Privacy Laws and the Franchise Relationship

Establishing clear legal and operational boundaries in the franchisor/franchisee relationship has always been essential. Today, with the growing complexity of data privacy and security regulations, it's more critical than ever for both franchisors and franchisees to address these issues proactively. Personal information, whether related to customers, employees, or vendors, is routinely exchanged in franchise systems. Ensuring compliance with applicable privacy laws through franchise agreements, operations manuals, and public-facing privacy policies is vital to mitigate legal and reputational risks.

Evolving Data Privacy Laws

Privacy regulations are expanding rapidly across the U.S., with over 20 states having enacted comprehensive privacy laws. Additionally, international laws like the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) impose specific contractual requirements when personal data is exchanged.

For example, under the CCPA, if a franchise agreement lacks certain language, a franchisor may inadvertently be deemed to be "selling" personal data to franchisees (or vice versa), thereby triggering consumer opt-out rights that simply won't work for the business. Even if a franchise system is not currently subject to these laws, establishing a robust privacy framework now will ease future compliance as thresholds are met or new laws come into effect.

Defining Personal Information in the Franchise Context

Franchise agreements should clearly define what constitutes personal information and address the data exchanged. Franchisees may collect personal data directly from employees and customers at their locations but only give franchisors access to customer data, while franchisors may gather customer data through centralized systems or mobile apps. Understanding these data flows is essential to determine legal responsibilities.

Clarifying Legal Roles

Once data flows are mapped, the franchise agreement or operations manual should specify which party acts as the "controller" or the entity that determines how and why personal data is processed and which party serves as the "processor" or "service provider," acting on behalf of the controller.

In many cases, franchisors will want to retain control over customer data, making them the controller and the franchisee the processor. In employment scenarios, franchisees typically hire their own staff, but if franchisors use employee data for their own purposes, they may also be considered controllers. These distinctions must be carefully documented to ensure compliance with privacy laws.

Website Privacy Policies and Advertising Technology

Franchisors often host websites that include franchisee-specific location pages. These websites must include a privacy policy that accurately reflects the franchise relationship. Failure to do so can expose the franchisor to liability depending on how the policy addresses the franchisee-franchisor relationship.

Moreover, the franchise agreement or operations manual may be more prescriptive and restrict franchisees from implementing advertising technologies such as tracking pixels or behavioral analytics tools on their location pages except in accordance with the privacy policy. These restrictions help maintain consistency and compliance across the franchise system, as well as mitigate the risk of plaintiff lawsuits regarding such tracking technologies.

Data Sharing, Security, and Breach Response

Franchise agreements or the operations manual should limit the processor's ability to share personal data, except with approved service providers bound by similar obligations. Both parties must implement strong cybersecurity measures and clearly define responsibilities for breach response, including notification procedures and legal compliance.

Consequences of Non-Compliance

The risks of failing to address privacy obligations are significant. In the EU, fines can reach €20 million or 4% of global revenue, whichever is higher. In the U.S., enforcement actions by state attorneys general, the California Privacy Protection Agency (CalPrivacy), and the Federal Trade Commission (FTC) have resulted in even higher penalties.

Beyond financial consequences, data breaches can severely damage a franchisor's reputation. Customers may lose trust and stop patronizing affected locations, leading to long-term revenue loss and brand erosion.

Conclusion

As privacy laws continue to evolve, franchisors and franchisees must collaborate to ensure franchise agreements, operations manuals, and privacy policies reflect current legal standards and best practices. Leveraging the operations manual to implement updates can streamline compliance across the system.

By proactively addressing data privacy, franchise systems can reduce legal exposure, protect their brand, and build a resilient foundation for future compliance.

For more information, contact

Chiara Portner
Chiara.Portner@lathropgpm.com
650.804.7672