CSR®
Privacy Made Simple℠

State of Missouri

Statutory Review for Breach & Consumer Notification

This summary of regulations is provided for information purposes only. No action based on this summary alone should be undertaken. Each individual or entity must obtain appropriate guidance for its specific circumstances.

48 states and the District of Columbia (Washington DC) have laws pertaining to the way they expect a breach to be handled and how they want their affected residents to be notified. If you have customers or have personal information pertaining to individuals that reside outside of your state, you will additionally need to ensure that you follow the laws of that corresponding state or country.

Following is a brief review of the Missouri laws pertaining to breach and consumer notification.

Personal Information
There is specific personal information that the state considers relevant to a breach. (This does not include elements that a federal agency or industry specific entity may consider relevant.)
Personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements: a) Social security number; b) Driver's license number or other unique identification number created or collected by a government body; c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; e) Medical information; or f) Health insurance information.

CSR Professional Services, Inc.
830 NE Pop Tilton Place / Jensen Beach / FL / 34957 / 888.294.6971 / www.csrps.com

CSR®
Privacy Made Simple℠

Who does the law apply to?
The state will identify who the law pertains to. The state may have different laws for state agencies or specialized fields such as medical or financial.
The law applies to any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri (data owner). Additionally, it applies to any person, or any person that conducts business in Missouri, that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license (vendor). If the vendor experiences a breach of security, they must notify the data owner immediately. The data owner is responsible to complete the reporting and consumer notification. There may be exemption for a person that is regulated by state or federal law.
Breach
There are many factors to take into consideration when deciding if the incident is considered a breach and when that breach is reportable. Some states have very specific factors while others leave the interpretation open to include a multitude of elements.
In Missouri, "Breach of security" or "breach", means unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. When considering reporting requirements, it would include, but not be limited to: • The combination of personal information breached; • If the data was computerized; • If the data was encrypted, redacted, or otherwise altered; • If the data included any kind of key, code or cipher; • If it was acquired by a person that may compromise the security, confidentiality, or integrity of the personal information; or • If, after an appropriate investigation by the person or the person's consultation with relevant federal, state, or local agencies responsible for law enforcement, it can be determined the risk of identity theft or other fraud to any consumer is not reasonably likely to occur. (Such a determination must be documented in writing and maintained for five years.)

CSR®
Privacy Made Simple℠

Breach Reporting
There may be specific time limits to report a breach and complete consumer notification. There may be specific entities to report to.
The notification may be delayed if law enforcement indicates the notification may impede a criminal investigation or jeopardize national or homeland security. The request must be made in writing or the data owner must document the name of the officer and their agency at the time the delay is requested. Notice must be provided following discovery or notification of a breach without unreasonable delay. The notice must include specific comprehensive information such as the description of the incident, the type of personal information that was obtained, etc. If more than 1,000 residents are required to receive notifications, the incident must also be reported to the attorney general and all consumer reporting agencies with specific information.
Notifications
Notifications to the consumer may require detailed information and sometimes provision of services. The notifications must be sent or delivered in a specific manner.
The notification may be delivered by mail, electronically (with a valid email address, consent to communications electronically and consistent with US Code Section 7001 of Title 15), or telephone, if such contact is made directly with the affected consumers). A substitute notice can be sent if the business demonstrates that the cost of providing the notice would exceed $100,000 or the persons to be notified exceeds 150,000, or they do not have sufficient contact information (to complete the methods in the first paragraph or consent). For insufficient contact information, the substitute notice only applies to those consumers unable to be identified. Substitute notice must consist of ALL of the following: email notice, conspicuous posting on their website, and notification to major statewide media.
Penalties
In almost all states, the state attorney general may bring action upon an entity that has not complied with their breach and/or consumer notification laws.
If the code if violated, the attorney general has exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

CSR®
Privacy Made Simple℠

Applicable Laws
For more information, review your state statutes.
The statutes include, but are not limited to: Missouri Revised Statutes: • Title XXVI Trade and Commerce Chapter 407 Merchandising Practices § 407.1500.1. All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.
Other Related Laws
In order to ensure protection of personal information BEFORE a breach happens, many states now have laws for data protection, data retention, and/or data disposal.
The statutes include, but are not limited to: Missouri Revised Statutes: • Title XXVI Trade and Commerce Chapter 407 Merchandising Practices "Credit User Protection Law" § 407.430 – 407.436.1 All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.