

2026 年 9 月 24 日

No. SME_003

データ保護ガイド

GDPR 及びその他のデータ保護に関する問題

日本のスポーツ、メディア及びエンターテインメント事業者のための実用ガイド

執筆者：外国法事務弁護士（オーストラリア クインズランド州法） イアン・S・スコット

／ドイツ連邦共和国弁護士* フランク・ベッカー

／ドイツ連邦共和国弁護士* アンドレス・マルティン-エーレルス博士

／弁護士 野邊健太

*但し、日本における外国法事務弁護士の登録はない。

本ガイドの使い方

対象者 EU/EEA 域内に所在するファン、視聴者又は加入者にサービスを提供している、あるいは今後提供する可能性のある日本のスポーツ、メディア及びエンターテインメント事業者—権利保有者、イベント主催者及びプロモーター、チケット販売及びチケット販売窓口担当チーム、放送及びストリーミング担当チーム、IT 及びシステム担当スタッフ、並びに社内法務やコンプライアンス担当者。

本ガイドの読み方 第 1 項のクイックスタートと、役割別ガイドからお読みください。GDPR が貴社に適用されるかどうかを判断するには第 2 項乃至第 3 項を、GDPR が日常業務にどのような影響を与えるかについては第 4 項乃至第 6 項を、そして段階的な導入ロードマップについては第 9 項をお読みください。チェックリストとテンプレートは、そのままコピーしてご利用いただけるように作成されています。

貴社の業務における活用方法 研修用資料として、コンプライアンス見直しの際の実務チェックリストとして、そして簡易的な社内プロジェクト計画の土台として活用してください。本ガイドは一般的な情報を提供するものであり、個別の状況に関する法的助言ではありません。

1. エグゼクティブサマリー及びクイックスタート

日本の多くのスポーツ、メディア及びエンターテインメント事業者は、欧州連合内に拠点を持たず、日本国内のみで事業を展開していることを理由に、EU一般データ保護規則（GDPR）は自社に関係がないと考えています。この認識は、多くの場合誤りです。

EU域内に事務所や従業員、銀行口座を持たない場合であっても、EU／EEA域内に所在するファン、加入者又は視聴者に対してチケット、コンテンツ、グッズ、会員登録などを提供している場合には、貴社の事業にGDPRが適用される可能性があります。スポーツ、メディア及びエンターテインメント分野では、権利保有者やプロモーターが想定しているよりも容易にこうした状況が発生します。例えば、英語対応のチケット販売サイト又はストリーミングサイト、国際的なチケット販売マーケットプレイスへの掲載、国際的な放送及びライセンス契約、又は海外のファン及び視聴者を対象としたマーケティング活動などが挙げられます。

GDPRが適用される場合、第三者チケット販売プラットフォーム又はストリーミング・パートナーを利用することそれ自体で、貴社が自身の義務を免れることはありません。プラットフォームは、自らのデータ収集を行います。貴社は、イベント、放送又は業務委託に関連して取得し、取り扱う個人データについて管理者として引き続き責任を負います（コンプライアンスに適合したプライバシー通知を提供すること、法的根拠を特定すること、データ主体の権利を尊重すること、及び特定のデータ侵害について厳格な期限内に通知することを含みます。）。

重要な5つのポイント

1. 「EU に拠点がない」からといって、「GDPR が適用されない」わけではありません。GDPR の適用は、貴社がどこに拠点を置いているだけでなく、誰にサービスを提供しているかによっても決まります。

2. チケット販売プラットフォームが法令を遵守していても、貴社がコンプライアンスを実行していることにはなりません。貴社は、自らが取得し、利用するデータについて引き続き管理者に該当します。
3. 貴社のプライバシー通知は、GDPR の記載基準を満たさなければなりません。通常、日本の個人情報保護法（APPI）の要件のみを満たすために作成されたポリシーは、それだけでは不十分です。
4. EU 域内のファン又は加入者が関係するデータ侵害が発生した場合、EU 当局に対する 72 時間以内の通知義務が生じる可能性があります。
5. 日本国内で GDPR に基づく制裁金の事例が公表されていないからといって、そのリスクが理論上のものに過ぎないことの証拠にはなりません。

1.1 クイックスタート：今月中に取るべき5つのステップ

10分しかない方は、まずはここから。各ステップは、その内容が詳しく説明されている該当の項を示しています。

1. **貴社がEU／EEA域内のファン、視聴者又は加入者を対象としているかをどうかの確認**
第2.2項の「はい／いいえ」チェックリストを使い、初期評価を行います。
2. **貴社のチケット販売チャネルとデータフローの整理**
第4項記載の1ページのデータフロー・テンプレートに記入します。
3. **貴社のプライバシー通知の見直し、調整**
第5項に照らして、表示方法、同意の分離及び内容を確認します。
4. **プラットフォームの利用状況及び管理者としての役割の明確化**
各チャネルについて管理者を確認します。－第3項
5. **72時間以内のインシデント対応手順の整備**
第6項の侵害チェックリストを文書化した計画に落とし込みます。

1.2 役割別ガイド

本ガイドは、法務部に留まらず、組織全体で回覧することを想定しています。以下は、役割別に推奨される読み方のガイドです。

役割	焦点
権利保有者／イベント主催者	第1項（クイックスタート）、第2項（適用の有無）及び第9項（ロードマップ）
チケット販売／チケット販売窓口	第4項（チケット販売チャネル）及び第5項（プライバシー通知）
IT部門及びシステムベンダー	第4項（データフロー）及び第6項（インシデント対応）
社内弁護士／コンプライアンス部門	本ガイドの全編に加えて、EU代理人との調整及びポリシーの作成

モジュール1

適用範囲及びリスク－GDPRは貴社に適用されるか？

2. GDPRは日本のスポーツ、メディア又はエンターテインメント事業者に適用されるか？

本項の内容

- EU域外の事業者にGDPRを適用する3つの基準 — 拠点、ターゲティング、行動モニタリング
- 貴社について初期評価を行うためのシンプルな「はい／いいえ」チェックリスト
- 3つの典型的なウェブサイト構成のうち最もリスクが高いものはどれか？

GDPRは、3つの独立した基準に基づき適用されます。EU域内の拠点（第3条第1項）、EU／EAA域内の個人を対象としたターゲティング（GDPR第3条第2項(a)）、及び行動モニタリング（第3条第2項(b)）です。いずれか一つに該当するだけで適用されます。

2.1 主要な概念の概要

拠点基準（第3条第1項） GDPRは、その取扱いが物理的にどこで行われるか否かを問わず、企業のEU域内の拠点の活動の過程における取扱いに適用されます。チケット販売、ライセンシング若しくは制作に関与する欧州オフィス若しくは欧州子会社、又はファン若しくはタレントのデータを取り扱うEU域内在住のスタッフを有する日本のスポーツ、メディア又はエンターテインメントグループは、この基準に基づき適用を受ける可能性があります。EU域内に拠点を持たない、純粋に日本国内向けの事業運営は、通常適用を受けません。

ターゲティング基準（第3条第2項(a)） 日本のスポーツ、メディア及びエンターテインメント事業者が最も該当するのがこの基準です。GDPRは、支払を要するか否かにかかわらず、商品又はサービスの提供に関連して、EU/EEA域内に所在する個人の個人データを取り扱う場合、EU域外の企業に適用されます。

重要なのは、貴者の事業がEU/EEA域内のファン、視聴者又は加入者にサービスを提供することを想定しているかどうかです。技術的に欧州からアクセス可能なウェブサイトだけを単に持っているだけでは、適用はありません。ただし、欧州データ保護会議（EDPB）では、それらを総合的に考慮した場合、事業者がEU/EEA域内の個人を対象としてターゲティングを行っているかを示し得る、さまざまな要因を示しています。スポーツ、メディア及びエンターテインメントに関連して、最も関連するものは以下のとおりです。

- 欧州言語（国際的なファン向けに英語、又は個別にドイツ語、フランス語、イタリア語等）でウェブサイト、チケット販売フロー又はストリーミングサービスを提供していること。
- ユーロ又はその他のEU/EEA通貨での支払を認めていること。
- 登録又はチケット販売フォームに、住所又は居住国としてEU/EEA国を記入することをファン又は加入者に認めていること。
- 国際的な若しくは欧州のファン及び視聴者に言及していること、又はEUを対象とした広告若しくは検索エンジンマーケティングを用いていること。
- EU/EEAから広くアクセス可能であり、実務上国際的なファンによって利用されている国際的なチケット販売マーケットプレイス又はプラットフォーム上でイベント、コンテンツ又はグッズを掲載していること。

どの要因も単独では決定的ではなく、評価は総合的に行われます。ただし、英語のチケット販売又はストリーミングフローを提供し、ファンが居住国として欧州の国を選択できるようにし、欧州のカード保有者にアクセス可能な方法で請求し、EU域内在住のファンからの予約又は登録を受け付けている事業者は、多くの場合、EU/EEA域内の個人に対しサービスを提供していると判断され、よって、GDPRの地理的適用範囲内にあるとみなされます。

モニタリング基準（第3条第2項(b)） EU域外の事業者がEU/EEA域内に所在する個人の行動をモニタリングしている場合も、当該行為がEU/EEA域内で行われる限り、GDPRが適用されます。スポーツ、メディア及びエンターテインメント分野において、モニタリングは、とりわけデジタルツール（ウェブサイト及びチケット販売フロー上のクッキー及びトラッキングピクセル、ファン向けアプリ又はストリーミングアプリ内のSDK及びデバイス識別子、ファン分析及び視聴者測定ツール、視聴又は購買行動のプロファイリング、並びにEU/EEA域内の利用者を対象とする、パーソナライズされた広告又はコンテンツのおすすめ）によって生じます。EDPBは、EU/EEA域内の個人に対するかかるトラッキング及びプロファイリング技術の使用をモニタリングの強力な指標と位置付けています。そのため、おすすめのためにEU域内の視聴者の視聴履歴をプロファイリングするストリーミングサービス、又はEU域内の訪問者に広告技術によるトラッキングを行っているクラブの公式ウェブサイトは、チケットやサブスクリプションが今までに販売されたことがない場合であってもGDPRの適用対象となる可能性があります。EU/EEA域内の利用者にクッキー又は類似の技術が使用される場合、加盟国のeプライバシー規則の同意に関する規定が並行して適用されるため、通常はEU/EEA域内の訪問者を対象とする同意管理プラットフォーム（CMP）が必要となります（第5項及び第10項も参照のこと。）。

2.2 実施すべきこと：適用性チェックリスト

貴社について、以下の質問にお答えください。該当するものすべてにチェックを入れてください。

- ☐ 購入時にEU/EEA域内に所在するファンに対し、チケット、サブスクリプション又はグッズを販売していますか？
- ☐ チケット販売又はストリーミングの経路（ウェブサイト又は購入フロー）は、英語又は別の欧州言語で利用できますか？
- ☐ 貴社のイベント又はコンテンツは、EU/EEA域内の視聴者に広く利用されているチケット販売マーケットプレイス又はプラットフォーム（Ticketmaster、SeatGeek、Eventbrite又は

国際的なストリーミング若しくはライセンシング・プラットフォーム等）に掲載されていますか？

- ☐ ファン又は加入者は、登録又はチケット販売フォームに、住所又は居住国としてEU/EEAの住所を記入することができますか？
- ☐ ユーロ建て又は欧州のカード保有者が容易に利用可能な方法で支払を受け付けていますか？
- ☐ 国際的な又は欧州のファン及び視聴者に向けて、マーケティング又は広告を行っていますか？

回答の見方

このチェックリストは、スクリーニング補助であり、法定基準ではありません。GDPR は、「『はい』が2つ」で判定するようなルールは存在せず、法的な判断基準は、あくまで第2.1項で説明したすべての事情を総合的に評価することにあります。とは言え、上記の2つ以上に「はい」と回答した場合、貴社のEU/EEA域内のファン、視聴者又は加入者の活動に関してGDPRが適用されると**想定して**、第3項乃至第6項に進み、第9項から貴社の行動計画を立てることをお勧めします。

上記のいずれにも「はい」と回答しなかった、又は1つだけに「はい」と回答した場合、GDPRが適用される可能性は低いといえます。しかし、一つの強力な要因だけで総合的な評価上十分となる場合もあるため、言語、チャネル、支払オプション又はマーケティングを変更した際は、その都度再評価することをお勧めします。第2.3項では、ウェブサイトの構成がこれにどのような影響を与えるかを示しています。なお、このチェックリストは、EU/EEA域内のターゲティングのみを検証するものであることにご留意ください。貴社が英国内のファンに対してもサービスを提供し又は英国のファンを対象としている場合、英国GDPRについても個別に同じ質問に回答してください。英国GDPRは、独自の代理人及び通知要件を有する個別の制度として並行して適用されます。

2.3 3つの典型的なウェブサイト構成

権利保有者及びプロモーターの方々から、どのウェブサイト構成が「安全」なのかというご質問をよくいただきます。3つの典型的なオプションとそれらの目安となるリスク特性は以下のとおりです。これらのリスクラベルは、あくまで初期スクリーニングのための出発点にすぎず、法的な類型を意味するものではありません。いずれの場合も、結論はターゲティング及びモニタリングに関するすべての指標（第2.1項）を総合的に評価した上で決まります。

構成	GDPR上の リスクの程度	コメント
世界中でアクセス可能な日本語サイト	中－高	言語はターゲティングに該当しないことを示唆するが、EU域内のファンが、特に国際的なチケット販売プラットフォームチャネルを併用して、チケットを購入することができ、かつ、実際に購入している場合は、言語だけでは[GDPRが適用されない]決定的な要素とはならない。
EU／EEAから技術的ブロックされている日本語サイト	低	最も防御力が高い。実効性のある地域制限に加えてアクセス通知を実施することは、ターゲティングを否定する強力な証拠となる。しかし、それだけであらゆるケースにおいて事業者がGDPRの適用対象外になるとは限らない。他のチャネル、トラッキング技術、あるいはEU向けのマーケティングが存在すれば、それによって取扱いがGDPRの適用範囲に含まれる可能性は依然として残る。IPによりブロックし、利用規約においてEU／EEA域内の個人を対象外と明記すること。
国際的なマーケットプレイス (Ticketmaster等) 経由でのチケット販売	低－中	プラットフォームがユーザー向け画面でのデータ収集を行うが、貴社も依然として管理者としてファンデータを取得し、取扱いを行う（第3項参照）。EU／EEA域内の販売がマーケットプレイスを通して積極的に求められる場合、実際のリスクはラベルが示すよりも高くなる。これを（リスク評価の）上限としてではなく、あくまで出発点として捉えること。

実態のチェック

ミュンヘン又はパリにいるファンが直接であるか又はチケット販売プラットフォーム経由であるかにかかわらず、貴社のイベント又はコンテンツをオンラインで探し、英語でチケットの購入又は登録を完了し、ドイツ又はフランスの住所を入力し、確認を受けることができる場合は、当該購入に GDPR が適用される可能性があるとして想定し、適宜計画すること。

2.4 本ガイドの対象となるスポーツ、メディア及びエンターテインメント事業者

前二項では、法的な検証について記載しました。実務上、日本のスポーツ、メディア及びエンターテインメント業界でよく見られる以下の事業タイプが該当します。このリストはあくまで目安であり、網羅的なものではありません。類型にかかわらず、ある事業者が適用対象であるか否かの最終的な判断は、第2.1項の機能面での検証によって行われます。

事業タイプ	GDPR/APPIの制度が通常適用される理由
スポーツクラブ、チーム及びリーグ	選手、スタッフ、会員及びファンデータ。規模にかかわらずAPPIが適用される。小規模事業者に対する適用除外はない。EU域内在住のファン、選手、スタッフ若しくはスポンサーにサービスを提供し、又はそれらが対象となっている場合、GDPRが適用される。
統括団体及び連盟	アスリート、役員及び会員に関する連盟データ（しばしばア krediteーションの記録やアンチ・ドーピングの記録を含む。）。規模や非営利であるかにかかわらず、APPIが適用される。EU域内のアスリート、役員又は加盟している各国内連盟が関与する場合、GDPRが適用される。
イベント主催者及び会場運営者	各イベントについてのチケット保有者、ア krediteーション、セキュリティ及びベンダーデータの取扱い。EU域内在住の来場者、メディア又は役員が参加するイベントであれば、両規制はそのイベントごとに適用される。

事業タイプ	GDPR/APPIの制度が通常適用される理由
放送事業者及び出版社	商取引データ（加入者、広告、人事）については、完全にAPPI及びGDPRの適用対象となる。APPI第57条（2022年4月改正前は第76条）に定める報道機関に対する適用除外は狭い範囲にとどまる。 すなわち、実際の報道活動のみを対象とし、事業のその他の部分には及ばない。
ストリーミング及びデジタルコンテンツ・プラットフォーム	加入者、視聴履歴及び支払データは通常、それ自体が両規制の適用対象となり、EU域内の加入者にサービスを提供する場合、GDPR第3条第2項に定めるターゲティング・テストの主たる対象となる。
映画、テレビ、音楽及び制作会社	キャスト、クルー、タレント及び位置データ。EU域内在住のキャスト／クルー又はEU配給契約にはGDPRが適用される。制作規模にかかわらず、日本側でのすべての取扱いにAPPIが適用される。
タレント、アスリート及びインフルエンサー・エージェンシー	代理する個人の、個人データ、財務データ及び肖像権（image right）に関するデータの管理。財務及び契約上の詳細が含まれるため、機微性が高くなる。エージェンシーに対しては直接、管理者として両規制が適用される。
チケット販売、グッズ販売及びECマース事業者	大量の決済、配送及びマーケティングデータの取扱い。GDPR第13条及び第14条に基づく基本的な通知義務、並びにAPPIが全面的に適用される。本ガイド第3項及び第4項の「プラットフォームか管理者か」という論点がしばしば問題となる。
スポンサー及び広告代理店	EUに本社を置くスポンサー又は代理店との間でしばしば越境共有される視聴者分析、キャンペーン及び連絡先データの取扱い。取扱い自体及びデータ共有の取決めに両規制が適用される。

事業タイプ	GDPR/APPIの制度が通常適用される理由
ゲーム、eスポーツ及び ファンタジースポーツ運 営事業者	オンラインプレイの性質上、プレイヤーアカウント、年齢確認及び決済データがしばしば越境。GDPRのターゲティング・テストに該当する可能性が高く、規模にかかわらず完全にAPPIの適用範囲内である。プレイヤー又はファンの中に未成年者がいる場合、GDPR第8条に基づきさらなる要件が追加される。情報社会サービスに対する子供自身の同意は、加盟国のデジタル同意年齢（基本的に16歳だが13歳としている加盟国もある。）を上回る場合にのみ有効であり、同年齢を下回る場合、保護者の同意又は許可が必要とされる。また、子供を対象とするマーケティング及びプロファイリングは、通常より厳格な制約を課さなければならない。APPI自体は、GDPR第8条に該当する法定「デジタル同意年齢」は定めていない。日本国内限定又は国内と海外が混在する利用者については、利用者が取引を理解する十分な能力のない未成年（実務上、概ね15歳未満とされることが一般的であるが、これは実務上の基準であり、法律上の明確な線引きではない。）である場合、PPCのガイダンス及び業界の標準的な慣行（JIS Q 15001、オンラインゲーム業界ガイドライン等）が代わりに保護者の同意を求めている。
テクノロジー及びアナリ ティクス業者	通常、上記の類型について処理者又は復処理者の役割を果たす。GDPR第28条に定める処理者契約義務及び同等のAPPI委託義務が直接適用される。
ホテル、旅行及びホス ピタリティ・パートナ ー企業	チーム、イベント又はホスピタリティ・パッケージのための宿泊又は旅行パートナー企業として関与する場合、また、スポーツ・エンタメ事業者がファンや来場者データをこれらのパートナー企業と共有する場合は常に該当する。パートナー側の分析については、ホテルや宿泊事業者向けに別途当事務所が提供するGDPRガイドを参照されたい。
非営利及びアマチュア 団体	非営利又はアマチュアであるかを問わず、同様の機能的判断に基づき、APPIが適用される。EU域内在住の会員、アスリート若しくは寄付者に対しサービスを提供し、又はそれらを対象とする場合は、同様にGDPRが適用される。

モジュール2

チケット販売チャネル及びプラットフォーム

3. 「チケット販売プラットフォームがGDPRに対応している」だけではどうして十分でないのか？

本項の内容

- 貴社が取得するファン又は加入者データについて貴社が管理者となる理由
- プラットフォームが遵守していても貴社が義務を免れない理由
- 第 27 条に基づく EU 代理人義務

非常によくある思い込みは、グローバルチケット販売マーケットプレイス又はストリーミング・プラットフォームがGDPRに準拠したプライバシー体制を独自に維持しているのだから、そのプラットフォームを通して販売を行う事業者は、それ以上何もする必要がないというものです。これは誤りであり、本ガイドが訂正しようとしている、最も重要な誤解です。

3.1 主要な概念の概要

取得データについては貴社が管理者 GDPR上、「管理者」とは、個人データの取扱いの目的及び手段を決定する事業体です。プラットフォームからファン又は加入者データを取得し、チケット又はサブスクリプションの履行、イベント又はサービスの管理、確認の送付、請求の処理、イベント又は放送終了後の案内を行うためにこれを使用する事業者は、当該取扱いの目的を決定することになります。よって、データが当初どのように収集されたかにかかわらず、当該事業者は独立した立場において、当該取扱いについて管理者となります。プラットフォームのプライバシー通知は、そのプラットフォーム自身の取扱いに適用されるものであり、貴社がデータ取得後に別途行う取扱いには適用されず、貴社を免責するものではありません。

処理者と管理者の関係ではなく、独立した管理者同士としての関係 標準的なプラットフォームと権利保有者間の関係は通常、独立した二管理者間の関係です。すなわち、プラットフォーム側の取扱いについてはプラットフォームが管理者であり、貴社が取得、利用するチケット販売、サブスクリプション又はファンデータについては、貴社が管理者となります。通常、プラットフォームは、

貴社のデータ処理者の役割を果たすものではなく、貴社は、あたかも自社のものであるかのようにプラットフォームの法的根拠又はプライバシー通知に依拠することはできません。実際の役割分担については、プラットフォームのパートナー利用規約（随時行われる変更を含みます。）に照らして、ご確認ください。

共同管理者は3つ目の可能性 一部の取決めにおいては、当事者らは単独ではなく、共同で取扱いの目的及び手段を決定します。例えば、リーグとそのクラブがファンデータを集約する場合、共同開催者が共同でイベントを開催する場合、又はスポンサーと権利保有者が共有のファン・エンゲージメント若しくは共同ブランドのチケット販売キャンペーンを実施する場合があります。これらの場合においては、当事者らは、GDPR第26条に基づく共同管理者であり、それぞれの責任、具体的には、プライバシー通知及びデータ主体者の権利の取扱いに対する責任を分担する透明性のある取決めを整備しなければならず、その要旨を関係するファンに提示しなければなりません。独立した管理者のパターンに該当すると決めつけずに、リーグ、スポンサーシップ、共同開催及びプラットフォームの取決めをそれぞれ本テストに照らして確認しましょう。

3.2 実施すべきこと

GDPRが適用される場合、EU／EEA域内のファン又は加入者データをプラットフォーム経由で取得する事業者は、最低でも、以下を行う必要があります。

- GDPRのコンテンツ要件（本ガイド第5項）を満たし、事業者自身の取扱いを対象とする、**独自のプライバシー通知を定めること。**
- 各活動について**法的根拠を特定すること**。一般的には、チケット又はサブスクリプションのための契約の履行自体。直接マーケティングについては、状況に応じて、正当な利益（GDPR第6条第1項(f)、前文第47項）又は同意を根拠とすることができ、適用されるeプライバシー又は国内ダイレクトマーケティング規則が要求する場合は、別途同意が求められます（第5.2項参照）。正当な利益に依拠する場合は、利益衡量テストを文書化しましょう。
- EU／EEA域内のファン及び加入者に対し、文書化された受付・対応手順を整備したうえで、**データ主体の権利**（アクセス、訂正、削除、異議申立て等）**を尊重すること**。要求には、不当な遅滞なく、原則として1か月以内に、回答しなければなりません。ただし、要

求が複雑又は多数にのぼる場合は、さらに2か月延長することがあります。ただし、最初の1か月以内にデータ主体にその旨通知しなければなりません（第12条第3項）。

- 事業者にとってデータを取り扱うIT又はサービスベンダーとの間で**処理者契約を締結すること**。
- 本ガイド第6項の通知義務に従って**データ侵害を管理すること**。

3.3 EU代理人（第27条）

日本の事業者がしばしば驚かされる義務がもう一つあります。ターゲティングに基づきGDPRが適用される場合（GDPR第3条第2項）で、例外が適用されない場合、貴社は書面でEU／EEA域内に拠点を置く代理人を指定しなければなりません（第27条）。代理人はデータ主体及び監督機関に対する現地窓口としての役割を果たし、貴社のプライバシー通知に明記されなければなりません。代理人は、貴社が取り扱うデータのデータ主体が所在する加盟国の一つ、実務上、貴社のEU／EEA域内のファン、視聴者又は加入者が集中する加盟国、に拠点を置いていなければなりません。これは形式的な要件ではありません。第27条に基づく代理人の不在自体が、非EU企業に対する執行決定においてしばしば指摘されるコンプライアンス違反の一つです。貴社がEU域内に拠点を有しない場合、一般的に外部EU代理人を選任することが本義務を満たす最も効率的な方法であり、当事務所がアレンジ可能なサービスです（末尾の項を参照）。

限定的な適用除外があります（第27条第2項）。データ取扱いの発生頻度が低く、特別な種類のデータ（第9条）又は有罪判決や犯罪と関連するデータ（第10条）の大規模な取扱いを含まず、個人の権利や自由に対しリスクを及ぼす可能性が低い場合は、代理人は必要とされません。EU／EEA域内のファン、視聴者又は加入者に継続的かつ構造的にサービスを提供する事業者については、この適用除外が適用されることは稀です。いずれの結論に至った場合でも、その検討過程を文書化しておきましょう。

代理人はデータ保護オフィサーではなく、二つの役割は兼任すべきではありません。EU代理人（第27条）は、データ主体及び監督機関のための現地窓口です。データ保護オフィサー（DPO）（第37条乃至第39条）は、単独で行為し、データ保護事項のすべての関与しなければならない監視機能です。第37条に基づきDPOの任命が必要かどうか別途ご確認ください。具体的には、貴社の主軸となる活動に大規模な継続的かつ体系的な個人のモニタリング（大規模なファン分析、ストリーミン

グ・プロファイリング又は広告トラッキング等)、又は特別な種類のデータの大規模な取扱いが含まれる場合となります。

最後に、二つ補足します。代理人の選任は、貴社の責任を転嫁するものではありません。選任は、管理者自身に対する法的措置を妨げるものではなく、管理者は引き続き全面的に責任を負います(第27条第5項)。また、代理人は貴社のEU拠点又は「主たる事業拠点」とはなりません。GDPRの一括管轄制度は、単に代理人が選任されたからといって適用されるものではありません。そのため、影響を受けるファンが所在する管轄地域のいずれのEU/EEA監督機関も、独自に措置を講じることができます。

4. チケット販売チャネルとデータフローの整理

本項の内容

- 直接収集するデータと、プラットフォームから取得するデータの違い
- ブランドライセンス契約及びフランチャイズ契約によって、責任の所在がどのように変わるか
- 貴社のイベント及びプロパティ(事業資産)について記入できる、1ページのデータフロー・テンプレート

スポーツ、メディア及びエンターテインメント事業者の多くは、複数のチケット販売チャネルや流通チャネルを利用しており、GDPR上、これらはそれぞれ異なる取扱いを受けます。まず最初に行うべきことは、誰がデータを収集し、誰がそれを取得し、どのような法的根拠に基づくのかを整理することです。特に重要なのは、次の二つの区別です。

4.1 主要な概念の概要

直接収集(第13条)とプラットフォームから取得するデータ(第14条)の違い 自社のチケット販売システムやストリーミングサービスの登録などを通じて、ファン又は加入者から個人データを直接収集する場合、GDPR第13条が適用され、データを収集する時点でプライバシーに関する情報を提供しなければなりません。プラットフォーム上のデータにどの規則が適用されるかは、単に入力

画面を誰が運営しているかではなく、プラットフォームの法的役割によって決まります。プラットフォームが、貴社の処理者として貴社に代わってデータを収集する場合（第28条）、その収集は貴社によるものとみなされ、収集時点で第13条が適用されます。独立したプラットフォームが、独立した立場において管理者としてデータを収集し、その後、貴社に当該データを送信する場合、貴社による処理にはGDPR第14条が適用されます。情報の提供は、データの取得後、合理的な期間内（遅くとも1か月以内）に、データをファンとの連絡に使用する場合には、遅くとも最初の連絡時までに、また、他の取得者への開示を予定している場合には、遅くとも当該データを最初に開示する時点までに、行わなければなりません（第14条第3項）。貴社とプラットフォームが目的及び手段を共同で決定する場合には第26条が適用され、共同管理者としての取決めにおいて情報提供義務の分担を定める必要があります（本ガイド第3.1項をご参照ください。）。GDPR第13条及び第14条に基づき要求される内容は実質的には同じですが、適用の契機、時期並びにデータの種類及び取得元に関する追加情報が異なります。

チャンネルの種類	収集者	適用される規則	通知の時期
自社のチケット販売システム	事業者が直接収集	GDPR第13条	データ入力時／送信前
Ticketmaster／SeatGeek／Eventbrite／マーケットプレイス	プラットフォーム	GDPR第14条	合理的な期間内（遅くとも最初の連絡時まで）
電話／Eメール／チケット販売窓口	事業者が直接収集	GDPR第13条	データの収集時

ブランドライセンス契約及びフランチャイズ契約 スポーツ、メディア及びエンターテインメント分野でよく見られる重要な仕組みの一つに、ブランドライセンス又はフランチャイズライセンスがあります。これは、チーム、イベント又はコンテンツプロパティが、著名なリーグ、連盟又は知的財産保有者のブランドの下で事業を行っているものの、実際には、そのブランド及び関連する標章の使用許諾を受けた別会社によって運営されるという仕組みです。この場合、通常、ブランド又は権利の保有者ではなく運営会社が、チケット販売、会員又は配信システムを運営し、ファン又は加入者のデータを収集及び処理します。当該データフローに関するGDPR上の責任は、一般的に、ブランド又は権利の保有者ではなく、管理者としての運営会社に帰属します。

ブランド及び権利の保有者にとって、これには2つの影響があります。第一に、ブランド保有者は通常、運営会社のチケット販売システム又は会員システムを通じて収集されるファンデータの管理者ではなく、運営会社に課されるGDPR上の義務を負いません。第二に、そのブランドはチーム、イベント又はコンテンツと密接に関連付けられているため、ブランド保有者は、ブランド及び評判に関するリスク管理の観点から、運営会社がGDPRに準拠したチケット販売又はファンデータの取扱いフローを運用することを確保する正当な利益を有します。データ保護に関する責任を、ブランドライセンス契約又はフランチャイズ契約に明示的に定めることが望ましい慣行です。

4.2 実施すべきこと：データフローマップの作成

イベント、プロパティ及びチケット販売チャネルごとに、以下の表の各行に必要な事項をご記入ください。この作業だけで実務上の不確実性の大部分が解消され、これが他のすべての作業の基礎となります。

イベント／ プロパティ	チャネル	収集者	取得者	第13条 ／第14 条	法的根拠	プライバシー 通知の表示の 有無
...	...	...	...	...	...	☐
...	...	...	...	...	...	☐
...	...	...	...	...	...	☐

モジュール3

プライバシー通知及び法的根拠

5. 適切なプライバシー通知の作成

本項の内容

- チケット購入又は登録フローにおいて、プライバシー通知をどのように提示すべきか（リンクによる提示でも可）
- マーケティングへの同意を、契約及びプライバシー通知とどのように分離するか

- 第13条を満たすために、プライバシー通知に実際にどのような事項を記載しなければならないか

プライバシー通知については、2つの異なる疑問が生じますが、これらはしばしば混同されがちです。それは、通知がどのように提示されるか、そして通知に何が記載されているか、という2点です。通知の提示方法が完璧であっても、内容が不十分な場合があります。同様に、内容が適切であっても、提示方法が不適切であれば、要件を満たしません。

5.1 提示方法：リンクでもよく、全文を画面上に表示する必要はない

GDPRでは、チケット購入画面又は登録画面にプライバシー通知の全文を表示することを義務付けていません。標準（GDPR第12条第1項及び第13条）によれば、データが取得された時点で、簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて情報を提供することが求められています。オンラインでのチケット購入又は登録フローにおいて、ファン又は加入者が個人データを送信する前に、明確に表示され、かつ内容が明確に分かる表示を付したプライバシー通知へのリンクを提示することにより、この要件を満たすことができます。この短い通知から通知の全文へのリンクを設ける「階層的な」アプローチは、EDPBによって明示的に支持されています。リンクが目立たない場合や、フロー中に合理的に認識可能でない場合には、リンクを設けるだけでは不十分です。

5.2 同意と、契約及びプライバシー通知との分離

チケット販売又は登録フローにおいては、以下の3つを分離する必要があります。

1. **利用規約／チケット販売条件への同意**は、契約に関連する事項です。
2. **プライバシー通知**は、第13条又は第14条に基づく情報提供義務であり、個人が「同意」するものではありません。チケット販売又はサブスクリプションに関するデータ処理の法的根拠は、通常、同意ではなく契約の履行です。
3. **マーケティングへの同意**は、適用されるeプライバシー規則又は各国のダイレクトマーケティング規則で同意が求められる場合に必要となります。EU域内のファンに対するEメール

ル、SMS及びプッシュ通知によるマーケティングについては、通常、同意が必要です。同意が必要とされる場合又は同意に依拠する場合には、同意は個別の、自由意思によるオプトイン行為でなければなりません。利用規約への同意とセットにしたり、あらかじめチェックが入っていたり、チケットの購入又は加入の条件とすることはできません。GDPR自体においては、ダイレクトマーケティングは、それ以外の場合には正当な利益を根拠とすることができます（第6条第1項(f)、前文第47項）。ただし、これにより、より厳格なeプライバシー規則及び各国のダイレクトマーケティング規則の適用を排除するものではありません。

「利用規約及びプライバシーポリシーに同意します。」という形式の、複数事項への同意を一括して求めるチェックボックスは、よく見られる問題点です。マーケティングへの同意を、別途、チェックを入れていないチェックボックスとして分離することが、この要件を満たすための最も簡単で確実な方法です。明確にすると、GDPRはチェックボックスの具体的な数を義務付けていません。義務付けられているのは、マーケティングへの同意を独立させることと、自由意思に基づくものとすることです。チェックボックスを分けることは手段であって、規則そのものではありません。EU域内のファンに対する電子マーケティング（Eメール、SMS、プッシュ通知）には、GDPRの同意要件に加えて、加盟国のeプライバシー規則及び不正競争に関する規則が適用される場合があることにご留意ください。例えばドイツでは、不正競争防止法（UWG）第7条第2項第2号及び同条第3項がこれに該当し、これらはGDPRの同意要件と併せて適用されます。

5.3 内容：APPIに準拠したポリシーだけでは通常不十分

個人情報保護法（APPI）を基に策定された、簡潔で概括的な企業のプライバシーポリシーには、通常、GDPR第13条で要求されるすべての事項が含まれていません。GDPRが適用される場合、通知には、とりわけ以下の事項を含める必要があります。

- 管理者の名称及び連絡先、並びに該当する場合は、そのEU代理人の名称及び連絡先（GDPR第27条）。
- データ保護責任者（DPO）が指名されている場合、DPOの連絡先
- 各取扱活動の目的及び法的根拠（正当な利益のために取扱いが必要となる場合（第6条第1項(f)）、追求される利益を含みます。）
- データの取得者又は取得者の類型

- EU／EEA域外への移転、及びその根拠
- 保存期間（又はその設定基準）
- データの提供が法令上若しくは契約上の要件であるか、又は契約締結に必要であるか、及び提供しなかった場合に生じ得る結果
- プロファイリングを含む自動化された意思決定（第22条）の有無、並びにそれに関与する論理、及びその重要性と結果に関する有意義な情報
- 第15条乃至第22条に基づくデータ主体の権利（同意を撤回する権利を含みます。）
- 監督機関に対して異議を申し立てる権利
- データが本人から取得されたものではない場合（第14条）、これらに加えて、対象となる個人データの種類及びデータの情報源（公衆がアクセス可能な情報源から来たものかどうかを含みます。）

実務上の解決策としては、通常、既存のAPPIポリシーを廃止するのではなく、GDPRが適用されるファン、視聴者又は加入者に対して、これらの点を網羅したGDPRに特化した通知（又は追加条項）を補足することが挙げられます。

モジュール4

インシデント管理及びAPPIとの関係

6. データ侵害：72時間の制限時間

本項の内容

- GDPRに基づくデータ侵害の通知義務及び72時間の制限時間
- APPIに基づき並行して課される義務
- 72時間以内の対応に関するチェックリスト、並びにイベントに関連するア Krediyteyeshyon／本人確認データに関する論点

スポーツ、メディア及びエンターテインメント事業者は、まさに攻撃者及び規制当局の双方の関心を引くようなデータを保有しています。具体的には、氏名、連絡先、場合によっては身分証明書やア Kredィテーション情報、決済カードデータ、及びイベントへの参加履歴、視聴履歴又は購入履歴等です。データ侵害は、GDPR 違反の中でも特に重い罰則が科される類型の一つであり、その義務には時間的制約があります。

6.1 主要な概念の概要

GDPR 上の要件 GDPR が適用される場合において、個人データ侵害が発生した場合、管理者は、その侵害が個人に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも 72 時間以内に、所轄監督機関に対し、通知しなければなりません（GDPR 第 33 条）。当該侵害が個人に対する高いリスクを発生させる可能性がある場合、影響を受けた個人に対しても、不当な遅滞なく、連絡しなければなりません（第 34 条）。72 時間の制限時間は、調査が完了した時点ではなく、侵害を認識した時点から始まります。したがって、インシデントが発生する前に、インシデント対応計画を策定しておく必要があります。完全な情報がまだ入手できない場合は、段階的に通知を行うことができます（第 33 条第 4 項）。さらに 2 つの義務が見落とされがちです。すなわち、処理者は、侵害に気づいた後、不当な遅滞なく、管理者に対して通知しなければなりません（第 33 条第 2 項）。そのため、これをベンダー及びプラットフォームとの契約書に、厳格な制限時間を設けて明記する必要があります。また、通知の有無にかかわらず、すべての侵害について社内で文書化しなければなりません（第 33 条第 5 項）。

APPI でもデータ侵害の通知義務が課される 日本の個人情報保護法（APPI）は、個人の権利及び利益を害するおそれのある侵害について、個人情報保護委員会（PPC）及び影響を受ける個人への通知を義務付けるよう改正されました。実務上、PPC への報告義務は一般的なリスクベースの基準ではなく、個人情報保護法施行規則第 7 条に基づく以下の 4 つのタイプのいずれかに該当する場合に限り、報告義務が生じます。(i)要配慮個人情報の漏洩、(ii)金銭的損失のリスクを生じさせる漏洩、(iii)不正な目的に起因すると疑われる漏洩、又は(iv)1,000 人以上の本人に影響を及ぼす漏洩。これらの類型に該当しない侵害については、個人に対するリスクが多少残っている場合でも、PPC への報告義務は生じません。したがって、EU/EEA 域内のファン又は加入者に影響を及ぼす侵害は、異なる基準及び制限時間が適用される、両規制に基づき並行した義務を生じさせる可能性があります。PPC の規則に基づき、報告は二段階で行われます。まず、侵害を認識後速やかに予備報告を行い（PPC の指針によれば、実務上は一般に概ね 3 日から 5 日以内とされていますが、個人情報保護法

施行規則では、これを「速やかに」行うことのみが求められており、法定期限として具体的な日数を定めていません。）、かつ、30 日以内（サイバー攻撃等、不正な目的に起因する可能性が高い場合は 60 日以内）に最終報告を提出します。必要な場合、影響を受ける個人には速やかに通知を行わなければならない、委託先のサービス提供者は、委託元企業に通知することにより、APPI に基づく自らの報告義務を免れることができます。両規制を満たす、単一のインシデント対応手順を策定しましょう。

プラットフォームの側面 事業者がチケット販売又は配信プラットフォームのパートナーポータルを通じてファン又は加入者のデータにアクセスする場合、そのアクセスポイント自体（例えば、スタッフの認証情報を狙ったフィッシング攻撃）が、侵害の原因となる可能性があります。第三者のプラットフォーム又は CRM ポータルを標的とした認証情報フィッシングは、消費者向け事業者全般において広く認識されている一般的な攻撃手法であり、侵害の通知の遅滞（72 時間を大幅に超えた場合）、執行措置における処分の加重要因として頻繁に挙げられています。ここから得られる教訓は 2 つあります。スタッフがプラットフォームのポータルへのアクセスに使用する認証情報を確実に保護すること、そして認識後速やかに報告することです。

6.2 実施すべきこと：72時間対応チェックリスト

いつ	措置
最初の 24 時間以内	インシデントを収束させ、インシデント対応責任者を招集し、インシデントを認識した時刻を記録し（この時点から制限時間のカウントが始まります。）、書面による記録を開始し、証拠を保全する。
72 時間以内	個人に対するリスクを評価し、通知義務がある場合は、所轄の EU 監督機関（及び APPI が適用される場合は PPC）に通知を行い、EU 代理人に連絡し、リスクが高い場合は、ファン／加入者へのお知らせを作成する。
72 時間経過後	必要な場合、影響を受ける個人に通知を行い、調査を完了させ、是正措置を記録し、管理措置及びスタッフ研修を見直し、更新する。

インシデント発生前に準備しておくべき事項

- ・ 指名されたインシデント対応責任者及び 24 時間 365 日対応の連絡窓口

- 72 時間の制限時間を組み込んだ、書面による侵害対応手順
- 通知先として事前に特定された EU 監督機関及び（該当する場合）EU 代理人
- フィッシング及びプラットフォーム・ポータル認証情報セキュリティに関するスタッフ研修

6.3 スポーツ、メディア及びエンターテインメント分野における本人確認及びア Kredィテーシ ョン・データの機微性

日本の旅館業法に基づき宿泊者名簿に関する特定の法的義務を負うホテルとは異なり、スポーツ、メディア及びエンターテインメント事業者は、一般的に、本人確認書類の収集を義務付ける単一の包括的な法律の適用対象となっておりません。これは、この業界に同様の懸念が存在しないことを意味するものではありません。機微性の高い本人確認データは、いくつかの典型的な状況で頻繁に生じますが、それぞれについて、一つの一般的な原則に従うことを想定するのではなく、固有の条件に応じて確認する必要があります。

最も一般的な例は、次のとおりです。イベントにおける各国の選手、役員及びチームの認定においては、通常、出入国管理及び認定を目的としてパスポート又は本人確認書類のデータが取り扱われます。また、世界アンチ・ドーピング規程及び日本では日本アンチ・ドーピング機構（JADA）が管轄するアンチ・ドーピング関連データと重複する場合があります。アンチ・ドーピング、医療及び治療使用に関するデータは健康に関するデータであるため、GDPR 第 9 条に基づく特別な種類の個人データに該当し、第 6 条の法的根拠に加えて、第 9 条に定める例外を満たす必要があります。会場及び中継設備エリアへの立入りのためのメディア及び放送スタッフの資格認定、イベント又は会場ごとのセキュリティ体制（大規模な国際イベントでは、組織委員会、会場又は関係当局が定める、個別に定められた認定及び審査要件が含まれる場合があります。）。これらのいずれかが適用される場合、機微性の高い本人確認データと同じ原則が適用されます。すなわち、具体的な認定、アンチ・ドーピング又はセキュリティ上の要件により実際に求められるデータのみを収集し、必要な期間に限り保持し、アクセスを制限した上で安全に保管し、本人確認書類の全体画像の写しを不必要に保存することは避けます。このような収集については、ケースバイケースで、事案ごとに具体的な法的又は契約上の根拠を確認し、包括的なルールが適用されると想定してはなりません。

EU/EEA との関連性の有無にかかわらず、これと並行する義務が日本法の下で生じ、また、JADA/アンチ・ドーピングに関する記録に関しては、おそらくより広範な義務が生じます。アンチ・ド

ーピング検査の結果及び治療使用特例（TUE）の記録を含む健康関連情報は、APPI 第 2 条第 3 項に基づく「要配慮個人情報」に該当します。このようなデータを取得するには、原則として本人の事前の同意が必要となります（APPI 第 20 条第 2 項）。また、通常の個人データについて利用可能なオプトアウトの仕組みに基づき、第三者に提供することはできません（APPI 第 27 条第 2 項但書き）。これは、日本人選手のデータを純粹に国内で取り扱う場合に適用されるものであり、上記の GDPR に関する分析とは別に、アクレディテーション・データ及びアンチ・ドーピング関連データの取扱手順において対応すべきものです。

生体認証によるアクセス管理については、別途言及する必要があります。顔認証による入場、生体認証による認定及び同様の会場へのアクセス技術では、個人を一意に識別する目的で生体認証データが取り扱われます。これは、GDPR 第 9 条に基づく特別な種類の個人データに該当し、特定の例外が適用されない限り、禁止されます（実務上は通常、本人の明示的な同意を取得し、かつ生体認証以外の実質的な代替手段を提供する必要があります）。EU/EEA 域内からの参加者がいるイベントにおいて、このようなシステムの導入が検討される場合は、高いリスクを伴う導入とみなし、通常は運用開始前に GDPR 第 35 条に基づくデータ保護影響評価を実施する必要があります。二つの点を強調しておく必要があります。第一に、第 9 条の例外は、第 6 条に基づく法的根拠の代わりではなく、これに加えて必要となるため、両方を特定してください。第二に、明示的な同意は、それが自由意志によって与えられた場合に限り、有効となります。そのためには、生体認証を用いない実質的な代替手段（例えば、従来のチケット又は認定の確認）を、不利益を被ることなく利用できることが前提となります。生体認証の登録を入場の条件とする場合、有効な同意によって正当化されません。

7. 執行及びリスク 「日本では事例がない」との見方が誤解を招く理由

本項の内容

- 日本における GDPR 事案数が、構造上ゼロとなる理由
- 公表されている執行実績が、実態の一部しか示していない理由
- EU 域外の企業に対する罰金が現実のものとなっている理由、及びそれが貴社にとって何を意味するか

GDPR が日本企業に対して実際に執行されているのか疑問に思われるのは、もっともです。率直な答えは、一概には言えませんが、安心できるような解釈をするのは誤りです。

7.1 PPCがGDPRを執行しないため「日本ではGDPRの事例がない」

GDPR は、EU／EEA の監督機関（及びこれと並行して施行されている英国 GDPR については、英国 ICO）によって執行されています。日本の個人情報保護委員会（PPC）は、別の制度である個人情報保護法（APPI）を執行しており、GDPR を執行することはありません。したがって、「日本における GDPR の執行事例」の件数は、構造上ゼロとなります。これはリスクが存在しないからではなく、単に日本の当局が GDPR を執行しないためです。日本での事例がないからといって、リスクについて何の判断材料にもなりません。日本企業に対する執行措置が講じられる場合、それは PPC によるものではなく、GDPR の域外適用範囲を適用する EU／EEA の監督機関によるものです。

7.2 公表されている記録は不完全であること

欧州内においても、GDPR に基づくすべての罰金が公表されているわけではありません。公表の慣行は監督機関によって異なり、一部の決定のみを公表する監督機関が複数あり、また罰金を科された事業者がその事実を公表することはほとんどありません。したがって、公開されている罰金追跡データベースには最小限の情報しか記録されておらず、全体像ではないため、公表されている記録はそうした点を踏まえて解釈する必要があります。

7.3 EU域外の企業に対する罰金は実在し、執行されている

過去最高額の GDPR 上の罰金が科されたのは、EU 域外に本社を置く企業に対してでした。単一の事案で最大 12 億ユーロ、また数億ユーロ規模の罰金が繰り返し科されています。一部は既に支払われていますが、最高額の罰金の中には、依然として不服申立て中のものがあります。しかし、不服申立てが行われているからといって、そのリスクが理論上のものになるわけではありません。その仕組みは単純明快です。これらの企業は、EU 域内に設立された事業体や事業拠点を維持しており、当局はこれらを通じて措置を講じることができます。EU 域内で積極的に事業を展開している日本企業グループ（例えば、ツアー、ライセンス、流通又は放送関連の子会社）は、原則として、これらの企業と同等の立場にあります。EU 域内に拠点を持たない純粋な日本の事業者に対する執

行は、実務上、より困難ですが、EU 域内に何らかの拠点が存在する場合、この分析は大きく変わります。

7.4 罰金だけが手段ではない

罰金に加え、EU 当局は、取扱いの停止命令、強制監査及び是正命令を発することができ、これらはいずれも、EU 域内に製品を販売し、又は EU 域内で事業運営している企業に多大な支障を及ぼす可能性があります。したがって、リスクの実態は、報道で取り上げられる罰金額という表面的な数字よりも広範囲に及んでいます。

リスクに関する結論

「日本では公表された GDPR 関連事例がない」というのは、公表された記録について述べたものにすぎず、リスクの程度を示すものではありません。EU/EEA 域内のファン、視聴者又は加入者にサービスを提供する日本のスポーツ、メディア又はエンターテインメント事業者、特にそのグループが EU 域内に拠点を有する場合には、本ガイドに記載されているコンプライアンス上の不備を、理論上の問題ではなく、現実のものであり、是正すべき課題として捉える必要があります。

8. GDPRとAPPIの関係性

GDPR への対応は単独で行うものではありません。既に個人情報保護法（APPI）の適用を受けて事業を営んでいる以上、両制度は EU—日本間の相互十分性認定を通じて関係しています。

2019 年 1 月に最初に採択され、2023 年 4 月に完了した第 1 回定期見直しにおいて確認された十分性認定の下、EU は日本のデータ保護制度、すなわち、個人情報保護委員会（PPC）の補完的ルールによって補完された APPI が十分なレベルの保護を提供していると認定しています。実務上の効果として、EU 起源のデータについて補完的ルールが遵守されることを条件に、標準契約条項等の追加的な移転手段を用いることなく、EU から日本の事業者への個人データの移転が可能となります。

スポーツ、メディア及びエンターテインメント事業者にとって重要な点が 2 つあります。第一に、十分性認定への依拠には条件があります。補完的ルールでは、EU 起源の個人データについて、例

例えば保存期間、第三国への再移転及び特定の種類のデータの取扱い等に関して具体的な要件が定められており、これらは実際に遵守されなければなりません。第二に、十分性認定は越境移転の仕組みのみを対象とするものであり、もともと GDPR が適用される場面において適用される実質的な GDPR 上の義務（通知、法的根拠、データ主体の権利、侵害通知）を免除するものではありません。最近の APPI 改正により、GDPR モデルにより近い侵害通知義務の規定等、両制度間の差異は縮小されましたが、依然として差異は残っており、両制度上の義務を同一であるとみなすのではなく、対照的に整理すべきです。

項目：	GDPR（適用される場合）	APPI
執行機関	EU／EEA の DPA、英国 ICO	PPC
侵害通知	72 時間以内に DPA へ（第 33 条）	PPC 及び個人への通知（リスクベース）
越境移転	十分性認定の対象は EU →日本の場合	EU 起源のデータについては補完的ルールが適用
プライバシー通知の内容	第 13／14 条（詳細）	利用目的を重視し、規定内容は相対的に少ない。
制裁金／過料の上限	最大 2,000 万ユーロ又は全世界の売上高の 4%のいずれか高い方	PPC による是正指導及び命令。命令違反及び不法な開示については刑事罰（法人罰金を含む。）が適用されるが、GDPR のような売上高ベースの制裁金制度はない。

8.1 逆方向の適用：APPIがEUの事業者に応用される場合

本ガイドは、主に GDPR の適用対象となる日本側の事業者を対象として作成されていますが、その関係は逆の方向にも当てはまります。ドイツその他の EU 加盟国のスポーツ、メディア及びエンターテインメント事業者は、日本に拠点を有していない場合でも、APPI の適用対象となる可能性があります。APPI の域外適用規定（第 171 条。2022 年 4 月の条文番号改定前の第 75 条）に基づき、外国の事業者が、日本国内の者に対する商品又はサービスの提供に伴い、かかる者を特定できる個人情報を取り扱う場合、同法が適用されます。

したがって、日本国内の者に対して試合のチケット、グッズ、ストリーミングサービスのサブスクリプション又はファンクラブの会員権を販売し、それらの取引に関連してかかる者の個人情報を取り扱う EU 事業者は、APPI の適用対象となる可能性があります。これは、第 2 項で取り上げた GDPR の分析とは概ね逆のものです。ただし、APPI 第 171 条の規定は、GDPR のターゲティング・テストとは異なる枠組みで定められています。

最低数量による適用除外はありません。5,000 人以下の個人に関する個人情報を取り扱う事業者に対する従来の適用除外規定は、2015 年の改正により、2017 年 5 月 30 日をもって廃止されました。

8.2 日本でイベント又はツアーを運営するEUのクラブ、プロモーター及び放送局

APPI の適用は、オンライン販売だけに留まりません。日本において試合、ツアー、フェスティバル、その他のイベントを開催する EU のクラブ、リーグ、プロモーター又は放送局は、通常、チケット保有者、認定メディア、現地スタッフ及びボランティア、ホスピタリティゲスト、出演者並びに委託業者に関する個人情報を取り扱います。運営会社が自己の事業活動において個人情報データベース又はこれに準ずるシステムを利用する場合、当該取扱いは一般的に APPI の適用対象となります。

イベント開催前に確認すべき事項としては、以下の点が挙げられます。APPI 第 17 条及び第 21 条に基づく利用目的の特定及び通知（通常、日本の参加者又は関係者に向けた情報については日本語で行います。）。現地のパートナー、会場又はスポンサーに個人データを開示する場合の、APPI 第 27 条に基づく同意及び第三者提供に関する規定。日本のサービス提供者が運営会社に代わってデータを取り扱う場合の、APPI 第 25 条及び第 27 条第 5 項第 1 号に基づく委託及び委託先監督の体制。報告の対象となるデータ侵害が発生した場合の、PPC 及び影響を受ける個人に対する APPI 第 26 条に基づく通知。

会場、スポンサー又はサービス提供者が、独立した第三者であるか、共同利用者であるか、又は委託を受けたサービス提供者であるかは、契約上の呼称ではなく、その実際の役割に基づいて判断されなければなりません。

取扱いが EU 内の拠点における活動の一環として行われる場合、その他 GDPR 第 3 条の適用対象となる場合には、GDPR が併せて適用される可能性があります。したがって、当該取扱い業務につい

ては、関係する個人の居住地や国籍によって適用される法律が決まると仮定するのではなく、両制度の下で整理すべきです。

8.3 EU－日本間のデータフロー：ツアー、ライセンシング及び共同制作

ツアー、コンテンツのライセンシング及び共同制作においては、出演者及びスタッフのリスト、協力者や出演者の情報、視聴者及び加入者の分析データ、ア Kredィテーション・データ及び権利保有者の連絡先を含む個人データが双方向でやり取りされることが日常的に行われています。

EU から日本へのデータ移転については、欧州委員会の十分性認定により、GDPR 第 45 条に基づき、同認定の対象となる日本の民間セクター取得者に対しては、標準契約条項やその他の第 46 条に基づく移転メカニズムを用いずとも、個人データの移転が認められています。十分性認定に基づき移転されたデータの日本の取得者は、当該データに適用される PPC 補完的ルールを遵守しなければなりません。

この取り決めは相互的なものです。日本の PPC は、EU/EEA 加盟国及びこれとは別に英国を、APPI 第 28 条第 1 項及び APPI 施行規則第 15 条に基づく「指定国」、すなわち日本と同等水準の個人情報保護制度を有すると認められる法域として指定しています。したがって、日本の事業者から EU 内の取得者への個人データの移転については、取得者が日本国外に所在しているという理由のみをもって、APPI 第 28 条に基づく特別な同意又は同等の措置の仕組みを必要とするものではありません。第三者への個人データの提供について規定する APPI の通常の規定（第 27 条並びに委託及び共同利用に関する例外を含みます。）は、引き続き適用されます。

ただし、PPC によって認定されていない国に所在する取得者への日本からの転送又は取得者が必要な同等措置を講じていない場合については、APPI 第 28 条が適用される場合があります。したがって、共同制作、配信及びライセンス契約においては、契約書の起草段階で、当事者それぞれの役割、利用目的、開示の許容範囲、再移転の条件、セキュリティ上の義務及び侵害発生時の協力義務を明確に定める必要があります。

こうした取決めは、メディア及び放送権、スポンサーシップに関する制限並びに独占的販売契約を含む、EU の商法及び競争法上の問題を引き起こす可能性もあります。当事務所の EU 競争法チームは、データ保護に関する分析と併せて、これらの問題についても助言を行っております。

モジュール 5

導入ロードマップとチェックリスト

9. 導入ロードマップ

本ロードマップは、本ガイドをプロジェクト計画へと落とし込むものです。各ステップを、担当と目標期日が定められた作業パッケージとして扱ってください。各ステップは順次行われることを前提としていますが、ステップ 1 の完了後は、複数のステップを並行して実行することができます。

ステップ 1

GDPR が適用されるかどうかを判断

各イベント、プロパティ及びチャネルについて、適用性チェックリスト（第 2.2 項）に記入し、結論を記録します。担当：イベント責任者／社内弁護士

ステップ 2

チャネル及びデータフローの整理

データフローのテンプレート（第 4.2 項）を記入します。これにより、チャネルごとに、誰が管理者であるか、また GDPR の第 13 条又は第 14 条のどちらが適用されるかがわかります。担当：チケット販売／営業及び IT 部門

ステップ 3

チケット販売フロー及びプライバシー通知の整備

第 5 項を適用します。通知を適切に提示し、マーケティングに関する同意を独立したオプトイン欄として分け、APPI ポリシーに GDPR の追加条項を盛り込みます。担当：チケット販売／営業及び弁護士

ステップ 4

プラットフォーム及び事業者の役割の明確化

プラットフォームパートナーの条件を確認し、ブランドライセンス又はフランチャイズに係るプロパティについてはライセンス又はフランチャイズ契約を確認し、管理者の割り当てを確定します（第 3 項－第 4 項）。担当：弁護士

ステップ 5

必要に応じて、EU 代理人の選任

GDPR 第 27 条を評価し、必要に応じて代理人に関する取決めを行います（第 3.3 項）。担当：弁護士

ステップ 6

インシデント対応態勢の整備

ステップ 7

72 時間手順及びチェックリスト（第 6.2 項）を採用し、フィッシングやポータル認証情報のセキュリティについてスタッフへの研修を実施します。担当：IT 部門及びイベント責任者

ガバナンスの定着

取扱いに関する記録、保存／削除スケジュール（アクレディテーション及び本人確認データを含みます。）、委託先との処理者契約及び定期的な見直し。担当：弁護士及び IT 部門

10. コンプライアンス・チェックリスト

以下のチェックリストは、ロードマップを優先度ごとに分類し、チェック可能な行動項目に落とし込んだものです。本チェックリストは、体系的な検討の出発点として利用するものであり、特定の状況に関する助言の代わりとなるものではありません。

即時対応（0～3 か月）

- ☐ すべてのイベント、プロパティ及びチケット販売又は配信チャネルについて、以下の情報を整理します。収集主体、取得主体、GDPR第13条又は第14条、法的根拠、該当する通知
- ☐ 各チャネルにGDPRが適用されるかどうかを判断（地理的適用範囲の評価）
- ☐ GDPRに準拠したプライバシー通知（又はAPPIの追加条項）を用意し、直接チケット販売又は登録の手続において、適切な段階で表示されるようにします。
- ☐ データ主体の権利に関する手続を整備します。受付経路、本人確認及び1か月以内の回答期限のトラッキング（第12条第3項）
- ☐ マーケティングに関する同意については、チェックが入っていない状態の、自発的に選択可能なオプトイン用のチェック欄を別途設けます。
- ☐ 72時間の制限時間を組み込んだ、書面による侵害対応手順を策定します。

短期対応（3～9月）

- ☐ プラットフォームパートナーの条件（チケット販売マーケットプレイス、ストリーミング及び配信プラットフォーム）を再確認し、データ管理者の割当て及びデータ利用の制限について再確認します。
- ☐ ブランドライセンス又はフランチャイズに係るプロパティについては、チケット販売やファンデータのフローに関するGDPRの遵守責任が誰にあるかを、ライセンス契約又はフランチャイズ契約で確認します。
- ☐ 各取扱活動について法的根拠を特定し、それを文書化します。
- ☐ 必要に応じて、GDPR第27条に基づきEU代理人を指定し、その氏名を通知に記載します。
- ☐ チケット販売、CRM、ストリーミングその他ベンダーと、GDPR第28条に基づく処理者契約を締結します。
- ☐ チケット販売、CRM、ストリーミング及び分析ベンダーと契約を締結する前に、ベンダーに対するデューデリジェンスを実施し、復処理者が開示及び承認され、かつ、同等の条件に拘束されることを確保します（GDPR第28条第2項及び第4項）。
- ☐ データ保護責任者の指定が必要かどうか（第37条）、また、計画されているデータの取扱い（生体認証による入場管理、大規模なファンプロファイリング、広範囲にわたるトラッキングなど）について、データ保護影響評価（第35条）が必要かどうかを確認します。
- ☐ 例えば、ダイレクトマーケティング又は分析について正当な利益（第6条第1項(f)）に依拠する場合、利益衡量テストを文書化します（正当な利益評価）。
- ☐ EU/EEA向けのサイト及びアプリにおいて、クッキー及びトラッキングに関するガバナンスを実施します。具体的には、同意管理プラットフォームの導入、同意記録の管理並びにクッキー、ピクセル、SDK及びアドテク業者に対する定期的な監査を行います。
- ☐ EU起源のデータについて、再移転を再確認し、補完的ルールを遵守しているようにします。

継続的ガバナンス

- GDPR第30条に基づき、取扱活動の記録を維持します。APPIには、この登録簿に相当する一般的な制度はありません。その代わりに、特定の記録、特に、第三者による個人データの提供及び取得に関する記録が必要となりますので、両方の書類を保管します。
- ファン及び加入者のデータについて、データ保存期間及び削除期間を設定し、適用します（記録保存の制限）。
- ファン向けの新しいシステム、アプリ及びイベントの展開において、データ保護バイデザイン（GDPR第25条）及び適切な技術的かつ組織的な安全管理措置（第32条－暗号化、アクセス制御、定期的なテスト）を構築します。
- チケット販売担当、ファンエンゲージメント担当、営業及びIT担当のスタッフに対し、ファンデータの取扱い、アクレディテーション／IDデータ、フィッシング及び侵害への対応について研修を行います。
- プログラムを定期的に、かつ、チャンネル、システム又は業者に重要な変更があった後はその都度、見直します。

11. 用語集

用語	意味
GDPR	EU一般データ保護規則（規則（EU）2016/679）
APPI	日本の個人情報の保護に関する法律
PPC	日本の個人情報保護委員会—APPIの執行機関
監督機関／DPA	GDPRを執行するEU／EEAのデータ保護機関（例：ドイツの各州データ保護機関、CNIL）。EU脱退以降、別途英国GDPRを執行する英国ICO。
管理者	個人データの取扱いの目的及び手段を決定する事業体
処理者	管理者に代わり、その指示に従って個人データを取り扱う事業体
データ主体	個人データが関係する、識別された又は識別可能な個人（本文書においては、ファン、加入者又はチケット保有者）

用語	意味
EU代理人（第27条）	ターゲティングを根拠としてGDPRが適用される場合に、EU域外の管理者が選任しなければならないEU／EEA域内に設立された代理人
十分性認定	EU域外の国の制度が十分な保護水準を提供していると認める旨のEUによる認定であり、追加的な保護措置なしにデータ移転を可能にするもの
補完的ルール	十分性認定に基づきEUから移転された個人データについて、APPIを補完するPPCのルール
チケット販売プラットフォーム／マーケットプレイス	チケット、コンテンツ又はサブスクリプションの掲載、販売、配信を代行する第三者プラットフォーム（例：Ticketmaster、SeatGeek、Eventbrite又はストリーミング／配信プラットフォーム）
チケット販売システム／CRM	チケット販売システム／顧客関係管理システム。チケット又はサブスクリプションの販売及びファン又は加入者データの管理に使用されるソフトウェア

渥美坂井法律事務所・外国法共同事業によるスポーツ、メディア及びエンターテインメント事業者向けサポート

スポーツ、メディア及びエンターテインメント業界において、データ保護は単なるコンプライアンス上の課題にとどまりません。GDPR及びAPPIに関する問題は、チーム、イベント、プラットフォーム又はコンテンツプロパティが、どのように所有、運営、ブランディング、マーケティングされ、さらにチケット販売、放送、スポンサーシップ及びファン管理の各システムとどのように連携しているかという点に直接起因しています。したがって、法的分析は、プライバシー通知だけでなく、その根底にある事業構造によっても異なります。具体的には、権利の保有者は誰か、イベントやプラットフォームの運営主体は誰か、チケット販売や配信の流れを管理しているのは誰か、どのプラットフォームやCRMシステムが使用されているか、ファンやタレントのデータを取得するのは誰か、またマーケティングやイベント後のコミュニケーションがどのように行われているか、といった点です。

渥美坂井法律事務所・外国法共同事業は、フランクフルトにおけるEU／ドイツのデータ保護に関する専門知識と、東京を拠点とするスポーツ、メディア及びエンターテインメント法務を融合させているため、これらの問題について適切な助言を提供できる体制が整っています。これにより、権利保有者、連盟、クラブ、プロモーター、放送局、代理店及びプラットフォームが実際に活動している商業的な文脈において、GDPR及びAPPIの遵守に対応することが可能となります。

特に、当事務所では以下の事項についてクライアントを支援しています。

- 日本のスポーツ、メディア、エンターテインメント事業者に対して、GDPRが適用されるか否か、またその適用範囲の評価（直接販売及びプラットフォームを通じたチケット販売チャネル、ストリーミング及び放送並びにEUに拠点を有するグループ構造を含みます。）
- GDPRに準拠したプライバシー通知、同意文言及びチケット販売／登録フローに関する開示事項の作成及び既存のAPPIポリシーとの整合
- チケット販売マーケットプレイス、ストリーミング及び放送プラットフォーム、CRM及びファンエンゲージメントシステム、決済サービスプロバイダー、マーケティングツール並びに委託されたIT業者について、データ保護上の影響の検討
- スポンサーシップ、ライセンシング、放送、フランチャイズ、ブランドライセンス、イベント運営及びプラットフォームに関する取決めにおけるデータ保護上の責任の割当て
- GDPR要件とAPPI及び日本特有の考慮事項との整合（必要に応じて、認定、アンチ・ドーピング及び本人確認書類データを含みます。）
- ファン、加入者、アスリート又はタレントのデータに関するインシデントに対する、侵害対応手順、内部エスカレーションプロトコル及び通知業務フローの策定
- GDPR第27条に基づき、EU代理人の選任が必要か否かの評価及び適切な代理人取り決めの実施支援
- デューデリジェンス、取引構造の策定及びクローリング後の統合におけるGDPR／APPIに関する問題の特定による、取引及び大規模プロジェクトの支援

渥美坂井法律事務所・外国法共同事業は、スポーツ、メディア、エンターテインメント法務の専門部門を有しています。本部門は、スポーツ、メディア及びエンターテインメントの各分野のクライアントに対し、放送、広告及びマーケティング、ブランド及び権利保護、スポンサーシップ、大規

模イベント、スポーツガバナンス及びインテグリティ並びにM&A、合併事業及びプライベート・エクイティに関する助言を行っています。

当チームは、シニアパートナーのイアン・S・スコット氏が率いています。同氏は、クイーンズランド州で弁護士資格を取得し、日本においても外国法事務弁護士として登録されているオーストラリアの弁護士であり、スポーツ、メディア及びエンターテインメント分野において25年以上の実務経験を有しています。同氏はCAS（国際スポーツ仲裁裁判所）の仲裁人であり、スポーツ法並びにメディア及びエンターテインメントの分野でBest Lawyers Japanに選出されており、また、日本のスポーツ法分野においてThe Legal 500 Hall of Fameに選出されました。

この組み合わせにより、当事務所は、権利保有者、運営事業者、ブランド所有者及び投資家に対し、単独のコンプライアンス対策としてではなく、スポーツ、メディア又はエンターテインメント事業における広範な法的及び商業的枠組みの一環として、データ保護に関する助言を提供することが可能となります。スポンサーシップ、放送、フランチャイズ、プラットフォーム又は取引に関する文書に、ファン、加入者、アスリート又はタレントに関するデータの問題が盛り込まれている場合、かかる助言はクライアントにとって特に重要となります。

執筆者

外国法事務弁護士（オーストラリア クィンズランド州法）

イアン・S・スコット（シニアパートナー、第二東京弁護士会）

Email : ian.scott@aplaw.jp

ドイツ連邦共和国弁護士* フランク・ベッカー

（Atsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater** マネージングパートナー）

Email : frank.becker@aplaw.de

ドイツ連邦共和国弁護士* アンドレス・マルティン-エーレルス博士

（Atsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater** パートナー）

Email : andres.martin-ehlers@aplaw.de

弁護士 野邊健太（パートナー、第一東京弁護士会）

Email: kenta.nobe@aplaw.jp

*但し、日本における外国法事務弁護士の登録はない。

**ドイツ連邦共和国における法務・税務サービス提供法人

お問い合わせ先

本ニュースレターに関する一般的なお問い合わせは、下記までご連絡ください。

渥美坂井法律事務所・外国法共同事業

スポーツ、メディア&エンターテインメントプラクティスチーム

Email: cpg_sports_entertainment@aplaw.jp

当事務所のニュースレターをご希望の方はニュースレター配信申込フォームよりお手続きをお願いいたします。

また、バックナンバーはこちらよりご覧いただけます。

このニュースレターは、現行の又は予想される規制を網羅的に解説したものではなく、著者が重要だと考える部分に限って、その概要を記載したものです。このニュースレターに記載されている意見は著者個人の意見であり、渥美坂井法律事務所・外国法共同事業（「渥美坂井」）の見解を示すものではありません。著者は明白な誤りを避けるよう合理的な努力は行いましたが、著者も渥美坂井もこのニュースレターの正確性を保証するものではありません。著者も渥美坂井も読者がこのニュースレターに依拠することによって生じる損害を賠償する責任を負いません。取引を行う場合には、このニュースレターに依拠せずに渥美坂井の弁護士にご相談ください。

東京オフィス Tokyo Head Office 〒100-0011 東京都千代田区 内幸町 2-2-2 富国生命ビル（総合受付：16F） 	大阪提携オフィス Osaka Affiliate Office （A&S 大阪法律事務所） 〒530-0005 大阪府大阪市北区 中之島 2-3-18 中之島フェスティバルタワー16階	福岡提携オフィス Fukuoka Affiliate Office （A&S 福岡法律事務所） 〒810-0001 福岡県福岡市中央区天神 2丁目 12-1 天神ビル 10階 
ニューヨーク提携オフィス New York Affiliate Office 1120 Avenue of the Americas, 4th Floor New York, New York 10036 	ロンドンオフィス London Office 85 Gresham Street, London EC2V 7NQ, United Kingdom 	フランクフルト提携オフィス Frankfurt Affiliate Office Barckhausstraße 1 (8th Floor), 60325 Frankfurt am Main, Germany 
ブリュッセルオフィス Brussels Office CBR Building, Chaussée de la Hulpe 185, 1170, Brussels, Belgium 	ホーチミンオフィス Ho Chi Minh Office 10F, The NEXUS building, 3A-3B Ton Duc Thang Street, Sai Gon Ward, Ho Chi Minh City, Vietnam 	