King & Spalding

Client Alert

Data, Privacy and Security

JANUARY 19, 2024

For more information, contact:

Jarno Vanto
+1 212 556 2210
jvanto@kslaw.com

Misty L. Peterson
+1 404 572 4939
mpeterson@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
34th Floor
New York, New York 10036
Tel. +1 212 556 2100

Atlanta
1180 Peachtree Street, NE
Suite 1600
Atlanta, Georgia 30309
Tel. +1 404 572 4600

New Hampshire Enacts Privacy Law

On January 18, 2024, New Hampshire's State Legislature enacted the Expectation of Privacy Act (the "**Act**"). Following the Governor's signature, the Act will take effect January 1, 2025.

SCOPE

The Act defines "**personal data**" very broadly, meaning any information that is linked or reasonably linkable to an identified or identifiable individual ("Personal Data"). The Act applies to "**controllers,**" defined as individuals or legal entities that, alone or jointly with others, determine the purposes and means of processing Personal Data, that:

- Conduct business in New Hampshire or produce products or services that are targeted to "**consumers**", defined as residents of New Hampshire; and
- During a one-year period either: (a) controlled or processed the Personal Data of not less than 100,000 consumers, excluding Personal Data controlled or processed solely for the purpose of completing a payment transaction; or (b) controlled or processed the Personal Data of not less than 25,000 consumers and derived more than 25 percent of their gross revenue from the sale of Personal Data.

In addition to excluding Personal Data relating to individuals acting in a commercial or employment context (*i.e.* business-to-business contact information and specified employee Personal Data), the Act also excludes certain entities and certain categories of Personal Data from its scope, including:

- Covered entities and business associates subject to Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as protected health information under HIPAA;

- Financial institutions and data subject to Gramm-Leach-Bliley Act (GLBA);
- New Hampshire governmental authorities;
- Nonprofit organizations;
- Institutions of higher education;
- National securities associations registered under 15 U.S.C. § 78o-3 of the Securities Exchange Act of 1934;
- Patient-identifying information for purposes of 42 U.S.C. § 290dd-2;
- Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. 46, as well as information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section that is maintained by a covered entity or business associate, program or qualified service organization;
- Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;
- The protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards set forth in this chapter, or other research conducted in accordance with applicable law;
- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq.;
- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq.;
- Information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;
- Information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities;
- The collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 et seq.;
- Personal Data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.;
- Personal Data regulated by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g et seq.;
- Personal Data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. 2001 et seq.;

- Data processed or maintained in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; as the emergency contact information of an individual under this chapter used for emergency contact purposes; or, that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under HIPAA and used for the purposes of administering such benefits; and,
- Personal Data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq., by an air carrier subject to the act, to the extent this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. 41713.

CONSUMER RIGHTS

The Act grants consumers broad rights, including rights to:

- Confirm whether a controller processes the consumer's Personal Data and accesses such Personal Data (unless such confirmation or access would require the controller to reveal a trade secret);
- Correct inaccuracies in the consumer's Personal Data;
- Delete Personal Data;
- Obtain a copy of the consumer's Personal Data held by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance; and
- Opt-out of the processing of Personal Data for the purposes of (a) targeted advertising; (b) the sale of Personal Data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

NO SENSITIVE PERSONAL DATA WITHOUT CONSENT

The Act defines "**sensitive data**" as Personal Data that includes data revealing any of the following:

- Racial or ethnic origin;
- Religious beliefs;
- Mental or physical health condition or diagnosis;
- Sex life;
- Sexual orientation; or
- Citizenship or immigration status.

Sensitive data also includes:

- Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual;
- Personal Data collected from a known child; or
- Precise geolocation data.

Under the Act, the controller must obtain a consumer's consent to process sensitive data. "Consent" under the Act means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of Personal Data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. The Act specifies that consent does not include:

- Acceptance of a general or broad terms of use or similar document that contains descriptions of Personal Data processing along with other, unrelated information;
- Hovering over, muting, pausing, or closing a given piece of content; or
- Agreement obtained through the use of dark patterns.

The controller must also provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, the controller must cease to process the consumer's Personal Data as soon as practicable, but not later than 15 days after the receipt of such request.

KEY OBLIGATIONS

1. Notice to Consumers

Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes, at a minimum, the following information:

- The categories of the Personal Data that the controller processes;
- The purposes for processing Personal Data;
- How consumers may exercise their consumer rights, including the controller's contact information and how a consumer may appeal a controller's decision with regard to the consumer's request;
- The categories of Personal Data that the controller shares with third parties, if any;
- An active email address or other online mechanism that the consumer may use to contact the controller; and
- If a controller sells Personal Data to third parties or processes Personal Data for the purposes of targeted advertising, the controller shall clearly and conspicuously disclose such sale or processing, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing.

2. Responding to Consumer Requests

Controllers have 45 days from their receipt of a consumer's request to respond with the information requested. This period may be extended by 45 additional days where reasonably necessary, considering the complexity and number of the consumer's requests, provided that the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension. The information must be provided by the controller free of charge once per consumer during any twelve-month period.

When a controller deems a consumer's opt-out request as fraudulent and denies it, the controller must notify the consumer who made such request, disclosing that the controller believes such request is fraudulent, why the controller believes such request is fraudulent and that the controller will not comply with the consumer's request.

A controller must also establish an appeal process for consumers whose requests the controller rejects. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

3. Data Protection Assessments

The Act requires that controllers engaging in processing of Personal Data that presents a heightened risk of harm must conduct and document a data processing assessment (the "**Assessment**"). Under the Act, processing that presents a heightened risk of harm to a consumer includes:

- The processing of Personal Data for the purposes of targeted advertising;
- The sale of Personal Data;
- The processing of Personal Data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, consumers, financial, physical or reputational injury to consumers, a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or other substantial injury to consumers; and
- The processing of sensitive data.

The Assessment must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. A controller must make the Assessment available to the New Hampshire Attorney General upon request. Data protection assessments shall be confidential and exempt from disclosure under RSA 91-A The disclosure of a data protection assessment pursuant to the Attorney General's request does not constitute a waiver of any attorney-client privilege or work-product protection. Data protection assessment requirements must apply to processing activities created or generated after July 1, 2024, and are not retroactive.

4. Written Agreements with Data Processors

As under the GDPR and many state privacy laws, the Act requires a written contract in place between the controller and the processor processing Personal Data on behalf of, and for the purposes of, the controller. The contract must, at a minimum, include:

- Instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties;
- A requirement that each person processing the Personal Data is subject to a duty of confidentiality with respect to the data;
- A requirement that any subcontractors enter into a written contract that requires the subcontractor to meet the obligations of the processor with respect to the Personal Data;

- A requirement that at the discretion of the controller, the processor must delete or return all Personal Data to the controller as requested at the end of the provision of services, unless retention of the Personal Data is required by law;
- A requirement that the processor makes available to the controller all information necessary to demonstrate compliance with the obligations in the Act;
- A requirement that the processor allows for, and contributes to, reasonable assessments and inspections by the controller or the controller's designated assessor.

The Act goes on to specify that if a processor begins, alone or jointly with others, determining the purposes and means of the processing of Personal Data, it will be deemed a controller with respect to the processing, and may be subject to an enforcement action under RSA 507-H:11.

ENFORCEMENT; NO PRIVATE RIGHT OF ACTION

The Act will be enforced by the state's Attorney General and it does not provide for a private right of action. Furthermore, the Act provides for a cure period, where, if a cure is deemed possible, the Attorney General issues a notice to the controller prior to bringing an enforcement action, giving the controller 60 days to cure the alleged violation. In the event the controller fails to cure the violation during that period, enforcement action may be brought.