

New Jersey's New Sensitive Data Law: What Employers Need to Know

Monday, September 28, 2026

On June 30, 2026, New Jersey Governor Mikie Sherrill signed Assembly Bill 5328 (A5328) into law, amending the New Jersey Data Privacy Act to impose stringent compliance requirements and significant civil penalties on individuals and legal entities that engage in covered sensitive-data activities. Most provisions took effect immediately, while the public registry is scheduled to open on April 1, 2027.

Because the Act expands the categories of regulated entities, employers and business owners should determine whether their data-sharing practices bring them within its scope. Businesses that are covered may face substantial compliance obligations and should make that assessment before the public registry opens in spring 2027.

New Jersey's Ban on Selling Sensitive Data

A5328 prohibits the sale of New Jersey consumers' "sensitive data." Sensitive data is defined as "revealing racial or ethnic origin; religious beliefs; mental or physical health condition, treatment, or diagnosis; financial information, which shall include a consumer's account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account; sex life or sexual orientation; citizenship or immigration status; status as transgender or non-binary; 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."

Notably, the ban on selling sensitive data applies to all individuals and legal entities without regard for the volume of consumers whose data is actually being collected.

Despite its broad reach, A5328 provides limited exemptions, for protected health information governed by the Health Insurance Portability and Accountability Act (HIPAA) and data of financial entities maintained under the Gramm-Leach-Bliley Act (GLBA).

Do You Qualify as a "Data Broker" or a "Data Collector"?

This bill particularly regulates two distinct and broadly defined groups: "data brokers" and "data collectors." New Jersey's inclusion of both groups in this legislation makes it even more pertinent that employers and businesses assess their data sharing policies to determine whether they are subject to this statute.

A5328 defines a "data broker" as a person or legal entity "that knowingly collects or purchases the personal data of a consumer with whom the person or legal entity does not have a direct relationship and sells or licenses that data to a third party."

By contrast, the Act defines a "data collector" as "a business, or units of a business, separately or together, that knowingly: (1) collect the personal data of a consumer with whom the data collector has a direct relationship; and (2) sell or license such personal data to a data broker." A direct relationship may exist when the consumer is a current or former customer, employee, independent contractor, agent, investor, or donor.

The bill outlines various exceptions to these definitions, excluding from its coverage government entities such as federal or state agencies, political subdivisions, and instrumentalities created by political subdivisions.

The Public Registry

Another critical aspect of this bill that employers and business owners should be aware of is the creation of a public registry by the Office of Consumer Protection in the New Jersey Division of Consumer Affairs. This public registry will require data brokers and data collectors to annually register and pay a fee with the division, or be subject to immense civil penalties.

Annual registration fees are based on the volume of New Jersey consumer data collected. The lowest tier is \$5,000 for entities collecting data concerning 100,000 or fewer consumers in the state, while the highest tier is \$1.5 million for entities collecting data concerning more than 4.5 million consumers in the state.

Further, the annual registration requires that data brokers and data collectors supply the following information to the division, subject to change as the division sees fit:

- Data broker or data collector's name, address, email address, and web address,
- The ability of individuals to opt out of the data collection practices, including the method, type, and limitations of the opt out,
- The ability of individuals to direct the deletion of their personal data in the data broker or data collector's possession,
- Specifications on the data collection, databases, or sales activities that an individual cannot opt out of,
- The data broker or data collector's use of a credentialing process,
- A history of past data breaches or cybersecurity events and an accounting of the number of individuals affected by such,
- Details surrounding the data collection, database, sales activities, and opt out methods applicable to persons under the age of 18, and
- The processors who, on the behalf of the data brokers and data collectors, process personal data.

The Cost of Violating A5328

A5328 establishes substantial civil penalties for the failure to comply with annual registration in the public registry and for violation's of the Act's substantive requirements.

A data broker or a data collector that fails to register with the division or submit the appropriate fee will be liable for the unpaid fee for each missed registration year, plus a civil penalty of \$2,500 for each day of noncompliance.

Selling sensitive data in violation of the Act may result in a civil penalty of \$50,000 for each record sold, offered for sale, or licensed in violation of the Act.

Key Takeaways for Employers

Because the Act is already operative, employers should review their data-collection and data-sharing practices now, identify whether they qualify as data brokers or data collectors, and prepare for the Office of Consumer Protection's public registry to open on April 1, 2027.

Further, employers should also monitor forthcoming guidance from the division, which has stated that it intends to publish additional information in the coming months.

If you are unsure whether your business is subject to the Act or need guidance regarding its data-collection, data-sharing, or registration requirements, call a member of the [Employment Law Team](#) at Wilentz, Goldman & Spitzer, P.A.

Practice

- Employment Law