THE VERMONT DATA PRIVACY & ONLINE SURVEILLANCE ACT: OPPORTUNITIES AND RESPONSIBILITIES FOR BUSINESSES & NONPROFITS

The Vermont Data Privacy & Online Surveillance Act creates new opportunities for businesses and nonprofits to build trust with consumers by demonstrating a commitment to data privacy. By taking proactive steps to understand and comply with the Act's basic requirements, many of which you may already be doing, small businesses can minimize their risk and safeguard all Vermonters digital privacy. Nineteen states have already passed privacy laws that contain most of these requirements.

Does the Act Apply to My Small Business? This Act applies to businesses that conduct business in Vermont or target products/services to Vermont residents **AND** meet certain thresholds regarding the amount of consumer data processed or revenue derived from the sale of personal data.

Your business is only subject to the Act if you answer yes to any of the following three questions:

1. Does your business hold the data of more than 25,000 consumers (excluding data used only to process payments)?
2. Does your business sell consumer data?
3. Does your business derive 25% of its gross revenue from selling the data of at least 12,500 consumers?

If the answer to those three questions is no, this law does not apply to your business.

What Does My Business Need to Do?

- Limit data collection and use to what's necessary for the product or service the consumer is asking for.
- Take reasonable data security measures to protect your customers' data.
- Provide transparent privacy notices to consumers.
- Offer your customers the ability to access, correct, and delete their data.
- Give consumers the right to opt-out of targeted advertising, the sale of their personal data, and profiling.
- If you're conducting high-risk data activities like selling data, you must do impact assessments (most small businesses won't be subject to these, and if you do them to comply with another state's law, that satisfies compliance with Vermont's law).
- Make sure you have contracts with any third-party processors who handle data on your behalf, such as credit card processors.
- Take extra care when collecting sensitive data like biometrics, health data, or data of minors.