41st ANNUAL IBA/IFA JOINT CONFERENCE
2026

NEWS FROM AROUND THE WORLD: AUSTRALIA

Vanessa Pareja Lerner
Dias Carneiro
Brazil

Brazilian Data Protection for Franchise Operations

ANPD Resolutions and the Digital ECA

IBA / IFA World Franchise Conference 2026

This document examines two regulatory layers that any foreign franchisor operating in Brazil must address: the recent resolutions issued by the Agência Nacional de Proteção de Dados – "ANPD"), which have materially altered the enforcement of Federal Law No. 13,709/2018 (General Data Protection Law - "LGPD"), and Federal Law No. 15,211/2025 (Online Minor Protection Act - "Digital ECA"), a separate legal framework with independent obligation enforcement mechanisms, particularly relevant to consumer-facing franchise operations.

These regimes are cumulative, not interchangeable. Franchisors whose Brazilian operations involve minors, including education networks, casual dining brands with children's areas, and gaming or entertainment business, must comply simultaneously with the LGPD baseline requirements and the additional obligations imposed by the Digital ECA. Treating both regimes as a single compliance framework creates regulatory blind spots and increases exposure to enforcement risk.

The ANPD Resolutions Layer

Between 2022 and 2024, the ANPD issued four resolutions that effectively transformed the LGPD from a principle-based statute into an operational regulatory framework. Each of these instruments directly impacts franchise structures, including the allocation of data controllership, cross-border data flows, incident response obligations, and eligibility for differentiated compliance regimes.

1.1 Resolution No. 19/2024 — International Data Transfers

Scope of change. International transfers now require the concurrent presence of a valid legal basis for processing and an appropriate transfer mechanism. Where transfers are not directed to jurisdictions recognized by the ANPD as providing an adequate level of data protection, controllers must adopt one of the following mechanisms: standard contractual clauses (as set forth in Annex II of Resolution No. 19/2024); specific contractual clauses; or binding corporate rules.

Specific contractual clauses and binding corporate rules are subject to prior ANPD approval. Standard contractual clauses are not but must be adopted in their entirety. Additional substantive requirements apply.

The controller must formally assess and document the data protection framework of the destination country. Data subjects must be clearly informed of the international transfer through a Portuguese-language notice published on the controller's Brazil-facing website. In addition, the controller must be able to demonstrate the validity and adequacy of the chosen transfer mechanism on a case-by-case basis.

The transitional period for incorporating standard contractual clauses into existing agreements expired on August 23, 2025.

Why is this relevant to franchises? A typical franchise structure involves at least two distinct cross-border data flows. The first occurs between the franchisor and the master franchisee,

encompassing brand standards, customer-experience analytics, loyalty program data, and franchisee performance metrics transferred from the Brazilian operation to headquarters. The second consists of a re-transfer flow, whereby the master franchisee, after collecting personal data in Brazil, transmits such data to the franchisor as part of global CRM, marketing automation, or business intelligence systems. Both flows qualify as international data transfers under Brazilian law and therefore require a valid transfer mechanism, including, where applicable, the Brazilian SCCs.

Compliance gap. Foreign franchisors typically rely on one of two instruments to governs theses transfers: (i) the SCCs incorporated into global GDPR compliance framework, often executed prior to entry into the Brazilian market; or (ii) a data protection provisions embedded in the Master Franchise Agreement, modeled on GDPR concepts. Neither approach, in isolation, satisfies the requirements of Resolution No. 19/2024. GDPR-based clauses do not constitute Brazilian SCCs, and the Resolution No. 19/2024 requires that the official text of the SCC be incorporated in full and without modification.

Any deviation from the approved SCCs, or the adoption of alternative mechanisms such as bespoke data-sharing agreements, is subject to prior approval by the ANPD and is only permitted in exceptional, duly justified circumstances. In practice, this approval process is incompatible with the timelines of most franchise rollouts, creating a material compliance risk if not addressed at the structuring stage.

Implication for the franchise agreement. Parties to an international franchise structure involving Brazil will, in most cases, need to execute Brazilian SCCs bilaterally for each segment of the data flow, including re-transfer scenarios in which personal data collected in Brazil is routed back to the franchisor's headquarters. Network-wide implementation based on a single set of SCCs executed at the master franchise level, on the assumption that sub-franchisees are automatically covered, do not meet the requirements of Resolution No. 19/2024. Each sub-franchisee that exports personal data, whether to a global POS provider, an offshore payment processor, or an international loyalty platform, must operate under its own valid transfer mechanism.

Resolution No. 19/2024 provided for a limited re-importation carve-out, under which personal data originally collected outside Brazil and transferred back exclusively to its jurisdictions of origin may fall outside the scope of the LGPD. his exception is narrowly construed and applies only where: (i) the destination jurisdiction has been formally recognized by the ANPD as providing an adequate level of data protection; and (ii) the applicable foreign legal framework governs the processing activity. In all other cases, data flows returning to headquarters remain subject to the international transfer requirements established by Resolution No. 19/2024.

The European Union adequacy decision. On January 26, 2026, the ANPD issued Resolution No. 32/2026, formally recognizing the European Union, the Island, Liechtenstein and Norway as providing an adequate level of data protection. As a result, transfers of personal data from Brazil to EU-based jurisdictions may rely on this adequacy determination, rather than on standard contractual clauses (SCCs), subject to any conditions established in the decision itself.

The scope of the adequacy recognition is expressly limited. It does extend to the United States, the United Kingdom, or any other non-EU jurisdiction. Transfers to these destinations must continue to rely on alternative transfer mechanism, including SCCs, BCRs, or specific clauses approved by the ANPD on a case-by-case basis.

In practical terms, the impact of the adequacy decision is confined to the European segment of a franchise's data flows.

Data transfers directed to the United States, where most global CRM and loyalty infrastructures are typically hosted, remain subject to the SCC framework, preserving the need for a structured and compliant transfer architecture.

1.2 Resolution No. 18/2024 — Effective Performance of the DPO

Scope of change. Resolution No. 18/2024 shifts the regulatory focus from a formal designation to demonstrable, effective performance of the DPO. A nominal appointment, such as listing the DPO in a privacy policy, is no longer sufficient. The designation must be formalized through a written, dated, and executed instrument that clearly defines the role and its scope. A substitute must also be formally appointed to cover absences, impediments, or vacancies.

Resolution No. 18/2024 further clarifies that the DPO function may be assigned to a legal entity, providing a basis for DPO-as-a-service models. Designation by a processor remains optional but is recognized as good governance practice for purposes of regulatory assessment and potential sanctions. In evaluating compliance, the ANPD will assess whether the DPO operates with technical autonomy, maintains direct access to senior management, has documented resources proportionate to the volume and risk profile of processing activities, and is effectively integrated into data protection decision-making, including incident response, contract review, transfer architecture, and data subject request handling.)

Why this matters for franchise structures. Foreign franchisors typically designate a central privacy lead at headquarters, such as a Chief Privacy Officer in the United States, a DPO in the European Union, or reginal privacy counsel in Asia. This individual is often referenced in global privacy notices and in data-sharing arrangements with master franchisee. However, under Resolution No. 18/2024, such designation will not, in most cases, satisfy the requirements for the Brazilian operation.

In practice, these individuals lack the necessary legal attribution to act as DPOs in Brazil, are not publicly identified in Brazil-facing disclosures, may not operate in Portuguese, and are typically not embedded in the day-to-day compliance dynamics of the Brazilian franchise network. As a result, they are unlikely to meet the "effective performance" standard established by Resolution No. 18/2024.

Core requirements. Controllers must disclose and maintain up-to-date information regarding the DPO's identity and contact details, ensuring publication in a prominent and easily accessible location on the Brazilian-facing website. A DPO referenced solely in internal documentation or in a global, English-language privacy notice does not meet this requirement.

Contractual arrangements must clearly allocate the DPO function across the franchise network, define autonomy and resource allocation, and establish formal communication channels for interaction with the ANPD. The Resolution also requires the controller to identify and mitigate potential conflicts of interest affecting the DPO function, whether through reassignment of duties, replacement of the DPO, or implementation of oversight mechanisms.

Failure to demonstrate these elements in a regulatory review may result in a finding that the controller is not compliant with LGPD requirements regarding the DPO function.

1.3 Resolution No. 15/2024 — Security Incident Notification

Scope of change. Resolution No. 15/2024 translated Article 48 of the LGPD into a structured and enforceable procedural framework. The notification trigger is cumulative: the incident must both (i) significantly impact the interests and fundamental rights of data subjects and (ii) involve at least one of a the following categories: sensitive data; data relating to children, adolescents, or the elderly; financial data; authentication credentials; data protected by legal, judicial, or professional confidentiality; or data processed at large scale.

The notification deadline is three business days, counted from the controller's awareness that personal data has been affected. The deadline doubles for small-scale agents qualifying under Resolution No. 02/2022. Supplementary information may be submitted within twenty business days. Notification must be filed through the official electronic system and submitted by the controller through the DPO, with evidence of the underlying legal or functional appointment, or by a duly authorized legal representative. Submission lacking supporting documentation may trigger a separate investigative procedure by the ANPD.

Article 10 further requires controllers to maintain comprehensive records of all security incidents, including those not reported, together with the documented rationale for non-notification, for at least five years.

Why this matters for franchise structures. The three-business-day deadline is operationally unworkable in most franchise networks absent contractual alignment. Incidents typically arise at the franchisee level, including compromised local POS systems, phishing attacks targeting franchisee personnel, or misconfigured loyalty or customer interface systems. Information flows upstream: the franchisee becomes aware first, followed by the master franchisee, and only subsequently the franchisor. By the time the designated controller becomes aware, the statutory deadline may already be running or have expired, creating immediate compliance exposure.

Contractual allocation. Franchise agreements must impose a binding internal escalation obligation, requiring each franchisee to notify the controller of record within twenty-four hours of becoming aware of any event that may qualify as a security incident. The same provision must require the franchisee to promptly provide all information necessary for the controller to conduct the risk assessment mandated by Resolution No. 15/2024, inf a format capable of being documented and produced before the ANPD if subsequently reviewed.

Franchisees must also be contractually bound to support the controller’s recordkeeping obligations, including for incidents that do not meet the notification threshold, and to assist in evidencing the legal functional relationship when notifications are submitted through the network’s DPO.

International incidents. In cross-border scenarios involving Brazil, two considerations are critical. First, when notifying an incident to the ANPD, the controller must disclose whether the same incident has been reported to foreign supervisory authorities. Failure to notify in Brazil within the applicable timeframe, even where notification obligations have been met in other jurisdictions, may be interpreted as a lack of diligence toward Brazilian data subjects.

Second, the ANPD has established cooperation agreements with multiple foreign regulators, including authorities within the EU and other jurisdictions. As a result, information shared with the ANPD may be exchanged with foreign authorities, and controllers should proceed with the assumption that incident-related information may circulate across regulatory frameworks.

1.4 Resolution No. 02/2022 — Small-Scale Processing Agents

Scope of application. Resolution No. 02/2022, as subsequently amended by Resolution No. 15/2024, establishes a differentiated compliance regime for small-scale processing agents, including microenterprises, small-sized companies, and startups, as defined in Resolution No. 02/2022. The regime provided procedural flexibility, including extended deadlines for certain obligations (notably, the doubled incident-notification deadline), simplified records of processing activities, and reduced formalities in areas such as DPO designation and governance documentation.

The regime does not constitute an exemption from the LGPD. Small-scale agents remain fully subject to the law's principles, the requirement for a valid legal basis, and civil liability for damages. Even where the differentiated regime applies, the adoption of governance measures and the formal designation of a DPO under Resolution No. 18/2024 remain relevant for purposes of regulatory assessment and sanctioning by the ANPD.

The franchise qualification constraint. The regime appears compatible with many Brazilian franchisees, particularly single-unit operators operating below the statutory revenue threshold, with localized managements and limited data processing activities. In practice, however, two structural features of franchise network frequently preclude qualification or make it difficult to sustain.

First, the regime does not apply to entities that are part of an economic group. Depending on how the franchise relationship is structured and interpreted, operational and contractual integration with a master franchisee or the franchisor may be sufficient to characterize group affiliation, thereby disqualifying the franchisee.

Second, the regime excluded processing activities classified as high-risk. Franchisee engaged in large-scale customer profiling, processing of children's data, or biometric processing fall outside the regime, irrespective of their size or revenue profile.

Practical implication. The handover package given to new franchisees should not presume eligibility for small-scale regime. A formal qualification assessment should be conducted at the outset, supported by documentation addressing revenue threshold, corporate structure, scope of processing activities, and risk classification.

Where eligibility is confirmed, the franchisee may benefit from meaningful regulatory flexibility. However, the burden of demonstrating qualification rest with the franchisee, not with the regulator. Where eligibility is uncertain or cannot be substantiated, the franchisee should be integrated into the full LGPD compliance framework.

Size is not a safe harbor. The first administrative fine imposed by the ANPD on a private entity targeted a microenterprise. The statutory cap of two percent of gross revenue was applied at its maximum, demonstrating that the proportional nature of the cap does not mitigate enforcement exposure at smaller scales.

Part II — The Digital ECA Layer

2.1 What the Digital ECA is, and why it is not the LGPD

The statute. The Digital ECA, regulated by Decree No. 12,880/2026, establishes Brazil's legal framework for the digital protection of children and adolescents (individual under eighteen years of age). It entered into force on March 17, 2026, and is enforced through multiple channels, including administrative, consumer protection, civil and criminal mechanisms. It operates as an autonomous statute, with its own scope, obligations, and sanctions, and its requirements apply

cumulatively with, rather than a substitute for = the LGPD baseline. The ANPD has also been appointed as the authority responsible for regulating and enforcing the Digital ECA, thereby consolidation oversight across both regimes.

The scope test. The statute applies to any information technology service that minors are likely to access. The relevant test is not intent based: applicability does not depend on whether the service is expressly directed at children or adolescents. Instead, it turns on likelihood of access, assessed based on factors such as the service's appeal to minors, the probability of use, ease of access, and the risk profile of the content or interaction offered.

Franchise models that do not actively target minors may nonetheless fall within scope where they are objectively attractive to younger audiences, including casual dining brands, entertainment venues, ice cream chains, and retail concepts involving branded merchandise.

The duty framework. The core duties are: age assurance and age verification through an effective, auditable, and reliable mechanism, with self-declaration expressly prohibited (including for the selling of products online); account linking for users under sixteen to a parent or guardian's account; functional parental control tools; suspension of advertising targeting and behavioral profiling for users under eighteen; removal of loot boxes from games likely to be accessed by minors; structured content moderation with non-anonymous reporting channels; biannual transparency reports for platforms above one million registered minor users; and, for foreign providers, the appointment of a legal representative in Brazil with authority to receive notifications, interact with authorities, and respond for compliance.

2.2 Where the Digital ECA lands in franchise verticals

The probable-access standard extends the statute's reach beyond intuitively child-focused sectors. A wide range of franchise models may fall within scope based on objective user behavior patterns rather than declared market positioning. While the intensity of obligations varies according to the risk profile and the nature of the service, the threshold inquiry remains constant: are minors likely to access or use the service?

Food service with children's areas, kids' clubs, and birthday programs

Casual dining and quick-service franchises models that operate kids' clubs, birthday programs, branded loyalty application, or in-store interactive features such as tablets and arcade systems all within the scope of the probable-access test. The risk profile is moderate, as the categories of personal data processed are typically limited to identification data (name, age range), contact details of the responsible adult, dietary information, and photographs captured during on-site activities, with relatively constrained levels of digital interaction.

The primary compliance pressure points arise in two areas. First, loyalty and mobile applications must incorporate compliant age assurance mechanism, must not engage in behavioral profiling of minors, and must implement parental control functionalities for users under sixteen. Second, in-store photography practices and related social media use must be restructured to comply with age-sensitive consent and processing requirements, ensuring that collection, storage, and publication of images involving minors are properly documented and legally supported.

Education franchises

Education franchises, including language schools, supplemental education providers, early childhood programs, and exam preparation services, are clearly within scope and operate at the higher end of the risk spectrum. Processing typically includes academic performance data,

attendance records, behavioral assessments, biometric data for access control, and communications flows between the institution, the student, and the parent or the guardian.

The Digital ECA applies as an additional regulatory layer over an LGPD framework that already imposes heightened protection standards for children's data. Risk is concentrated in three areas. First, the legal basis for processing, including the application of the best-interest standard, the structuring of parental consent mechanisms, and the maintenance of supporting documentation. Second, the implementation of age assurance and account-linking architectures within educational platforms, particularly for users under sixteen. Third, the distinction between permissible educational analytics and prohibited behavioral profiling, which requires clear technical and governance boundaries to avoid regulatory breach. Entertainment venues, gaming centers, and esports cafés

Family entertainment centers, arcade franchises, gaming cafés, and esports venues, whether operating as standalone units or embedded within retail or food service environments, fall at the highest end of the Digital ECA risk matrix. These models typically combine mobile applications, ranking and leaderboard systems, in-game purchases, voice communication features, and user-to-user interaction, thereby triggering the full scope of statutory obligations.

Compliance requirements include robust age assurance mechanisms, implementation of parental control systems, prohibition of targeted advertising to minors, and the removal of loot box mechanics in games likely to be accessed by underage users. In addition, operators must implement structured content moderation frameworks supported by identifiable reporting channels, ensuring traceability and responsiveness.

Esports formats introduce an additional contractual and governance layer. Participation of minors in tournaments, leagues, or team-based structures requires formal parental authorization mechanisms aligned with the statute's account-linking requirements for users under sixteen, as well as clear allocation of responsibility across operators, sponsors, and platform providers.

Retail of children's products and family retail

Retail operations involving toys, children's apparel, baby and infant products, and family-oriented department store concepts fall within scope where their digital interfaces — including e-commerce platforms, loyalty applications, and in-store interactive systems — are likely to be accessed by minors. The risk profile is moderate, but not negligible.

Key compliance pressure points arise in three areas. First, advertising and recommendation systems must not engage in behavioral profiling of minors, requiring segmentation logic capable of distinguishing underage users and suppressing targeted advertising functionalities. Second, customer service and complaint channels must be structured to accommodate identifiable (non-anonymous) reporting where minors are involved, consistent with the statute's transparency and accountability requirements. Third, loyalty program architectures must clearly differentiate between parent or guardian accounts and minor user accounts, ensuring proper account-linking mechanisms for users under sixteen.

2.3 Age assurance is not age verification

The statute draws a clear distinction between age assurance and age verification, and the compliance approach must reflect that distinction.

Age assurance refers to a calibrated mechanism designed to ensure that the service environment, content, and functionalities are appropriate to the user's age group, particularly where content is restricted or unsuitable for certain age brackets but not inherently unlawful. It

is risk-based and proportional, focusing on aligning the user experience with expected age categories.

Age verification, by contrast, involves deterministic confirmation of a user's specific age, typically required where access to certain content or transactions is legally prohibited for minors, including alcohol purchases, gambling mechanics such as loot boxes, or adult content.

For most franchise models, age assurance will be the relevant standard, while age verification will apply only in more limited, high-risk scenarios.

Self-declaration, as a standalone mechanism, is no longer compliant in any context. However, the ANPD has not yet issued detailed technical parameters defining acceptable age assurance methodologies, creating a degree of regulatory uncertainty. In practice, this requires controllers to adopt defensible, risk-based solutions capable of demonstrating effectiveness, auditability, and proportionality until further guidance is issued.

2.4 The enforcement architecture

A single violation under the Digital ECA may trigger multiple parallel enforcement tracks. The ANPD exercises jurisdiction over both data protection and Digital ECA compliance, with authority to impose administrative sanctions under each framework. Consumer protection authorities, including Procon at the state level and Secretaria Nacional do Consumidor - SENACON at the federal level, act on consumer law grounds, including misleading practices, abusive contractual terms, and unlawful advertising directed at minors. The Public Prosecutor's Office holds independent standing to pursue collective redress, and, where applicable, criminal enforcement. Parallel individual and collective civil actions brought by associations or consumers may proceed concurrently.

These enforcement channels operate independently and are not procedurally coordinated. As a result, a single instance of non-compliance may generate simultaneous proceedings across multiple forums, each applying distinct legal standards, procedural rules, and remedies.

The franchise allocation problem.

Franchise structures must address enforcement exposure contractually. A single network-wide compliance failure, such as deployment of a uniform loyalty application without a compliant age assurance mechanism, may trigger parallel proceedings across regulatory, consumer, civil, and potentially criminal jurisdictions.

Default allocation assumptions are insufficient. The conventional approach, under which franchisees bear responsibility for consumer-facing liabilities while franchisors retain responsibility for data protection compliance, does not hold where control over the relevant practice is functionally divided. In many cases, the franchisor controls the digital interface, while the franchisee manages the direct customer relationship, creating overlapping exposure.

The franchise agreement must therefore establish a clear and operational allocation of responsibility, aligned with actual decision-making authority over the relevant activity or system. This allocation must also include mandatory cooperation obligations, ensuring that parties coordinate defense strategies, share information, and support remediation efforts across parallel proceedings.

Absent explicit allocation, the network is exposed to fragmented defenses, inconsistent positions across jurisdictions, and increased regulatory and litigation risk.

A Thirty-Day Operational Grid

The framework below maps key regulatory obligations to the contractual instruments within a franchise network and identifies the minimum operational steps required for initial compliance. It is not a substitute for a comprehensive legal assessment; but rather a structured first-pass tool for foreign franchise counsel preparing a Brazilian rollout or reviewing an existing structure.

Cross-border data architecture

- **Replace, do not supplement.** Brazilian standard contractual clauses (SCCs) must be executed bilaterally for each segment of the international data flow, including re-transfer scenarios from the master franchisee back to headquarters. Pre-existing GDPR-based clauses do not satisfy Resolution No. 19/2024.
- **Document the destination country assessment.** The data importer's evaluation of the data protection framework in the destination jurisdiction must be maintained as a standalone, auditable record, rather than embedded as a contractual recital within the SCCs.
- **Map all transfers.** Compliance must be demonstrable on a transfer-by-transfer basis. A single SCC executed at the master franchise level does not extend to sub-franchisee transfers involving global service providers or platforms. The data-sharing framework
- **Align legal roles with operational reality.** The ANPD evaluates actual decision-making authority over data processing, rather than formal contractual labels. Controller, processor, and joint controller roles must be reassessed and documented based on how data flows and decisions occur in practice across the network.
- **Address LGPD-specific obligations.** GDPR-based contractual templates do not fully capture LGPD requirements. All data-sharing provisions must be reviewed and adapted to ensure compliance with Brazilian legal standards, including local regulatory expectations.

The DPO function

- **Formalize the designation.** The DPO responsible for Brazilian operations must be formally appointed through a written, dated, and executed instrument, clearly defining scope and responsibilities.
- **Demonstrate effective performance.** Compliance is measured by function, not title. The DPO must have documented resources, operational autonomy, direct access to senior management, and integration into decision-making processes involving personal data. The incident response protocol
- **Implement franchisee-to-controller escalation. E**ach franchisee must be contractually bound to notify the controller of any potential security incident within twenty-four hours of becoming aware of it. Without this internal escalation layer, compliance with the statutory deadline is operationally unachievable.
- **Align with Brazilian timing requirements.** The notification deadline is three business days from the controller's awareness, not seventy-two calendar hours. The official notification form of the ANPD and its required content establish the minimum reporting threshold.
- **Maintain comprehensive incident records.** Controllers must document all incidents, including those not reported, together with the justification for non-notification, and retain such records for the applicable statutory period.

The Digital ECA overlay

- **Apply the probable-access test to every digital interface.** This includes loyalty applications, learning platforms, in-store tablets, esports systems, e-commerce platforms, and interactive retail displays. The relevant inquiry is whether minors are likely to access or use the service, not whether the network actively targets them.
- **Calibrate age assurance to the specific vertical and use case.** Different interfaces within the same franchise network may require distinct age assurance mechanisms, depending on risk and functionality. Self-declaration, as a standalone method, is no longer compliant.
- **Prohibit targeted advertising and behavioral profiling for users under eighteen.** This restriction extends to recommendation engines in retail, loyalty platforms in food service, and content personalization systems in education and entertainment environments.
- **Remove loot boxes and analogous monetization mechanisms.** This applies to any game or interactive system likely to be accessed by minors. A conservative interpretation includes any randomized reward mechanism involving payment, including virtual or in-game currency, where the specific outcome is not disclosed prior to the transaction.
- **Appoint a legal representative in Brazil.** This is mandatory for foreign service providers under the Digital ECA and is independently reinforced by binding precedent from the Supreme Federal Court of Brazil.
- **Allocate enforcement** responsibility across all regulatory channels. The franchise agreement must explicitly define responsibility for defense and remediation across the ANPD, the Ministry of Justice and Public Security (MJSP), consumer protection authorities, and the Public Prosecutor's Office, as well as parallel civil proceedings. This allocation must reflect actual control over the relevant practice or system, rather than relying on a default division between franchisor and franchisee.