International Working Group
on Data Protection
in Technology

Working Paper on "Smart Cities"

Adopted at the 70th Meeting on 29th-30th November 2022,
written procedure prior to 71st Meeting on 7th-8th June 2023

1. Introduction

Cities are essential to human flourishing. Aristotle famously said in his *Politics* that "a human being is by nature an animal meant for a city"[1] and that a city exists not simply for the sake of promoting commerce or preventing injustice, but above all for the sake of granting its citizens a "complete and self-sufficient life"[2].

Cities across the world are adopting new and innovative processing to achieve their goals. This could involve introducing new technologies or adopting new processing with existing data. The journey towards making cities "smart" or "connected" requires meaningful data governance from the beginning and present throughout to maintain the trust of citizens and individuals visiting the city.

Smart cities can involve numerous actors and processing activities. This paper does not seek to define smart cities; rather, it explores the topic of digitalisation of cities as a process in the three stages Data Collection, Data Analysis and Decision. In the following, some examples for practices of these stages are presented:

[1] Aristotle, *Politics*, I.2 1253a3, trans. Joe Sachs. Indianapolis: Hackett, 2012.
[2] Ibid., III.9 1280b30–33.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

Data Collection:

- Sensor networks such as Internet of Things
- Images produced by CCTV, and drones, etc.
- Re-use of data held by public authorities[3] , municipalities[4], and other partners[5]
- Data gathered from public communications networks like public transportation Wi-Fi networks.
- Data gathered from services offered by the municipality such as bike or scooter rentals

Data Analysis:

- Data matching
    - Combining the contents of two datasets to derive new insights. For example, using smart thermostat data and social benefit datasets to identify households in fuel poverty.
- Artificial intelligence
    - Use of computers to perform tasks normally requiring human intelligence. For example, traffic flow management through data captured via the traffic system.
- Profiling
    - Use of personal data to evaluate or predict aspects, which could relate to a natural person. For example, using profiling to predict a person's location or movement through the city.
- Digital twins
    - The construction of a digital representation of the city, precisely mapping the physical city for experimentation of new policies or assessing proposed urban developments.

Decision:

[3] By public authority the paper means a body delivering a public service, such as an education institution or a social benefit agency.
[4] By municipality we mean a city's governing body, or a region or district governing body.
[5] By partners in we mean any collaborator a city may work with. This could be subcontractors, cities with which they are collaborating, services in the city that share data with the city government. We continue to use the phrase partners as shorthand for the different types of actors that cities work with in smart city projects.

- Management of city resources such as public transportation
- Management of city functions or processes such as traffic control
- Outputs used by cities as evidence for further decisions, e.g., policymaking on social housing stock or social services

Each of these stages engage some form of data protection and privacy issue. From lawfulness, fairness and transparency to security and integrity, and the rights of individuals. There is a wide breadth of purposes that a city can adopt technology for. From transport management to social welfare management, to energy consumption, to city planning via digital twins. Adoption of new technology or processing by a city for any of these illustrative purposes also raises questions as to the interaction with other rights and freedoms.

This paper presents a series of data protection and privacy principles relating to each of these stages of data use in a city context. These principles represent some of the stages of data protection by design and default. Readers may find it helpful to explore further areas of data protection by design and default and consider their relevance in a smart city context[6]. This paper unpacks the risks that exist with respect to each thematic set of protections and principles, provides an illustrative case study, and finishes with recommendations for city governments, regulators, and private sector involved in the delivery of data-driven services.

2. Accountability and Governance

To achieve and demonstrate compliance with all data protection principles and protection of individual rights, prior to beginning of any processing, cities and their partners should ensure they carry out a rigorous accountability and governance assessment, including data protection impact assessments where relevant. The process should involve the data governance teams, such as the Data Protection Officer, at an early stage. Key decision-making occurs in the initial stages, which can have a significant effect on the scope of governance, and the establishment of effective measures. Not following this process risks failing to build in appropriate

[6] Guidelines 4/2019 on Article 25 Data Protection by Design and Default, European Data Protection Board

data protection compliance in new smart city processing initiatives, causing societal harms such as damage to information and public discourse.

One of the key questions will include whether the processing relates to identifiable individuals. Identifiability should be a question considered about the specific processing, but also in relation to associated processing. For example, in deciding whether to install new sensors to measure footfall in a public place, the city should answer the question whether the sensors collect data that is directly identifiable. They should also consider whether other technology operating in the same public place causes a change in the identifiability, where a combination of new sensors and existing systems (for instance closed-circuit cameras) might allow for the indirect identification of individuals.

Cities should consider the identifiability question widely as the processing moves from the collection stage to the analysis stage. Consider what data processing is occurring in the analysis phase? Will there be data matching that could create paths for identifiability? Is the storage period such that further collection will allow for the establishment of individuals' movement patterns?

This discussion of identifiability defines the necessary scope for governance. If cities conclude that processing will involve identified or identifiable individuals, then the governance process should move towards relevant data protection and privacy governance standards. This includes conducting an impact assessment to identify and mitigate risks to individuals because of the processing. The impact assessment should also include a consideration of the effect on other human rights and freedoms.[7]

Smart city applications should always be inspired by fairness. Data of poor quality or data which does not reflect the variety of the groups in the population might lead to unfair or discriminatory decisions. This aspect should also be examined and considered during the impact assessment. In particular, cities should assess whether the quality of the data used to draw decisions with potential impacts on the rights and freedoms of individuals is adequate and representative of the population characteristics. Many factors may impair data quality and

[7] Preamble, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.

representativeness. For example, the sample size of the population, whether many individuals have opted-out or objected to the processing, or have required their data to be deleted. If cities cannot guarantee the highest data quality or data representativeness standards with respect to the processing purpose, they should abstain from using those data any longer for that purpose.

Additionally, establishing proper transparency mechanisms to inform individuals about the processing and putting in place technical and organisation measures to ensure the establishment of privacy practices at the earliest possible stage is part of the accountability obligations.

This discussion should occur between the city and any partners that are participating in the processing. This is important to ensure that the city assigns appropriate roles and responsibilities between the actors involved in the processing. If the system is solely for the use by the city, discussions may focus on the system design. This must include access controls for any teams accessing the data. If this includes service provision by an industry partner, such as analysis like data matching, then alongside system design there needs to be a further discussion about data governance, including the controller – processor relationship, or joint controllership. This is necessary because by providing a service the partner may be determining the means and purpose of data matching, or using proprietary data they hold, or adding their own data. This changes the nature of the relationship and would require joint governance arrangements.

Completion of governance and accountability processes must happen prior to processing commencing to ensure that proper systems are in place including technical safeguards, and agreement on roles and responsibilities between the parties. The outcome of the accountability process should remain under periodic review to ensure it remains relevant in its description of processing, assessment of risks, and deployment of mitigations. This should also be reviewed when a new technology or initiative is introduced in the monitored area, or in the relevant service for the city. For example, a new monitoring device introduced into a public square that has ongoing data collection, or new analytical systems for managing public transport demand.

Regulators can assist in the governance discussion by producing guidance on establishing accountability and governance procedures. It would be useful to produce guidance relating to scenarios where there are multiple actors, services, and technologies involved.

2.1 Accountability Example: Enschede

In September 2017, the municipality of Enschede decided to start 24/7 Wi-Fi tracking in the city centre[8]. Its purpose was to measure the effectiveness of municipal investments, in view of responsible funds. It contracted a delivery partner, who then contracted another party to install and maintain the sensors and collect and validate the data gathered by the sensors.

Information collected and temporarily stored on the sensor included MAC-addresses, date and timestamp of exposure, signal strength. The sensor sent the information to a central server, with the MAC-address hashed and the sensor ID added. The server stored the collected information for a period between 6 and 7 months. Starting from early 2019, the partner put in place additional anonymization measures by truncating the hashed MAC-addresses. The municipality ordered the delivery partner to switch off the sensors in 2020.

The municipality argued the data was sufficiently anonymised in such a way that no personal data processing occurred. The municipality also argued that it was not a data controller in this case.

The AP (Dutch Data Protection Authority) concluded that the chosen anonymization method of truncating a small part of the hashed MAC address did not sufficiently exclude the risk of singling out, linking, or deducing a person's identity.[9] The AP came to the decision based on the collection of a pseudonymous identifier + timestamp + location information (available via the sensor ID). As a result of this the data processed by the municipality constituted personal data. According to the AP the municipality was the controller because it has decided on the means and purposes of personal data processing by issuing the orders about the specifics of the processing.

[8] AP (The Netherlands) - Gemeente Enschede - GDPRhub
[9] WP29 Opinion 05/2014 on Anonymisation Techniques

2.2 Accountability and Governance Recommendations:

Cities should clearly document the scope of their processing across their services.

Cities should ensure that data used in decisions is adequate for the purpose of the processing and representative of the population characteristics.

Cities should put in place technical and organisational measures to establish proper governance and safeguards for data processing.

Cities should conduct impact assessments prior to beginning processing to identify and mitigate risks and consider the impact on other rights and freedoms during the assessment.

The impact assessments should remain under periodic review and should be fully revisited by the city when new technology is introduced into the monitored area, or the relevant city service.

Cities should involve their data governance teams at an early stage and consult with them throughout the process.

Cities should conduct appropriate consultation with the public and other relevant stakeholders as part of the accountability and governance process.

Regulators should produce guidance on accountability measures and governance structures, including guidance on processing with multiple actors, services, and technologies involved.

3. Data Minimisation

The principle of data minimisation aims to ensure that controllers only collect data that is relevant, adequate, and necessary for a specific, lawful purpose. In a smart city context, the purpose is often to understand trends, such as footfall or traffic density, from a 'bird's eye view'. These purposes often involve seeking to assess data in an aggregate form.

Where trends analysis is the aim, data minimisation requires the aggregation, and stripping of identifiers, as soon as possible in the collection stage. This reduces identifiability for the analysis stage. Failing to do this means there is a risk of over collection of personal data and creating unnecessary intrusion into citizen's privacy.

To put data minimisation into practice, cities should clearly define the data needed to achieve the specific purpose of processing. This should occur prior to beginning processing. Defining the purpose at the design stage means that systems have a better chance of reflecting that specified purpose. This should also allow for embedding minimisation practices into the collection system itself. For example, by procuring sensors that only collect the specified data or strip identifiers before sending the data on for analysis. There should also be clear policies relating to the automated deletion of collected data when no longer necessary to reduce the risk of loss of data.

Achieving this aggregation could involve the adoption of privacy enhancing technology (PETs). PETs can assist in rendering the data anonymous, or pseudonymous. The adoption of these technologies at an early stage in the processing cycle represents good privacy by design practice. Doing so in a way that embeds the functionality into the system in such a way that it is mandatory ensures that the processing will always demonstrate data minimisation standards.

Data protection authorities could add benefit by providing guidance on the use of anonymization and PETs in processing. This guidance could suggest available techniques to reduce the risks of identifying individuals to a sufficiently remote level. Guidance can help to shape the types of products that industry market towards cities, and the processing that industry embeds into its products to ensure the establishment of data minimisation.

3.1 Data Minimisation example: Transport for London wi-fi data collection

Transport for London (TfL), the transport authority that runs the day-to-day operation of London's public transport network, sought to better understand how

customers move through stations[10]. They did not need to identify specific individuals to achieve this understanding.

To achieve their aim, TfL opted to collect Wi-Fi connection data from a number of stations. Wi-Fi connection "provides a far better understanding of how customers move through stations." This method meant the collection of location of devices on the Wi-Fi network, meeting the definition of personal data.

If the device finds a Wi-Fi network that is known to the device, it will automatically connect to that network. If the device finds unknown networks, it will list these in an individual's device settings so an individual can decide whether to connect.

All data collected is automatically hashed using a revolving cryptographic function. This, according to TfL, ensures it is unable to identify any individual. The system performed this immediately after data collection.

TfL had no plans to match the Wi-Fi connection data with other data held about individuals by the authority (e.g., travel card data), and because of the immediate pseudonymisation process there is no way systematically to do so, according to TfL.

TfL used the aggregated Wi-Fi connection data to understand how busy London Underground stations are throughout the day. This information has helped individuals plan their journey as well as contributing to TfL understanding of station use.

3.2 Recommendations on Data Minimisation

Cities should clearly define the data needed to achieve the purpose and develop systems to reflect that purpose.

Cities should ensure that systems always minimise data by embedding technical and organisational measures as early as possible in the collection of personal data.

[10] Wi-Fi data collection - Transport for London (tfl.gov.uk)

Cities should ensure measures for data minimisation persist throughout the whole lifecycle including implementing adequate retention periods and establishing secure deletion processes.

Regulators should provide guidance to cities and industry on methods for minimising data, including aggregation.

4. Purpose limitation

Cities play multiple roles in the lives of their citizens, from traffic management to public safety, through to education and emissions control. Technical systems should reflect the different data and different purposes through separation of processing activities. Organisational measures should be in place to ensure that staff cannot use data collected for one purpose for another without proper assessment, documentation, and legal basis.

There should be clear communication of the purpose of processing needs at the point of collection and governance measures must reflect that purpose. Failing to establish proper purpose limitation within processing systems risks sharing data beyond the original purpose. This causes harm to individuals through loss of control of data.

In some situations, data may be used for a different purpose, for example, in the analysis phase datasets from multiple sources may be combined, compared, or matched for the purposes of identifying individuals entitled to social benefits. This carries a high risk for individuals' loss of control of personal data and could also contribute to a lack of autonomy, or manipulation of people's choices. The processing should only proceed if the new purpose is compatible with the original purpose, or the individual validly consents, or the controller clearly identifies a defined legal obligation.

A controller should perform a compatibility assessment to determine whether the plan to use or disclose personal data for an additional purpose is compatible. The controller should make this new purpose clear to individuals to begin to mitigate the risks of loss of control of personal data. The controller should assess the new

processing for its fairness, which begins to address the risk of loss of autonomy and manipulation.

Industry should build systems to have flexibility to establish different organisational measures and adopt technical measures to meet privacy by design standards. This could mean having strong role-based access controls in place so that only those teams working to the specified purpose can access the collected data. Technical measures could include log functions that record who access what data, allowing for audits to be carried out as part of reviews.

4.1 Purpose limitation example: Smart Homes

Increasingly, social housing provided by public authorities and cities have sensors installed within them that monitor moisture and damp levels. The purpose of this is to ensure that the accommodation provided is safe and healthy for the occupant, and to enable proactive maintenance to rectify emerging issues before they become more extensive and expensive for the provider to address.

Industry suppliers of these systems also offer apps to better inform tenants about the energy use within the home. The data could also provide insight about the occupants' eligibility for social benefits. For example, consistently low temperature data could indicate a household that is in fuel poverty. Public authorities could then make social benefits available to that household.

There are three different purposes in this example: upkeep of social housing accommodation; informing occupants about their energy use; and identifying eligibility for social benefits. The original purpose in this example is upkeep of social housing accommodation, additional purposes require an assessment for their compatibility to that original purpose. If the new purpose is not compatible with the original purpose, then there must be a clear obligation or function set out in law to allow for this new purpose, or the valid consent of the individual.

Interventions into individual's lives for social benefits, even if considered positive, are a fundamentally different purpose to monitoring the state of a home to ensure timely repairs. In this example, the third purpose would need to establish a clear obligation in law or have the consent of the occupant before processing goes ahead.

Further, it is necessary to inform the individual of these purposes, and consent gathered where appropriate.

Systems design should also reflect these different purposes. For instance, the housing provider should receive data that indicates the state of the house, which may not be personal data at all. The app interface should provide adequate and relevant data to the user about their energy consumption. And it is necessary to have in place a data sharing programme between the housing provider and social support team if they decide to pursue the third purpose. This may involve some data matching between housing data and the personal data of the occupant.

4.2 Recommendations on purpose limitation

Cities should ensure that they process data only for its specified purposes by adopting technical and organisational measures. Cities should document these purposes and make the documentation available to individuals.

Cities should conduct compatibility assessments, when they are using data for a different purpose than originally collected.

Cities should take appropriate governance steps following the compatibility assessment including where relevant, requesting the consent of the individual for the new purpose, and the establishment of data sharing agreements between actors.

Industry should build systems that have flexibility to establish organisational measures and adopt technical measures to meet purpose limitation.

5. Integrity and Confidentiality

The expansion of processing activities by cities brings with it an increase in points of collection, volume of data collected, and in some cases expansion of storage of this data. This creates new challenges for maintaining the integrity and confidentiality of personal data collected. Sensor-based networks in particular play

a significant role in increasing data collection opportunities for cities, while being a consistent source of concern for security standards.[11]

Integrity and confidentiality of processing systems is a whole cycle concern. Cities should ensure that procurement activities include discussions of integrity and confidentiality. Cities could support these procurement discussions by establishing standards for assessing a proposed systems implementation of privacy standards. From procurement onwards there needs to be adequate resourcing for continued assessments of the integrity of systems to ensure that teams are addressing new and emerging risks.

Industry has a key role to play for integrity and confidentiality of processing systems. The development of sensor-based systems should demonstrate integrity and confidentiality, while also carrying sufficient capacity to receive security updates and patches following the identification of future vulnerabilities.

5.1 Integrity and Confidentiality Example: Emerging legislative initiatives and international consensus on IoT Security

There are various initiatives from across the world that demonstrate the need to ensure IoT device security. The United Kingdom's Product Security and Telecommunications Bill[12] aims to improve consumer-facing cyber security, with a particular focus on product security. This includes a ban on the use of default passwords, a requirement for manufacturers to manage the reporting of security vulnerabilities and a requirement to inform consumers at the point of sale the minimum period that the product will receive security updates.

Further, actors across industry, academia and policymaking recognise the need to improve the security of IoT devices. The joint statement of support on consumer IoT device security[13] called for the widespread development of baseline IoT security standards to ensure basic security features in every connected IoT device.

[11] Connected Places Cyber Security Principles - NCSC.GOV.UK
[12] Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets - GOV.UK (www.gov.uk)
[13] Joint statement of support on consumer IoT device security | Cybersecurity Tech Accord (cybertechaccord.org)

Cities should exercise caution in the adoption of IoT devices to offer municipal services. Citizens have no alternative to the system offered by the city and therefore cities should be able to demonstrate implementation of necessary technical, organisational, and legal means to ensure data security of IoT devices.

5.2 Recommendations on integrity and confidentiality

Cities should establish assessment standards for the procurement of new systems to determine the implementation of privacy considerations.

Cities should require the demonstration of security standards prior to the procurement of processing systems.[14]

Cities should establish audit practices that regularly test all parts of a data processing system, through the whole data life cycle, to ensure that it maintains the levels of integrity and confidentiality required.

Industry should ensure that their products reflect industry best practices such as the ability to receive security upgrades, operate a vulnerability disclosure policy, and do not carry universal default passwords.

6. Right to be informed

Transparency of processing is a particularly unique challenge for smart cities. The data collection phase is often passive. Passive in this sense means the collection technically can occur without individual opt-in for collection, or the re-use of previously collected data for a new initiative can occur without ever notifying the individual. These activities, when handled without proper transparency, are invisible processing – processing data not directly obtained from the individual- with the associated harms of loss of control of data for individuals but also societal harms related to loss of trust in the city and other institutions to handle their data fairly and transparently.

[14] For example, see the IEEE Recommended Practices for Privacy Considerations for IEEE 802 Technologies (https://1.ieee802.org/security/802e/)

While it is difficult to inform individuals of smart city processing, it is achievable. There are steps that cities should be taking to better inform citizens about the type of processing that is occurring.[15] In some circumstances, the data collected will be personal data and there will be a legal requirement to inform individuals of the collection. In other circumstances, where the data is not identifiable directly or indirectly, there is an ethical question of what good practice looks like for adopting new and innovative processing.

Cities should consider how they are informing citizens of each processing activity, and the scope of processing across the city. Cities should make information available at the point of collection for the specific processing activity. Individuals should receive information about subsequent analysis and decision-making stages, which speak to the purpose of the collection, where relevant.

Cities have unique opportunities for methods of communication to inform citizens about the wider aims. They may have opportunity to communicate projects in public transport hubs, disseminate information through schools, or use local news to inform citizens of their wider intentions or use citizen facing employees as information points on the nature of processing. Cities also can hold debates in their democratic institutions on smart city initiatives, and can consult and gather views from community members.

Some cities have explored public registers of processing activities. The now defunct Sidewalk Labs smart city development in Toronto had intended to establish a device registry. The registry would have been a publicly accessible log of all data collection devices – what data they collected, why, how and by whom. The Amsterdam Algorithm Register[16] is an initiative from the City of Amsterdam to list, in one place, the processing by algorithms that are currently occurring in the city. Where cities are keen to embrace the insight opportunities of technology there should be an equal embrace of greater levels of transparency and awareness raising that technology can provide.

[15] Also note that there exist innovative approaches, one example is the imec-SMIT-VUB's Data protection on the ground project that has organised data walks (https://smit.vub.ac.be/policy-brief-57-walkshops). Another example is the IoT Privacy Infrastructure that maps IoT sensors in the public space including cities such as Amsterdam and Brussels (https://www.iotprivacy.io).

[16] Amsterdam Algoritmeregister –

These examples demonstrate some unique opportunities to communicate wider processing. However, it is vital to recognise that in some circumstances, where cities collect personal data, there is a need to communicate clear information to individuals at the time of collection. This information should contain details about the data collected, its purpose, the actors involved in the processing, and key governance points such as length of retention and any de-identification measures that are taking place. This is a fundamental responsibility that needs sufficient attention, as well as exploring the wider communication opportunities.

6.1 Example of citizen transparency: TfL Wi-Fi tracking

Returning to the example of Transport for London's Wi-Fi tracking set out in the data minimisation section above. During the pilot phase, TfL recognised the need to inform citizens about the initial collection of data, prior to de-identification. They approached the task of informing customers through a series of different activities.

During the pilot phase TfL adopted a layered approach.[17] The week before launching the pilot TfL issued a press release that set out the scope of the project and intended benefits. TfL used Metro, the local newspaper, to publicise the project details. Throughout the pilot a webpage was available with further information

More than three hundred large posters were put up across the pilot area, a particularly important information dissemination activity at the point and location of collection. Employees at those stations had briefings about the trial too so they could answer questions or direct individuals to sources of further information.

6.2 Recommendations on right to be informed

As a precondition for the collection of personal data cities should establish methods for providing meaningful information to individuals prior to collection.

[17] Review of the TfL WiFi pilot - our findings

Cities should provide publicly available information that explains the scope of processing across the city, including third parties involved in the processing and their roles.

7. Individual rights

The rights of individuals to control their personal data is a responsibility of cities and their partners as controllers of personal data. This could include access to data, objection to processing, rectification of factual errors, or erasure of data. Due to the multiple processing operations that could operate in a smart city it is vitally important that cities establish clear and accessible procedures to meet individual's rights.

Individuals' have their rights best met where there is a clear understanding from all involved. This understanding incorporates the role actors play in data processing, and understanding who is responsible to meet an individual's rights. The need for clarity also extends to individuals' right to know about the processing of their data, and the rights they have towards that data, where relevant.

Those in control of the purpose and means of the processing have a responsibility to inform individuals about the processing, and the rights relating to that data. The design phase should allow for answering and documentation of these questions and reflects on the accountability and governance recommendations set out in the Accountability section above.

Where cities contract out delivery to partners, such as communication providers for public Wi-Fi, there may be a need to hold joint responsibility for those roles. The city should make this clear in the licence and contracting for this service. Where the city is collecting and using data via that network, and deciding the purpose, they will have sole responsibility for individual rights and establish policies and processes accordingly.

Regulators can meaningfully contribute to the discussion by providing guidance to cities for meeting individual rights. Regulators can also provide publicly accessible information about individual rights and their exercise.

7.1 Example of individual rights: Cities' plans to increase individual control

Toronto's Digital Infrastructure Strategic Framework[18], published in March 2022, includes a commitment to "digital autonomy" which, among other aims, includes increasing residents' control over the collection and sharing of their personal data. While this Framework is too recent to have produced a working model it shows an intention from cities to recognise a stronger commitment to individual rights.

Helsinki announced their intention to create a Helsinki Profile dashboard[19], where people can manage data consent for various services centrally. Helsinki is part of the MyData Global Network. A concept for personal information management which allows for people to understand the data collected from them and provide consent for its use.

7.2 Recommendations on individual rights

Cities should establish systems compliant with individual rights, ensuring products purchased can meet these needs.

Cities and industry partners delivering projects collaboratively should address together governance issues in relation to individual rights, prior to beginning processing.

Regulators should provide meaningful information on citizens' rights in relation to processing of personal data in smart city initiatives.

8. Concluding remarks

The scope of personal data processing by and within cities is likely to grow. This is due to the introduction of new technologies for collection and opportunities for innovative use of data to better meet the challenges of modern cities. With that increased scope comes the need to establish policies and systems for the

[18] Digital Infrastructure Strategic Framework (toronto.ca)
[19] Mikko Rusama, Helsinki: Writing the rule book on personal data - Cities Today (cities-today.com)

protection of personal data throughout the cycle of collection – analysis – decision that is set out in the Introduction above.

The proposed recommendations reflect the important responsibilities from the increased processing and the opportunities that cities have for improving trust in that processing. These include the need to clearly identify roles and responsibilities of actors involved in these projects, minimise data collection to necessary levels, and design systems that establish meaningful restrictions around the use of data. Opportunities include expanding awareness of city-wide processing for the public benefit, adopting new privacy enhancing practices to allow for responsible innovation, and better meeting the rights of citizens in relation to collected personal data.

Smart cities have been long in development. We have seen various forms of this idea, from areas of existing cities given over to tech companies through to the development of entirely uninhabited land for new cities. Some of these ideas have never gone beyond the blueprint phase. Now, these projects are becoming more commonplace in cities that we live in today. This means our personal data is becoming more of an active concern. It is vital that governance arrangements are in place to reflect that increased processing.

While cities will hold many of the responsibilities in making these projects successful, the private sector, regulators and indeed citizens themselves will play a key role in keeping the projects accountable for the data they process and helping it stay human-centred in its outcomes.

Summary of recommendations

Cities

- Cities should conduct impact assessments prior to beginning processing to identify and mitigate risks and consider the impact on other rights and freedoms during the assessment.
- Cities should ensure that data used in decisions is adequate for the purpose of processing and representative of the population characteristics.
- The impact assessments should remain under periodic review and should be fully revisited by the city when new technology is introduced into the monitored area, or the relevant city service.
- Cities should involve their data governance teams at an early stage and consult with them throughout the process.

- Cities should conduct appropriate consultation with the public and other relevant stakeholders as part of the accountability and governance process.
- Cities should clearly define the data needed to achieve the purpose and develop systems to reflect that purpose.
- Cities should ensure that systems always minimise data by embedding technical and organisational measures as early as possible in the collection of personal data.
- Cities should ensure measures for data minimisation persist throughout the whole lifecycle including implementing adequate retention periods and establishing secure deletion processes.
- Cities should ensure that they process data only for its specified purposes by adopting technical and organisational measures. Cities should document these purposes and make it available to individuals.

- Cities should conduct compatibility assessments, when they are using data for a different purpose than originally collected.
- Cities should take appropriate governance steps following the compatibility assessment including where relevant, requesting the consent of the individual for the new purpose, and the establishment of data sharing agreements between actors.
- Cities should establish assessment standards for the procurement of new systems to determine the implementation of privacy considerations.
- Cities should require the demonstration of security standards prior to the procurement of processing systems.
- Cities should establish audit practices that regularly test all parts of a data processing system, through the whole data life cycle, to ensure that it maintains the levels of integrity and confidentiality required.
- Cities should establish methods for providing meaningful information to individuals at the time of collection of personal data.

- As a precondition for the collection of personal data cities should establish methods for providing meaningful information to individuals prior to collection.
- Cities should provide publicly available information that explains the scope of processing across the city, including third parties involved in the processing and their roles.
- Cities must establish systems compliant with individual rights, ensuring products purchased can meet these needs.
- Cities and industry partners delivering projects collaboratively should address governance issues together, prior to beginning processing.

Industry

- Industry should build systems that have flexibility to establish organisational measures and adopt technical measures to meet purpose limitation.
- Industry should ensure that their products reflect industry best practices such as the ability to receive security upgrades, operate a vulnerability disclosure policy, and do not carry universal default passwords.
- Cities and industry partners delivering projects collaboratively should address governance issues together, prior to beginning processing.

Regulators

- Regulators should produce guidance on accountability measures and governance structures, including guidance on processing with multiple actors involved.
- Regulators should provide guidance to cities and industry on methods for minimising data, including aggregation.
- Regulators should provide meaningful information on citizens' rights in relation to processing of personal data in smart city initiatives.