ECKERT SEAMANS
ATTORNEYS AT LAW

February 13, 2023

Legal Update

Massachusetts Gaming Commission Issues Emergency Privacy and Security Regulations on the Gaming and Sports Betting Industry

By Sarah Stoner, Matthew Meade, Elizabeth Wilson, Roger LaLonde and Zachery Wallack

Effective December 22, 2022, the Massachusetts Gaming Commission (Commission) adopted new emergency privacy and security requirements, which coincide with the recent adoption of sports wagering in Massachusetts and may complicate compliance efforts by gaming licensees and sports wagering operators in the Commonwealth who are trying to navigate different privacy legal regimes in the various jurisdictions in which they operate. Any covered licensee or operator who violates these regulations may have their licenses conditioned, suspended, or revoked. In some instances, licensees may also incur civil administrative penalties.

These new emergency privacy and security requirements in Massachusetts are found in: the Sports Wagering Account Management regulation (205 CMR 248.00); and the amended Uniform Standards of Accounting Procedures and Internal Controls (205 CMR 138.00 (a redlined version is found here)). Both regulations require compliance with Massachusetts law M.G.L. c. 93H, which governs cybersecurity and data breaches.

Sports Wagering Account Management Regulation (*205 C.M.R. § 248.00*)

Scope: 205 C.M.R. § 248.00 applies to sports wagering operators. A sports wagering operator is defined as any entity permitted to offer sports wagering in Massachusetts. The regulation applies equally to those sports wagering operators who manage sports wagering accounts created and/or used at brick-and-mortar facilities as well as digital or mobile web sites, applications and platforms.

What Information is Protected: Any personally identifiable information (PII) of a person who is registering a sports wagering account (Data Subject) is subject to this regulation. Examples of PII listed in the regulation include date of birth, Social Security number or other forms of government identification, personal financial information, and any other information that may be used to verify the person's identity, such as user IDs, passwords, PINs, and other authentication credentials.

Compliance Requirements: Compliance requirements under this regulation mirror many privacy requirements under the European Union's General Data Protection Regulation (GDPR) and comprehensive consumer privacy laws enacted in other U.S. states recently, by including privacy notice requirements, new data subject rights, restrictions on automated decision-making, and new security requirements to protect PII. One key feature of the regulation is that Data Subject privacy notices must include the identity and contact details of the sports wagering operator and all "sports wagering vendors" (defined under 205 C.M.R 202.00) the operator uses as a third-party provider of goods and services, to the extent such vendors may access or use PII in relation to sports wagering operations.

Uniform Standards of Accounting Procedures and Internal Controls (*205 C.M.R. § 138.00*)

Scope: This regulation applies to Massachusetts gaming licensees. A gaming licensee is defined as an entity licensed to operate a gaming establishment in Massachusetts.

What Information is Protected: Any PII obtained and maintained with respect to a gaming patron, regardless of the patron's residency, is subject to this regulation. The regulation uses the PII designation without providing a clear definition of the categories of data it encompasses, but Personal Information is defined in Massachusetts law (under M.G.L. c. 93H) as an individual's full name in combination with any one or more of the following: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. Publicly available information, or information from government records lawfully made available to the public, is not classified as "personal information."

Compliance Requirements: This regulation for Massachusetts gaming licensees has similarities to the GDPR, new comprehensive consumer privacy laws in other states, and the regulation for sports wagering operators, described above. One notable requirement is that the required internal controls and procedures implemented by a gaming licensee under this regulation must be communicated to the Commission.

The Commission is accepting public comments on both of these new regulations and has scheduled a public hearing to discuss the new rules on **Tuesday, February 28, 2023 at 9:15 a.m. EST**. Instructions on how to submit comments and attend the hearing may be found here.

Table- Comparison of Compliance Requirements between 205 C.M.R 248.00 and 205 C.M.R 138.00

		Sports Wagering Account Management 205 C.M.R. § 248.00	Uniform Standards of Accounting Procedures And Internal Controls 205 C.M.R. § 138.00
Privacy Policy		X	X
Data Subject Rights	Delete / Correct	X	X
	Object/ Restrict Access	X	X
	Access / Portability	X	X
	Withdraw Consent	X	X
	File a Complaint	X	
	Confirm Processing		X
Rules on Automatic Decision-making		X	X
Specific Data Security Requirements		X	
Specific Internal Controls and Procedures		X	X

Compliance To Do List

Sports wagering operators and gaming licensees should initiate the following steps to comply with these new regulations.

1. Conduct a data mapping exercise to understand your data processing activities.

2. Create or modify your privacy policy in accordance with the new regulations.

3. Have a process in place to verify and respond to requests from Data Subjects.
4. Analyze how automated decision-making is derived (e.g. to prevent bias) and implement compliant processes.
5. Review and update security policies and practices (including data breach response plans).
6. Implement internal policies and procedures to ensure privacy compliance, including appointing a person or group responsible for privacy protection.
7. Review and update third party contracts to ensure compliance with the new regulations.

ECKERT SEAMANS ATTORNEYS AT LAW

This Legal Update is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Sarah Stoner at 717.237.6026 or sstoner@eckertseamans.com, Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, Roger LaLonde at 215.851.8503 or rlalonde@eckertseamans.com, Zachary M. Wallack at 617.342.6815 or zwallack@eckertseamans.com, any other attorney in our Gaming and Cybersecurity, Data Protection & Privacy Practice Groups, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.