CHAPTER 50: AURORA RESPONSIBLE DATA CENTER ORDINANCE

Section 50-1. Definitions.

a. Data Center: Has the same definition as in Section 49-103.3 of the Aurora Zoning Ordinance.

b. Greenhouse Gas (GHG): Any gas that contributes to atmospheric greenhouse effect, including CO_2, CH_4, N_2O, SF_6, HFCs, PFCs.

c. Power Usage Effectiveness (PUE): Has the same definition as Section 49-104.3(c)(25) of the Aurora Zoning Ordinance.

d. Water Usage Effectiveness (WUE): Has the same definition as Section 49-104.3(c)(25) of the Aurora Zoning Ordinance.

e. Noise Performance Standard: Has the same definition as Section 49-104.3(c)(25) of the Aurora Zoning Ordinance.

Section 50-2. Applicability.

This Chapter applies to all Data Centers within city limits.

Section 50-3. Performance Standards.

a. All Data Center Facilities developed after April 1, 2026, must meet the standards in Section 49-104.3(c)(25) of the Aurora Zoning Ordinance.

b. Any replacement equipment, including but not limited to generators, chillers, and screening, must meet the standards in Section 49-104.3(c)(25) of the Aurora Zoning Ordinance for any Data Center Facilities developed after April 1, 2026.

c. For purposes of this Section 50-3, “developed” means Data Center Facilities which do not have zoning entitlements pursuant to Chapter 49 of this Code as of April 1, 2026.

Section 50-4. Annual Reporting Required.

All Data Center Facilities must submit annually on or before April 1 of each year to the city’s Department of Development Services the following:

a. An annual energy and water use data report via ENERGY STAR® Portfolio Manager for the previously calendar year; and

b. Third party tested noise level reports for the previous calendar year during both daytime hours and nighttime hours at the property line.

If the Data Center has not been operating for a full year, the data center must submit data for the months it has been in operation. The Director of Development Services ensure that the annually reported data is made publicly available by June 1 of each year.

Section 50-5. Enforcement.

Violations of this Chapter are municipal offenses subject to fines up to and including $1,000 per day per occurrence and any other corrective action the administrative court or circuit court deems appropriate.

CHAPTER 51 –Data Center Privacy Protection Ordinance

Sec. 51-1. Purpose.

To protect Aurora resident privacy and establish rules modeled on the Illinois Biometric Information Privacy Act (“BIPA”) regardless of its status under state law.

Sec. 51-2. Short title.

This Section may be cited as the Data Center Privacy Protection Ordinance.

Sec. 51-3. Legislative findings; intent.

In 2008, the Illinois General Assembly, when passing BIPA, stated that they found all of the following, all of which continue to be true:

“(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."

Sec. 51-4. Definitions.

For the purposes of this Ordinance, the following definitions apply:

a. “Biometric Identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other

medical condition or to further validate scientific testing or screening.

b. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

c. "Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

d. "Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

e. “Data Center” means a facility, whether a single building, or a series of buildings rehabilitated or constructed, which house working servers that primarily

provide the storage, management, distribution, and processing of digital data. These facilities include essential infrastructure like networked computers, data storage systems, environmental controls, and security systems. These uses include but are not limited to electronic storage data center facilities and cryptocurrency center facilities.

f. “Data Center Business” means any company, entity, or organization that provides the storage, management, and/or processing of digital data, or that is doing business as or within a data center.

Sec. 51-5. Application.

No Data Center or Data Center Business located within Aurora City boundaries can violate the provisions within this Ordinance.

Sec. 51-6. Retention; collection; disclosure; destruction.

a. Any Data Center or Data Center Business in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information

has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

b. No Data Center or Data Center Business may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

1. informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

2. informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

3. receives a written release executed by the subject of the biometric identifier or

biometric information or the subject's legally authorized representative.

c. No Data Center or Data Center Business in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

d. No Data Center or Data Center Business in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

1. the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

2. the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

3. the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

4. the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

e. A Data Center or Data Center Business in possession of a biometric identifier or biometric information shall:

1. store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

2. store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Sec. 51-7. Enforcement.

a. Applicability. This Section applies to all Data Centers and Data Center Businesses operating within the City of Aurora that collect, store, process, transmit, or otherwise handle Biometric Identifiers or Biometric Information, as defined under applicable law.

b. Enforcement Authority.

1. The City shall have authority to enforce this Ordinance through its Corporation Counsel or designated enforcement officer.

2. The City may investigate suspected violations, require production of relevant records (subject to lawful confidentiality protections), and conduct compliance reviews.

3. The City may issue notices of violation and impose administrative penalties as provided herein.

4. The City may recover costs associated with enforcement if entity is found in violation of this Ordinance.

c. Violations. It shall constitute a violation of this Ordinance to:

1. Violate any provision of the Aurora Data Center Privacy Protection Ordinance;

2. Fail to maintain required biometric data policies, retention schedules, or security safeguards;

3. Fail to timely file the Annual Certificate of Compliance required herein; or

4. Submit false, misleading, or incomplete information to the City. Each day a violation continues shall constitute a separate offense.

d. Annual Certificate of Compliance.

1. Annual Filing Required. On or before April 1 of each calendar year, each Data Center and Data Center Business subject to this Ordinance shall file with the City Clerk an Annual Certificate of Compliance.

2. Contents of Certification. The Certificate shall be signed under penalty of perjury by a duly authorized corporate officer and shall attest that:

i. The Data Center or Data Center Business is in full compliance with BIPA and this Ordinance;

ii. The Data Center or Data Center Business has not been found liable for any violation of BIPA during the

preceding calendar year, or if such finding occurred, it has disclosed the nature of the violation and corrective actions taken;

iii. All required written biometric data policies, consent procedures, and retention/destruction schedules are in effect and actively implemented;

iv. Reasonable industry-standard administrative, technical, and physical safeguards are maintained.

3. Disclosure of Claims. The Certificate shall disclose any pending BIPA-related litigation, settlement, administrative action, or regulatory investigation involving operations within the City.

4. Independent Review. The City may require, upon reasonable cause, submission of a third-party compliance audit summary prepared by an independent privacy professional.

e. Penalties

1. Administrative fines of not less than $1,000 and not more than $5,000 per violation.

2. Suspension or revocation of local operating permits for repeated or willful violations.

3. Ineligibility for local tax incentives or development agreements during periods of non-compliance.

4. The City may seek injunctive relief in a court of competent jurisdiction.

f. Cumulative Remedies. The remedies provided herein are cumulative and shall not preclude enforcement under state law, including BIPA.

Sec. 51-8. Right of action.

Any person aggrieved by a violation of this Ordinance shall have a right of action in the 18th Judicial Circuit Court of Kane County or as a supplemental claim in a state or federal district court against an offending party. A prevailing party may recover for each violation:

a. against a private entity that negligently violates a provision of this Ordinance, liquidated damages of $1,000 or actual damages, whichever is greater;

b. against a private entity that intentionally or recklessly violates a provision of this Ordinance, liquidated damages of $5,000 or actual damages, whichever is greater;

c. reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

d. other relief, including an injunction, as the State or federal court may deem appropriate.

Sec. 51-9. Construction.

a. Nothing in this Ordinance shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

b. Nothing in this Ordinance shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

c. Nothing in this Ordinance shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

d. Nothing in this Ordinance shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

e. Nothing in this Ordinance shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

SECTION 3. Effective Date

This Ordinance shall take effect 30 days after approval by City Council.