wiley

NEWSLETTER

Protect Your Customer Data: An Overview of GDPR Compliance

June 12, 2018

Franchise Watch

In most franchise relationships, data is crucial, and the ability to collect and share data is at the heart of the franchise relationship. However, the new European Union (EU) privacy regulation – the General Data Protection Regulation (GDPR) – which took effect May 25, 2018, fundamentally changes how franchisors and franchisees with connections to the EU must handle data.

When is GDPR a factor in your franchise relationship? First, you need to determine if GDPR applies to your business. If either the franchisor or franchisee is located in the EU, offers goods and/or services to individuals in the EU, or monitors (tracks) individuals in the EU—including monitoring through common online tools such as tracking cookies, GDPR requirements *may* apply. The breadth of this regulation's scope means that many U.S.-based businesses are now subject to its requirements.

What are the most relevant compliance considerations for franchisors or franchisees that are subject to GDPR? GDPR is a broad and complex regulation. Working through the following considerations with your franchisees will be key, and will help you identify any weak spots in your compliance plan.

- Determine what data you have and what data you want to collect in the future. If that data includes personal data from an individual in the EU, you must implement specific safeguards. Be aware – the definition of personal data in the EU is broader than that in the United States. Personal Data can be generally defined as information that directly (name, address, email,

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

identity number) or indirectly (device information, IP address) identifies a person.

- If you are collecting any sensitive data—which includes among other things, health, race, ethnicity, information about political opinions, trade union membership—perhaps from employees, franchisees, or customers based in the EU, be careful. The processing of sensitive data requires extra safeguards and specific types of detailed consent.
- If you no longer need the personal data you have collected, get rid of it. Only collect the data you specifically need and only keep it for as long as needed to provide the service or product. For example, if a customer closes their account, consider whether you still need their personal data or whether it could be anonymized or deleted.
- Evaluate whether you control or process the personal data—or perhaps you do both. Both controllers and processors of data are subject to GDPR, but their responsibilities and obligations differ. Data controllers are the "decision-makers;" they decide what data to collect and what to do with it. Data processors follow the directions of the controller in processing (collecting, using, storing) the data. Data controllers must have a contract with data processors that provides instructions on how the personal data should be processed. Consider whether and how the franchisor and franchisee are sharing data and determine which party is the controller and which is the processor (or whether they share those roles), then document each party's responsibilities with regard to the data.
- Ensure you have a lawful basis to collect and use data. GDPR recognizes several lawful bases for data processing, including consent, contractual, legal obligation, and legitimate interest—the key is that you have to have at least one. If your lawful basis is the customer's consent, the customer notice must be clear, specific, and transparent. Consent cannot be an "opt-out" procedure, it must be "opt-in."
- Take time to review the structure of your internal data processing and protection policies. Create an internal policy that identifies how you will handle and protect data. Identify who within the organization is responsible for each element of compliance.
- Check your data security. Make sure you have a system in place to guard against cyber-attacks and breaches. Review your data breach notification procedures to ensure you have a plan in case of a breach. GDPR requires that you notify the relevant EU authority within 72 hours of a detected breach.
- Confirm that you can honor the rights of individuals to their data. Upon request, you are required to update or delete an individual's personal data, or provide them with a copy of their data. If the personal data was shared with your franchisees, make sure you have a system in place to notify them of the request. Consider adding a feature to your websites that allow users with accounts to review, update, correct, or delete their personal data.
- Know where your data is going. If data is being transferred out of the EU or the European Economic Area to a franchisor or franchisee located in the U.S., determine if your franchise agreement includes standard contractual clauses (or model clauses) approved by the EU or relies on another mechanism such as the EU-US Privacy Shield. The EU-U.S. Privacy Shield is a voluntary certification program administered by the Federal Trade Commission. The EU restricts the transfer of personal data from the EU to a country that it deems to have inadequate data security safeguards—such as the US. The EU-U.S.

Privacy Shield allows individual U.S.-based companies to demonstrate they have adequate data security protections in place to allow the receipt of personal data from the EU.

This list is not meant to be a comprehensive list to evaluate GDPR compliance; rather, it is meant to help you start the compliance conversation with your franchisor or franchisees. Failure to comply with GDPR can have serious consequences for both parties in a franchise relationship. Take the time now to check in with your franchisor or franchisees to ensure that personal data collected from individuals in the EU is being handled in compliance with GDPR.