HINSHAW

Alerts

Q&A: New Hampshire Becomes the Fourteenth State to Pass a Data Privacy Law—With More States Waiting in the Wings

March 13, 2024
Privacy, Cyber & AI Decoded

New Hampshire is the fourteenth state with a comprehensive privacy law, as signed by Governor Sununu on March 6, 2024. The new law will go into effect on **January 1, 2025**. Continue reading for our Q&A on the "trusted" number 14!

Who Does the New Hampshire Law Apply to?

The law does not have a revenue threshold. It applies to entities doing business in New Hampshire or that produce products or services that are targeting New Hampshire consumers during a one-year period that:

> (1) Control or process the personal data of at least 35,000 unique consumers, excluding personal data processed or controlled solely for a payment transaction; or
>
> (2) Control or process the personal data of at least 10,000 unique consumers and derive more than 25 percent of their gross revenue from the sale of personal data.

The sale of personal data is defined as monetary and other valuable considerations.

- This definition of the sale of personal data excludes personal data controlled or processed by a third party to provide products or services or disclosed at the direction of the consumer.

Does Your Business Fall Within One of These Broad Exceptions to the Law?

- It does not apply to personal information of employees and business-to-businesses.
- It does not apply to nonprofit organizations.
- It has exceptions for organizations otherwise regulated under:
  - Health Insurance Portability and Accountability Act (HIPAA): data and covered entity exception;
  - Gramm–Leach–Bliley Act (GLBA);

Attorneys

Cathy Mulrow-Peattie

Service Areas

Biometric Information Privacy Act

Privacy, Security & Artificial Intelligence

- Family Educational Rights and Privacy Act (FERPA):data-related exception and entity exception for institutions of higher education; or
- personal data processed under the Fair Credit Reporting Act (FCRA) by a consumer reporting agency.

What Specific Provisions Should You Look Out for?

In addition to the requirements for standard data subject access rights and the requirement for an accessible, clear privacy notice, organizations should consider the following four key provisions:

1. Sensitive Personal Data

There is an expansive definition of sensitive personal data, which includes physical and mental health conditions, genetic or biometric information, and precise geolocation. This relates to similar requirements in states with new comprehensive privacy laws, such as Delaware and New Jersey. A business must provide opt-consent to use this sensitive data.

2. Increased Provisions for Processing Teen Data

Businesses that process personal data for targeted advertising or sell personal data from 13–16-year-old consumers will need to obtain consent prior to processing, similar to California.

3. Data Protection Assessments

New Hampshire follows New Jersey and other state laws that require data protection assessments for use cases and projects that have a heightened data protection risk of harm. The New Hampshire Attorney General has the right to request a copy of these DPAs in the event of an investigation.

Under this law, a heightened risk of harm has an expansive definition that includes:

1. targeted advertising;
2. the sale of personal data;
3. processing of personal data for profiling; and
4. processing of sensitive data.

We recommend that organizations subject to this comprehensive state privacy law review these requirements that go into effect on **July 1, 2024**, although enforcement does not occur until **January 1, 2025**.

4. Universal Opt-Outs

Once the law goes into effect on **January 1, 2025**, New Hampshire will join other state comprehensive privacy laws that require opt-out preference signal acceptance. New Hampshire's law requires that businesses implement an opt-out preference signal for consumers to allow them to opt out of the processing of their personal data for targeted advertising or sales.

Businesses should plan to implement opt-out preference signals if they have not already, as they increasingly become the norm. As we stated in an earlier alert, we recommend covered businesses put this requirement on their privacy technology roadmap for 2024.

How is the Law Enforced?

While there is no private right of action, this new comprehensive privacy law provides even greater enforcement power to the New Hampshire Attorney General's office, which already has broad authority to enforce the state's consumer protection laws.

Although the effective date of this comprehensive privacy law is **January 1, 2025,** for the first year, the statute allows fo**r** a 60-day cure period for organizations for privacy violations before the Attorney General's office brings an enforcement action. However, the Attorney General has to determine that a cure is generally possible. To do so, the Attorney General may consider:

- The number of violations;
- The size and complexity of the business;
- The nature and extent of the businesses' processing activities;
- The substantial likelihood of injury to the public;
- The safety of persons or property; and
- Whether the violation was caused by human or technical error.

After **January 2026**, the cure period will be permitted only on a discretionary basis.

What's Next?

The above summary provides an overview of the key provisions of this law but is not a full analysis. And, Kentucky is on its way to passing a comprehensive state privacy law, becoming state number fifteen.

In addition, we are seeing legislation regarding health care, location data, artificial intelligence, and data of children in state legislatures, as well as recurring Biometric Information Privacy Act (BIPA)-style legislation and private rights of action.

Subscribe to our *Privacy, Cybersecurity, & AI* alerts to stay informed on the ever-changing data privacy laws your business needs to comply with.

Law clerk Sabrina Messar contributed to this post. She is not currently admitted to practice law.