

To: Self Storage Association Members

From: Joseph L. Doherty, Esq.
Daniel T. Bryant, Esq.

Re: Nevada Data Privacy Law

I. Introduction & Background

Nevada recently passed Senate Bill 220 (SB 220), which amends the state's existing data privacy law and takes effect on October 1, 2019. SB 220 grants consumers the power to direct businesses to not sell their data. **Covered businesses, as defined below, have obligations even if they do not sell consumer data.** The law is similar to the *California Consumer Privacy Act of 2018*, but it is more limited in scope. SSA members that meet the criteria outlined below should quickly familiarize themselves with the requirements of the law and implement compliance programs as soon as possible in advance of the fast-approaching deadline.

II. Who Must Comply

SB 220 requires a business to comply if it:¹

- Owns or operates an internet website or online service for commercial purposes;
- Collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service; and,
- Purposely directs its activities toward Nevada or consummates some transaction with Nevada or one of its residents.

It is important to note that businesses without a physical presence in Nevada could be subject to the statute. If a business meets all the elements above, it must comply with the additional requirements of the law described in more detail below.

III. What Must Businesses Do

A business meeting the definition above (a "covered business") must establish a procedure that allows consumers to direct the business to cease selling any of their "covered information." Covered information means any one of the following collected by a business through its website or online service and maintained by the business in an accessible form²:

- A first and last name;
- A home or other physical address which includes the name of a street and the name of the city or town;
- An email address;

¹ The law does provide some exemptions, but none are relevant to the self storage industry.

² Neither "website or online service" nor "accessible form" is defined in the law.

- A telephone number;
- A social security number;
- An identifier that allows a specific person to be contacted either physically or online; or,
- Any other information concerning a person collected from the person through the website of the covered business and maintained by that business in combination with an identifier in a form that makes the information personally identifiable.

Each covered business is required to establish a “designated request address” that allows a consumer to submit a “verified request,” directing that business to cease sales of any covered information to a third party. A verified request is:

- Submitted by a consumer to a covered business; and,
- For which the covered business can reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means.

A designated request address is an email address, toll-free number or internet website established by a covered business through which a consumer may submit its verified request. Once a covered business receives that request, it must respond within sixty (60) days after receipt and must stop the sale of any covered information.

Importantly, the law defines sale³ to cover the exchange of covered information for money. As a result, any business that is exchanging consumer data for other compensation may be able to continue to do so even if it receives a verified request from a consumer. The business should consult with experienced legal counsel to determine the appropriate course of action.

IV. 2017 Requirements

In addition to the new requirements that take effect in 2019, Nevada’s existing privacy law requires a smaller group of covered businesses to provide notice to consumers that:

- Identifies the categories of covered information that the business collects through its internet website and the categories of third parties with whom the business may share that information;
- If it exists, provide a description of the process for a consumer who uses or visits the internet to review and request changes to any of his or her covered information that is collected;

³ The terms “sale” expressly does not cover: disclosure of covered information by a business to a person who processes the covered information on behalf of the business; the disclosure of covered information by a business to a person with whom the consumer has a direct relationship for the purposes of providing a product or service requested by the consumer; the disclosure of covered information by a business to a person for purposes which are consistent with the reasonable expectations of a consumer considering the context provided by the covered information to the business; the disclosure of covered information to a person who is an affiliate, as defined in NRS 686A.620; or the disclosure or transfer of covered information to a person as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the person assumes control of all or part of the assets of the business.

- Describes the process the business uses to notify consumers who use its website of material changes to its notice;
- Discloses whether any third party may collect covered information about the consumer as a result of the consumer's use of its website; and,
- States the effective date of the notice.

Importantly, there is an exemption to the notice requirement for a business that:

- Is located in Nevada;
- Whose revenue is derived primarily from a source other than the sale or lease of goods or services on internet websites; and,
- Whose website has fewer than 20,000 unique visitors per year.

If a business meets all these requirements, it does not have to comply with the 2017 notice provisions of the law. However, that business must still comply with the 2019 amendments regarding the sale of consumer data and must establish a procedure for consumers to make verified requests.

V. Enforcement

The Nevada Attorney General is tasked with enforcement of the law. A business that receives notice of non-compliance has thirty (30) days to remedy the issue. If the issue is resolved, no further action will be taken. However, if the business fails to cure the violation, the Attorney General can seek injunctive relief or impose a civil penalty up to \$5,000 per violation.

VI. Conclusion

SSA members should already be familiar with the 2017 requirements and, if required, have appropriate notices on their websites. If not, businesses should update their privacy policies as soon as possible to avoid any potential issues.

SSA members should familiarize themselves with the 2019 amendments of the data privacy law regarding the sale of consumer data. **Even if they do not sell covered information, businesses must still establish a designated request address for consumers to make verified requests.** Those businesses must also still respond to requests but may inform the consumer that they do not engage in data sales. If a company sells covered information, it must respond to requests and honor requests to cease those activities upon receipt.

Thankfully, the requirements of SB 220 are less onerous than its California counterpart, but it will still require covered businesses to set up a procedure to field and respond to requests. However, while the California law becomes effective on January 1, 2020, SB 220 has an effective date of October 1, 2019. With that date just around the corner, SSA members should act quickly to ensure compliance.