Senate Bill 161

By: Senators Kennedy of the 18th, Gooch of the 51st, Dolezal of the 27th, Robertson of the 29th, Anavitarte of the 31st and others

A BILL TO BE ENTITLED

AN ACT

To amend Chapter 60 of Title 36 of the Official Code of Georgia Annotated, relating to general provisions applicable to counties and municipal corporations, so as to ensure that counties and municipalities are protected from cyber attacks directed at contractors and suppliers by requiring certain provisions in county and municipal contracts; to amend Chapter 25 of Title 50 of the Official Code of Georgia Annotated, relating to the Georgia Technology Authority, so as to ensure that state agencies are protected from cyber attacks directed at contractors and suppliers by requiring certain provisions in contracts entered into by the state and its agencies; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 60 of Title 36 of the Official Code of Georgia Annotated, relating to general provisions applicable to counties and municipal corporations, is amended by adding a new Code section to read as follows:

"36-60-30.

(a) As used in this Code section, the term:

(1) 'Contractor' means any person entering a contractual relationship with a local government that is either based upon a written contract or that provides a person with electronic or physical access to any local government computer system, data systems, or facility controlled or affiliated with such local government, and shall include all subcontractors of such person.

(2) 'Data breach' means unauthorized access or disclosure of data under the contractor's control or in the contractor's possession contrary to the terms of a contract between the contractor and local government.

(3) 'Local government' means any county or municipality of this state.

(4) 'Person' means any natural person, partnership, corporation, trust, association, or any other legal entity, other than the federal government or the state or a political subdivision, agency, or authority thereof.

(5) 'Personally identifiable information' means an individual's first name, last name, home address, personal phone numbers, date of birth, email addresses.

(b) The following requirements shall apply to all local government contracts entered into or renewed after January 1, 2024, in this state:

(1) That the contractor shall remain compliant with the external data privacy program outlined in this Code section, and upon written request by the local government, shall provide any evidence demonstrating compliance via written response within seven days or less;

(2) In the event of a data breach, the contractor shall use reasonable efforts to notify the local government immediately of such data breach unless notification to an alternative or additional entity is provided in the contract. The contractor shall take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the data breach. The contractor shall give highest priority to immediately correcting any data breach and shall devote such resources as may be required to accomplish that goal. The contractor shall provide the local government with all information necessary to enable the

local government to fully understand the nature and scope of the data breach, the scope of such information being at the discretion of the local government; and

(3) The contractor shall enact an external data privacy program that shall include, at a minimum, the following elements:

(A) The contractor shall perform, at a minimum, quarterly scans for each of its employees' personally identifiable information:

(i) Across at least 350 known data brokers or people search websites, using such site's public onsite search functionality; and

(ii) Using at least one major internet search engine, determine what information is returned and easily obtainable using such search.

Such quarterly scans may be accomplished by manual effort or using an automated service, so long as such scans are definitive;

(B) The contractor shall maintain a report of the information discovered from the scans provided in subparagraph (A) of this paragraph. Using such information, the contractor shall conduct an annual privacy risk assessment to evaluate its ongoing privacy policies and security and access practices against standards identified in the contract based on the data such contractor will have access to or otherwise handle pursuant to its contract with the local government;

(C) The reports described in subparagraph (B) of this paragraph shall be maintained by the contractor for a period of no less than three years, including after the conclusion of the contract period, and shall be made available within seven days of a request from the local government or alternative entity provided in the contract in the event a past data breach is found to have occurred, of a suspected data breach, or of an actual data breach described in subparagraph (A) of paragraph (2) of this Code section. The contract between the local government and contractor may provide that the local government maintain such records; and

(D) The contractor shall certify to the local government that it conducts at least annually a privacy training for such contractor's employees that includes information on its external data privacy program, and the risks associated with data brokers and external data privacy, including, but not limited to, that external data exposures are used to craft highly targeted social engineering and spear phishing attacks. Such privacy training shall not preclude or supplant any privacy training the contractor already provides to its employees.

(c) Contractors shall certify to the local government that it maintains or otherwise includes as part of its operations an external data privacy program no less stringent than the external data privacy program as described in subparagraph (b)(3)(D) of this Code section. This external data privacy program shall not preclude or supplant any similar program already provided.

(d) This Code section shall not apply to any intergovernmental contracts or agreements a local government enters with another local government, the federal government, the state, or a political subdivision, agency, or authority thereof.″

SECTION 2.

Chapter 25 of Title 50 of the Official Code of Georgia Annotated, relating to the Georgia Technology Authority, is amended by revising Code Section 50-25-7.3, which is reserved, as follows:

″50-25-7.3.

(a) As used in this Code section, the term:

(1) 'Contractor' means any person entering a contractual relationship with the authority that is either based upon a written contract or that provides a person with electronic or physical access to any state or agency computer system, data systems, or facility controlled or affiliated with the State of Georgia or one or more of its agencies, and shall include all subcontractors of such person.

(2) 'Data breach' means unauthorized access or disclosure of data under the contractor's control or in the contractor's possession contrary to the terms of a contract between the contractor and the agency or authority.

(3) 'Person' means any natural person, partnership, corporation, trust, association, or any other legal entity, other than the federal government or the state or a political subdivision, agency, or authority thereof.

(4) 'Personally identifiable information' means an individual's first name, last name, home address, personal phone numbers, date of birth, email addresses.

(b) The authority shall, pursuant to its authorization under this chapter, apply the following contractual requirements applicable to contractors, vendors, suppliers, and other entities contracting or renewing a contract with an agency after January 1, 2024, apply which shall include the following:

(1) That the contractor shall remain compliant with the external data privacy program outlined in this Code section, and upon written request by either the authority or the agency, shall provide any evidence demonstrating compliance via written response within seven days or less;

(2) In the event of a data breach, the contractor shall use reasonable efforts to notify the authority and the agency immediately of such data breach unless notification to an alternative or additional entity is provided in the contract. The contractor shall take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the data breach. The contractor shall give highest priority to immediately correcting any data breach and shall devote such resources as may be required to accomplish that goal. The contractor shall provide the authority and the agency with all information necessary to enable the authority and the agency to fully understand the nature and scope of the data breach, the scope of such information being at the discretion of the authority; and

(3) The contractor shall enact an external data privacy program that shall include, at a minimum, the following elements:

(A) The contractor shall perform, at a minimum, quarterly scans for each of its employees' personally identifiable information:

(i) Across at least 350 known data brokers or people search websites, using such site's public onsite search functionality; and

(ii) Using at least one major internet search engine, determine what information is returned and easily obtainable using such search.

Such quarterly scans may be accomplished by manual effort or using an automated service, so long as such scans are definitive;

(B) The contractor shall maintain a report of the information discovered from the scans provided in subparagraph (A) of this paragraph. Using such information, the contractor shall conduct an annual privacy risk assessment to evaluate its ongoing privacy policies and security and access practices against standards identified in the contract based on the data such contractor will have access to or otherwise handle pursuant to its contract with the local government;

(C) The reports described in subparagraph (B) of this paragraph shall be maintained by the contractor for a period of no less than three years, including after the conclusion of the contract period, and shall be made available within seven days of a request from the local government or alternative entity provided in the contract in the event a past data breach is found to have occurred, of a suspected data breach, or of an actual data breach described in subparagraph (A) of paragraph (2) of this Code section. The contract between the agency or the authority and contractor may provide that the agency or the authority maintain such records; and

(D) The contractor shall certify to the authority and the agency that it conducts at least annually a privacy training for such contractor's employees that includes information on its external data privacy program, and the risks associated with data brokers and

external data privacy, including, but not limited to, that external data exposures are used to craft highly targeted social engineering and spear phishing attacks. Such privacy training shall not preclude or supplant any privacy training the contractor already provides to its employees.

(c) Contractors shall certify to the authority and the agency that it maintains or otherwise includes as part of its operations an external data privacy program no less stringent than the external data privacy program as described in subparagraph (b)(3)(D) of this Code section. This external data privacy program shall not preclude or supplant any similar program already provided.

(d) This Code section shall not apply to any intergovernmental contracts or agreements an agency enters with another agency, the federal government, the state, or a local government, political subdivision, agency, or authority thereof. ~~Reserved~~."

SECTION 3.

All laws and parts of laws in conflict with this Act are repealed.