

Illinois' Stringent Data Privacy Laws: Are You Handling Data Correctly?

Illinois has recently enacted new laws enhancing rights and obligations related to privacy. Companies active in Illinois or collecting information from Illinois residents need to evaluate how these laws may apply to them.

Illinois Personal Information Protection Act

A new version of the Illinois Personal Information Protection Act, 815 ILCS 530, et seq., went into effect making the Illinois law one of the most stringent data breach laws in the country.

The Act places a number of requirements on companies and other organizations that handle, collect, disseminate, or otherwise deal with nonpublic personal information. Nonpublic personal information includes either (a) a username or e-mail address along with its accompanying password or other method to access an online account or (b) an individual's first name or first initial and last name in combination with a social security number, driver's license number, state identification card number, an account number, credit or debit card number, medical information, health insurance information, or unique biometric data (such as scans of hand or face geometry).

The Act requires companies and organizations with personal information of Illinois residents to implement and maintain reasonable security measures to protect data from unauthorized access, acquisition, destruction, use, modification, or disclosure. Additionally, the Act requires any contract under which one company transmits personal information to another company to include a provision requiring the recipient of the information to implement and maintain reasonable security measures. For example, a contract with a data storage vendor would need a provision requiring the vendor to have reasonable security measures.

The Act also specifies a number of required actions, should a data breach occur. A company or organization that owns or licenses personal information must notify Illinois residents of a breach to their computerized data in the most expedient time possible and without unreasonable delay. The breach notification must include toll-free numbers, addresses, and websites of consumer reporting

POSTED:

Aug 29, 2017

RELATED PRACTICES:

[Employee Benefits](#)

<https://www.reinhartlaw.com/practices/employee-benefits>

[Litigation](#)

<https://www.reinhartlaw.com/practices/litigation>

RELATED SERVICES:

[Accounting and Financial Professionals](#)

<https://www.reinhartlaw.com/services/accounting-and-financial-professionals>

[Data Privacy and Cybersecurity](#)

<https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity>

[Arizona/California/Florida/Illinois/South Dakota Law Consultations](#)

<https://www.reinhartlaw.com/services/arizonacaliforniafloridailinoisouth-dakota-law-consultations>

[Software, Technology and Licensing](#)

<https://www.reinhartlaw.com/services/software-technology-and-licensing>

[Commercial and Competition Law](#)

<https://www.reinhartlaw.com/services/commercial-and-competition-law>

agencies and the Federal Trade Commission. The breach notification must also explain how to obtain fraud alerts and security freezes. A company or other organization that stores or maintains personal information must notify the owner or licensee of a data breach. HIPAA-regulated entities (covered entities and business associates) are exempt from complying with the Act; however, these entities must send an additional breach notification to the Illinois Attorney General.

The Act further provides that a violation allows consumers to sue the offending company or organization under the Consumer Fraud and Deceptive Business Practices Act. The Illinois Attorney General may also bring an action against a company for violations and seek an injunction, a revocation of the right to do business in Illinois, restitution, and a fine.

Biometric Information Privacy Act

The Biometric Information Privacy Act has gained recent attention due to a series of class action suits brought on behalf of consumers. The Act requires entities to obtain written consent from consumers prior to collecting any biometric information, such as fingerprints, voiceprints, or scans of hand or face geometry. Facebook, Google, Shutterfly, and Snapchat have all been targets of lawsuits, as they collect facial recognition data from posted photographs. Other states are now proposing similar data privacy legislation.

Companies and other organizations that handle, collect, disseminate, or otherwise deal with nonpublic personal information of Illinois residents should be particularly vigilant. Affected companies are now required to implement and maintain reasonable security measures and must comply with new breach notification requirements. To demonstrate good faith compliance, best practice requires (a) implementing information security policies and protocols, (b) preparing and regularly reviewing incident response policies and procedures, (c) identifying and defining the role of data security team members, (d) reviewing contracts involving the use or disclosure of personal information, and (e) educating employees.

If you have any questions regarding the Illinois Personal Information Protection Act or any matters involving data security and privacy, please contact [Martin McLaughlin](#) or a team member from Reinhart's [Data Privacy and Cybersecurity Group](#).

RELATED PEOPLE:

[Martin J. McLaughlin](#)

<https://www.reinhartlaw.com/people/martin-mclaughlin>



These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.