second one in December 2019 against both Recruit Career and its parent operating company Recruit Co., Ltd. MHLW issued a parallel administrative guidance under the 職業安定法. The case directly accelerated the 2020 APPI amendment.

What Recruit was doing.

The Rikunavi platform built a model to predict 内定辞退率 — the probability a student would decline an offer. Predictions were sold to 35 enterprise clients (Toyota, Mitsubishi, Denso, Honda's research arm, others) for follow-up prioritization. Some 7983 students initially — later expanded to 26,060 — had not given valid consent for third-party provision. Recruit's Cookie-hash workaround was rejected: the PPC found Recruit could still re-identify, and the recipients could re-identify on their end.

What it established for AI scoring.

Three principles flowed out of the case, and they apply directly to any AI recruiting platform operating in Japan today.

One. AI prediction or scoring of candidate data is a use that must be specifically disclosed to the data subject — generic "to improve our services" language does not cover it.

Two. Providing AI-generated predictions about candidates to employer clients is third-party provision of personal data, even when the predictions are derived rather than copied. Article 27 applies.

Three. Hashing or pseudonymization fails when the receiving party can re-identify. The PPC rejected the argument as 極めて不適切 — "extremely inappropriate."

07 THE 2026 AMENDMENT

Surcharges enter the picture.

On April 7, 2026, the Japanese Cabinet approved an APPI amendment bill and submitted it to the Diet. The bill is, in substance, a recalibration: it loosens consent requirements for some statistical and AI-training uses while sharply tightening enforcement on serious violations. Effective date is expected within 2 years of promulgation.

Three changes that matter for AI recruiting.

1. Administrative surcharges (課徴金). The bill introduces a surcharge regime for serious violations where the operator obtained economic benefit from the unlawful handling. The amount is calculated from the financial benefit obtained, not from turnover — closer to disgorgement than to GDPR's percentage-of-revenue framework. Three eligibility conditions apply cumulatively: the violation must affect more than 1000 individuals, the operator must have failed to exercise reasonable care, and there must be concrete rights or interest harm. The five surcharge-eligible offense types are enumerated and limited (improper use, improper acquisition followed by use, unconsented third-party provision, provision to a third party expected to use the data unlawfully, and breach of the new statistical-creation special-rule conditions). Surcharges do not apply to ordinary security-measure failures or accidental leaks.

2. Heavier criminal penalties for unlawful provision. The bill raises the statutory penalty for unlawful provision of a personal-information database (currently 1 year's imprisonment or a ¥500,000 fine under Art. 179) and extends the offense to provision carried out for the purpose of causing harm, in addition to the existing offense of provision for unlawful profit. The bill also creates a new offense for unlawful acquisition by deception or unauthorized access.

3. The processor (処理者) concept formalized. Clearer statutory treatment for data-processor relationships — the legal layer currently handled by 委託 framing for OpenAI, Google, AWS, and similar overseas infrastructure. Favorable for compliant AI operators; harder for non-compliant operators to hand-wave the cross-border processing question.

> ### The combined picture.
>
> *The 2022 ESA amendment criminalized unfiled crawler-type platforms. The 2026 APPI amendment adds disgorgement-style surcharges on top. Quieter than the EU's framework — but real.*

08 WHAT COMPLIANT OPERATION LOOKS LIKE

Ten items, split across two pages.

There is no certification body that can stamp a platform "compliant." What exists is a defensible posture — a set of design choices, registrations, and disclosures that, taken together, satisfy both regulatory regimes. The framework below is what compliance counsel will look for; this page covers the foundational five.

ITEM	WHAT IT ACTUALLY MEANS	SOURCE
1. Lawful data sources	Data acquired from licensed providers or candidate submissions, with documented provenance per record. No scraping of TOS-protected sites.	APPI Art. 20
2. MHLW filing	Filed as 特定募集情報等提供事業者 under the correct 号 classification, before commencement of business.	ESA Art. 43-2
3. Purpose disclosure	Specific, public, covering AI scoring, candidate matching, presentation to clients, scout-mail generation.	APPI Art. 17, 21
4. Article 27 compliance	Each provision to a client characterized cleanly as consent, opt-out, or 委託 — and the chosen path actually working.	APPI Art. 27
5. Article 23 / 28 compliance	External-environment understanding for overseas processors, documented security measures, US-jurisdiction assessment.	APPI Art. 23, 28

Items 6 through 10 follow on the next page. Together they cover ongoing obligations — candidate rights, ranking transparency, data accuracy, complaints handling, and annual reporting — that distinguish a one-time filing posture from operational compliance.

08 CONT. · ITEMS 6 THROUGH 10

Ongoing obligations, not one-time filings.

ITEM	WHAT IT ACTUALLY MEANS	SOURCE
6. Candidate rights	Accessible disclosure, correction, deletion, and cessation-of-use mechanisms for any data subject.	APPI Art. 32–35
7. Ranking factor disclosure	Principal scoring factors public; algorithm code and weights can remain proprietary as 営業秘密.	ESA Art. 43-6
8. Data accuracy measures	Regular synchronization with upstream data providers; documented correction process.	ESA Art. 5-4 + 43-3
9. Complaints handling	Accessible complaints window with a documented response procedure and a designated owner.	ESA Art. 43-7
10. Annual reporting	概況報告書 submitted to MHLW each August for the prior June 1 status.	ESA Art. 43-5

Reading the ten items together is more useful than reading any one of them. A platform with strong purpose disclosure and weak data sourcing is not partially compliant; it is exposed at the upstream layer. A platform with clean acquisition but no MHLW filing has criminal exposure regardless of how well-drafted its privacy policy reads. The items are gates, not points to be averaged.

> “Compliance is a configuration. Either every gate is open in the right direction, or the configuration is broken — regardless of how nice the privacy policy reads.

08 CONT. · THE 優良認定 CEILING

Above the floor: audited certification.

Beyond the basic 届出 filing, MHLW commissions a voluntary audited certification — the 優良募集情報等提供事業者認定制度. The audit covers seven categories: legal compliance, accurate display, personal-information handling, information disclosure, advertiser-side vetting (審査), complaints handling, and other governance items. The certification is the closest thing Japan has to a publicly visible compliance benchmark for recruiting platforms.

優良認定 · 認定事業者一覧 · AS OF APRIL 1, 2026

42 entities certified across all four categories.

42	1	3-yr
TOTAL CERTIFIED ENTITIES	CERTIFIED ENTITY OPERATING IN 第4号	CERTIFICATION TERM, RENEWABLE

A single entity in this category currently holds 優良認定. The remaining 5 are not certified.

The numbers are worth pausing on. There are 6 services filed in the 第4号 category. Of those, 1 is currently 優良-certified. The audit is not theatre — entities pursuing it submit to independent review across the seven categories above and are listed publicly on MHLW's 人材サービス総合サイト. For HR procurement teams, the certification is one of the few signals available that does not depend on the vendor's own marketing claims.

> **The compliance question, for any candidate-sourcing platform, eventually reduces to one: are you on this list?**

09 THE CUSTOMER'S LIABILITY

The buyer is also exposed.

APPI does not stop at the platform. When a Japanese employer or recruiting firm receives personal data from a third-party provider, the receiving party has its own confirmation duty under Article 30. The duty is straightforward: confirm the identity of the provider, confirm how the provider acquired the data, and confirm that the provider has a lawful basis for the provision. The duty is on the recipient, not the provider.

What this means for procurement.

A Japanese enterprise — particularly a TSE-listed one — that buys candidate data from a non-compliant foreign platform inherits a piece of the compliance problem. If the upstream platform cannot demonstrate lawful acquisition, the recipient cannot satisfy Article 30. The data may still be useful to recruiters, but the company has signed up for direct APPI exposure if the matter ever surfaces — through a candidate complaint to the PPC, a competitor disclosure, or a regulatory inquiry.

This is not theoretical. Compliance-conscious Japanese enterprises are increasingly asking the question explicitly during procurement. The expected answer is documentation: a copy of the upstream platform's 届出 filing, a written description of data sources, and confirmation of Article 23 / 28 / 27 posture. Vendors who cannot produce these documents are increasingly being filtered out at the procurement stage, before they reach a pilot.

> **The procurement question, in one line.**
>
> *"Show me your 特定募集情報等提供事業 届出受理通知 and your data-source documentation." A platform that cannot produce both, in a few days, on a Japanese client's request, is a platform whose risk has been transferred to that client.*

> **"The non-compliant vendor sells you data. The non-compliant vendor also sells you their compliance problem. Article 30 is the receipt.**

10 A SELF-AUDIT YOU CAN RUN TODAY

Seven questions for any platform on your shortlist.

Use these questions during your next vendor evaluation. Score one point per "yes" supported by a document the vendor will email you within 48 hours. Anything else is a "no."

1. Is the vendor filed as a **特定募集情報等提供事業者** with MHLW? Provide the 届出受理通知 number and the 号 classification.
2. For each candidate record, can the vendor produce the **data source and acquisition path**? Was the source's terms-of-service consulted, and is automated collection permitted there?
3. Does the vendor's **privacy policy** specifically disclose AI scoring, candidate matching, presentation to clients, and scout-mail generation as purposes of use? Is the disclosure in Japanese as well as English?
4. For overseas AI processing, has the vendor performed **外的環境の把握** on the relevant foreign jurisdictions (United States in particular), and is the assessment documented?
5. Are the **principal ranking factors** publicly disclosed in compliance with ESA Article 43-6?
6. Is there a **candidate-side mechanism** for disclosure, correction, deletion, and cessation-of-use requests, with a published response timeline?
7. For email outreach functionality, does the vendor obtain **opt-in consent** from each candidate before commercial messaging — as required by 特定電子メール法?

SCORE INTERPRETATION

6–7 yes: Vendor has done the compliance work. Conduct the technical evaluation on its merits.
4–5 yes: Material gaps. Conditional engagement only, with documentation as a contractual closing condition.
2–3 yes: Compliance posture is incomplete. Procurement risk is high; legal review required before any pilot.
0–1 yes: Vendor has not done the work. Buying their data buys their problem.

11 HEADHUNT.AI, AGAINST THE FRAMEWORK

Headhunt.AI, against the framework.

The remainder of this briefing is general. The next two pages are not. They walk the operator behind Headhunt.AI — ExecutiveSearch.AI K.K. — through each item in Sections 8 and 10, in the same order any other operator should be able to walk through them. Some items are confirmed today; some are in process and explicitly framed that way. The exercise is included for transparency, not as a compliance certificate.

ITEM 01 · MHLW FILING

Status: in process (申請手続中). ExecutiveSearch.AI K.K. (法人番号 T5011001118882) is in the process of completing its 第4号 特定募集情報等提供事業 filing with the 厚生労働大臣 under 職業安定法 第43条の2第1項. The filing will appear on the 人材サービス総合サイト upon issuance of the 届出受理番号. Headhunt.AI's commercial launch is timed to follow that issuance.

ITEM 02 · LAWFUL DATA SOURCES

Status: confirmed. Headhunt.AI does not directly scrape personal data from the open internet. The candidate database underlying the service is sourced through commercial licensing arrangements with established global data providers, governed by formal license agreements that authorize ExecutiveSearch.AI's use of the data and the production of derived analytical outputs (such as candidate match scores) for delivery to enterprise users. The underlying agreements are maintained on file as a matter of contractual record. Provider data is collected from publicly available sources in compliance with applicable data-protection law in the jurisdictions of collection.

ITEM 03 · PURPOSE-OF-USE DISCLOSURE

Status: in current Privacy Policy. ExecutiveSearch.AI's Privacy Policy enumerates the purposes for which personal information is processed within Headhunt.AI: AI-based candidate scoring and relevance assessment; matching candidate profiles against client-specified job requirements; presentation of candidate information to authorized client users; and generation of personalized outreach communications for use by client users. Each purpose is disclosed in advance of data being used for it, in accordance with 個人情報保護法 第17条 and 第21条.

11 CONT. · ITEMS 4 THROUGH 7

ITEM 04 · 外的環境の把握 DISCLOSURE

Status: in current Privacy Policy. Headhunt.AI's processing infrastructure includes United-States-based vendors for cloud and AI inference. The Privacy Policy includes a 外的環境の把握 disclosure identifying these foreign jurisdictions and the relevant legal regimes (notably US federal and state privacy law, including the California Consumer Privacy Act). Data Processing Agreements with each foreign vendor obligate the vendor to safeguards including no use of ExecutiveSearch.AI data for vendor model training, minimum-necessary transmission, short retention periods, and incident notification.

ITEM 05 · RANKING FACTOR DISCLOSURE

Status: published on the 職安法 compliance disclosure page. The candidate ranking surfaced as the ESAI Score is generated by an AI model evaluating candidate profiles against client-specified job requirements. The principal factors considered (work-history relevance, educational background, skill alignment, language proficiency fit, industry experience) are publicly disclosed on ExecutiveSearch.AI's 職安法 compliance page, in keeping with the transparency framework contemplated by 職業安定法 第43条の6 and the relevant ministerial guidelines. Specific algorithmic weights and proprietary scoring logic are not disclosed; these are treated as the company's 営業秘密. The ESAI Score is presented to client users as a screening aid, not as a definitive evaluation of any candidate; candidates are not informed of their score, and the score is not used as a basis for direct candidate communication.

ITEM 06 · COMPLAINT AND INQUIRY CHANNEL

Status: monitored business-day inbox with named owner. ExecutiveSearch.AI maintains a dedicated complaint and inquiry channel for privacy and personal-data matters at `privacy-complaints@executivesearch.ai`. The channel is monitored on business days by a designated internal owner, and is referenced in both the Privacy Policy and the 職安法 compliance page. It serves as the primary intake point for the complaint-handling system maintained under 職業安定法 第43条の7.

ITEM 07 · 優良認定 FORWARD-LOOKING

Status: aspirational, not committed. ExecutiveSearch.AI's compliance approach is structured to align with the operational and governance standards associated with the 優良募集情報等提供事業者認定 framework. The company intends to consider applying for 優良認定 in a future certification cycle, once the operational track record required to support such an application has been established. This is a forward-looking intention rather than a commitment, and ExecutiveSearch.AI makes no representation about the timing or outcome of any future application.

12 THE HONEST TAKE

The honest take.

The Japan AI recruiting market is in the early innings of a regulatory consolidation that, in retrospect, will look obvious. The 2022 amendment criminalized operating without filing. The 2026 amendment adds disgorgement-style surcharges. The PPC has reach, the MHLW has a public registry, and Japanese enterprise procurement teams are increasingly asking the right questions before they sign.

The platforms that did the compliance work early — registered, disclosed, structured their data supply chain — will compound their position through this period. The platforms that operated on the assumption that "Japan won't enforce" or that "the data is public" will discover, in stages, that the assumption was wrong. Some will adjust. Some will lose their Japan footprint when the first orders are issued and the first clients perform Article 30 due diligence.

For HR directors and procurement leads inside Japanese enterprises, the practical implication is simpler than the legal text suggests. The compliance question is no longer "can we get away with using this platform." It is "does the platform's legal posture survive a one-page procurement memo."

The audit is not elaborate. Pull every AI candidate-sourcing tool currently in use across your company — the ones procurement signed off on, and the ones an enterprising recruiter put on a corporate card or personal expenses. Run the seven questions in Section 10 against each. Headhunt.AI was built to clear that bar; its operator's posture is documented item-by-item in Section 11. Most foreign tools sold into Japan today were not built that way, and cannot.

REMINDER

These systems are the worst they will ever be today. The pace of improvement in AI is not linear — **invest now to stay ahead of your competition, or fall behind.**

> **"Doing nothing is a decision, the same as any other. It just looks more like the present.**

about HEADHUNT.AI · FOR JAPAN

Built by an agency. Built for Japan.

Headhunt.AI is the AI sourcing platform built and operated by ExecutiveSearch.AI K.K., a Tokyo recruiting firm running an AI-first model since 2018 and a wholly-owned subsidiary of Monstarlab Inc. (TSE: 5255). The platform was designed from the ground up around the two-law framework above — not retrofitted onto a global product after the fact. Section 11 walks each compliance item through, in the same order any operator should be able to walk through it.

Our 4M+ profile Japan-focused database, the ESAI Score, the bilingual scout-mail engine, and the production figures cited in earlier briefings in this series are all from the same platform that runs our own desk today. We license it to peer agencies and to corporate in-house TA teams who want to make the same operational shift — on terms that we use ourselves.

This whitepaper is for educational purposes only and does not constitute legal advice. Specific compliance questions should be directed to qualified Japanese counsel. Statements about ExecutiveSearch.AI's compliance posture in Section 11 reflect the company's status as of April 2026; status of items currently in process will be updated when the underlying registrations and disclosures are complete.

Headhunt.AI

START WITH A COMPLIANCE REVIEW

One JD. One ranked list. Full data-provenance documentation.

Send us one open requisition. We will run it through Headhunt.AI and return a shortlist with the scoring evidence on every candidate — together with our compliance documentation pack covering the items in Section 11. Two-minute test of the platform; one-document review of the legal posture.

SALES@EXECUTIVESEARCH.AI · HEADHUNT.AI · TOKYO, JAPAN