S. 71 Testimony
April 29, 2026
House Commerce & Economic Development Committee
Emma Paradis, Common Good Vermont Co-Director, United Way of Northwest Vermont

Common Good Vermont is a statewide program of United Way of Northwest Vermont dedicated to uniting, strengthening, and advocating for Vermont's nonprofit sector.

Thank you for the opportunity to provide testimony on S. 71. We appreciate the intent of this bill and know all too well that in this moment, strong data privacy practices are especially critical for nonprofits facing not only the heightened cybersecurity risks of today's reality, but also increased public scrutiny and politically motivated government overreach that presents its own set of data-related challenges. For mission-driven organizations whose credibility is foundational to their impact, protecting personal data is not just a legal or technical responsibility, it is an ethical imperative essential to maintaining the safety, trust, and rights of those they engage with.

The 6,400 nonprofits serving our state are diverse in size, service area, and mission, but together, represent a sector that employs one in five Vermont workers, is an economic driver, and makes Vermont a better place to live, work, and play. Most of these organizations are volunteer run or managed by small teams, with 70% generating less than $100K per year in annual revenue. Others are much larger, delivering programs and services Vermonters rely on at scale. What most of these organizations have in common is that they are operating under significant resource- and capacity constraints.

When I talk to nonprofits about data privacy legislation, I'm often met with a mixed reaction. On the one hand, organizations care deeply about protecting the data of their donors, clients, and partners. Responsible data stewardship is not only critical to maintaining trust, which is essential to achieving their mission, but also something they intrinsically value. After all, Vermont nonprofits are led by fellow Vermonters who expect their information to be handled with the same care by others.

This support for data privacy protection, however, is often quickly followed by questions and concerns. What would these changes mean for our organization? Will the systems we have in place be sufficient? What specific categories of data do we hold? Do I have room in my budget to consult an expert and make necessary updates or invest in new technology?

Do my staff have the capacity to undertake a new project or add new steps to their workflow? How does this change how we collaborate with partners?

These concerns don't stem from malintent or apathy; rather, they are reflective of a sector that is all too familiar with being subjected to new requirements without the resources to effectively adopt them.

Nonprofits rely on data to carry out their missions for the common good – they are not selling data, products, or services for profit. The data they collect and process help them serve clients, deliver programmatic and fundraisings messages to those who are most likely to benefit, make decisions, and assess impact. While the vast majority have strong data security measures in place, often utilizing third-party services, they also operate in an imperfect environment.

Many work collaboratively with other organizations or government entities in ways that require the sharing of data. Some hold client information that doesn't squarely fit into one data category. Some may inadvertently wind up holding sensitive data while helping clients access services or benefit programs. These are just a few examples of the many scenarios nonprofits may experience, but they speak to the need not only for clarity, but also acknowledgement that policies designed to protect consumers may also make it harder for nonprofits to help them. Staff may hesitate to provide certain types of assistance or document information that helps them serve clients, spend more time managing data that they could be spending on mission work, or have to divert resources from programming to cover legal or compliance council. These changes may also be confusing or frustrating for the clients they serve.

As the state nonprofit association, Common Good Vermont has a necessary preference to exempt nonprofits from this legislation. In a moment where organizations are facing decreasing resources, increased need, and uncertainty at the federal level, S. 71 poses yet another challenge to navigate. Beyond logistical concerns, coming into and maintaining compliance will also be an additional expense, potentially including consulting services, new technology, and legal support. Most nonprofits, especially those of scale, are already practicing responsible data stewardship, minimizing the realized benefit to the consumer compared to cost to the organization.

In lieu of an exemption, and in the interest of strengthening data privacy, effective implementation of this legislation means offering the support, clarity, and resources nonprofits need to successfully understand, adapt, and comply.

To this end, we recommend:

- **Investing in Technical Assistance**: As we've discussed this session, nonprofits do not have access to technical assistance services as small businesses, municipalities, or other comparable entities do. An appropriation through Common Good Vermont would support public compliance trainings, resource development, and access to 1:1 technical assistance to address unique circumstances. Nonprofits need to understand what is expected of them and how to accomplish that.
- **Education & Outreach:** Education and outreach to potentially impacted entities by the Attorney General, in coordination with stakeholders, should be explicitly required in the bill. This should include plain language guidance, public messaging, information sessions, and a helpline and/or email address to answer compliance questions.
- **Third Party Registry:** To support nonprofits and others in choosing third party services that are compliant and demonstrate strong data protection practices, it would be helpful to have a verified list/registry of vetted companies. Those who register would be rewarded for taking the extra step by gaining additional business.
- **Clarified Data Categories and Reasonable Applicability Thresholds:** Definitions of data categories need to be clear to support compliance, especially when it comes to what is classified as sensitive data. Since controlling one piece of sensitive data triggers applicability, the definition is quite broad, or the threshold is quite low. For example, consumer health data reads to include information as seemly inconsequential as a food allergy – a common registration field for any event where food will be provided. Similarly, while not interchangeable, would listing pronouns (such as they/them) on a record be interpreted as revealing non-binary status? These are common data fields, provided voluntarily by and for the benefit of the consumer, that could trigger applicability for even a tiny, volunteer run food shelf, for example.
- **Delayed Effective Date:** We would ask for an effective date of no earlier than January 1, 2028 to allow time for education and outreach and give an adequate runway for organizations to come into compliance.

In closing, whether nonprofits are exempted or not, there is a strong desire in the nonprofit community to do right by their clients and supporters, mitigate risk to their organization, and enhance data security measures. It's not buy-in that stands in the way, it's time, resources, and expertise. If Vermont is serious about protecting consumer data, it needs to create supportive conditions. This means making space to collaboratively navigate policy nuances as they play out in real time without fear of penalty, providing guidance and

opportunities to ask questions, and reducing financial barriers. Common Good is here as a partner and resource and we look forward to working with you to achieve this shared goal.