

# Georgia

## Data Breach Notification Statute (Full Text)

### Ga. Code Ann. § 10-1-911 Definitions

As used in this article, the term:

(1) “Breach of the security of the system” means unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) “Data collector” means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term “data collector” shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

(3) “Information broker” means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

(4) “Notice” means:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or

(D) Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed \$50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

(i) E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified;

(ii) Conspicuous posting of the notice on the information broker’s or data collector’s website page, if the information broker or data collector maintains one; and

(iii) Notification to major state-wide media.

Notwithstanding any provision of this paragraph to the contrary, an information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in

compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

(5) "Person" means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. The term "person" as used in this article shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.

(6) "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, when either the name or the data elements are not encrypted or redacted:

(A) Social security number;

(B) Driver's license number or state identification card number;

(C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

(D) Account passwords or personal identification numbers or other access codes; or

(E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

## Ga. Code Ann. § 10-1-912 Notice of breach of security.

(a) Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.

The statutes and Constitution are current with Acts 281 to 295, 298 to 342, 344 to 364, 366 to 370, 372 to 409, 411 to 413, 416 to 419, 422 to 466, 468 to 478, 480 to 550, and 552 to 561 of the 2018 legislative session. The statutes are subject to changes by the Georgia Code Commission.

## Ga. Code Ann. § 46-5-210

### Definitions

(a) As used in this article, the term:

(1) "Breach of telephone records" means the unauthorized acquisition of telephone records that compromises the security, confidentiality, or integrity of that information as maintained by the telecommunications company.

(2) "End user" means any person, corporation, partnership, firm, municipality, cooperative, organization, governmental agency, building owner, or other entity provided with a telecommunications service for its own consumption and not for resale.

(3) "Notice" means:

(A) Written notice;

(B) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or

(C) Substitute notice, if the telecommunications company demonstrates that the cost of providing notice would exceed \$250,000.00, that the affected class to be notified exceeds 500,000 individuals, or that the telecommunications company does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

(i) E-mail notice, if the telecommunications company has e-mail addresses for the individuals to be notified;

(ii) Conspicuous posting of the notice on the telecommunications company's website, if the telecommunications company maintains one; and

(iii) Notification to major state-wide media.

(4) "Telephone record" means information retained by a telecommunications company that relates to the telephone number dialed by the customer, the number of telephone calls directed to a customer, or other data related to the telephone calls typically contained on a customer telephone bill, such as the time the calls started and ended, the duration of the calls, the time of day the calls were made, and any charges applied. For purposes of this article, any information collected and retained by, or on behalf of, customers utilizing caller identification or other similar technology does not constitute a telephone record.

## Ga. Code Ann. § 46-5-214

### Notification required in the event of breach; procedures; violations

(a) In the event of a breach of a telephone record concerning a Georgia resident, the telecommunications company must provide notice to the Georgia resident immediately following discovery or notification of the breach if such breach is reasonably likely to cause quantifiable harm to the Georgia resident. The notice must be made in

the most expedient manner possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the telephone record.

(b) Notwithstanding any provisions of this article to contrary, a telecommunications company that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Code section shall be deemed to be in compliance with the notification requirements of this Code section if it notifies the individuals who are the subject of the notice in accordance with its policies in the event of a breach of the security of the system.

(c) The notice required by this Code section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this Code section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(d) A violation of this Code section constitutes an unfair or deceptive practice in consumer transactions within the meaning of Part 2 of Article 15 of Chapter 1 of Title 10, the "Fair Business Practices Act of 1975."

End of Document.