Atsumi & Sakai Newsletter
JAPAN
NEW YORK
LONDON
FRANKFURT
BRUSSELS
HO CHI MINH

September 2026
No. SME_003

Data Protection Guide
The GDPR and Other Data Protection Issues

A Protection Guide for Sports, Media & Entertainment Businesses in Japan

How to use this guide

Who it is for. Sports, media and entertainment businesses in Japan that serve, or may serve, fans, audiences or subscribers located in the EU/EEA — rights holders, event organizers and promoters, ticketing and box-office teams, broadcast and streaming teams, IT and systems staff, and in-house counsel or compliance.

How to read it. Start with the Quick Start (Section 1) and the role guide below. Work through Sections 2–3 to decide whether the GDPR applies to you; Sections 4–6 for what it means in daily operations; and Section 9 for a step-by-step implementation roadmap. The checklists and templates are designed to be copied and used directly.

How to use it in your business. Use it as a training document, as a working checklist for a compliance review, and as the basis for a short internal project plan. It is general information, not legal advice on any specific situation.

1. Executive Summary and Quick Start

Many sports, media and entertainment businesses in Japan assume that, because they have no establishment in the European Union and operate exclusively in Japan, the EU General Data Protection Regulation (GDPR) does not concern them. This assumption is often incorrect.

The GDPR can apply to your business even where you have no EU office, no EU staff and no EU bank account, if you offer tickets, content, merchandise or membership to fans, subscribers or audiences located in the EU/EEA. In sport, media and entertainment this happens more easily than rights holders and promoters expect — through an English-language ticketing or streaming website, listings on international ticketing marketplaces, international broadcast and licensing deals, or marketing aimed at overseas fans and audiences.

Where the GDPR applies, using a third-party ticketing platform or streaming partner does not, by itself, discharge your own obligations. The platform handles its own data collection, but your business remains responsible, as a controller, for the personal data it receives and processes in connection with the event, broadcast or engagement — including providing a compliant privacy notice, identifying a legal basis, honouring data subject rights, and notifying certain data breaches within strict time limits.

The five points to take away

1. "No EU office" does not mean "no GDPR". The GDPR can apply based on who you serve, not only where you are established.

2. Ticketing-platform compliance is not your compliance. You remain a controller for the data you receive and use.

3. Your privacy notice must meet GDPR content standards — a policy written only to satisfy Japan's Act on the Protection of Personal Information (APPI) is usually not enough on its own.

4. Data breaches involving EU fans or subscribers can trigger a 72-hour notification duty to an EU authority.

5. The absence of a published GDPR fine in Japan is not evidence that the risk is theoretical.

1.1. Quick Start: five steps to take this month

If you have only ten minutes, start here. Each step points to the section where it is explained in full.

1. **Identify whether you are targeting EU/EEA fans, audiences or subscribers.** Use the Yes/No checklist in Section 2.2 to make a first assessment.
2. **Map your ticketing channels and data flows.** Complete the one-page data-flow template in Section 4.
3. **Review and adjust your privacy notices.** Check presentation, consent separation and content against Section 5.
4. **Clarify your use of platforms and your controller role.** Confirm who is controller for each channel — Section 3.
5. **Establish a 72-hour incident-response procedure.** Put the breach checklist in Section 6 into a written plan.

1.2. Who should read what

This guide is designed to circulatewithin your organisation, not to sit only with the legal team. The following is a suggested reading guide by role.

Role	Focus on
Rights holders / event organisers	Sections 1 (Quick Start), 2 (does it apply?), and 9 (roadmap).
Ticketing / box office	Sections 4 (ticketing channels) and 5 (privacy notices).
IT and system vendors	Sections 4 (data flows) and 6 (incident response).
In-house counsel / compliance	The full guide, plus coordination of the EU representative and policy drafting.

MODULE 1 **Scope and Risk — Does the GDPR Apply to You?**

2. Does the GDPR Apply to a Japanese Sports, Media or Entertainment Business?

What this section covers

– The three ways the GDPR can apply to a business outside the EU: establishment, targeting, and monitoring of behaviour.

– A simple Yes/No checklist to make a first assessment for your business.

– Which of the three common website set-ups carries the most risk.

The GDPR applies on the basis of three independent criteria — an establishment in the EU (Article 3(1)), the targeting of people in the EU/EEA (Article 3(2)(a)), and the monitoring of their behaviour (Article 3(2)(b)). Any one of them is sufficient.

2.1. Key concepts in brief

Establishment criterion (Article 3(1)). The GDPR applies to processing carried out in the context of the activities of an establishment of a company in the EU, regardless of where the processing physically takes place. A Japanese sports, media or entertainment group with a European office, a European subsidiary involved in ticketing, licensing or production, or EU-based staff handling fan or talent data may be caught on this basis. A purely domestic Japanese operation with no EU presence generally is not.

Targeting criterion (Article 3(2)(a)). This is the criterion that most often catches Japanese sports, media and entertainment businesses. The GDPR applies to a company outside the EU where it processes the personal data of people located in the EU/EEA in connection with the offering of goods or services to them — whether or not payment is required.

The key question is whether your business envisages offering its services to fans, audiences or subscribers in the EU/EEA. Merely having a website that is technically accessible from Europe is not, by itself, enough. But the European Data Protection Board (EDPB) has identified a range of factors that, taken together, can show that a business is targeting EU/EEA individuals. In the sport, media and entertainment context, the most relevant are:

- offering the website, ticketing flow or streaming service in a European language (for example, English aimed at international fans, or specifically German, French, Italian, etc.);
- allowing payment in euro or another EU/EEA currency;
- allowing fans or subscribers to enter an EU/EEA country as their address or country of residence in the registration or ticketing form;
- mentioning international or European fans and audiences, or using EU-targeted advertising or search-engine marketing;
- listing events, content or merchandise on international ticketing marketplaces or platforms which are widely accessible from the EU/EEA and are in practice used by international fans.

No single factor is decisive; the assessment is cumulative. But a business that offers an English-language ticketing or streaming flow, lets fans select a European country of residence, charges in a way accessible to European cardholders, and accepts bookings or sign-ups from EU-based fans will, in many cases, be

found to be offering its services to people in the EU/EEA — and therefore within the territorial scope of the GDPR.

Monitoring criterion (Article 3(2)(b)). The GDPR also applies to a business outside the EU where it monitors the behaviour of people located in the EU/EEA, as far as that behaviour takes place there. In sports, media and entertainment this is triggered above all by digital tools: cookies and tracking pixels on websites and ticketing flows, SDKs and device identifiers in fan or streaming apps, fan analytics and audience-measurement tools, profiling of viewing or purchasing behaviour, and personalised advertising or content recommendations aimed at EU/EEA users. The EDPB treats the use of such tracking and profiling techniques on people in the EU/EEA as a strong indication of monitoring. A streaming service that profiles EU viewers' watch history for recommendations, or a club website running ad-tech tracking on EU visitors, can therefore be caught even where no ticket or subscription is ever sold to them. Where cookies or similar technologies are used on EU/EEA users, Member-State ePrivacy rules on consent apply in parallel, so a consent-management platform (CMP) covering EU/EEA visitors is usually needed (see also Sections 5 and 10).

2.2. What you should do: the applicability checklist

Answer the following questions for your business. Tick each one that is true.

- ☐ Do you sell tickets, subscriptions or merchandise to fans who are located in the EU/EEA at the time of purchase?
- ☐ Is your ticketing or streaming path (website or purchase flow) available in English or another EU language?
- ☐ Are your events or content listed on ticketing marketplaces or platforms (e.g. Ticketmaster, SeatGeek, Eventbrite, or international streaming or licensing platforms) that are widely used by EU/EEA audiences?
- ☐ Can fans or subscribers enter an EU/EEA address or country of residence in your registration or ticketing form?
- ☐ Do you accept payment in euro, or in a way readily usable by European cardholders?
- ☐ Do you market to, or advertise for, international or European fans and audiences?

How to read your answers

This checklist is a screening aid, not a statutory threshold: the GDPR contains no "two-Yes" rule, and the legal test remains the overall assessment of all circumstances described in Section 2.1. That said, if you answered "Yes" to two or more of the above, you should assume the GDPR may apply to your EU/EEA fan, audience or subscriber activity and continue with Sections 3 to 6, then build your action plan from Section 9.

If you answered "Yes" to none or only one, the GDPR is less likely to apply — although even a single strong factor can suffice in the overall assessment, so reassess whenever you change languages, channels, payment options or marketing. Section 2.3 shows how website set-up affects this. Note that this checklist tests EU/EEA targeting only: if you also serve or target fans in the United Kingdom, run the same questions separately for the UK GDPR, which applies in parallel as a distinct regime with its own representative and notice requirements.

2.3. The three common website set-ups

Rights holders and promoters frequently ask which website configuration is "safe". The three typical options, and their indicative risk profile, are set out below. The risk labels are starting points for a first

screening, not legal categories: in each case the outcome turns on an overall weighing of all targeting and monitoring indicators (Section 2.1).

Configuration	GDPR risk	Comment
Japanese-language site, accessible worldwide	Medium–High	Language points away from targeting, but is not decisive if EU fans can and do purchase, especially alongside an international ticketing-platform channel.
Japanese-language site, technically blocked from the EU/EEA	Low	Most defensible. Genuine geo-blocking plus an access notice is strong evidence against targeting, but it does not by itself place the business outside the GDPR in every case — other channels, tracking technologies or EU-directed marketing can still bring processing into scope. Block by IP and exclude individuals located in the EU/EEA in the terms.
Ticket sales via an international marketplace (e.g. Ticketmaster)	Low–Medium	The platform handles front-end collection, but you still receive and process fan data as controller (see Section 3). Where EU/EEA sales are actively pursued through the marketplace, the realistic risk is higher than the label suggests — treat it as a starting point, not a ceiling.

Reality check

If a fan sitting in Munich or Paris can find your event or content online, complete a ticket purchase or sign-up in English, enter a German or French address, and receive a confirmation — whether directly or via a ticketing platform — then you should assume the GDPR may apply to that purchase, and plan accordingly.

2.4. Which Sports, Media & Entertainment Businesses This Guide Is For

The two preceding sections set out the legal tests. In practice, they translate into the following business types commonly found in the Japanese sports, media and entertainment sector. This list is indicative, not exhaustive — the functional test in Section 2.1 is what ultimately determines whether a given business is in scope, regardless of category.

Business type	Why the GDPR / APPI regime typically applies
Sports clubs, teams and leagues	Player, staff, member and fan data. APPI applies regardless of size — there is no small-business exemption. GDPR applies if EU-based fans, players, staff or sponsors are served or targeted.
Governing bodies and federations	Athlete, official and member-federation data, often including accreditation and anti-doping records. APPI applies regardless of size or non-profit status; GDPR applies where EU athletes, officials or affiliated national federations are involved.

Business type	Why the GDPR / APPI regime typically applies
Event organisers and venue operators	Handle ticket-holder, accreditation, security and vendor data for each event. Both regimes apply on a per-event basis wherever EU-based attendees, media or officials participate.
Broadcasters and publishers	Fully within APPI and GDPR for commercial data (subscribers, advertising, HR). The APPI Article 57 (Article 76 in the pre-April 2022 numbering) press exemption is narrow — it covers actual news-reporting activity only, not the rest of the business.
Streaming and digital-content platforms	Subscriber, viewing-history and payment data typically trigger both regimes directly, and are a principal target of the GDPR Article 3(2) targeting test where EU subscribers are served.
Film, television, music and production companies	Cast, crew, talent and location data. GDPR applies to EU-based cast/crew or EU distribution deals; APPI applies to all Japan-side processing regardless of production size.
Talent, athlete and influencer agencies	Manage personal, financial and image-rights data for represented individuals — high sensitivity given the financial and contractual detail involved. Both regimes apply directly to the agency as controller.
Ticketing, merchandising and e-commerce companies	Process payment, delivery and marketing data at volume. Core Article 13/14 GDPR notice obligations and full APPI application; frequently the "platform vs controller" question addressed in Sections 3 and 4 of this guide.
Sponsors and advertising agencies	Handle audience analytics, campaign and contact data, often shared cross-border with EU-headquartered sponsors or agencies. Both regimes apply to the processing itself and to the data-sharing arrangement.
Gaming, esports and fantasy-sports operators	Player accounts, age-verification and payment data, frequently cross-border by the nature of online play. A strong candidate for the GDPR targeting test, and fully within APPI regardless of scale. Where minors are among the players or fans, Article 8 GDPR adds further requirements: a child's own consent to information-society services is valid only above the Member State's age of digital consent (16 by default; as low as 13 in some Member States), parental consent or authorization is required below it, and marketing and profiling directed at children must be markedly more restrained. APPI itself has no statutory "digital age of consent" equivalent to GDPR Article 8; for Japan-only or mixed users, PPC guidance and prevailing sector practice (e.g. JIS Q 15001, online-game industry guidelines) instead call for guardian consent where the user is a minor lacking sufficient capacity to understand the transaction — commonly treated in practice as under around 15 years of age, though this is a practical threshold rather than a bright-line statutory age.
Technology and analytics vendors	Typically act as processors or sub-processors for the categories above. Article 28 GDPR processor-agreement obligations and the equivalent APPI outsourcing (委託) duties apply directly.
Hotels, travel and hospitality partners	Relevant wherever engaged as accommodation or travel partners for teams, events or hospitality packages, and wherever an S&E business shares fan or attendee data with them. See our companion GDPR guide for hotel and accommodation operators for the partner-side analysis.

Business type	Why the GDPR / APPI regime typically applies
Nonprofits and amateur associations	APPI applies on the same functional basis regardless of non-profit or amateur status. GDPR applies identically if EU-based members, athletes or donors are served or targeted.

MODULE 2 Ticketing Channels and Platforms

3. "The Ticketing Platform Handles the GDPR" — Why That Is Not Enough

What this section covers

- Why your business is a controller for the fan or subscriber data it receives.
- Why platform compliance does not discharge your own obligations.
- The EU representative obligation under Article 27.

A very common assumption is that, because a global ticketing marketplace or streaming platform maintains its own GDPR-compliant privacy framework, the business that sells through that platform has nothing further to do. This is incorrect, and it is the single most important misunderstanding this guide seeks to correct.

3.1. Key concepts in brief

You are a controller for the data you receive. Under the GDPR, a "controller" is the entity that determines the purposes and means of processing personal data. A business that receives fan or subscriber data from a platform and then uses it to fulfil the ticket or subscription, manage the event or service, send confirmations, handle billing and carry out post-event or post-broadcast communications is determining the purposes of that processing. It is therefore a controller for that processing in its own right — regardless of how the data was first collected. The platform's privacy notice covers the platform's own processing; it does not cover, and does not discharge, the separate processing your business performs once it has the data.

Independent controllers, not processor and controller. The standard platform/rights-holder relationship is generally one between two independent controllers: the platform as controller for its platform-side processing, and the business as controller for the ticketing, subscription or fan data it receives and uses. The platform is not, in the usual case, acting as your data processor, and you cannot rely on the platform's legal basis or privacy notice as if it were your own. Confirm the exact allocation against the platform's partner terms, which can change from time to time.

Joint controllership is a third possibility. In some set-ups the parties do not act independently but jointly determine the purposes and means of processing — for example, a league and its clubs pooling fan data, co-promoters staging a joint event, or a sponsor and a rights holder running a shared fan-engagement or co-branded ticketing campaign. In those cases the parties are joint controllers under Article 26 GDPR and must put in place a transparent arrangement allocating their respective responsibilities – in particular for the privacy notice and for handling data-subject rights — the essence of which must be made available to the fans concerned. Check each league, sponsorship, co-promotion

and platform arrangement against this test rather than assuming the independent-controller pattern applies.

3.2. What you should do

Where the GDPR applies, a business receiving EU/EEA fan or subscriber data via a platform must, as a minimum:

- **Provide its own privacy notice** meeting the GDPR content requirements (Section 5), covering the business's own processing;
- **Identify a legal basis** for each activity — typically performance of the contract for the ticket or subscription itself; direct marketing can, depending on the circumstances, rest on legitimate interests (Article 6(1)(f), recital 47) or on consent, and a separate consent is required where the applicable ePrivacy or national direct-marketing rules demand it (see Section 5.2). Where you rely on legitimate interests, document the balancing test;
- **Honour data subject rights** (access, rectification, erasure, objection, etc.) for EU/EEA fans and subscribers — with a documented intake and response procedure: requests must be answered without undue delay and in principle within one month, extendable by two further months for complex or numerous requests provided the individual is informed within the first month (Article 12(3));
- **Put processor agreements in place** with any IT or service vendors that handle the data on the business's behalf;
- **Manage data breaches** in line with the notification duties in Section 6.

3.3. The EU representative (Article 27)

There is one further obligation that often surprises Japanese operators. Where the GDPR applies on the targeting basis (Article 3(2)) and no exemption applies, your business must designate, in writing, a representative established in the EU/EEA (Article 27). The representative acts as a local point of contact for data subjects and supervisory authorities, and must be named in your privacy notice. The representative must be established in one of the Member States where the data subjects whose data you process are located — in practice, the Member State where your EU/EEA fans, audiences or subscribers are concentrated. This is not a token requirement: the absence of an Article 27 representative is itself a frequently cited compliance failure in enforcement decisions against non-EU companies. If you have no EU establishment of your own, appointing an external EU representative is usually the most efficient way to meet this obligation — a service we can arrange (see the closing section).

There is a narrow exemption (Article 27(2)): no representative is required where the processing is only occasional, does not include large-scale processing of special categories of data (Article 9) or of data relating to criminal convictions and offences (Article 10), and is unlikely to result in a risk to the rights and freedoms of individuals. For a business that serves EU/EEA fans, audiences or subscribers on a regular, structural basis, this exemption will rarely be available — document the assessment either way.

The representative is not a data protection officer, and the two roles should not be merged. The EU representative (Article 27) is a local point of contact for data subjects and supervisory authorities; the data protection officer (Articles 37–39) is an oversight function that must act independently and be involved in all data-protection matters. Check separately whether you must designate a DPO under Article 37 — in particular where your core activities involve regular and systematic monitoring of individuals on a large scale (for example, large-scale fan analytics, streaming profiling or ad tracking) or large-scale processing of special categories of data.

Finally, two clarifications. Appointing a representative does not transfer your responsibility: the designation is without prejudice to legal actions against the controller itself, which remains fully liable for compliance (Article 27(5)). Nor does the representative create an EU establishment or a "main

establishment" for your business — the GDPR's one-stop-shop mechanism does not apply merely because a representative has been appointed, so any EU/EEA supervisory authority in whose territory affected fans are located can act.

4. Mapping Your Ticketing Channels and Data Flows

What this section covers

- The difference between data you collect directly and data you receive from a platform.
- How brand-licence and franchise arrangements shift responsibility.
- A one-page data-flow template you can complete for your events and properties.

Most sports, media and entertainment businesses use more than one ticketing or distribution channel, and the GDPR treats them differently. Your first task should be to map who collects the data, who receives it, and on what legal basis. Two distinctions matter.

4.1. Key concepts in brief

Direct collection (Article 13) vs. data received from a platform (Article 14). Where your business collects personal data directly from the fan or subscriber — for example, through its own ticketing engine or streaming sign-up — Article 13 GDPR applies, and the privacy information must be given at the time the data is collected. Which rule applies to platform data depends on the platform's legal role, not merely on who operates the input screen. Where the platform collects the data on your behalf as your processor (Article 28), the collection is attributed to you and Article 13 applies at the point of collection. Where an independent platform collects the data as a controller in its own right and then transmits it to you, Article 14 GDPR applies to your processing: the information must be given within a reasonable period after obtaining the data, at the latest within one month; if the data are used for communication with the fan, at the latest at the time of the first communication; and if disclosure to another recipient is envisaged, at the latest when the data are first disclosed (Article 14(3)). Where you and the platform jointly determine purposes and means, Article 26 applies and the joint-controller arrangement must allocate the information duties (see Section 3.1). The content required under Articles 13 and 14 is essentially the same; the trigger, the timing and the additional detail on data categories and sources differ.

Channel type	Who collects	Which rule	Timing of notice
Own ticketing engine	The business directly	Article 13 GDPR	At the point of data entry / before submission
Ticketmaster / SeatGeek / Eventbrite / marketplace	The platform	Article 14 GDPR	Within a reasonable time; at latest at first contact
Phone / e-mail / box office	The business directly	Article 13 GDPR	At the time data is taken

Brand-licence and franchise arrangements. A frequent and important structure in sport, media and entertainment is the brand or franchise licence: a team, event or content property trades under a well-known league, federation or IP owner's brand, but is in fact operated by a separate company under a

licence to use the brand and associated marks. In that case, the operating company — not the brand or rights owner — typically runs the ticketing, membership or distribution system and collects and processes the fan or subscriber data. The GDPR responsibilities for that data flow generally rest with the operating company as controller, not with the brand or rights owner.

For brand and rights owners, this has two consequences. First, the brand owner is usually not the controller for fan data collected by the operator's ticketing or membership system, and does not carry the operator's GDPR obligations. Second, because the brand is prominently associated with the team, event or content, the brand owner has a legitimate interest — as a matter of brand and reputational risk management — in ensuring that the operator runs a GDPR-compliant ticketing or fan-data flow. It is good practice to address data protection responsibilities expressly in the brand-licence or franchise agreement.

4.2. What you should do: complete a data-flow map

For each event, property and ticketing channel, complete one row of the table below. This single exercise resolves most of the practical uncertainty and is the foundation for everything else.

Event / Property	Channel	Who collects	Who receives	Art. 13 / 14	Legal basis	Notice shown?
…	…	…	…	…	…	☐
…	…	…	…	…	…	☐
…	…	…	…	…	…	☐

MODULE 3 Privacy Notices and Legal Bases

5. Getting the Privacy Notice Right

What this section covers

- How a notice should be presented in the ticketing or registration flow (a link is fine).
- How to separate marketing consent from contract and from the notice.
- What the notice must actually contain to meet Article 13.

Two separate questions arise about privacy notices, and they are frequently confused: how the notice is presented, and what the notice says. A notice can be presented perfectly and still be deficient in content; equally, good content presented badly will not comply.

5.1. Presentation: a link is fine; full text on the screen is not required

The GDPR does not require the full text of a privacy notice to appear on the ticketing or registration screen. The standard (Articles 12(1) and 13) is that the information be provided in a concise, transparent, intelligible and easily accessible form, in clear and plain language, at the time the data is obtained. In an online ticketing or registration flow, a clearly visible and clearly labelled link to the privacy notice, presented before the fan or subscriber submits personal data, can satisfy this. This "layered" approach — a short notice linking through to the full notice — is expressly endorsed by the EDPB. A link by itself is not enough only if it is buried or not reasonably visible in the flow.

5.2. Separate consent from contract — and from the privacy notice

Three things should be kept apart in the ticketing or sign-up flow:

1. **Acceptance of the terms of service / ticketing conditions** — a contractual matter.
2. **The privacy notice** — an information obligation under Article 13/14, not something the individual "consents" to. The legal basis for processing ticketing or subscription data is normally performance of the contract, not consent.
3. **Marketing consent** — required where the applicable ePrivacy or national direct-marketing rules call for consent, as they usually do for e-mail, SMS and push marketing to EU fans. Where consent is required or relied on, it must be a separate, freely given, opt-in action: it cannot be bundled with acceptance of the terms, cannot be pre-ticked, and cannot be a condition of buying a ticket or subscribing. Under the GDPR itself, direct marketing can otherwise rest on legitimate interests (Article 6(1)(f), recital 47) — but that does not displace the stricter ePrivacy and national direct-marketing rules.

A single combined checkbox of the form "I agree to the Terms and the Privacy Policy" is a common weak point. Separating marketing consent into its own unticked box is the simplest reliable way to meet the requirement. To be clear: the GDPR does not mandate a specific number of checkboxes — what is mandatory is that marketing consent is separate and freely given. Separating the boxes is the means, not the rule itself. Bear in mind that electronic marketing (e-mail, SMS, push) to EU fans can additionally engage Member-State ePrivacy and unfair-competition rules — in Germany, for example, section 7(2) no. 2 and section 7(3) of the Act against Unfair Competition (UWG) — which apply alongside the GDPR's consent requirements.

5.3. Content: an APPI-style policy is usually not sufficient on its own

A short, high-level company privacy policy framed around the APPI typically does not contain everything Article 13 GDPR requires. Where the GDPR applies, your notice must include, among other things:

- the identity and contact details of the controller and, where applicable, its EU representative (Article 27);
- where a data protection officer has been designated, the DPO's contact details;
- the purposes of, and legal basis for, each processing activity — including, where processing rests on legitimate interests (Article 6(1)(f)), the interests pursued;
- the recipients or categories of recipients of the data;
- any transfers outside the EU/EEA and the basis for them;
- the retention period (or the criteria used to set it);
- whether providing the data is a statutory or contractual requirement or necessary to enter into the contract, and the possible consequences of not providing it;

- the existence of any automated decision-making, including profiling (Article 22), with meaningful information about the logic involved and its significance and consequences;
- the data subject rights under Articles 15–22, including the right to withdraw consent;
- the right to lodge a complaint with a supervisory authority.
- where the data were not obtained from the individual (Article 14): in addition, the categories of personal data concerned and the source of the data, including whether it came from a publicly accessible source.

The practical solution is usually not to discard your existing APPI policy, but to supplement it with a GDPR-specific notice (or add-on) that covers these points for fans, audiences or subscribers to whom the GDPR applies.

MODULE 4 Incident Management and the APPI Interface

6. Data Breaches: The 72-Hour Clock

What this section covers

- Your GDPR breach-notification duty and the 72-hour clock.
- The parallel duty under the APPI.
- A 72-hour response checklist and the accreditation/identity-data points relevant to events.

Sports, media and entertainment businesses hold exactly the kind of data that attracts both attackers and regulators: names, contact details, sometimes ID or accreditation information, payment card data, and event, viewing or purchase histories. Data breaches are one of the most heavily penalised categories of GDPR failure, and the obligations are time-critical.

6.1. Key concepts in brief

What the GDPR requires. Where the GDPR applies and a personal data breach occurs, the controller must notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it (Article 33), unless the breach is unlikely to result in a risk to individuals. Where the breach is likely to result in a high risk to individuals, the affected individuals must also be informed without undue delay (Article 34). The 72-hour clock runs from awareness, not from full investigation — so an incident-response plan must be in place before an incident occurs. Notification may be made in phases where full information is not yet available (Article 33(4)). Two further duties are easy to miss: a processor must notify the controller without undue delay after becoming aware of a breach (Article 33(2)) — pass this through in vendor and platform contracts with a tight timeframe — and every breach must be documented internally, whether or not it is notified (Article 33(5)).

The APPI also imposes breach-notification duties. Japan's APPI was amended to require notification to the Personal Information Protection Commission (PPC) and to affected individuals for breaches likely to harm individual rights and interests. In practice the PPC reporting duty is not a general risk-based standard: it is triggered only where the breach falls within one of four categories under Article 7 of the Enforcement Rules for APPI — (i) leakage of 要配慮個人情報 (special-care-required personal

information); (ii) leakage creating a risk of financial loss; (iii) leakage suspected to result from a wrongful purpose; or (iv) leakage affecting more than 1,000 data subjects. A breach outside these categories does not trigger the PPC reporting duty even where some risk to individuals remains. A breach affecting EU/EEA fans or subscribers can therefore trigger parallel obligations under both regimes, with different thresholds and timelines. Under the PPC's rules, reporting is two-staged: a preliminary report promptly after becoming aware (per PPC guidance, generally within around three to five days as a matter of practice — the Enforcement Rules for APPI require only that this be done "speedily" (速やかに), without fixing a specific number of days as a statutory deadline) and a final report within 30 days — 60 days where the breach is likely attributable to a wrongful purpose, such as a cyberattack. Affected individuals must be notified promptly where required, and an entrusted service provider can discharge its own APPI reporting duties by informing the entrusting business. Design a single incident-response procedure to satisfy both regimes.

The platform dimension. Where businesses access fan or subscriber data through a ticketing or distribution-platform partner portal, that access point can itself be the source of a breach — for example, through phishing of staff credentials. Credential phishing against third-party platform or CRM portals is a recognised and common attack vector for consumer-facing businesses generally, and late notification of a breach (well beyond 72 hours) is a frequently cited aggravating factor in enforcement outcomes. The lesson is twofold: secure the credentials your staff use to access platform portals, and report promptly once aware.

6.2. What you should do: the 72-hour response checklist

When	Action
Within the first 24 hours	Contain the incident; convene the incident lead; record the time you became aware (the clock starts here); begin a written log; preserve evidence.
Within 72 hours	Assess risk to individuals; if notifiable, notify the competent EU supervisory authority (and PPC where the APPI applies); inform your EU representative; prepare fan/subscriber communications if high risk.
After 72 hours	Notify affected individuals where required; complete the investigation; document remediation; review and update controls and staff training.

Have these ready before an incident

- A named incident lead and a 24/7 contact route.
- A written breach-response procedure with the 72-hour clock built in.
- A pre-identified EU supervisory authority and (if applicable) EU representative to notify.
- Staff training on phishing and on platform-portal credential security.

6.3. Identity and accreditation data — sensitivities for sports, media and entertainment

Unlike hotels, which face a specific statutory guest-registry obligation under Japan's Hotel Business Act, sports, media and entertainment businesses are not generally subject to a single, blanket law requiring identity-document collection. That does not mean the sector is free of comparable sensitivities — high-

sensitivity identity data commonly arises in several recurring scenarios, each of which should be checked on its own terms rather than assumed to follow one general rule.

The most common are: international athlete, official and team accreditation at events, which typically involves passport or ID data for immigration and accreditation purposes, and can overlap with anti-doping data governed by the World Anti-Doping Code and, in Japan, the Japan Anti-Doping Agency (JADA) — anti-doping, medical and therapeutic-use data are data concerning health and therefore special categories of personal data under Article 9 GDPR, requiring an Article 9 exception in addition to an Article 6 legal basis; media and broadcast crew credentialing for venue and compound access; and event-specific or venue-specific security arrangements, which for major international events can include bespoke accreditation and screening requirements set by the organising committee, the venue or the relevant authorities. Where any of these apply, the same principles hold as for any sensitive identity data: collect only what the specific accreditation, anti-doping or security requirement actually calls for, retain it only as long as necessary, store it securely with restricted access, and avoid keeping unnecessary full-image copies of identity documents. Confirm the specific legal or contractual basis for any such collection on a case-by-case, event-specific basis — do not assume a blanket rule applies.

A parallel — and, for JADA/anti-doping records, arguably broader — obligation arises under Japanese law, regardless of any EU/EEA nexus. Health-related information, including anti-doping test results and therapeutic-use exemption (TUE) records, falls within "要配慮個人情報" (special-care-required personal information) under Article 2(3) of the APPI. Acquiring such data generally requires the individual's prior consent (Article 20(2) APPI), and it cannot be provided to a third party under the opt-out mechanism otherwise available for ordinary personal data (Article 27(2) proviso, APPI). This applies to purely domestic processing of Japanese athletes' data and should be addressed in the accreditation and anti-doping data-handling procedure independently of the GDPR analysis above.

Biometric access control deserves separate mention. Facial-recognition entry, biometric accreditation and similar venue-access technologies process biometric data for the purpose of uniquely identifying a person — a special category of personal data under Article 9 GDPR, prohibited unless a specific exception applies (in practice usually the explicit consent of the individual, with a genuine non-biometric alternative offered). Where such systems are considered for events with EU/EEA attendees, treat them as a high-risk deployment that will normally require a data protection impact assessment under Article 35 GDPR before go-live. Two points deserve emphasis. First, an Article 9 exception is needed in addition to — not instead of — an Article 6 legal basis: identify both. Second, explicit consent is valid only if freely given, which presupposes a genuine non-biometric alternative (for example, a conventional ticket or accreditation check) available without disadvantage — entry conditioned on biometric enrolment is not supported by valid consent.

7. Enforcement and Risk — Why "No Cases in Japan" Is Misleading

What this section covers

- Why the count of GDPR cases in Japan is structurally zero.
- Why the published enforcement record understates the real picture.
- Why fines against non-EU companies are real — and what that means for you.

You may reasonably ask whether the GDPR is really enforced against Japanese businesses. The honest answer is nuanced, and the comfortable reading of it is the wrong one.

7.1. "No GDPR cases in Japan" — because the PPC does not enforce the GDPR

The GDPR is enforced by EU/EEA supervisory authorities (and, for the parallel UK GDPR, the UK ICO). Japan's PPC enforces the APPI, a separate regime; it does not enforce the GDPR. So the count of "GDPR

enforcement cases in Japan" is, structurally, zero — not because the risk is absent, but because the GDPR is simply not enforced by Japanese authorities. The absence of a Japanese case tells you nothing about exposure: where enforcement against a Japanese business occurs, it comes from an EU/EEA supervisory authority applying the GDPR's extraterritorial scope — not from the PPC.

7.2. The published record is incomplete

Even within Europe, not every GDPR fine is published: publication practice varies between supervisory authorities, several publish only selected decisions, and fined entities rarely publicise them. Public fine trackers therefore record a minimum, not the complete picture, and the published record should be read accordingly.

7.3. Fines against non-EU companies are real and are enforced

The largest GDPR fines on record have been imposed on companies headquartered outside the EU — up to EUR 1.2 billion in a single case, and repeatedly in the hundreds of millions of euro. Some have been paid; some of the largest remain under appeal — but an appeal does not make the exposure theoretical. The mechanism is straightforward: these companies maintain EU-established entities or operations through which authorities can act. A Japanese group with active EU operations (for example, touring, licensing, distribution or broadcast subsidiaries) is, in principle, in a comparable position. Enforcement against a purely Japanese operator with no EU footprint is harder in practice; but the existence of any EU presence materially changes that analysis.

7.4. Fines are not the only tool

Beyond fines, EU authorities can issue orders to stop processing, mandatory audits, and corrective orders, any of which can be highly disruptive for a business that sells into, or operates in, the EU. The risk picture is therefore broader than the headline-fine figures.

> **The bottom line on risk**
>
> "No published GDPR case in Japan" is a statement about the public record, not a measure of exposure. For a Japanese sports, media or entertainment business that serves EU/EEA fans, audiences or subscribers — and especially one whose group has any EU presence — the compliance gaps in this guide should be treated as real and worth closing, not as theoretical.

8. How the GDPR and the APPI Fit Together

You do not face the GDPR in isolation; you already operate under the APPI, and the two regimes are connected through the EU–Japan mutual adequacy arrangement.

Under the adequacy decision first adopted in January 2019 and confirmed in the first periodic review completed in April 2023, the EU recognises Japan's data protection regime — the APPI as complemented by the PPC's Supplementary Rules — as providing an adequate level of protection. The practical effect is that personal data can flow from the EU to businesses in Japan without additional transfer tools such as standard contractual clauses, provided the Supplementary Rules are complied with for EU-origin data.

Two points matter for sports, media and entertainment businesses. First, reliance on adequacy is conditional: the Supplementary Rules impose specific requirements for EU-origin personal data — for example, on retention, on onward transfers to third countries, and on the treatment of certain categories of data — and these must actually be observed. Second, adequacy addresses the cross-border transfer mechanism only; it does not remove the substantive GDPR obligations (notice, legal basis, data subject rights, breach notification) that apply where the GDPR applies in the first place. Recent APPI

amendments have narrowed the gap between the two regimes — including a breach-notification duty closer to the GDPR model — but gaps remain, and the two sets of obligations should be mapped together rather than assumed to be identical.

Topic	GDPR (where applicable)	APPI
Enforcing authority	EU/EEA DPAs; UK ICO	PPC
Breach notification	72 hours to DPA (Art. 33)	To PPC + individuals, risk-based
Cross-border transfers	Adequacy covers EU→Japan	Supplementary Rules for EU-origin data
Privacy notice content	Article 13/14 (detailed)	Purpose-of-use focus; less prescriptive
Max administrative fines	Up to EUR 20 million or 4% of global turnover, whichever is higher	PPC corrective guidance and orders, backed by criminal penalties (including corporate fines) for order violations and unlawful disclosure; no GDPR-style turnover-based administrative fines

8.1. The reverse direction: when the APPI reaches EU businesses

This guide is written primarily for Japan-side businesses that fall within the GDPR, but the relationship also runs the other way. A German or other EU sports, media or entertainment business may be subject to the APPI even if it has no establishment in Japan. Under the APPI's extraterritorial-application provision (Article 171; Article 75 before the April 2022 renumbering), the Act applies where a foreign business handles personal information identifying a person in Japan in connection with supplying goods or services to that person.

Accordingly, an EU business that sells match tickets, merchandise, streaming subscriptions or fan-club memberships to persons in Japan and processes their personal information in connection with those transactions may fall within the APPI. This is broadly the reverse of the GDPR analysis addressed in Section 2, although Article 171 APPI is framed differently from the GDPR's targeting test.

There is no minimum-volume exemption. The former exemption for businesses handling personal information relating to no more than 5,000 individuals was abolished by the 2015 amendments with effect from 30 May 2017.

8.2. EU clubs, promoters and broadcasters running events or tours in Japan

The APPI's relevance is not limited to online sales. An EU club, league, promoter or broadcaster that stages a match, tour, festival or other event in Japan will normally process personal information relating to ticket-holders, accredited media, local staff and volunteers, hospitality guests, performers and contractors. Such processing will generally fall within the APPI where the operator uses a personal-information database or equivalent system for its business activities.

Points to address before the event include: specifying and communicating the purposes of use under Articles 17 and 21 APPI, normally in Japanese where information is directed to Japanese attendees or personnel; the consent and third-party-provision rules under Article 27 APPI where personal data is disclosed to local partners, venues or sponsors; the entrustment and vendor-supervision regime under Articles 25 and 27(5)(i) APPI where Japanese service providers process data on the operator's behalf; and

notification to the PPC and affected individuals under Article 26 APPI where a reportable data breach occurs.

Whether a venue, sponsor or service provider is an independent third party, a joint user or an entrusted service provider must be determined from its actual role rather than its contractual label.

The GDPR may apply in parallel where the processing is carried out in the context of the activities of an EU establishment or otherwise falls within Article 3 GDPR. The relevant processing operations should therefore be mapped under both regimes rather than assuming that the residence or nationality of the individuals concerned determines which law applies.

8.3. EU–Japan data flows: touring, licensing and co-production

Touring, content licensing and co-production routinely involve personal data moving in both directions, including cast and crew lists, contributor and talent information, audience and subscriber analytics, accreditation data and rights-holder contacts.

For the EU→Japan leg, the European Commission's adequacy decision permits personal data to be transferred under Article 45 GDPR to Japanese private-sector recipients falling within the scope of the decision without standard contractual clauses or another Article 46 transfer mechanism. A Japanese recipient of data transferred under the adequacy decision must comply with the PPC Supplementary Rules applicable to that data.

The arrangement is reciprocal. Japan's PPC has designated the EU/EEA member states — and, separately, the UK — as the "designated countries" under Article 28(1) APPI and Article 15 of the Enforcement Rules for APPI, i.e. jurisdictions whose personal-information protection system is recognised as maintaining standards equivalent to Japan's. Consequently, a transfer by a Japanese business to a recipient in the EU does not, solely because the recipient is located outside Japan, require the special consent or equivalent-measures mechanism under Article 28 APPI. The ordinary APPI rules governing provision of personal data to third parties, including Article 27 and the exceptions for entrustment and joint use, remain applicable.

Article 28 APPI may nevertheless become relevant to onward transfers from Japan to recipients in countries that have not been recognised by the PPC or where the recipient has not implemented the required equivalent measures. Co-production, distribution and licensing agreements should therefore allocate the parties' respective roles, purposes of use, permitted disclosures, onward-transfer conditions, security obligations and breach-cooperation duties at the drafting stage.

These arrangements may also raise EU commercial and competition-law issues, including media and broadcasting rights, sponsorship restrictions and exclusive-distribution arrangements, on which our EU competition team advises alongside the data-protection analysis.

MODULE 5 Implementation Roadmap and Checklists

9. Implementation Roadmap

This roadmap turns the guide into a project plan. Treat each step as a work package with an owner and a target date. The steps are sequential, but several can run in parallel once Step 1 is complete.

STEP 1 **Decide whether the GDPR applies**

Complete the applicability checklist (Section 2.2) for each event, property and channel. Record your conclusion. Owner: event lead / in-house counsel.

STEP 2 **Map your channels and data flows**

Fill in the data-flow template (Section 4.2). This tells you, for every channel, who is controller and whether Article 13 or 14 GDPR applies. Owner: ticketing/commercial + IT.

STEP 3 **Fix the ticketing flow and privacy notice**

Apply Section 5: present the notice properly, separate marketing consent into its own opt-in box, and supplement your APPI policy with a GDPR add-on. Owner: ticketing/commercial + counsel.

STEP 4 **Clarify platform and operator roles**

Review platform partner terms and, for brand-licensed or franchised properties, the license or franchise agreement, to confirm controller allocation (Sections 3–4). Owner: counsel.

STEP 5 **Appoint an EU representative if required**

Assess Article 27 GDPR and put a representative arrangement in place where needed (Section 3.3). Owner: counsel.

STEP 6 **Stand up incident response**

Adopt the 72-hour procedure and checklist (Section 6.2); train staff on phishing and portal-credential security. Owner: IT + event lead.

STEP 7 **Embed governance**

Records of processing, retention/deletion schedules (including accreditation and identity data), vendor processor agreements, and periodic review. Owner: counsel + IT.

10. Compliance Checklists

The following checklists translate the roadmap into tickable actions, grouped by priority. They are a starting point for a structured review, not a substitute for advice on a specific situation.

Immediate (0–3 months)

- ☐ Map every event, property and ticketing or distribution channel: who collects, who receives, Article 13 or 14 GDPR , legal basis, which notice.
- ☐ Confirm whether the GDPR applies to each channel (territorial-scope assessment).
- ☐ Ensure a GDPR-compliant privacy notice (or APPI add-on) is available and shown at the right point in each direct ticketing or registration flow.
- ☐ Set up a data-subject-rights procedure: intake route, identity verification, and tracking of the one-month response deadline (Article 12(3)).

- ☐ Separate marketing consent into its own unticked, freely given opt-in box.
- ☐ Put a written breach-response procedure in place with the 72-hour clock built in.

Short-term (3–9 months)

- ☐ Review platform partner terms (ticketing marketplaces, streaming and distribution platforms) to confirm the controller allocation and data-use limits.
- ☐ For brand-licensed or franchised properties, confirm in the licence or franchise agreement who is responsible for GDPR compliance of the ticketing or fan-data flow.
- ☐ Identify a legal basis for each processing activity and document it.
- ☐ Designate an EU representative under Article 27 GDPR where required, and name it in the notice.
- ☐ Put Article 28 GDPR processor agreements in place with ticketing, CRM, streaming and other vendors.
- ☐ Carry out vendor due diligence before onboarding ticketing, CRM, streaming and analytics vendors, and ensure sub-processors are disclosed, approved and bound by equivalent terms (Article 28(2) and (4) GDPR).
- ☐ Check whether a data protection officer must be designated (Article 37) and whether any planned processing — biometric entry, large-scale fan profiling, extensive tracking — requires a data protection impact assessment (Article 35).
- ☐ Where you rely on legitimate interests (Article 6(1)(f)) — for example for direct marketing or analytics — document the balancing test (legitimate-interests assessment).
- ☐ Implement cookie and tracking governance for EU/EEA-facing sites and apps: a consent-management platform, records of consent, and a regular audit of cookies, pixels, SDKs and ad-tech vendors.
- ☐ Review onward transfers and ensure Supplementary-Rules compliance for EU-origin data.

Ongoing governance

- ☐ Maintain records of processing activities under Article 30 GDPR. The APPI has no general equivalent of this register; it requires specific records instead — notably of third-party provision and receipt of personal data — so keep both sets of documentation.
- ☐ Set and apply data retention and deletion periods for fan and subscriber data (storage limitation).
- ☐ Build data protection by design and by default (Article 25 GDPR) and appropriate technical and organisational security measures (Article 32 — encryption, access controls, regular testing) into new fan-facing systems, apps and event deployments.
- ☐ Train ticketing, fan-engagement, commercial and IT staff on fan-data handling, accreditation/ID data, phishing, and breach response.
- ☐ Review the programme periodically and after any material change to channels, systems or vendors.

11. Glossary

Term	Meaning
GDPR	EU General Data Protection Regulation (Regulation (EU) 2016/679).
APPI	Japan's Act on the Protection of Personal Information.
PPC	Japan's Personal Information Protection Commission — the authority enforcing the APPI.
Supervisory authority / DPA	An EU/EEA data protection authority that enforces the GDPR (e.g. the German state DPAs, CNIL); the UK ICO, which post-Brexit enforces the separate UK GDPR.
Controller	The entity that determines the purposes and means of processing personal data.
Processor	An entity that processes personal data on behalf of, and on the instructions of, a controller.
Data subject	The identified or identifiable individual to whom personal data relates (here, the fan, subscriber or ticket-holder).
EU representative (Art. 27)	A representative established in the EU/EEA that a non-EU controller must appoint where the GDPR applies on the targeting basis.
Adequacy decision	An EU decision recognising a non-EU country's regime as offering adequate protection, enabling data transfers without extra safeguards.
Supplementary Rules	PPC rules that supplement the APPI for personal data transferred from the EU under the adequacy decision.
Ticketing platform / marketplace	A third-party platform that lists, sells or distributes tickets, content or subscriptions on your behalf (e.g. Ticketmaster, SeatGeek, Eventbrite, or streaming/distribution platforms).
Ticketing System / CRM	Ticketing System / Customer Relationship Management system — the software used to sell tickets or subscriptions and manage fan or subscriber data.

How Atsumi & Sakai can support sports, media and entertainment businesses

For sports, media and entertainment businesses, data protection is not a stand-alone compliance topic. GDPR and APPI issues arise directly from how a team, event, platform or content property is owned, operated, branded, marketed and connected to ticketing, broadcast, sponsorship and fan-management systems. The legal analysis therefore depends not only on the privacy notice, but also on the underlying business structure: who owns the rights, who operates the event or platform, who controls the ticketing or distribution flow, which platforms and CRM systems are used, who receives fan or talent data, and how marketing and post-event communications are handled.

Atsumi & Sakai is well placed to advise on these issues because we combine EU/German data-protection expertise in Frankfurt with a Japan-based Sports, Media & Entertainment Law practice in Tokyo. This allows us to address GDPR and APPI compliance in the commercial context in which rights holders, federations, clubs, promoters, broadcasters, agencies and platforms actually operate.

In particular, we assist clients with:

- assessing whether and where the GDPR applies to Japanese sports, media and entertainment businesses, including direct and platform ticketing channels, streaming and broadcast, and group structures with an EU presence;
- preparing GDPR-compliant privacy notices, consent wording and ticketing/registration-flow disclosures, and aligning them with existing APPI policies;
- reviewing the data-protection implications of ticketing marketplaces, streaming and broadcast platforms, CRM and fan-engagement systems, payment-service providers, marketing tools and outsourced IT vendors;
- allocating data-protection responsibilities in sponsorship, licensing, broadcast, franchise, brand-licence, event-management and platform arrangements;
- aligning GDPR requirements with APPI and Japan-specific considerations, including accreditation, anti-doping and identity-document data where relevant;
- preparing breach-response procedures, internal escalation protocols and notification workflows for incidents involving fan, subscriber, athlete or talent data;
- assessing whether an EU representative is required under Article 27 GDPR and supporting the implementation of suitable representative arrangements;
- supporting transactions and major-event projects by identifying GDPR/APPI issues in due diligence, transaction structuring and post-closing integration.

Our Sports, Media & Entertainment capability

Atsumi & Sakai has a dedicated Sports, Media & Entertainment Law practice. This practice advises on broadcasting, advertising and marketing, brand and rights protection, sponsorship, major events, sports governance and integrity, and M&A, joint ventures and private equity for clients across the sport, media and entertainment sectors.

The team is led by Ian S. Scott, Senior Partner, an Australian lawyer admitted in Queensland and registered as a foreign lawyer in Japan, with over 25 years' experience in the business of sport, media and entertainment. He is a CAS arbitrator and holds Best Lawyers Japan recognition in Sports Law and Media & Entertainment, and was inducted into The Legal 500 Hall of Fame for Sports Law in Japan.

This combination enables us to advise rights holders, operators, brand owners and investors on data protection as part of the broader legal and commercial structure of their sport, media or entertainment business — not as an isolated compliance exercise. For clients, this is particularly important where fan, subscriber, athlete or talent data issues are embedded in sponsorship, broadcast, franchise, platform or transaction documentation.

Authors

Ian S. Scott
Registered Foreign Lawyer (The Laws of Australia, State of Queensland)
Senior Partner
Daini Tokyo Bar Association
E: ian.scott@aplaw.jp

Frank Becker*
Managing Partner, Atsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater**
E: frank.becker@aplaw.de

Andrés Martin-Ehlers*
Partner, Atsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater**
E: andres.martin-ehlers@aplaw.de

Kenta Nobe
Partner
Dai-Ichi Tokyo Bar Association
E: kenta.nobe@aplaw.jp

Contact

E-mail: cpg_sports_entertainment@aplaw.jp

If you would like to sign up for A&S Newsletters, please fill out the sign-up form.
Back issues of our newsletters are available here.

*Not registered as a Foreign Lawyer in Japan
**A corporation registered in Germany providing legal and tax advisory services

---

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm with a dynamic and innovative approach to legal practice; it has been responsible for a number of ground-breaking financial deal structures and was the first Japanese law firm to create a foreign law joint venture and to admit foreign lawyers as full partners. Expanding from its highly regarded finance practice, the Firm now acts for a wide range of international and domestic companies, banks, financial institutions and other businesses, offering a comprehensive range of legal expertise.

Atsumi & Sakai has an outward-looking approach to its international practice, and has several foreign lawyers with extensive experience from leading international law firms, providing its clients with the benefit of both Japanese law expertise and real international experience.

We are the only independent Japanese law firm with affiliated offices located in New York, London, Frankfurt, Brussels and Ho Chi Minh City which, together with our Tokyo office, Osaka affiliated office and Fukuoka affiliated office, enables us to provide real-time advice on Japanese law to our clients globally.

Atsumi & Sakai

www.aplawjapan.com/en/

Tokyo Head Office
Fukoku Seimei Bldg. (Reception: 16F)
2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011 Japan

Osaka Affiliate Office
Nakanoshima Festival Tower 16F,
2-3-18 Nakanoshima, Kita-ku, Osaka City, Osaka 530-0005 Japan

Fukuoka Affiliate Office
Tenjin Bldg. 10F
2-12-1 Tenjin, Chuo-ku, Fukuoka-shi, Fukuoka 810-0001 Japan

New York Affiliate Office
1120 Avenue of the Americas, 4th Floor, New York, New York 10036

London Office
85 Gresham Street, London EC2V 7NQ, United Kingdom

Frankfurt Affiliate Office
Barckhausstraße 1 (8th Floor), 60325 Frankfurt am Main, Germany

Brussels Office
CBR Building
Chaussée de la Hulpe 185, 1170, Brussels, Belgium

Ho Chi Minh Office
10F, The NEXUS building
3A-3B Ton Duc Thang Street, Sai Gon Ward, Ho Chi Minh City, Vietnam