Model Policy

Privacy Impact Assessment

G20 Global Smart Cities Alliance

This policy is considered foundational to the G20 Global Smart Cities Alliance policy roadmap's principles of **privacy & transparency.** You can find supplementary content on our website[1] to provide practical support for adopting and implementing this policy.

Background

Cities around the globe are growing at an incredible rate, with residents flocking to the economic opportunities and amenities that they provide. City governments are responding to their continued growth in part by deploying technologies and "smart city" solutions that enable more citizen-centred services and progress to more sustainable, inclusive, and open cities. In order to achieve these goals, cities and communities of all sizes must ensure that

[1] Visit https://globalsmartcitiesalliance.org/

data generated by these technologies about individuals and their communities is appropriately protected and secured.

The collection of data occurs in every day city operations, from paying a utility bill, to browsing a web page, and increasingly walking down a city street, riding public transit, or driving on a city-maintained road. The use of smart city technologies -- such as sensors, connected devices, and always-on data flows that manage transportation systems, support real-time infrastructure maintenance, automatically administer public services, enable transparent governance and open data, and support emergency services in public areas -- can provide real benefits to governments and communities. While well-intentioned, they can also create the risk of individual privacy harms and raise fears of surveillance that negate the benefits of city life and actively discourage individuals from engaging with public spaces.

The increasing changes and complexity of emerging technologies, business systems, laws and regulations, as well as increased public scrutiny, require cities to take appropriate steps to proactively and methodically embed privacy and data protection into their activities. While privacy is traditionally understood as a wider concept encompassing different rights, data protection involves the protection of the individual in relation to the collection, use, and processing of personal data.

Cities must balance their own need to use and share data to conduct business with the broader public welfare and individual privacy interests in a way that builds and maintains public trust. Without public trust, the benefits of smart city technologies will be ultimately unsustainable. Cities must invest in policies and practices that will help individuals, local communities, and technology providers maximize the benefits of responsible data use while minimizing privacy risks to individuals and communities.

By implementing Privacy Impact Assessment (PIA) policies, cities can establish a consistent method for identifying, evaluating, and addressing privacy risks. Drafting a model PIA policy is a complicated process, as wide variation exists in cultural and legal approaches to privacy and data protection around the world. In this policy, we hope that by prescribing the process that should be followed and the issues that must be considered, we increase the likelihood that cities will more confidently consider and address privacy risks in a manner consistent with community expectations.

Contents

Model Policy

Objectives

A City must work to find a fair balance between gathering information to provide needed services and protecting the public's privacy, especially when deploying innovative smart city technologies. Privacy Impact Assessments (PIAs) are essential privacy assessment tools. PIAs consist of a set of processes to identify and manage privacy risks throughout the complete data lifecycle, from collection through disposal. Conducting a PIA prior to the acquisition or use of technologies in a smart city can increase transparency and accountability; support public trust; mitigate potential privacy harms or disparate impacts before they occur; improve compliance and reduce legal risk; and enable more confident and consistent decision-making about data and technology by city officials, their partners, and the public.

A City's PIA Policy should identify issues to be addressed and processes to be followed in the identification and mitigation of privacy risks. Specifically, a PIA Policy should:

- Articulate specific purposes for data and technologies as well as potential privacy risks and mitigation measures, and assess them against the City's and community members' values, priorities, and legal rights.
- Be integrated throughout the full project and data lifecycle (including intersections with the City's obligations around procurement, data security, accessibility, and public records).
- Address all data collected by a technology or service, not just data considered "personal" or "personally identifiable" at a particular moment in time.
- Facilitate communication and cooperation about privacy practices internally and externally, and create a clear understanding about when the City should reconsider a particular technology or notify its communities, partners, and technology providers.
- Encourage innovation by supporting ethical decision-making and optimizing beneficial uses of data while minimizing adverse consequences to individual privacy and society as a whole.
- [More participatory option]: Incorporate meaningful and inclusive opportunities for public engagement and decision-making about data and technology practices.

Examples:

- http://www.longbeach.gov/globalassets/health/healthy-living/office-of-equity/clb_toolkitbook_singlepages
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Foundations for Privacy Impact Assessments

Foundational procedural components to support the specific goals of the PIA policy, and its overall objective of maximizing societal benefits and minimizing risks to individuals and communities.

1. Organizational Values and Risk

a. Cities should explicitly identify the public values, priorities, and privacy principles against which particular technologies or services will be assessed during the PIA process.

Examples:

- NYC's IOT Guidelines
- Seattle's Privacy Principles
- Barcelona's Digital Service Standards
- India's DataSmart Cities Strategy

b. Cities should explicitly identify the legal standards and authority, as well as existing City policies and principles, against which particular technologies or services will be assessed during the PIA process.

c. PIAs should take into account considerations beyond legal compliance when assessing risks and benefits, including ethics, equity, and public engagement. These considerations should include not just impact on individuals but also groups.

d. [Higher maturity option]: The PIA process may include a rough preliminary scoring of opportunities based on values identified above.

Examples:

- https://wellington.govt.nz/~/media/about-wellington/emergency-management/files/covid-19/wcc-privacy-impact-assessment-digital-contact-tracing.pdf?la=en

e. [More participatory option]: Engage city staff and the public, especially vulnerable populations, to determine these broader public values, principles, and risk thresholds. Models include citizens' councils, citizens steward program, citizens' assemblies, digital models to upvote or budget city finances, public annotation of drafts, and/or social media engagement.

2. Scope and Timing

a. An Initial Assessment (or other threshold analysis to determine whether a full PIA is required) should be conducted:

i. As early as possible in the development or procurement of any new technology [and privacy-conscious protections built into the procurement criteria or development path for a technology]. Retrofitting a system to reduce privacy risks after it is designed or implemented has proven to be expensive.

ii. When planning material changes to existing processes and systems, including project updates that may include new data activity or changes in scope.

b. A full or an updated PIA should be conducted when required by regulation or City policy or when the Initial Assessment indicates that:

i. New technologies, new purposes, or new processes for data that may personally identify individuals are to be introduced.

ii. Significant changes to policies, business processes or systems are planned that may affect the physical or logical separation of personal information from other information within a system.

iii. Sensitive data is to be processed, or the technology or service may enable high-risk data processing [(such as scoring/profiling individuals, systematic monitoring, large scale processing, merging or matching data from multiple sources, targeting of children or vulnerable individuals, risk of physical harm, or the use of new technologies or the novel application of existing technologies)].

iv. When the technology or system enables automated or assisted decision making that may have legal or similarly significant effects on individuals.

c. When required, a PIA should be conducted before the acquisition or deployment of a data collecting technology into the city's environment or into the decision-making processes of a local government.

d. PIAs should be used to evaluate all data collected by a technology or service, not just data considered legally "personal" or "personally identifiable" at the time it is collected.

e. A PIA should be only one part of a comprehensive privacy program. It should sit alongside methods such as non-collection of data, privacy skills training, regulation, and auditing and publishing of PIAs within each local government or authorities' methods.

3. Tools and Components

a. Cities should develop and conduct a preliminary Initial Assessment or other threshold analysis in order to reveal whether further review is required, such as the completion of a full PIA [or an ethical impact assessment for non-personal data].

b. Initial Assessments should contain a preliminary assessment of privacy risks engendered by the system, product, or service, and may include high-level data flow diagrams or preliminary data and use characteristics.

> **Examples:**
> - Helsinki Initial Assessment
> - Seattle's PIA Policies
> - Toronto's PIA Policies

c. If it is determined that a full PIA is required, it should comprise the following components (see "Fundamentals of a PIA" below):

i. An assessment of privacy risks - Conducting a privacy risk assessment helps an organization to identify privacy risks engendered by the system, product, or service and prioritize them to be able to make informed decisions about how to respond to the risks.

ii. A risk response determination - In determining how to respond to assessed risks, cities should refer to their organizational values and risk tolerance determination. Response approaches include:

- **mitigation** (risks are mitigated to an acceptable level of residual risk through technical and policy measures such as data minimization),
- **transfer/sharing** (risks are shared with other parties such as through contracts or insurance; consent mechanisms are a form of risk sharing with individuals. Individuals should be able to reasonably understand the relevant risks before being asked to provide consent),
- **avoidance** (cities may choose not to use certain technologies or conduct certain types of data processing where the risks outweigh the benefits, or
- **acceptance** (cities may choose to accept the risk where the likelihood or impact of adverse consequences are low, and the benefits are great).

iii. Requirements and selected controls that enable the City to

- **meet applicable legal obligations** (organizational-level privacy requirements are a means of expressing the legal obligations, privacy values, and policies to which a city intends to adhere. Organizational-

level privacy requirements may be derived from a variety of sources, including legal environment (e.g., laws, regulations, policies or cultural values; relevant standards; and privacy principles) and

- **address the risks** determined to be mitigated.

d. Cities should consult local data protection authorities and other privacy and data protection experts for specialized guidance, templates, and tools for conducting PIAs and assessing privacy risk (See Additional Guidance below)

> A proven method in conducting a PIA is the workshop method, which starts with an initial meeting, to which all necessary stakeholders are invited. The assignment of responsibilities takes place at the initial meeting. At the impact assessment workshop (or workshops) after the initial meeting the experts have in advance sorted out aspects connected to their responsibilities, whereas the documentation of the data into the tool can be made jointly.

4. Roles and Responsibilities

a. A designated senior official, such as a Chief/City Privacy Officer (CPO) [with the support of a dedicated privacy team] should be responsible for:

i. Developing appropriate templates, resources, and components for the City's Initial Assessment and PIA tools,

ii. Setting the standards and qualifications of the resources permitted to conduct a PIA,

iii. Reviewing Initial Assessment or otherwise determining where a PIA is necessary (including re-review of existing PIAs),

iv. Conducting and approving of PIAs, including providing requirements and recommendations to mitigate privacy impacts.

v. Liaising with other officials to resolve privacy and security concerns raised during the course of the PIA, and

vi. Determine the City's response to identified privacy risks.

b. Agency/department/programmatic officials should be responsible for:

- **i.** Providing appropriate information and documentation about the proposed technology and its use (e.g., technology functionality, business case, proposed purposes, costs for ongoing privacy and security protections, etc.),
- **ii.** Completing Initial Assessment and assisting in the completion of a full PIA, where appropriate,
- **iii.** Implementing the data use and management plan and all appropriate safeguards identified in the PIA as necessary to mitigate risks associated with the proposed technology,
- **iv.** Ensure that the PIA policy is communicated to staff, and that staff are given sufficient time and resources to participate in the PIA process, and
- **v.** Authorize and approve PIAs, as appropriate, prior to the implementation of privacy-impacting technologies.

c. An executive or senior official, such as a City Manager or Chief Technology Officer, should have authority to oversee compliance with the PIA Policy, including:

- **i.** Ensuring the PIA Policy is communicated to all staff, implemented, and enforced,
- **ii.** Ensure information is shared and accessible to the greatest extent possible, while respecting privacy and security requirements,
- **iii.** Provide appropriate budget and organizational structure to enable the designated senior official for privacy and other staff to routinely conduct PIAs,
- **iv.** Develop and implement appropriate accountability measures (e.g., escalation procedures, staff training and awareness, reporting systems and intake for complaints or potential threats related to privacy),
- **v.** Monitor the effectiveness and outcomes of the PIA policy, and
- **vi.** Review alignment of PIA schedules with Smart City project schedules.

d. Additional City officials and external stakeholders should be consulted where appropriate given the nature of the particular technology or service, such as:

i. An executive representative to advise the PIA program and champion department participation,

ii. CISO or other IT experts to assist in design of technology systems and assessment and mitigation of data security risks,

iii. City attorneys or legal counsel to ensure compliance with legal standards, including applicable data protection regulations,

iv. Public records officers and open data officials to identify circumstances in which data might be disclosed (intentionally or by law),

v. Procurement officials,

vi. Officials from other City agencies to identify additional interests in the data or technology,

vii. External subject matter experts,

viii. Technology partners, and

ix. Members of impacted communities.

e. [More mature option]: A senior privacy officer is supported by specialized data protection, risk management, and security professionals who are experts in conducting PIAs. The data privacy team is supported by a citywide network of "privacy champions," who are subject matter experts within particular departments able to assist in the PIA process. The PIA team is able to build institutional knowledge and best practices, support more consistent privacy decision-making across the City, and identify opportunities to improve PIA processes and outcomes.

> **Examples:**
> - Toronto RMIS w/in I&T division
> - Seattle privacy champions

f. [More participatory option]: An external body or organization is engaged to provide input, make recommendations, utilize community expertise, or provide approval to

> **Examples:**
> - Seattle Surveillance Working Group
> - Oakland Privacy Advisory Commission

PIAs. The group includes diverse stakeholder representatives, including privacy and data protection experts and members of the community.

5. Monitoring and Recordkeeping

a. All Initial Assessments and PIAs should be thoroughly documented in writing, and be maintained in accordance with the City's record retention schedule. Examples: Helsinki Data Register, Seattle PIA Reviews

b. Any technologies determined to be exempt from PIA review should also be logged and documented in writing.

c. PIAs may be classified and categorized if there are multiple PIAs for a city.

d. Local Governments should create a secondary, aggregated PIA process, performed [three yearly] to assess the way systems and data interact to prevent data that was once considered non-personal from, over time, become identifiable; by evaluating all data generated by an IOT technology or service together, cities can future-proof their assessments to a greater degree.

e. A designated senior official for privacy should review the PIA policy annually (or sooner if necessary), and update it as necessary.

f. City departments, divisions, or programs and any partners or service providers should assess their own degree of compliance with the PIA Policy, [such as by conducting internal audits, program reviews, or program evaluations].

g. In the event that the City receives a privacy complaint or experiences a privacy breach, a designated senior official for privacy should investigate and make recommendations, as necessary, to remedy the situation.

h. [Higher maturity option]: Cities should develop and maintain an inventory of systems/products/services that process data, including the roles of owners or

Precedents:

- Seattle's inventory of surveillance tech
- Amsterdam's IoT Registry
- Barcelona's Sentilo
- City of Boston's pilot of Digital Transparency in the Public Realm
- NIST privacy framework

operations with respect to the systems and their components; the data provenance; the data actions of the inventoried systems; the purpose(s) for the data actions and the data processing environment.

6. Transparency & Engagement

a. To the extent possible, Cities should make all PIAs available to the public on an easily accessible, outward-facing website.

> **Precedents:**
> - Seattle PIA and SIR inventory
> - Wellington DCTT PIA

b. Cities should develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

c. Cities should develop additional mechanisms (e.g., notices, internal or public reports) to communicate data processing purposes, practices, and privacy risks associated with smart city technologies, informed by relevant PIAs.

d. [More participatory option]: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.

> **Supplementary guidance:**
> - PIAs should avoid using acronyms, slang, or other terms which will not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.
> - Signage should be provided in-situ as needed to comply with relevant local privacy regulations [and should be considered for novel or new deployments of IoT technologies more broadly in order to inform the public of data collection and processing activities].

This section describes the fundamental issues or questions that a PIA should address, in order to enable cities and their partners to effectively identify and mitigate potential privacy risks while maximizing the public benefits of data and technology.

A PIA should clearly and understandably:

1. Identify the City departments, divisions, or programmes and any partners or service providers who will use or be accountable for the technology.

2. Describe the technology to be designed or acquired and a description of its general capabilities, functionality, the type of data that it is reasonably likely to generate, and the sources and accuracy of any personal information collected, including reasonably foreseeable surveillance capabilities outside of the City department's proposed use.

3. Describe the purpose and proposed use of the technology, including its intended value and benefit to individuals, the community, and society at large [and any data or research demonstrating those benefits]. Describe the problem the technology seeks to solve, and whether any less invasive alternatives exist.

4. Describe the City's authority to collect, use, and disclose personal data relevant to the proposed technology, as appropriate.

5. Describe any public values, principles, legal standards, and organizational risk frameworks against which the technology is being assessed.

6. Assess and describe the potential privacy risks associated with the proposed use of the technology, [including the likelihood of such risks occurring and the severity of the potential impact on individuals and communities.]

7. Describe the City's risk response to the identified risks, given organizational values and risk tolerance (e.g., mitigation of risks, transfer/sharing of risks, avoidance of risks, or acceptance of risks).

8. Describe a clear use and data management policy for the proposed use of the technology, including:

    a. How and when the technology will be deployed or used and by whom (including, as appropriate, descriptions of who has ownership or licensing rights to the data under what conditions).

    b. Any additional rules that will govern the technology (including legal standards that must be met before the technology is used, such as for the purposes of a criminal investigation).

c. How data will be securely stored and destroyed or de-identified.

d. How long data will be retained in identifiable and non-identifiable forms.

e. How access to data will be monitored and controlled, [including access logs and audits].

f. Whether the technology or data will be shared, and if so under what conditions (including both routine sharing, such as with partners or service providers, other government entities, researchers, public records requests, or open data, and in exigent circumstances).

g. What training and accountability measures will help ensure that all personnel who operate the technology or access data use it only in compliance with City policy.

h. What safeguards are in place to ensure the confidentiality, integrity, and availability of data (including protection from threats like ransomware, malware, or IoT vulnerabilities).

i. Any other legal, organizational, physical, and technical safeguards intended to mitigate potential privacy risks associated with use of the technology.

9. Describe any community engagement held and any future community engagement plans, any comments received and City responses given, and City conclusions about potential neighbourhood and disparate impacts that may result from the acquisition and use of the technology.

10. Describe any emergency or civil defence legislation that may change the way the data is used or the processes governing it.

11. Describe how the potential impacts of the technology on civil rights and liberties and potential disparate impacts on marginalized communities have been taken into account and mitigated.

12. Describe the availability of funding for ongoing privacy and data protection costs related to operation of the technology (such as personnel, legal compliance, auditing, data retention, and security costs).

Additional Guidance & Resources

Examples of City PIAs

- Helsinki Data Register and DPIA tools
- Huron County Privacy Impact Assessment Policy
- Santa Clara County Surveillance Use Policies
- Seattle PIA Reviews and Surveillance Reports
- Toronto Privacy Impact Policy
- Wellington Digital Contact Tracing PIA

Guidance on conducting a PIA or DPIA

- The former Article 29 Working Party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (2017) + EU member state DPIA whitelists and blacklists (2019)
- French DPA/CNIL -- Privacy Impact Assessment resources *(available in French and English),* including guidance, templates, knowledge bases, IoT examples, infographic, and a free software tool (2018)
- Spanish DPA/AEPD's modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) dirigido a Administraciones Públicas (2019) *(available in Spanish)*
- Australian OAIC -- Public Sector Chief Information Officer Council (PSCIOC) Guide to undertaking privacy impact assessments
- New Zealand Privacy Commissioner -- Privacy Impact Assessment Handbook
- Canadian OPC -- PIAs guidance
- Bureau of Justice Assistance -- U.S. Department of Justice, Guide to Conducting Privacy Impact Assessments: for State, Local, and Tribal Justice Entities (2012)
- NIST Privacy Framework A Tool for Improving Privacy through Enterprise Risk Management
- Sidewalk Labs, Responsible Data Use Assessment - Digital Innovation Appendix Section 2.2.3, page 237 - 295

- UN Global Pulse, Risks, Harms, and Benefits Assessment
- SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond

Acknowledgements

Co-leads

Kelsey Finch, Senior Counsel, Future of Privacy Forum

Michael Mattmiller, Director of Government Affairs, Microsoft

Task Force Members:

Pasquale Annicchino, Lex Digital and Archimede Solutions

Sean Audain, Wellington City Council

Chandra Bhushan, Quantela

Dylan Gilbert, Privacy Policy Advisor, NIST

Naomi Lefkovitz, Program Manager, NIST

Jacqueline Lu, Co-Founder, Helpful Places

Eugene Kim, Associate Director, Privacy and Data Governance, Sidewalk Labs

Dan Wu, Immuta

Contributors and reviewers:

Hector Dominguez-Aguirre, City of Portland

Dilip Krishnaswamy, VP of New Tech R&D, Reliance Jio

Masaru Yarime, Ph.D., Associate Professor, Division of Public Policy (PPOL), Hong Kong University of Science and Technology

About the G20 Global Smart Cities Alliance

Established in June 2019, the G20 Global Smart Cities Alliance on Technology Governance unites municipal, regional and national governments, private-sector partners and cities' residents around a shared set of principles for the responsible and ethical use of smart city technologies. The World Economic Forum, the International Organization for Public-Private Cooperation, serves as secretariat for the Alliance.

Through the Alliance, global experts from government, private-sector partners and civil society, are compiling and analysing policies from around the world to identify model policies necessary for successful, ethical smart cities.

You can find more model policies and more details about the Alliance at:
https://globalsmartcitiesalliance.org/

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Cover: Forum Stock Images