

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<sub>2</sub>, CH<sub>4</sub>, N<sub>2</sub>O, SF<sub>6</sub>, 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.
- ~~a. All generators providing back-up power for Date Center Facilities developed after April 1, 2026, must continue to meet the requirements outlined in 49-104.3(c)(25)(c) of the Aurora Zoning Ordinance. Unless the generators are supplying backup electrical supply during a power outage, testing of generators, regardless of~~

~~2026 February 27, 2026~~

whether installed before or after April 1, 2026, may only occur between the hours of 9:00 am and 5:00 pm Monday through Friday, and not on holidays. No more than two (2) generators may be tested simultaneously.

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

1 Director of Development Services ensure that the annually reported data  
2 is made publicly available by June 1 of each year.

3

4

5 Section 50-5. Enforcement.

6 Violations of this Chapter are municipal offenses subject to fines up to  
7 and including \$1,000 per day per occurrence and any other corrective  
8 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

1 compromised, the individual has no recourse, is at heightened risk  
2 for identity theft, and is likely to withdraw from biometric-  
3 facilitated transactions.

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

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

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

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

17  
18 Sec. 51-4. Definitions.

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

- 20 a. "Biometric Identifier" means a retina or iris scan,  
21 fingerprint, voiceprint, or scan of hand or face geometry.  
22 Biometric identifiers do not include writing samples, written  
23 signatures, photographs, human biological samples used for  
24 valid scientific testing or screening, demographic data,  
25 tattoo descriptions, or physical descriptions such as height,

1 weight, hair color, or eye color. Biometric identifiers do not  
2 include donated organs, tissues, or parts as defined in the  
3 Illinois Anatomical Gift Act or blood or serum stored on behalf  
4 of recipients or potential recipients of living or cadaveric  
5 transplants and obtained or stored by a federally designated  
6 organ procurement agency. Biometric identifiers do not include  
7 biological materials regulated under the Genetic Information  
8 Privacy Act. Biometric identifiers do not include information  
9 captured from a patient in a health care setting or information  
10 collected, used, or stored for health care treatment, payment,  
11 or operations under the federal Health Insurance Portability  
12 and Accountability Act of 1996. Biometric identifiers do not  
13 include an X-ray, roentgen process, computed tomography, MRI,  
14 PET scan, mammography, or other image or film of the human  
15 anatomy used to diagnose, prognose, or treat an illness or  
16 other medical condition or to further validate scientific  
17 testing or screening.

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

24 c. "Confidential and sensitive information" means personal  
25 information that can be used to uniquely identify an individual

1 or an individual's account or property. Examples of  
2 confidential and sensitive information include, but are not  
3 limited to, a genetic marker, genetic testing information, a  
4 unique identifier number to locate an account or property, an  
5 account number, a PIN number, a pass code, a driver's license  
6 number, or a social security number.

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

10 e. "Data Center" means a facility, whether a single building, or  
11 a series of buildings rehabilitated or constructed, which  
12 house working servers that primarily provide the storage,  
13 management, distribution, and processing of digital data.  
14 These facilities include essential infrastructure like  
15 networked computers, data storage systems, environmental  
16 controls, and security systems. These uses include but are not  
17 limited to electronic storage data center facilities and  
18 cryptocurrency center facilities.

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

23  
24 Sec. 51-5. Application.

~~2026~~ ~~February 27, 2026~~

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

3  
4 Sec. 51-6. Retention; collection; disclosure; destruction.

5 a. Any Data Center or Data Center Business in possession of  
6 biometric identifiers or biometric information must develop a  
7 written policy, made available to the public, establishing a  
8 retention schedule and guidelines for permanently destroying  
9 biometric identifiers and biometric information when the  
10 initial purpose for collecting or obtaining such identifiers  
11 or information has been satisfied or within 3 years of the  
12 individual's last interaction with the private entity,  
13 whichever occurs first. Absent a valid warrant or subpoena  
14 issued by a court of competent jurisdiction, a private entity  
15 in possession of biometric identifiers or biometric  
16 information must comply with its established retention  
17 schedule and destruction guidelines.

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

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

- 1 2. informs the subject or the subject's legally  
2 authorized representative in writing of the  
3 specific purpose and length of term for which a  
4 biometric identifier or biometric information is  
5 being collected, stored, and used; and
- 6 3. receives a written release executed by the subject  
7 of the biometric identifier or biometric  
8 information or the subject's legally authorized  
9 representative.

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

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

- 19 1. the subject of the biometric identifier or  
20 biometric information or the subject's legally  
21 authorized representative consents to the  
22 disclosure or redisclosure;
- 23 2. the disclosure or redisclosure completes a  
24 financial transaction requested or authorized by  
25 the subject of the biometric identifier or the

1 biometric information or the subject's legally  
2 authorized representative;

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

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

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

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

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

20  
21 Sec. 51-7. Enforcement.

22 a. Applicability. This Section applies to all Data Centers and  
23 Data Center Businesses operating within the City of Aurora  
24 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

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

4 d. Annual Certificate of Compliance.

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

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

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

15 ii. The Data Center or Data Center Business  
16 has not been found liable for any  
17 violation of BIPA during the preceding  
18 calendar year, or if such finding occurred,  
19 it has disclosed the nature of the  
20 violation and corrective actions taken;

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

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

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

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

12 e. Penalties

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

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

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

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

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

~~2026~~ ~~February 27, 2026~~

1 Sec. 51-8. Right of action.

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

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

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

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

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

16 Sec. 51-9. Construction.

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

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

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

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

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

14  
15 SECTION 3. Effective Date

16 This Ordinance shall take effect ~~30 days after approval by City~~  
17 ~~Council~~ April 1, 2026.