Coming Soon to an Apartment Near You: Data Privacy and Protection

Over the past decade, data protection and privacy has garnered increased attention by state and federal legislators, regulators, international governing bodies, consumers and the media. While the attention started with revelations of huge national data breaches, it has since expanded to focus on the way in which large social media companies are using consumer data.

These issues have spurred policymakers to consider a wide range of responses—from mandatory breach notifications and credit monitoring, to more transparency from firms about what information companies are collecting on individuals and individuals' authority regarding how their information is collected, used and shared by others.

While much of the conversation has centered on the tech giants, the apartment sector is not free of scrutiny and therefore runs the potential risk of being swept up in government regulations. This is particularly true as political leaders here and abroad consider, and in some cases enact, data privacy and security regulatory regimes with far-reaching global impacts.

NMHC has partnered with Manatt, Phelps & Phillips, LLP to issue a forthcoming white paper that provides an overview of the emerging data privacy regulatory landscape, highlights potential associated challenges and offers practical considerations to help apartment firms navigate the complexities of the rapidly evolving frameworks.

Existing Data Protection Regulations & the Urgency of CCPA

At their core, privacy laws inform—and, in effect, govern—how organizations collect and process data about individuals. Since apartment firms often collect, use and maintain vast amounts of information about residents, prospective residents and employees, evaluating the scope and potential impact of the constantly evolving privacy and security regulatory landscape is critical to maintaining successful business operations free from regulatory or consumer backlash. Relatedly, the industry's use of and reliance on smart home technology likely will create additional complexities and challenges in managing and implementing information governance programs.

In May 2018, the European Union's (EU) enacted a new privacy regime, the General Data Protection Regulation (GDPR), that set a new benchmark in the way data privacy is regulated by centering on individuals' rights over their personal information. Recent developments in the U.S. also brought a drastically new privacy framework stateside, likely impacting those companies that may have avoided falling within GDPR's scope.

The most significant example is the landmark California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020, and adopts many of the same sweeping provisions of GDPR. CCPA applies to any business servicing California consumers, regardless of whether the business has a physical location in the state.

Given the population size of California and its broad impact on the nation's economy, CCPA has both

overhauled the U.S. approach to privacy regulation and created momentum for other U.S. states, and potentially the U.S. Congress, to introduce sweeping new privacy requirements.

The impact of these new standards on U.S. businesses is important for three key reasons. First, many of the new regimes are intended to be industry agnostic. This means that traditional exceptions or carve outs for certain industries may not be available, and sector-specific considerations may not be taken into account as new requirements are developed.

Because of the extraterritorial nature of many of these laws, businesses that collect information on individuals located in multiple jurisdictions can be subject to numerous laws, often with differing, and potentially conflicting, requirements that can create implementation and compliance challenges. Finally, and perhaps most importantly, emerging privacy laws have increased companies' liability and risk exposure with respect to the storage and processing of individuals' data.

Understanding the scope of these new regulations requires firms to understand the differences between data breach notification (identifying the time required to notify consumers), data security (reasonable security protocols) and data privacy (how data is used). Each of these may be regulated separately or collectively depending on the regulatory regime at issue. GDPR, for example, addresses all three themes.

To date, there is no federal law marrying all three into a comprehensive legislative package despite Congressional efforts to do so for several years. Absent federal action, state legislators have acted. As a result, today there is a patchwork of 50 different state breach notification laws (plus laws in D.C., Guam, Puerto Rico and the Virgin Islands). Further, states continually are amending and expanding these laws, which is why NMHC and the industry must take a broader view.

NMHC's white paper provides a framework for developing strong data privacy practices that support apartment firms' efforts to comply with existing and evolving data privacy laws and standards, regardless of jurisdiction. Of course, apartment firms will need to work with internal legal and technology teams to ensure compliance with each law. But NMHC advises firms to look for commonalities and ways to bolster consumer privacy protections across the board in an effort to stay ahead of the curve and ahead of coming regulations. Specifically, the paper identifies and defines the common themes seen across current laws and proposed legislation, including:

- A broad definition of covered information and what it means
- Increased transparency and disclosure regarding data processing practices
- Individual rights over their information
- Oversight over third-party companies' handling of data
- Mandated corporate governance as to data privacy and security practices
- Increased potential liability and regulatory enforcement authority.

Finally, it details the high-level practical considerations companies should consider as they analyze whether emerging privacy requirements apply to their business practices and offers guidance on how to address each one. The paper covers many key steps that firms should take to begin working towards compliance with the array of laws pending or enacted. The list is provided in greater detail in the white paper. Some of the steps include:

- Implement an organization-wide data mapping effort to understand the nature and types of data maintained across the organization and what has to be maintained or discarded.

- Engage internal stakeholders across key functions and business lines.

- Identify the full data lifecycle.

- Analyze the purposes and use cases for the data.
- Understand third-party relationships and contractual obligations related to security and privacy protection.
- Identify the company's role in processing the data.
- Implement robust contractual requirements.
- Establish internal procedures for responding to consumer data subject requests.
- Establish external procedures for third parties who maintain, use, or store your business data such as property management firms, software and cloud providers or financial firms to determine the appropriate way to address each request.
- Consider technical and operational requirements or challenges.
- Ensure disclosures are complete and accurate.
- Regularly assess applicability of requirements.

The data privacy regulatory landscape is far from established. Companies that proactively and programmatically account for privacy and security considerations in their business operations will be better positioned to adapt practices and procedures as new requirements continue to develop, let alone avoid harsh regulatory consequences for failing to adequately protect their data and their residents' privacy.