



Report Number: C2019-0560
Meeting: Combined Meeting of Council
Meeting Date: 2019 April 29

NOTICE OF MOTION

RE: CITY OF CALGARY CITIZEN PRIVACY DATA PRACTICES

Sponsoring Councillor: COUNCILLOR DIANE COLLEY-URQUHART

1. WHEREAS there are three Alberta laws that have specific requirements relating to privacy and the protection of personal information (personal data) including the Freedom of Information and Privacy Act (FOIP), the Health Information Act (HIA) and the Personal Information Protection Act (PIPA);

2. AND WHEREAS in Alberta, all public bodies are encouraged to complete Privacy Impact Assessments (PIA) for proposed legislative schemes, projects, administrative practices or information systems/technologies that involve the collection, use and/or disclosure of personal data (particularly where the projects involve a level of information sharing amongst multiple parties);

3. AND WHEREAS citizen data held by The City of Calgary (The City) becomes a government record that may be shared internally with the unifying One Calgary approach between Business Units (if done in accordance with the statutory privacy principles applicable to The City);

4. AND WHEREAS any internal sharing of citizen data within The City has the potential to result in the comingling of personal data point sets that were previously maintained in a separate or partitioned manner;

5. AND WHEREAS The City and its entities (example CMLC, AHCC) while operating under the Municipal Government Act (MGA) also collect a significant amount of personal data from citizens in order to deliver community programs and services;

6. AND WHEREAS City Administration is in the process of undertaking work with all Business Units with regard to:

- a. Knowing what data they possess and classifying and protecting;
- b. Working cohesively and sharing in a cross-functional way to coordinate program and service delivery;
- c. Defining the use of personal data in accordance with such delivery requirements;
- d. Addressing the appropriate retention schedule; and
- e. Defining the restrictions on the sharing of personal data with third parties.

7. AND WHEREAS it is vital for citizens to know when and how their personal data is collected, how it is used, how it is disclosed, how long it is kept, and what privacy principles City Council subscribes to in guiding the Administrative actions taken by all Business Units that collect and handle citizen data;

8. AND WHEREAS The International Data Corporation (IDC) defines 'Smart Cities' development as the use of smart initiatives combined to leverage technology investments with common platforms increasing efficiency, data being shared across systems, along with IT investments and third party vendors; with a 'Smart Cities' using IoT sensors and technology to connect components across a city to derive personal data and improve the quality of life for citizens and visitors in the delivery of programs and services;

9. AND WHEREAS The City is in the process of migrating toward ‘Smart Cities’ initiatives, whereby the data of our urban environments and our citizens are leveraged to make life better – more connected, more accessible, faster, cleaner, safer and sustainable into the future. As such, City Council must ensure citizen privacy is paramount within the ‘Smart Cities’ context (following, for instance, the example set by the County of Santa Clara, California), whereby The City would work proactively to identify privacy concerns and coordinate targeted information privacy measures in order to respond in a timely manner;

10. AND WHEREAS Privacy by Design (PbD) has become a worldwide hallmark of proactive best practice (Ontario Information and in the development and delivery of programs, services and projects - particularly those involving Smart Cities programs within One Calgary) and technologies, with PbD requiring that privacy is an integral proactive aspect of an organization's critical thinking and risk management culture;

11. AND WHEREAS the relevance of meaningful privacy governance in the context of municipal decision-making, whether generally or in relation to Smart Cities initiatives, has moved to the fore – such as in the recent controversial case of the City of Toronto’s Sidewalk Labs initiative;

12. AND WHEREAS there is a strategic governance requirement for City Council to lead in the overall public domain of digital governance, by ensuring administrative controls are in place over The City’s data (including citizen data) when deploying Smart Cities technologies. And, as part of our legislative responsibility and social contract obligation with citizens, ensure that a comprehensive Administrative Privacy Program is in place to uphold the public’s trust and confidence.

NOW THEREFORE BE IT RESOLVED that City Council direct the Chief Security Officer/Chief Information Security Officer, the Chief Information Technology Officer and the City Clerk in consultation with appropriate City staff and leading external privacy experts to:

- a. Provide an analysis of The City’s current privacy practices that includes but is not limited to:
 - i. The collection of personal information process and its intended uses;
 - ii. Personal data handling practices;
 - iii. Personal data retention policies and how consistently these are observed;
 - iv. Use of third party services or technologies; and
 - v. Open Data practices.
- b. Develop a visible, accessible and overarching strategic Privacy Framework associated with digital infrastructure (‘Smart Cities’) and a Workplan for implementation for Council consideration, including but not limited to a:
 - i. Privacy Vision, Privacy Principles and a Privacy Charter;
 - ii. Privacy Statement aligned with existing statutory obligations and privacy best practice more broadly;
 - iii. Privacy Awareness, for both City employees and citizens;
 - iv. Operational Privacy Toolkit;
 - v. Privacy Auditing and Review Processes;
 - vi. Merits of having a Chief Privacy Officer;
 - vii. Privacy Complaints Management; and
 - viii. Digital tools that assist with tracking and managing City projects involving data collection, use and disclosure – particularly where personal information is involved.

- c. In scoping the work to be undertaken, consider the Council Innovation Fund (CIF) which encourages innovation that has the potential to support or contribute to the goals of Council with city-wide application that have the potential to change city-wide policies, practices and procedures; and
- d. Consider conducting a city-wide public consultation process on the Privacy Framework and data governance principles.

Report back directly to Council no later than December 2019 with a status update.