To: Public Agencies

From: Office of the Attorney General, Privacy Section
Office of Policy and Management, Chief Data Officer

Date: June 14, 2026

Subject: Guidance

---

Pursuant to the recently enacted **CONN. GEN. STAT. § 4-67ee, Public agency disclosure of personal information. Restricted. Exceptions. Attorney General action** ("the Act"),[1] the Attorney General, in conjunction with the Chief Data Officer, issues the following guidance to public agencies.

**Overall**. The Act provides: "(a) No public agency, … or employee, appointee, officer or official or any other individual acting on behalf of a public agency shall disclose an individual's Personal Information that is not a matter of public record to any other individual or entity that is not a public agency or employee, appointee, officer or official or any other individual acting on behalf of a public agency" unless under certain circumstances set forth in the Act.[2]

The act defines "personal information" as: "(1) an individual's address; (2) an individual's workplace or hours of work; (3) an individual's school or school hours; or (4) the date, time or place of an individual's hearings, proceedings or appointments with a public agency."[3] ("Personal Information").

The act defines "public agency" as defined "in section 1-200 of the general statutes," or as: "(A) Any executive, administrative or legislative office of the state or any political subdivision of the state and any state or town agency, any department, institution, bureau, board, commission, authority or official of the state or of any city, town, borough, municipal corporation, school district, regional district or other district or other political subdivision of the state, including any committee of, or created by, any such office, subdivision, agency, department, institution, bureau, board, commission, authority or official, and also includes any judicial office, official, or body or committee thereof but only with respect to its or their administrative functions, and for purposes of this subparagraph, "judicial office" includes, but is not limited to, the Division of Public Defender Services; (B) Any person to the extent such person is deemed to be the functional equivalent of a public agency pursuant to law; or (C) Any "implementing agency", as defined in section 32-222." ("Public agency").

**Purpose.** As a guiding principle, the clear intent of the Act is to prevent disclosure of the time or location of individuals that is not otherwise public by public agencies. If that

[1] Enacted through 2025 Conn. Acts No. 25-3 (Spec. Sess.) [hereinafter "the Act"].
[2] CONN. GEN. STAT. 4-67ee (a)(1-6) (2025).
[3] Note that the Office of Legislative Research Bill Analysis issued Nov. 13, 2025, lists the categories as conjunctive ("workplace *and* work hours") (italics added). However, the statute is disjunctive, and each element is "Personal Information" for the purposes of the Act. *N.B.* that "Personal Information" must be associated with an individual.

information is already a matter of public record, it may be disclosed.[4] In the event the Act conflicts with Connecticut's Freedom of Information Act ("FOIA"), FOIA prevails.[5]

**Impact.** Prior to the Act, Personal Information that was not public record was not disclosable, though that non-disclosure was governed by specific law, regulation, or policy. Now, the Act specifically makes the prohibition on disclosure statutory, subject to injunctive relief.[6]

**Process.** In order to comply with the Act, public agencies should undertake the following processes.

1. **Public agencies should maintain and regularly update an inventory of the agency's data.** Executive branch agencies[7] are required to develop an annual inventory of data.[8] Public agencies outside the executive branch should consider a similar best practice, to document the data "collected or possessed" by the public agency and should include in their data inventory a list of the categories of Personal Information contained in the Act.[9] Implementing this best practice to document the scope of personal information managed by the public agency will help prevent any disclosure of personal information by the public agency or those working on its behalf that would violate the Act.

2. The list of categories of personal information includes: (1) an individual's address; (2) an individuals' workplace or hours of work; (3) an individual's school or school hours; and (4) the date, time or place or an individual's hearings, proceedings or appointments with a public agency.[10] Locations that are reasonably ascertainable by physical address, name of location, or precise geolocation data should be presumptively included. For example, "State Office Building," or "165 Capitol Avenue," as well as any other sufficient descriptors to ascertain a person's whereabouts are functionally equivalent terms for "workplace". Similarly, hours or time that is reasonably ascertainable by description should be included in "hours of work," or "school hours." For example, "8:00 a.m. to 5:00 p.m.," or "Business Hours" are functionally equivalent terms.

---

[4] CONN. GEN. STAT. § 4-67ee(a).
[5] *Id*. at (e).
[6] *Id*. at (c).
[7] CONN. GEN. STAT. § 4-67o(2).
[8] CONN. GEN. STAT. § 4-67p(g).
[9] CONN. GEN. STAT. § 4-67ee(b).
[10] *See supra* note 3.

3. **Public agencies should determine if Personal Information is a public record.**[11] This determination may be made in conjunction with the Agency's Data Inventory whether the categories of Personal Information are already public record. If the categories are not already public record, a determination as to how the data is being used must be made prior to disclosure of such Personal Information. If the Personal Information is public record, disclosure is in compliance with the Act.

4. **Public agencies should determine their authority to disclose Personal Information.** If the Personal Information is to be shared with anyone other than an agency or employee, appointee, officer or official or any other individual acting on behalf of an agency, that processing must be under cover of authority, including statute, regulation, contract, or data use agreement.[12] If disclosure of the Personal Information is otherwise permitted by existing state statute, regulation, contract, or data use agreement, disclosure is in compliance with the Act.[13] This also applies to permissible disclosure under certain Federal laws, particularly with respect to student exchange programs[14] and to health information[15]. Also, if the Personal Information is customarily publicly disclosed, such disclosure is in compliance with the Act.[16]

5. **Public agencies should develop policies and procedures for managing requests for information.** Executive branch agencies are required to develop "procedures to ensure that requests for data that the agency receives are complied with in an appropriate and prompt manner."[17] Other public agencies should consider implementing a similar best practice to ensure that requests for Personal Information are adequately reviewed for the authority to release the information and compliance with the Act.

6. **Public agencies should determine if a law enforcement exception exists.** Absent authority, an agency may still disclose Personal Information in furtherance of a criminal investigation so long as such disclosure is not otherwise prohibited by law.[18] If the Personal Information is required in furtherance of a criminal investigation other

---

[11] "Public record" for the purposes of the Act has the same meaning as the Freedom of Information Act. CONN. GEN. STAT. § 1-210(a).
[12] CONN. GEN. STAT. § 4-67ee (a)(3-5).
[13] *Id*. at (a)(3).
[14] *Id*. at (a)(4).
[15] *Id*. at (a)(5).
[16] *Id*. at (a)(6). Examples include, but are not limited to, occupational or business license verification, voter registration and research data.
[17] CONN. GEN. STAT. § 4-67p(b).
[18] CONN. GEN. STAT. § 4-67ee(a)(2). However, see exceptions related to civil immigration detainers, as applied to law enforcement. Conn. Gen. Stat. § 54-192h. For additional guidance on the Trust Act, CONN. GEN. STAT. . § 54-192h, please see this guidance memorandum.

than related to a civil immigration detainer, disclosure is in compliance with the Act. The purpose of the Act was to increase existing data protection, not eliminate them. Thus, to the extent other statutes may prohibit disclosure of the same information for the purpose of a criminal investigation, such disclosure remains prohibited.[19] To demonstrate compliance, agencies receiving requests from law enforcement agencies should document the request and retain all relevant materials. As described earlier, developing a process to manage requests for a public agency's data is a best practice and will facilitate compliance with the Act.

7. **Public agencies should determine if consent through written authorization has been given.** An agency may disclose Personal Information if the agency has written authorization from the individual to whom the information pertains.[20] Nothing in the Act requires the agency to seek written authorization, but nothing in the Act prevents agencies from seeking consent in lieu of performing any other analysis. Agencies in many instances are required to gather written authorization or consent from individuals. In the event that disclosure is performed through consent, agencies may need to revise existing consent forms and should have in place a process to document, retain and update consent as needed to demonstrate compliance with the Act.

8. **Public agencies should review and update contracts and data use agreements to assist in compliance with the Act.** Contracts and data use agreements that allow Personal Information to be shared or accessed should be reviewed for compliance with the Act prior to renewal or amendment.[21] While reviewing contracts, agencies should consider whether defining Personal Information should be designated as "Confidential Information" [22] in order to add contractual protections since the Act does not apply to entities, but only individuals. New contracts or data use agreements should contain similar protections.

---

[19] For example, the Connecticut Shield Act prohibits disclosure of patient information "in furtherance of any interstate investigation or proceeding seeking to impose civil or criminal liability upon a person or entity for (1) the provision, seeking or receipt of or inquiring about reproductive health care services, as defined in section 52-571m, that are legal in this state, or (2) assisting any person or entity providing, seeking, receiving or responding to an inquiry about reproductive health care services, as defined in section 52-571m, that are legal in this state." CONN. GEN. STAT. § 54-155a.

[20] CONN. GEN. STAT. § 4-67ee(a)(1). Note that written authorization must be from a parent or guardian if the individual is a minor.

[21] *N.B.* The Act applies only to "any other individual acting on behalf of a public agency," and not any other *person*. The Act does not apply to *entities* with which an agency has a contract but would apply to the individuals working for the vendor on behalf of the contracting agency. The term "person" includes both natural persons (or individuals) or legal persons, including entities.

[22] CONN. GEN. STAT. § 4e-70(a)(4).

9. **Public agencies should provide notice to recipients where appropriate.** Public agencies that share or provide "Personal Information" should provide notice of the Act to the parties to the contracts or data use agreement who are recipients of Personal Information. At a minimum, this notice should occur upon renewal, updating, or revision of the applicable contract or data use agreement. Notice should also occur if there is a substantial or procedural change in the sharing or provision of data with that counterparty. For example, if a data sharing agreement is in place that covers Personal Information, but that Personal Information has not yet been previously shared or provided, notice of the Act should be sent to the receiving party prior to actually sharing the Personal Information or making it available.

10. **Public agencies should establish or update remedial measures.** In the event of impermissible disclosure of Personal Information, public agencies should take steps to remedy the disclosure, including, as appropriate, contacting the receiving party to request secure disposal of the data, notifying the individual to whom the information applies, and documenting the remedial efforts. If an agency is aware of an impermissible disclosure of Personal Information by an individual acting on behalf of that agency, the agency should notify that individual as well as the entity employing that individual to take remedial steps. If the agency is unable to secure remediation in this instance, the agency should refer the matter to the Attorney General's Office.

11. **Public agencies should keep in mind that agencies, public officials and employees remain liable for knowing and willful violations of certain provisions of FOIA.** While addresses of individuals constitute Personal Information for the purposes of the Act, agencies should be aware that the knowing and willful disclosure of residential addresses of certain individuals is still subject to action by the Freedom of Information Commission.[23] Such action is separate and distinct from any action by the Attorney General pursuant to the Act.[24]

12. **Public agencies should take note of the remedies afforded under the Act.** In the event of violation of the Act, the Attorney General may request injunctive relief in the Superior Court.[25]

---

[23] CONN. GEN. STAT. § 1-217.

[24] CONN. GEN. STAT. § 4-67ee (e).

[25] *Id*. at (c). Note, however, that such injunctive relief does not apply where an agency, officer, or employee is acting in an official capacity and indemnification, as determined by the Attorney General, would apply.