

**LOCAL LAWS
OF
THE CITY OF NEW YORK
FOR THE YEAR 2021**

No. 151

Introduced by Council Members Brooks-Powers, Yeger, Kallos, Louis and Barron (by request of the Mayor).

A LOCAL LAW

To amend the administrative code of the city of New York, in relation to agency actions and licensee disclosures in the event of a breach of security

Be it enacted by the Council as follows:

Section 1. Section 10-501 of the administrative code of the city of New York, as added by local law number 45 for the year 2005, is amended to read as follows:

§ 10-501. Definitions. For the purposes of this chapter,

a. The term [“personal identifying information” shall mean any person's date of birth, social security number, driver's license number, non-driver photo identification card number, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person. This term shall apply to all such data, notwithstanding the method by which such information is maintained.] *“personal information” shall mean any information concerning an individual that because of a name, number, symbol, mark or other identifier, can be used to identify that individual.*

b. The term “private information” shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element alone or the combination of such information plus the data element is not encrypted, or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver’s license number or non-driver identification card number;

(3) account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual’s financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access an individual’s financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual’s unique physical characteristics, such as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, any of which is collected, retained, converted, stored or shared to identify an individual; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

“Private information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

[b.] *c. The term “breach of security” shall mean the unauthorized access, acquisition, disclosure or use [by an employee or agent of an agency, or the unauthorized possession by*

someone other than an employee or agent of an agency, of personal identifying information] *of computerized data* that compromises the security, confidentiality or integrity of [such] *private information maintained by an agency*. Good faith or inadvertent [possession of] *access, acquisition, disclosure, or use of* any [personal identifying] *private* information by an employee or agent of an agency for the legitimate purposes of the agency, and good faith or legally mandated disclosure of any [personal identifying] *private* information by an employee or agent of an agency for the legitimate purposes of the agency shall not constitute a breach of security, *but in such instances an agency must comply with the protocols issued pursuant to subdivision i of section 10-502.*

d. The term "consumer reporting agency" shall mean any person that, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

§ 2. Section 10-502 of the administrative code of the city of New York, as added by local law number 45 for the year 2005, is amended to read as follows:

§ 10-502. Agency disclosure of a [security breach] *breach of security*. a. Any city agency that owns [or], leases, or licenses data that includes [personal identifying information and any city agency that maintains but does not own data that includes personal identifying] *private* information[,] shall [immediately] *promptly* disclose to the [police department] *chief privacy officer, office of cyber command and department of information technology and telecommunications* any breach of security following discovery by a supervisor or manager, or

following notification to a supervisor or manager, of such breach if such [personal identifying] *private* information was, or is reasonably believed to have been, *accessed*, acquired, *disclosed*, or *used* by an unauthorized person.

b. Subsequent to compliance with the provisions set forth in subdivision a of this section, any city agency that owns [or], leases, or *licenses* data that includes [personal identifying] *private* information shall disclose, in accordance with the procedures set forth in [subdivision] *subdivisions d, e and f* of this section, any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to any [person] *individual* whose [personal identifying] *private* information was, or is reasonably believed to have been, *accessed*, acquired, *disclosed*, or *used* by an unauthorized person.

c. [Subsequent to compliance with the provisions set forth in subdivision a of this section, any] *Any* city agency that maintains but does not own, *lease*, or *license* data that includes [personal identifying] *private* information shall disclose[, in accordance with the procedures set forth in subdivision d of this section,] any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to the owner, lessor or licensor of the data if the [personal identifying] *private* information was, or is reasonably believed to have been, *accessed*, acquired, *disclosed*, or *used* by an unauthorized person.

d. The disclosures required by subdivisions b and c of this section shall be made as soon as practicable by a method reasonable under the circumstances[. Provided], *provided* said method is not inconsistent with the legitimate needs of law enforcement or any other investigative or protective measures necessary to restore the [reasonable] integrity of the data system[,

disclosures]. *Disclosures required by subdivision b of this section shall be made to each affected individual by at least one of the following means:*

1. Written notice [to the individual at his or her last known address]; or

2. [Verbal notification to the individual by telephonic communication] *Telephonic notification, provided that a log of each such notification is maintained by the agency that notifies the affected individuals; or*

3. Electronic notification [to the individual at his or her last known e-mail address], *provided that the affected individual has expressly consented to receiving such notification in electronic form and a log of each such notification is maintained by the agency that notifies affected individuals in such form; provided further, however, that in no case shall any city agency, individual, or business require an individual to consent to accepting notification in such form as a condition of establishing any relationship or engaging in any transaction.*

e. Should disclosure pursuant to paragraph one, two or three of subdivision d be impracticable or inappropriate given the circumstances of the breach and the identity of the victim, such disclosure shall be made by a mechanism [of the agency's election, provided such mechanism] *that is reasonably targeted to the individual in a manner that does not further compromise the integrity of the [personal] private information.*

f. *In the event that five thousand or more New York residents are to be notified at one time pursuant to this section, the agency shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected individuals. Such notice shall be made without delaying notice to affected New York residents.*

g. Notice to affected individuals under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the agency reasonably determines, in accordance with the protocols established pursuant to subdivision i of this section, that such exposure will not likely result in misuse of such information, or financial, personal, or reputational harm to the affected individuals. Such a determination must be documented in writing and maintained for at least five years.

h. If notice of a breach of security is made to affected individuals pursuant to any law or rule of the state of New York, or pursuant to a law described in paragraph b of subdivision 2 of section 208 of the state technology law, nothing in this section shall require any additional notice to those affected individuals, but notice still shall be provided pursuant to subdivision a of this section.

i. The office of cyber command, in consultation with the chief privacy officer and the department of information technology and telecommunications, shall issue protocols for agency coordination and recordkeeping for any breach of security and any incident that is not a breach of security but involves the good faith or inadvertent access, acquisition, disclosure, or use of any private information by an employee or agent of an agency for the legitimate purposes of the agency. Such protocols may apply to all agencies or a subset thereof.

j. Notifications made pursuant to this section may overlap with notifications required pursuant to chapter 12 of title 23, including the regulations, policies and protocols issued by the chief privacy officer pursuant to such chapter. Nothing in this section or such chapter shall require duplicate notifications, as long as any notice provided meets any applicable requirements of both this law and such chapter.

§ 3. Section 10-503 of the administrative code of the city of New York, as added by local law number 45 for the year 2005, is amended to read as follows:

§ 10-503 Agency disposal of [personal identifying] *private* information. An agency that discards records containing any individual's [personal identifying] *private* information shall do so in a manner intended to prevent retrieval of the information contained therein or thereon.

§ 4. Chapter 1 of title 20 of the administrative code of the city of New York is amended by adding a new section 20-117 to read as follows:

§ 20-117 *Licensee disclosure of breach of security, notification requirements. Any person who is required to be licensed pursuant to chapter two of this title or pursuant to provisions of state law enforced by the department, and who is also required to make a notification pursuant to subdivision 2 or 3 of section 899-aa of the general business law, shall promptly submit a copy of such notification to the department. Such notice shall be made without delaying notice to any individual whose private information was, or is reasonably believed to have been, accessed, acquired, disclosed, or used by an unauthorized person.*

§ 5. Subchapter 1 of chapter 3 of title 17 of the administrative code of the city of New York is amended by adding a new section 17-302 to read as follows:

§ 17-302 *Licensee disclosure of breach of security, notification requirements. Every recipient of a license issued pursuant to this title who is required to make a notification pursuant to subdivision 2 or 3 of section 899-aa of the general business law shall promptly submit a copy of such notification to the department. Such notice shall be made without delaying notice to any individual whose private information was, or is reasonably believed to have been, acquired by an unauthorized person.*

§ 6. Section 19-546 of the administrative code of the city of New York is amended by adding a new subdivision d to read as follows:

d. Every recipient of a license obtained pursuant to this chapter who is required to make a notification pursuant to subdivision 2 or 3 of section 899-aa of the general business law shall promptly submit a copy of such notification to the commission. Such notice shall be made without delaying notice to any individual whose private information was, or is reasonably believed to have been, acquired by an unauthorized person.

§ 7. This local law takes effect 120 days after it becomes law.

THE CITY OF NEW YORK, OFFICE OF THE CITY CLERK, s.s.:

I hereby certify that the foregoing is a true copy of a local law of The City of New York, passed by the Council on November 10, 2021 and returned unsigned by the Mayor on December 13, 2021.

MICHAEL M. McSWEENEY, City Clerk, Clerk of the Council.

CERTIFICATION OF CORPORATION COUNSEL

I hereby certify that the form of the enclosed local law (Local Law No. 151 of 2021, Council Int. No. 2410-A of 2021) to be filed with the Secretary of State contains the correct text of the local law passed by the New York City Council, presented to the Mayor and neither approved nor disapproved within thirty days thereafter.

STEPHEN LOUIS, Acting Corporation Counsel.