IFI Policy Recommendation

IFI Policy Recommendation No.20 March 2023

Smart City Data Governance Guidelines

Toshiya Watanabe

Professor, Data Governance Research Unit, Institute for Future Initiatives, The University of Tokyo

Tadashi Mima

Director, Hitachi Consulting Co., Ltd.

東京大学未来ビジョン研究センター
Institute for Future Initiatives, The University of Tokyo

【Policy Recommendations】

Smart City Data Governance Guidelines

Background of Policy Recommendations

Smart cities are sustainable cities and regions that can solve various urban and regional problems by utilizing new technologies such as IoT and AI. From FY2021, the government is promoting the "The Vision for a Digital Garden City Nation initiative" which aims to revitalize rural areas and create a sustainable economic society through the use of digital technology, and it is expected that smart city initiatives in various regions will become more active.

On the other hand, there have been cases in which the development of smart city initiatives has been stalled due to a disconnect with the awareness of citizens caused by the prior utilization of data. While there is no doubt that the possibilities of smart cities are expanding with the advancement of technology, advancing with a focus on technology, or collecting data in order to make use of technology first, may result in opposition from citizens and society.

Therefore, we have compiled the Smart City Data Governance Guidelines (hereinafter referred to as the Guidelines) to present approaches to data governance in the promotion of smart cities. The purpose of the Guidelines is to enable the creation of value in smart cities as it should be (i.e., human-centered), rather than prioritizing the use of technology and data,. Data governance refers to frameworks that set rules for data handling in smart cities and control suitable usage on this basis. Data governance includes a process that ensures no misunderstandings with citizens or society, contributing to the promotion of appropriate smart cities.

To center human beings (citizens) and balance the protection of their rights with the creation of services (benefits), the Guidelines explain procedures, etc., for suitable governance of data handling in smart cities.

The formulation of these guidelines was conducted as an activity of the Habitat Project of Hitachi's University of Tokyo Laboratory, and organized and directed by Data Governance Research Unit of the Institute for Future Initiatives (IFI, https://ifi.u-tokyo.ac.jp/units/data-governance/). In formulating these guidelines, we conducted detailed interviews and analysis of the smart city initiatives by Hitachi UTokyo Labs (http://www.ht-lab.ducr.u-tokyo.ac.jp/research/), particularly the Kashiwanoha Smart City project, with the UDCK (Kashiwanoha Urban Design Center), Mitsui Fudosan, and other stakeholders.

The draft guidelines were then presented to a panel of experts at the public workshop "Smart Cities and Data Governance: Policies and Guidelines" held on March 20, 2023 and the final version of guideline has been decided. The expert panelists are listed below: Dr. Oscar Huerta, Policy Analyst on Urban Development and Governance ,OECD), Yuko Harayama (Visiting Researcher, IFI, The University of Tokyo, Professor Emeritus, Tohoku University), Noriyoji Sawaki (Digital Rural City, Cabinet Secretariat) (Director, Councilor, Digital Rural City State Planning Council, Cabinet Secretariat), Hiroki Habuka (Specially Appointed Professor, Faculty of Law, Kyoto University), Kenzaburo Tamaru (National Technology Officer, Microsoft Japan), Asoko Meguro (Director, International Office, Commerce and Information Policy Bureau, METI), Tomoyo Sasao (Project Assistant Professor, Habitat Innovation Research and Social Collaboration Division, Graduate School of Frontier Sciences, The University of Tokyo).

Smart City Data Governance Guidelines

February 2023

Data Governance Research Unit

Institute for Future Initiatives, University of Tokyo

Contents

1. Objectives of the Guidelines

1.1. Background and purpose

As digitalization advances throughout society, development of the metaverse and other virtual spaces has also progressed. Initiatives aiming to fulfill Society 5.0[1], a vision established for Japan's future society, are moving forward steadily. Smart cities are sustainable cities and regions that solve urban and regional problems through advanced management (planning, organization, management, operation, etc.) and new technologies such as the IoT and AI, also they are continuously creating new value. As the spaces at the forefront of fulfilling Society 5.0, many regions have effort to make smart cities.

In addition, the government has been promoting its Vision for a Digital Garden City Nation since fiscal 2021, aiming to revitalize the provinces while making the most of regional uniqueness, working toward a sustainable economic society, with using digital technology. Promotion subsidies provided through the Vision for a Digital Garden City Nation initiative are expected to further energize smart city initiatives in Japan.

Elsewhere, in some smart city initiatives, the use of data has moved far ahead without public intentions and causing the initiatives to fail (see Toronto, etc.). Sometimes, the application of advanced technology creates gaps in the awareness and perceptions of the people who constitute the city or region and society overall, and it causes problems. While the progress of technology has unquestionably expanded the potential of smart cities, promoting excessive technology application and data collection may end up provoking a public or social backlash.

We have compiled the Smart City Data Governance Guidelines (hereinafter referred to as the Guidelines) to present approaches to data governance in the promotion of smart cities. The purpose of the Guidelines is to enable the creation of value in smart cities as it should be (i.e., human-centered), rather than prioritizing the use of technology and data,. Data governance[2] refers to frameworks that set rules for data handling in smart cities and control suitable usage on this basis. Data governance includes a process that ensures no misunderstandings with citizens or society, contributing to the promotion of appropriate smart cities.

To center human beings (citizens) and balance the protection of their rights with the creation of services (benefits), the Guidelines explain procedures, etc., for suitable governance of data handling in smart cities.

1.2. Expected readers

The expected readers of the Guidelines are the staff in charge of smart cities at organizations such as regional municipalities or community-building promotion organizations.

In addition to these staff members, it is expected that mayors, managers, those involved in smart city promotion, and/or residents of smart cities, etc., may read the Guidelines.

[1] A human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space.

[2] According to the DAMA Data Management Body of Knowledge V2 (DMBOK2), data governance is defined as "the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets."

2. Perspectives on smart cities

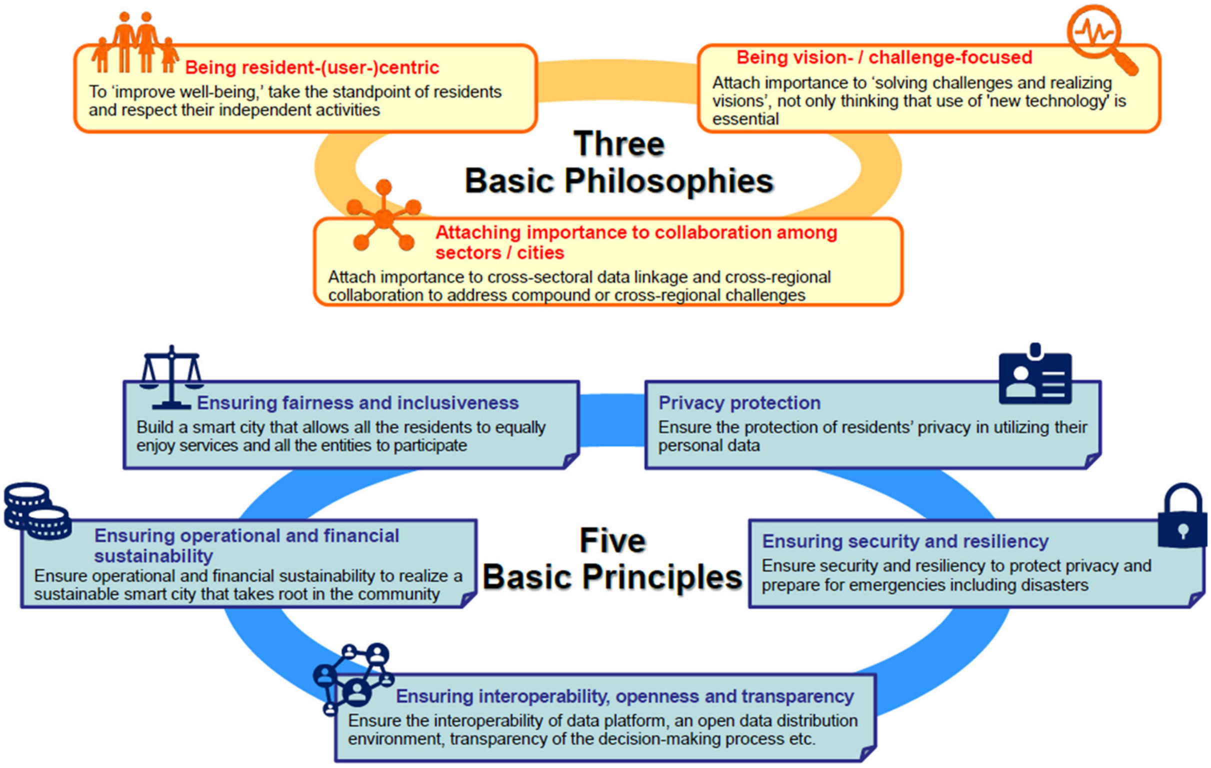
2.1. What is a smart city?

While there exist various approaches to smart cities, the Guidelines refer to the definition in the Cabinet Office "Smart City Guidebook." The Guidebook lists the following three characteristics to define smart cities:

- By providing services to support each one of residents using new technologies, such as ICT, and various public and private data, and by enhancing management in various fields (e.g. planning, development, management / operation) (Means)
- Solves challenges faced by cities and regions, and continues to create new value (Action)
- Being a sustainable city / region where Society 5.0 is realized ahead of the others (State)

In addition to these characteristics, smart cities are anticipated to proceed based on three basic philosophies and five basic principles. In particular, the five basic principles are also closely related to data governance and must be thoroughly examined and considered in regions promoting smart city initiatives.

Fig. 2-1 Basic philosophies and principles of smart cities



Three Basic Philosophies

Being resident-(user-)centric
To 'improve well-being,' take the standpoint of residents and respect their independent activities

Being vision- / challenge-focused
Attach importance to 'solving challenges and realizing visions', not only thinking that use of 'new technology' is essential

Attaching importance to collaboration among sectors / cities
Attach importance to cross-sectoral data linkage and cross-regional collaboration to address compound or cross-regional challenges

Five Basic Principles

Ensuring fairness and inclusiveness
Build a smart city that allows all the residents to equally enjoy services and all the entities to participate

Privacy protection
Ensure the protection of residents' privacy in utilizing their personal data

Ensuring operational and financial sustainability
Ensure operational and financial sustainability to realize a sustainable smart city that takes root in the community

Ensuring security and resiliency
Ensure security and resiliency to protect privacy and prepare for emergencies including disasters

Ensuring interoperability, openness and transparency
Ensure the interoperability of data platform, an open data distribution environment, transparency of the decision-making process etc.

Source: Cabinet Office/MIC/METI/MLIT/Smart City Public–Private Partnership Platform Secretariat, "Smart City Guidebook"

Reference

[Smart City - Society 5.0 - Science and Technology Policy - Cabinet Office (cao.go.jp)]

2.2. Understanding smart cities

Based on the Cabinet Office “Smart City Guidebook,” there is a tendency to think of smart cities as that have a big concept, plan, or overall vision with vertical organizational system, but in the broader sense, all initiatives using ICT, etc. for the benefit of citizens can be considered part of smart cities.

That is, even when not actually using the term “smart city”, any policy or initiative using (personal) data to solve regional problems is a smart city initiative in a sense, requiring appropriate data governance.

Naturally, as in the first of the Guidebook’s basic philosophies, the most important premise of the smart city is most certainly that it is “citizen-(user-)centered.” The Guidelines likewise discuss smart city data governance with, first and foremost, a human-centered foundation.

“Human-centered”

The purpose of smart cities is to enhance the benefits of the people living there; their purpose must not shift to promoting the use of ICT or data. Therefore, it is essential that they be developed premised on an orientation toward enhancing citizen benefits, etc., and on the protection of their privacy and dignity.

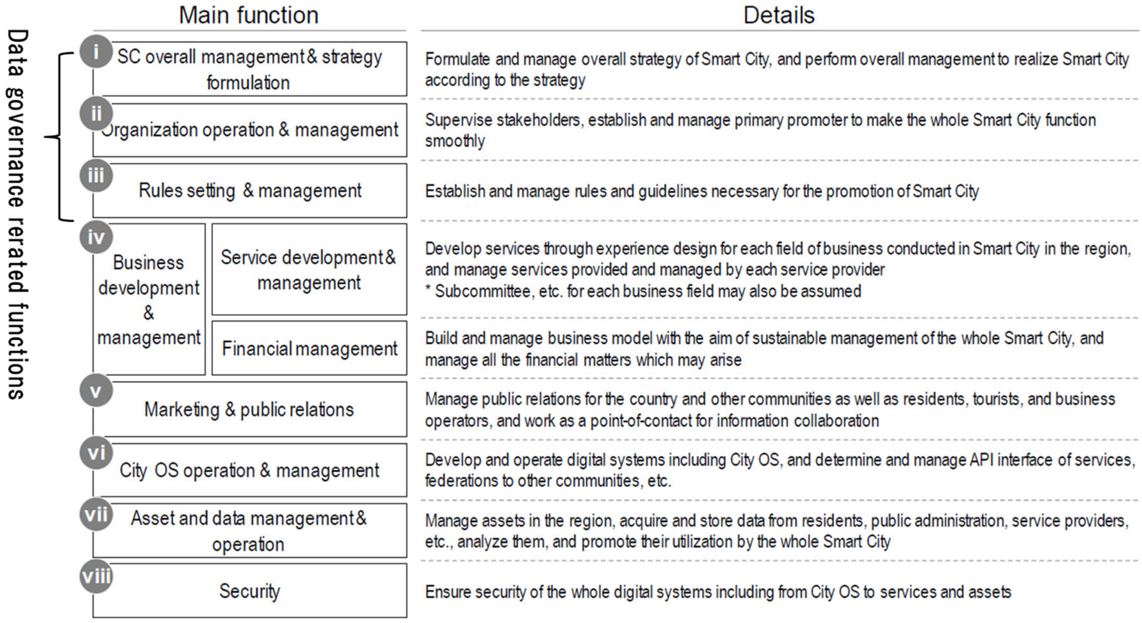
2.3. Organizations promoting smart cities

The promotion of smart cities involves diverse stakeholders so that a promotion organization is required to coordinate their opinions and get them moving in the same direction. Composed of multiple agents (industry, government, academia, citizens, etc.) guaranteeing neutrality, this organization needs to provide the functions required for smart city promotion. Specifically, these diverse functions may include smart city strategy planning, service development, public relations, city OS[3] operation, and coordination among stakeholders, in addition to data governance, such as rule planning and management. The Guidelines describes concepts and processes of data governance based on the assumption that a smart city promotion organization will be at the heart of the initiative.

Naturally, in some cases, regional municipalities conduct digital policy initiatives without using the term “smart city,” as noted above. These can, in fact, also be grasped within the sphere of smart cities; in these cases, it is essential that the policy promoter (for instance, the regional municipality) promote data governance as well.

[3] An overall term for IT systems facilitating the introduction of services in various fields to smart cities, aggregating functions commonly used by the region attempting to create the smart city.

Fig. 2-2 Examples of the functions of smart city promotion organizations



Data governance rerated functions

	Main function		Details
i	SC overall management & strategy formulation		Formulate and manage overall strategy of Smart City, and perform overall management to realize Smart City according to the strategy
ii	Organization operation & management		Supervise stakeholders, establish and manage primary promoter to make the whole Smart City function smoothly
iii	Rules setting & management		Establish and manage rules and guidelines necessary for the promotion of Smart City
iv	Business development & management	Service development & management	Develop services through experience design for each field of business conducted in Smart City in the region, and manage services provided and managed by each service provider * Subcommittee, etc. for each business field may also be assumed
		Financial management	Build and manage business model with the aim of sustainable management of the whole Smart City, and manage all the financial matters which may arise
v	Marketing & public relations		Manage public relations for the country and other communities as well as residents, tourists, and business operators, and work as a point-of-contact for information collaboration
vi	City OS operation & management		Develop and operate digital systems including City OS, and determine and manage API interface of services, federations to other communities, etc.
vii	Asset and data management & operation		Manage assets in the region, acquire and store data from residents, public administration, service providers, etc., analyze them, and promote their utilization by the whole Smart City
viii	Security		Ensure security of the whole digital systems including from City OS to services and assets

Source: Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2, Big-data and AI-enabled Cyberspace Technologies/Smart City Architecture Development/Smart City Architecture Design and Promotion of Related Verification Research “How to Use Smart City Reference Architecture,” amended by the author

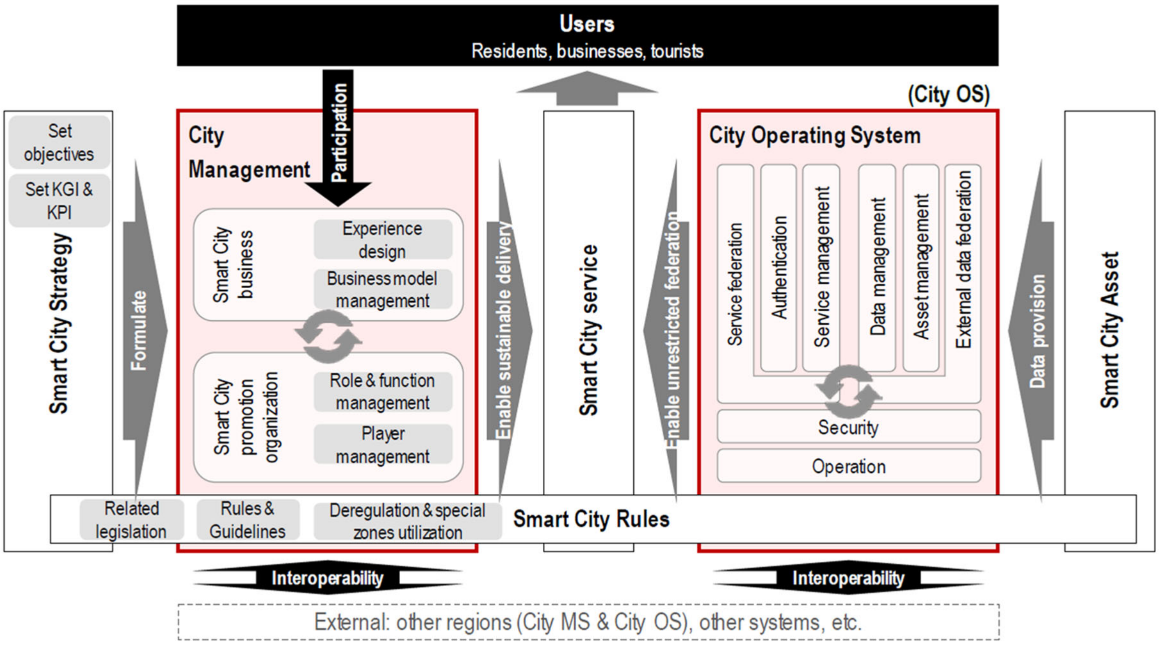
3. Concepts of data governance

3.1. Service first

While the main topic of the Guidelines is data governance, consideration of smart cities must, as stated above, be human-centered, with services (benefits) coming first. As in the Cabinet Office’s “White Paper on Smart City Reference Architecture” (Fig. 3-1), (smart city) services are provided to users (i.e., such as residents(citizens), businesses(corporations), and tourists). These services are then supported by a basis in city management (business, organizations, etc.) and ICT platforms such as the city OS. Smart city rules are fundamental parts supporting services, city management, and ICT, it is necessary to consider such relationships, so-called the system architecture[4] (layered structure).

While the Guidelines discuss data governance, regions working on smart cities must begin considering them from the point of view of services (benefits), addressing data governance based on the content of those services. Considering data governance also requires that these smart city elements be clarified, smart city architecture (layered structure) should be organized in advance.

Fig. 3-1 Smart city system architecture (layered structure)



Source: Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2, Phase 2, Big-data and AI-enabled Cyberspace Technologies/Smart City Architecture Development/Smart City Architecture Design and Promotion of Related Verification Research “How to Use Smart City Reference Architecture”

Reference

Cross-ministerial Strategic Innovation Promotion Program/Outcomes of the Architecture Design and Related Verification Research/Science and Technology Policy/Cabinet Office (cao.go.jp)

[4] In principle, “architecture” in this context describes “relationships between the system and the exterior” and “relationships among elements composing the system,” intended to accomplish a specific purpose.

Services (benefits) must be suited to the purposes of smart cities and must unambiguously lead to “improved well-being through provision of services in accordance with the needs of individual citizens.” However, smart city purposes may vary according to regional contexts, social issues, citizen awareness, and so on. The Cabinet Office’s “Smart City Guidebook” demonstrates smart city services (benefits) as below.

Table 3-1 Examples of smart city services (benefits)

(1) Realization of a safe, high-quality residents’ life / urban activity (Society)

✓ The effect of realizing social inclusion that enables all the residents to enjoy an equal, convenient and affluent life through the provision of more efficient urban services in all areas, including administrative procedures, purchase, transportation, medical care, health and tourism, as well as the provision of the services that meet individual attributes and preferences

✓ The effect of providing a safe and secure life by taking data-based prompt measures in emergencies, such as during a disaster or the spread of infectious disease, or by offering a new remote / real space for living / working in new normal life

(2) Realization of sustainable and creative city management / city economy (Economy)

✓ The effect of producing an environment in which a variety of services for residents and companies are created one after another using various data and new technologies, revitalizing the regional economy

✓ The effect of moving a regional economy through the consumption and purchase of services by residents and visitors who come and go in a safe, convenient and comfortable town, as well as creating diverse innovations through interactions

✓ The effect of increasing the efficiency of systems at companies and governments, improving productivity

(3) Realization of environmentally friendly cities / regions (Environment)

✓ The effect of optimizing the use of energy / resources in line with the actual travel of people and goods in all situations, such as business operations, daily lives and travel behaviors, realizing a decarbonized society

Source: Cabinet Office/MIC/METI/MLIT/Smart City Public–Private Partnership Platform Secretariat, “Smart City Guidebook”

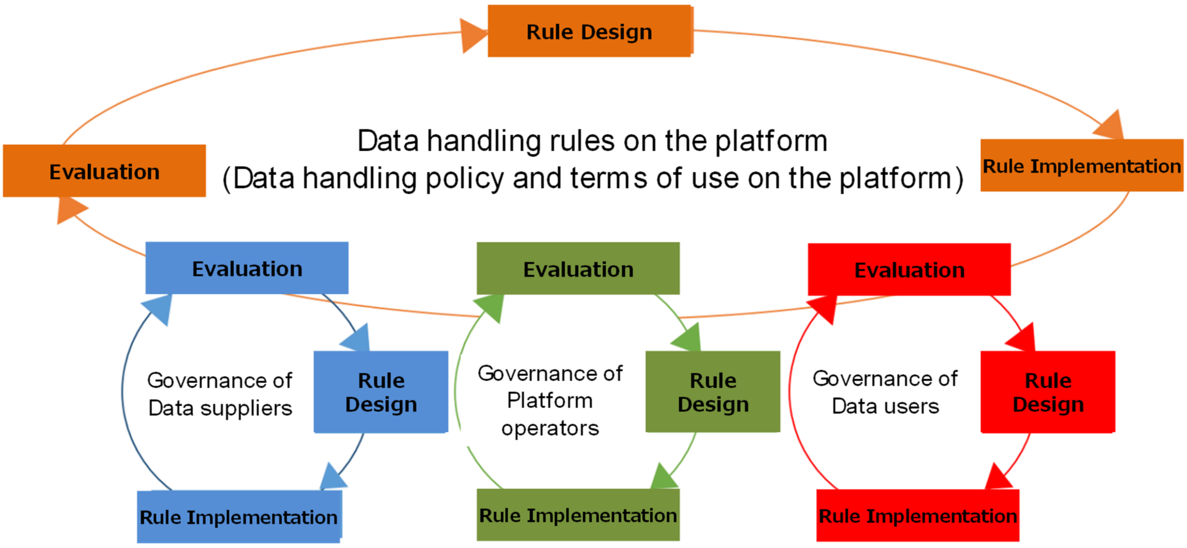
3.2. Perspective by data focused

While it is essential to consider services first, the perspective by data focused is ideal to realize and operate smart cities appropriately, with respect for personal privacy and dignity. Using the metaphor of the human body, if services are the things that a person does, then the processes of data collection, distribution, analysis, and use play the roles of blood vessels within the smart city "body," and inappropriate handling may seriously damage the privacy and dignity (functions) of the individuals (cells) composing the smart city. To repeat once again, the data life cycle (information processing) is an essential element in service generation, and its appropriate control leads in the end to appropriate services (benefits).

Various data can be distributed and used in the smart city for the benefit of citizens and the region. Data would have providers and users and there might be platformers (platform operators) who also distribute the data. Through such stakeholders, it is important in smart cities that data be suitably handled by certain rules. Governance is formed through the management cycle of determining rules, putting those rules into operation, and evaluating their suitability.

Figure 3-2 depicts an image of data handling rules for platforms as shown in "Implementation Guidance for Platform Data Handling Rules Ver. 1.0" of the Digital Agency and Cabinet Office Intellectual Property Strategy Headquarters. The basic structure for data governance in smart cities can be constructed in a similar manner. That is, there are rules for the city OS, the smart city platform, and city management, with rules also required for control of the individual stakeholders involved in the data life cycle.

Fig. 3-2 Data-centered governance



Source: Digital Agency and Cabinet Office Intellectual Property Strategy Headquarters, "Implementation Guidance for Platform Data Handling Rules Ver. 1.0"

Reference

Implementation Guidance for Platform Data Handling Rules Ver. 1.0 (digital.go.jp)

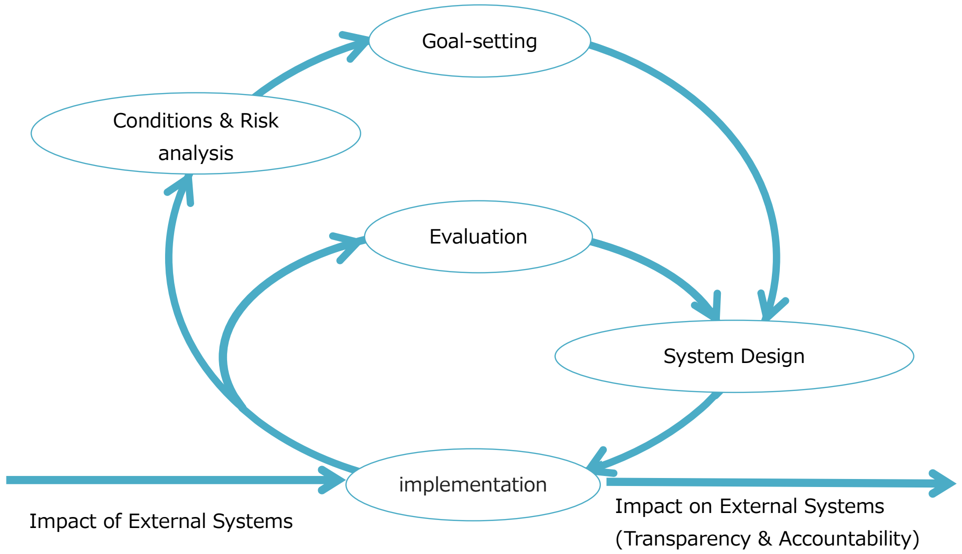
3.3. Agile governance

The diverse range of services (benefits) handled by smart cities spans a wide range including transportation, health and medical care, disaster prevention, education, environment and energy, tourism and community building, infrastructure maintenance and management, and logistics. Many of these services are provided not in all contexts but services are often selected and concentrated in line with local needs. In addition, these initiatives do not always go according to plan, and project revisions must be allowed for. Smart cities are a form of trial and error intended to improve cities, and attitudes toward data governance must reflect this. In other words, it is important not to create perfect rules from the start but to adopt "agile governance," which keeps the cycle of operating, evaluating, and revising rules moving rapidly during the smart city initiative.

Agile governance is defined in METI's "Governance Innovation Ver. 2.0: A Guide to Designing and Implementing Agile Governance" as "a model where a diverse range of stakeholders, including governments, businesses, individuals, and communities, carry out ongoing analysis of the conditions they find themselves in; set the goals they seek to achieve; design various systems for achieving these goals; and carry out ongoing dialogue-based evaluations of outcomes to make improvements to these systems." In Society 5.0, including smart cities, the ideal solutions must be continuously reviewed based on the constantly changing environment and goals. To this end, the fixed governance model, where goals and methods are determined in advance and not changed, is not applicable. The required governance model involves multiple stakeholders keeping the cycle of environmental conditions and risk analysis, goal setting, system design, implementation, evaluation, and improvement moving rapidly and continuously.

In smart city data governance as well, based on the concept of agile governance, while remaining focused on services (benefits), it is necessary not to adhere to the original plan but to keep the cycle of rule design, implementation, and evaluation constantly moving.

Fig. 3-3 Agile governance


Goal-setting
Conditions & Risk analysis
Evaluation
System Design
implementation
Impact of External Systems
Impact on External Systems
(Transparency & Accountability)

Source: METI "Governance Innovation Ver. 2.0: A Guide to Designing and Implementing Agile Governance"

Reference

Report on "Governance Innovation Ver. 2: A Guide to Designing and Implementing Agile Governance" completed (METI)

3.4. Human-centered governance

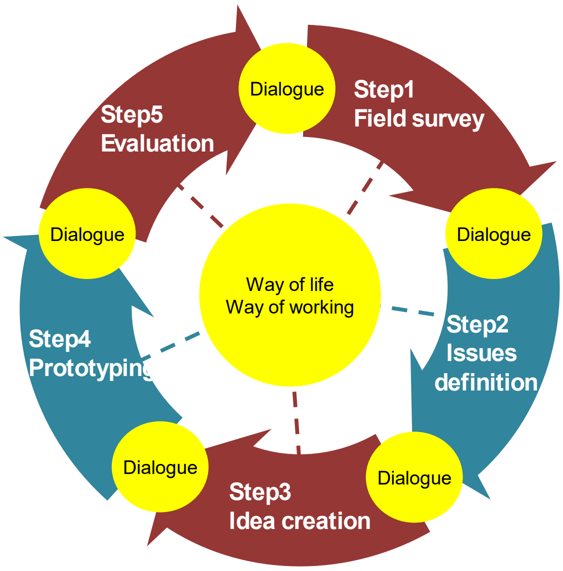
When thinking from a human-centered perspective, data governance in smart cities is not something that can be applied unilaterally. That is, the values of stakeholders, such as citizens, differ by region, and the rules and so on must likewise change accordingly. For example, For example, in regions where there are concerns about people getting lost while out and about accidents while walking alone due to an aging population, citizens may be acceptable to install street cameras to monitor people, but in city centers with constantly shifting populations, privacy concerns may make monitoring cameras unacceptable. In this way, data governance varies by region.

In addition, when considering human-centered data governance, the participation of citizens and others living in the smart city is essential; depending on the services (benefits) realized, diverse stakeholders such as other organizations, businesses, and so on must also be involved without the regional municipality or other promoting agency organizing the rules alone.

Living labs are one method of involving citizens and others. Living labs are a method of putting open innovation into practice in living spaces, defined as "a series of actions in which residents and providers such as corporations experiment together on complex social issues in living spaces, creating new services and products from competition, implementation, evaluation, and improvement." Numerous regions working on smart cities have put the living lab method into practice, including Osaka, Kashiwa, Kamakura, and Yokohama. The use of this method is considered possible for smart cities as well; rules and data governance can also be considered within living labs.

To consider services (benefits) within the physically limited space of the city, unlike national policies, smart cities have the advantage of stakeholders meeting face-to-face (with infection countermeasures) to work on promoting the smart city based on more direct discussion. This advantage should be put to good use when considering data governance as well.

Fig. 3-4 Living lab processes



Source: METI, "Living Lab Introduction Guidebook"

Reference

Living Lab Introduction Guidebook

3.5. Concept of trust

Because of the diverse stakeholders involved in smart cities, it is important to make use of the concept of trust[5] to facilitate appropriate collaboration on data among stakeholders. In other words, we adopt the perspective that it is impossible for stakeholders, such as citizens, to understand and confirm the safety and reliability of all other stakeholders, and therefore, the smart city promotion organization will ideally take up this role (ensuring the reliability of the smart city overall), reducing the burden on individual stakeholders. For example, when promoting smart cities as a way to improve citizen health using PHR services provided by the private sector through the use of medical data, citizens are unlikely to understand the safety and reliability of each PHR service. Therefore, it is expected that the smart city promotion organization would make trust within a framework evaluating and selecting PHR services, enabling citizens to use them easily and with peace of mind. This process is required in relationship between the smart city promotion organization and the regional municipalities or medical institutions providing the medical data as well, so it is necessary to designs that include rules and technical countermeasures ensuring the reliability of the services overall.

In addition, while the concept of trust becomes more important in cyberspace where everything takes place online, it is important to note that smart cities exist amid the physical connections of their regions. Because smart cities involve a combination of connections with real-life aspects of society, rather than the high level of trust called for in services designed for cyberspace alone (for instance, using the electronic certificates as multifactor authentication to handle the problem of identification), a more appropriate and simpler "trust" can be created. For example, a stronger trust can be built through the existence of "gathering spaces" where people come together physically or online, enabling citizens to work together on health improvement, and through links with PHR services as mentioned above.

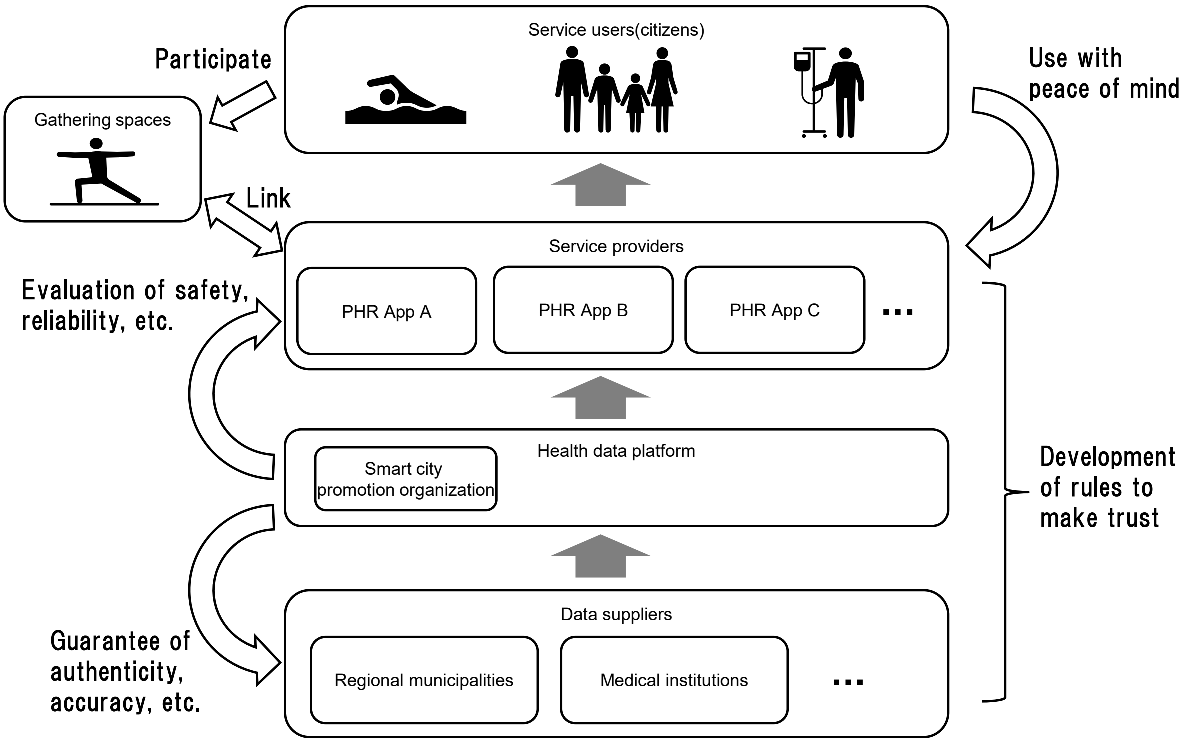
For private-sector firms participating in data linkage to gain citizens' trust, they might also receive third-party certification with regard to the handling of personal information. Privacy marks[6] are a typical example now obtained by over 17,000 businesses. The certification basically provides assurance that management systems are compliant with the Act on the Protection of Personal Information and can be obtained by small businesses as well. The Personal Data Bank Certification[7] by the Information Technology Federation of Japan's (ITrenmei) is another option for stakeholders who act as hubs to pass on data obtained through data linkage. The Personal Data Bank is a framework storing personal information provided by individuals and providing the information where they need it; ITrenmei's certification validates the safety of this framework. Certification standards are compliant with the "Guidelines on Certification of Information Trust Functions" created by the MIC/METI "Committee on Certification Schemes for Information Trust Functions." Because departments as well as legally established corporations can be certified, a municipality's city OS, for instance, could also receive certification.

[5] In addition to its dictionary meaning, the concept of "trust" takes on varying significance according to the field, the target, or the purpose, as confirmed by the Digital Agency in the "Report of the Sub-working Group for Trust-Assured Digital Transformation." The Working Group notes that ensuring "trust" should include not only ensuring online authenticity (the creator, sender, or time of existence matches what is described) and tamper resistance but also ensuring data truthfulness (data contents are correct, not fabricated, etc.), the accuracy of the sender (organization, person, object) information, and longitudinal trust over a long period of time.

[6] https://privacymark.jp/

[7] https://tpdms.jp/

Fig. 3-5 Visual concept of trust



3.6. DFFT

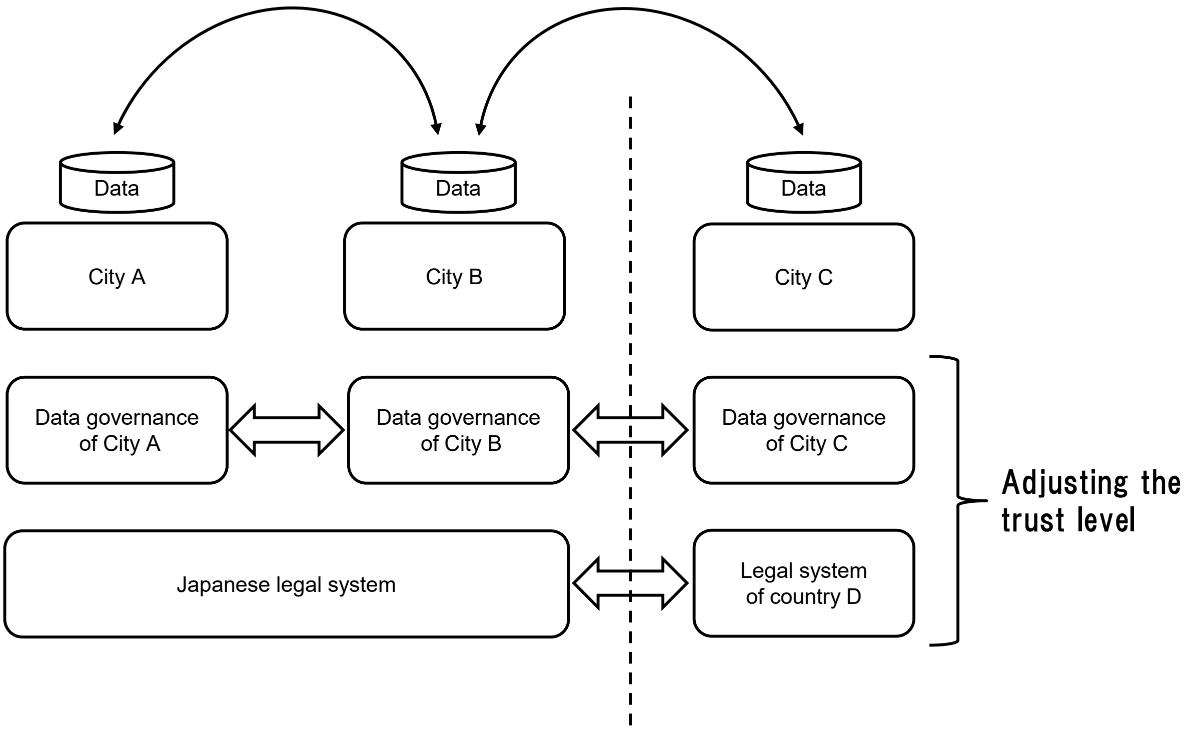
DFFT is the acronym of Data Free Flow with Trust, a concept advocated by the Japanese government at the January 2019 World Economic Forum Davos conference: “free and reliable data flow for freedom, fairness and safety.”

Smart cities may also require data linkage with other cities or other countries to enable entry of people from overseas as residents or tourists. DFFT is intended to facilitate data linkage in these contexts: as noted above, “trust” is the key to data linkage.

For example, when transferring personal data across countries, it is often necessary to obtain the consent of individuals, but thorough confirmation is required to make sure suitable management is taking place at the destination end. DFFT is a concept that by coordinating the trust level including data governance(level of rules including legal systems), in advance, it realize smooth data linkage.

Data linkage across regions and countries is expected to be required for developing smart cities; in particular, international linkage requires coordination at the national level, meaning that it is necessary to consider national policy trends, etc. For example, with regard to personal information within the EU, businesses handling personal information who receive data based on adequacy certification must comply with the Personal Information Protection Commission’s “Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision.”

Fig. 3-6 Visualized DFFT


Data
Data
Data
City A
City B
City C
Data governance of City A
Data governance of City B
Data governance of City C
Japanese legal system
Legal system of country D
Adjusting the trust level

4. Data governance process

4.1. Smart city promotion process and data governance

The Cabinet Office's "Smart City Guidebook" organizes the smart city promotion process into five levels shown below. Data governance is implemented continuously from the planning (strategy) formulation stage through the verification/implementation and establishment/development stages.

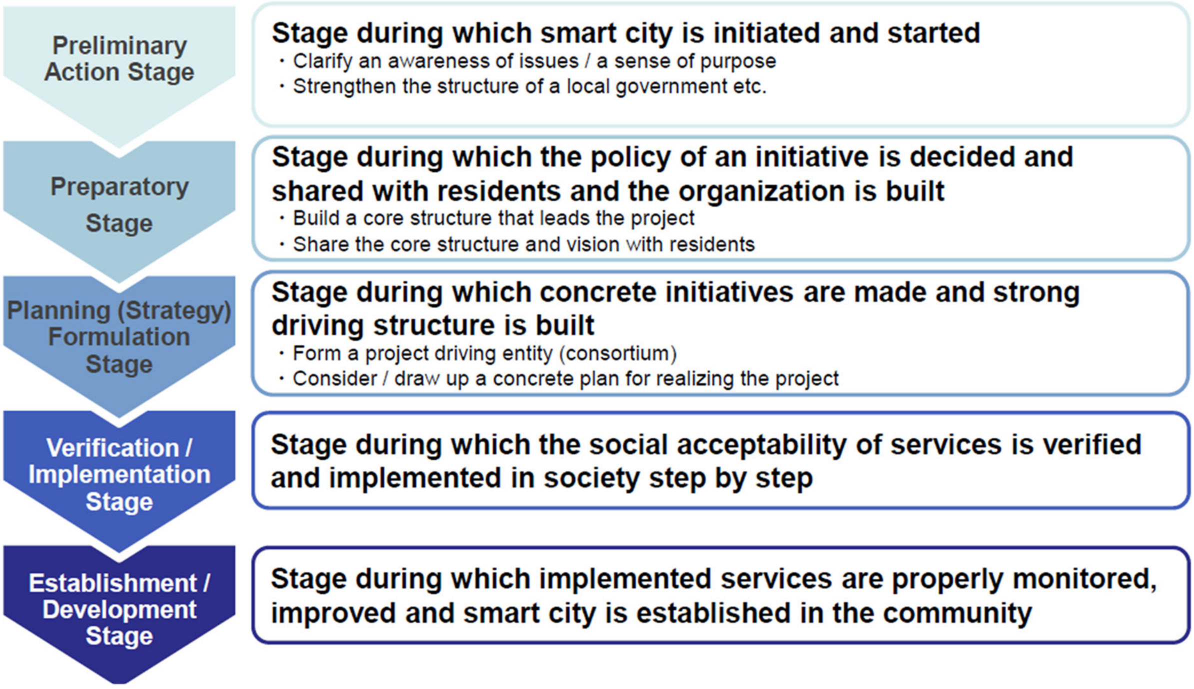
Data governance must be examined deliberately from the planning formulation stage of a smart city project onward, covering what rules and what kind of governance are needed along with the discussion of specific plans for the details of benefits (services).

At the verification/implementation stage, it is essential to verify and confirm the feasibility of the data governance framework being examined along with the benefits (services).

At the establishment/development stage, the benefits (services) will be implemented along with the data governance framework; the latter must be regularly evaluated and improved along with the former.

For the details of the process regarding smart cities, see the Cabinet Office "Smart City Guidebook."

Fig. 4-1 The smart city promotion process



Preliminary Action Stage

Stage during which smart city is initiated and started
- Clarify an awareness of issues / a sense of purpose
- Strengthen the structure of a local government etc.

Preparatory Stage

Stage during which the policy of an initiative is decided and shared with residents and the organization is built
- Build a core structure that leads the project
- Share the core structure and vision with residents

Planning (Strategy) Formulation Stage

Stage during which concrete initiatives are made and strong driving structure is built
- Form a project driving entity (consortium)
- Consider / draw up a concrete plan for realizing the project

Verification / Implementation Stage

Stage during which the social acceptability of services is verified and implemented in society step by step

Establishment / Development Stage

Stage during which implemented services are properly monitored, improved and smart city is established in the community

Source: Cabinet Office/MIC/METI/MLIT/Smart City Public–Private Partnership Platform Secretariat, "Smart City Guidebook"

Reference

Smart City - Society 5.0 - Science and Technology Policy - Cabinet Office (cao.go.jp)

4.2. Process of data governance process

The elements related to data governance are extracted from the smart city process and organized as shown below..

First, organize a project overview based on benefits (services) for citizens and others. As noted above, this takes place at the planning (strategy) formulation of the smart city promotion process, not an individual process of data governance.

Next, organize which laws and regulations are relevant to the project field. These include the Act on the Protection of Personal Information, laws with cross-disciplinary relevance, and laws relevant to the project field. In addition, consider the so-called soft laws[8] or guidelines created by the national government, industry organizations, and so on.

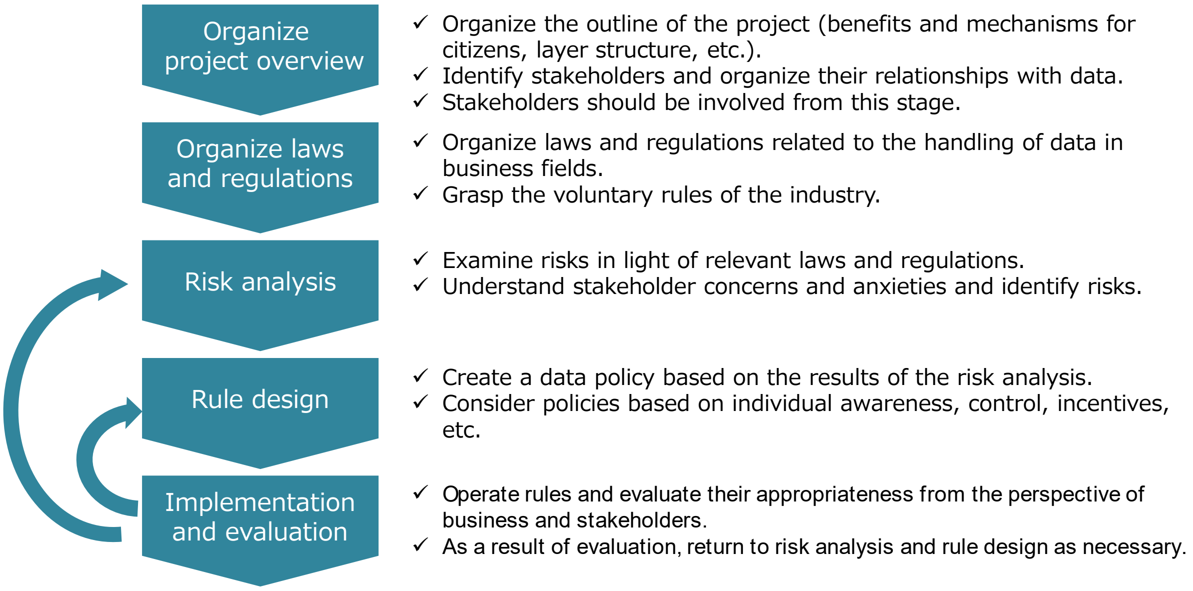
Next, conduct risk analysis based on the project overview and the relevant laws. Risk analysis must include not only reference to the relevant laws but also the perspectives of diverse stakeholders.

Based on the results of the risk analysis, design the rules, for example, by creating data policies. However, while risk reduction is essential, it is also important to take care that the services (benefits) expected of the smart city are not hampered by excessive rules.

Finally, implement and evaluate the rules in practice. As noted above, regular evaluation and improvement are also essential in the smart city process, using evaluation results to then return to risk analysis and rule design.

This process itself is carried out by the smart city promotion organization, but this organization should also keep various stakeholders involved, including citizens as described above.

Fig. 4-2 Data governance process


Organize project overview
Organize laws and regulations
Risk analysis
Rule design
Implementation and evaluation

✓ Organize the outline of the project (benefits and mechanisms for citizens, layer structure, etc.).
✓ Identify stakeholders and organize their relationships with data.
✓ Stakeholders should be involved from this stage.

✓ Organize laws and regulations related to the handling of data in business fields.
✓ Grasp the voluntary rules of the industry.

✓ Examine risks in light of relevant laws and regulations.
✓ Understand stakeholder concerns and anxieties and identify risks.

✓ Create a data policy based on the results of the risk analysis.
✓ Consider policies based on individual awareness, control, incentives, etc.

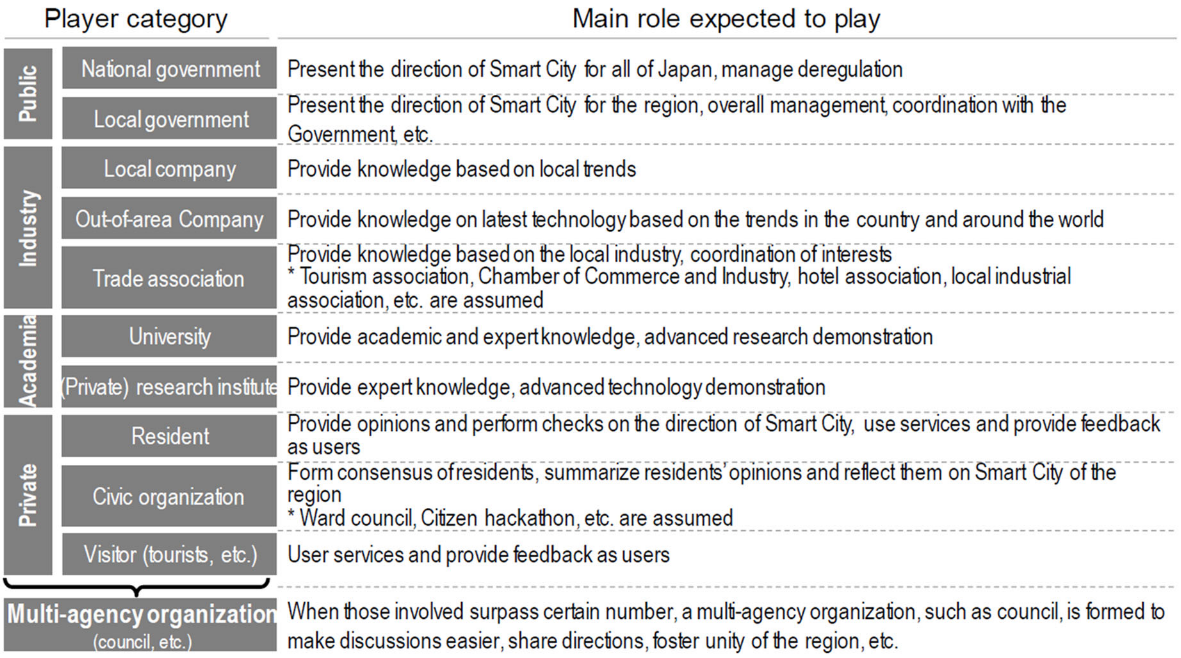
✓ Operate rules and evaluate their appropriateness from the perspective of business and stakeholders.
✓ As a result of evaluation, return to risk analysis and rule design as necessary.

[8] A broad concept including guidelines independently created by the private sector as well as legal interpretations provided by governmental authorities.

4.3. Involving stakeholders

Smart cities include various stakeholders; for data governance to function effectively, the involvement of important stakeholders in the process itself is essential. That said, it is not realistic for all stakeholders to be equally involved. Therefore, when organizing individual project overviews, stakeholder analysis will be called for.

Fig. 4-3 Stakeholders related to smart cities



Player category		Main role expected to play
Public	National government	Present the direction of Smart City for all of Japan, manage deregulation
	Local government	Present the direction of Smart City for the region, overall management, coordination with the Government, etc.
Industry	Local company	Provide knowledge based on local trends
	Out-of-area Company	Provide knowledge on latest technology based on the trends in the country and around the world
	Trade association	Provide knowledge based on the local industry, coordination of interests * Tourism association, Chamber of Commerce and Industry, hotel association, local industrial association, etc. are assumed
Academia	University	Provide academic and expert knowledge, advanced research demonstration
	(Private) research institute	Provide expert knowledge, advanced technology demonstration
Private	Resident	Provide opinions and perform checks on the direction of Smart City, use services and provide feedback as users
	Civic organization	Form consensus of residents, summarize residents' opinions and reflect them on Smart City of the region * Ward council, Citizen hackathon, etc. are assumed
	Visitor (tourists, etc.)	User services and provide feedback as users
Multi-agency organization (council, etc.)		When those involved surpass certain number, a multi-agency organization, such as council, is formed to make discussions easier, share directions, foster unity of the region, etc.

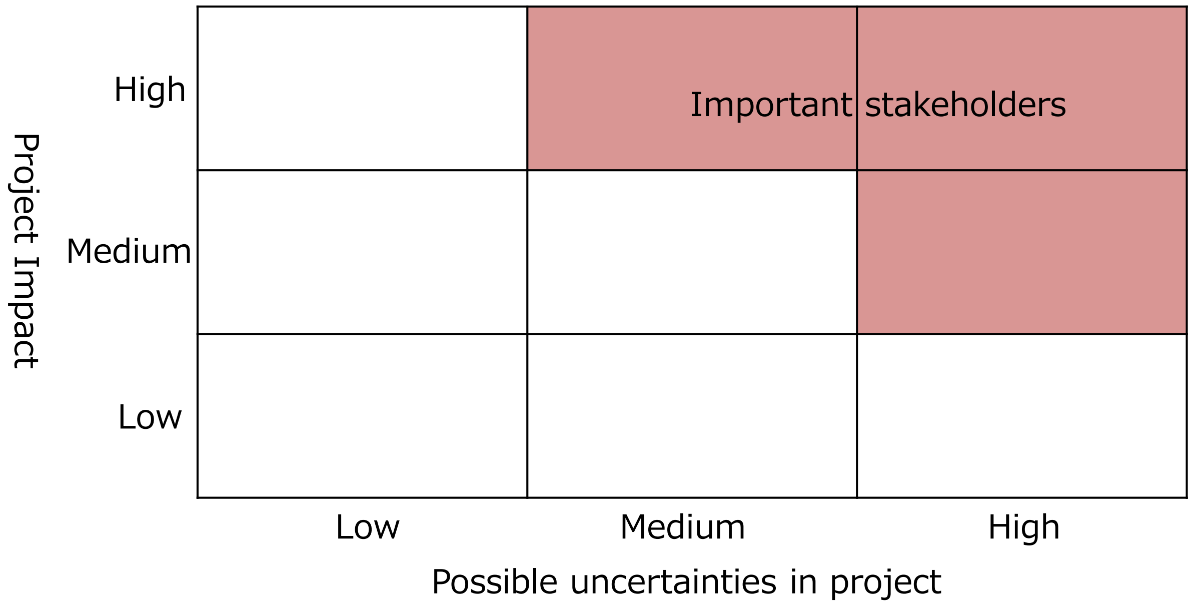
Source: Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2, Big-data and AI-enabled Cyberspace Technologies/ Smart City Architecture Development/Smart City Architecture Design and Promotion of Related Verification Research “Smart City Reference Architecture White Paper”

The January 2020 World Economic Forum Davos Conference drew attention to its focus on the theme of “Stakeholders for a Cohesive and Sustainable World,” at which reference was made to the term “stakeholder capitalism.” Stakeholder capitalism refers to long-term corporate management, aiming to make a contribution to stakeholders through corporate activities, that concept would apply similarly to smart city initiatives. In other words, smart cities are called on to create services (benefits) from a long-term perspective, including contribution to stakeholders.

Stakeholders directly involved in businesses, service provision and reception, or data exchange can tend to be the focus of attention, but it is essential to also consider indirectly involved or affected stakeholders such as industry organizations and competing services. For example, when starting a project relating to healthcare for citizens, it is easy to think of the stakeholders only as the citizens and the service providers and/or the medical and care staff involved; however, there are others as well, such as local doctors’ associations, NPOs volunteering in the field, and so on.

Consider the importance of stakeholders and make selections based on the degree of impact to the project and the potential for introducing uncertainties (negative influences). Uncertainties, meaning the potential to affect stakeholders’ rights or existing benefits, are considered and evaluated in terms of elements causing stakeholders’ unease.

Fig. 4-4 Selecting important stakeholders

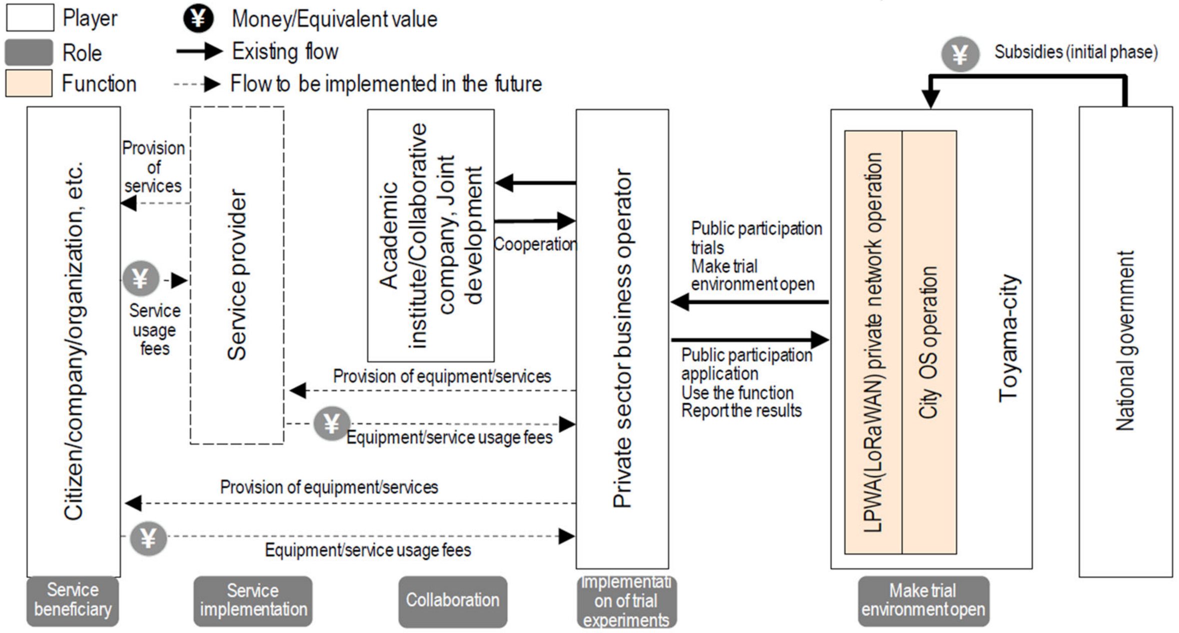


5. Detail of data governance process

5.1. Organize project overview

The first step is to organize the project overview. This is synonymous with planning (strategy) formulation of the smart city; items to be organized include the objective, the initiative content, implementing agents, stakeholders, promotion policies, and schedule (roadmap). At this point, the most important thing is services (benefits) for citizens and society and the question of whether the project is centered thereupon. Along with clarifying the smart city project architecture (layered structure) centered on services (benefits) (see 3.1), the project's stakeholders are also identified and the business model is organized, including the relationships between benefits, data, etc. Note that indirect stakeholders may not be represented in the architecture or business model; when organizing the project overview, indirect stakeholders are to be included in reference materials, etc.

Fig. 5-1 Example of a smart city business model


Player
Role
Function
Money/Equivalent value
Existing flow
Flow to be implemented in the future
Subsidies (initial phase)
Citizen/company/organization, etc.
Provision of services
Service usage fees
Service provider
Academic institute/Collaborative company, Joint development
Cooperation
Private sector business operator
Provision of equipment/services
Equipment/service usage fees
Provision of equipment/services
Equipment/service usage fees
Public participation trials
Make trial environment open
Public participation application
Use the function
Report the results
LPWA(LoRaWAN) private network operation
City OS operation
Toyama-city
National government
Service beneficiary
Service implementation
Collaboration
Implementati on of trial experiments
Make trial environment open

Source: Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2, Big-data and AI-enabled Cyberspace Technologies/ Smart City Architecture Development/Smart City Architecture Design and Promotion of Related Verification Research "Smart City Reference Architecture White Paper"

At this point, or at the smart city preparation stage, analyze stakeholders; ideally, important stakeholders should be involved not only in the smart city project but also in the data governance process. As noted above, the important stakeholders are evaluated based on the degree of impact to the project and the potential for introducing uncertainties (negative influences), sometimes including indirect stakeholders. Examination of stakeholder engagement based on their specific qualities is required. General stakeholder engagement can be framed as in Table 5-1. For particularly important stakeholders, potential methods of involvement/cooperation should be examined.

Table 5-1 Methods of stakeholder engagement

Format	Method
Information distribution	Individual notification of stakeholders, media PR, etc.
Information gathering	Questionnaires, social media analysis, councils of experts, etc.
Two way	Individual negotiations, information meetings, etc.
Involvement/cooperation	Project participation, living labs, partnerships with stakeholders, multi-stakeholder processes[9], etc.

In addition, when involving diverse stakeholders, because their potential contributions and interests differ, it is important to find consensus on the lowest common denominator. Ideally, the following should be organized and agreed in advance: the services (benefits) the smart city is aiming for; a rough division of roles to achieve that end; the rules for cooperation (participation methods, handling of outcomes/intellectual property, etc.).

[9] Processes in which at least three stakeholders hold a meeting for participation/discussion on an equal ground, working toward communication such as consensus building on issues difficult to resolve as individuals or in pairs.

5.2. Organize laws and regulations

The first condition to be met when considering data governance is legal compliance. Smart cities in violation of the law will fail to obtain citizens' trust and struggle to attain the benefits they should. In accordance with the progress of digitalization, laws in various fields are undergoing revision; the relevant laws should be examined in collaboration with experts well read in the program fields. Naturally, the basic laws across different fields when handling data must be considered, such as the Act on the Protection of Personal Information. Compliance with these laws is an absolute necessity. In the Cabinet Office's "Smart City Reference Architecture White Paper," examples of relevant laws are listed as in Table 5-2.

For example, the R&D for an AI to prevent frailty in older people, which is being conducted in Kashiwa-no-ha Smart City, is examining a framework of data governance based not only on Kashiwa City's ordinance on personal information protection but also on other laws, including the national Act on Assurance of Medical Care for Elderly People, the National Health Insurance Act, and the Long-Term Care Insurance Act, to make use of the medical and care-related information possessed by the regional municipality. Although, the municipality's ordinance on personal information protection is to be integrated into the Act on the Protection of Personal Information, which will come into effect in April 2023 in Japan.

Table 5-2 Laws relevant to smart cities

Area	**Relevant laws and regulations**
Traffic and mobility	Road Traffic Act, Road Transportation Act, Road Trucking Vehicle Act, Railway Business Act, Civil Aeronautics Act, etc.
Health and welfare	Medical Service Act, Long-Term Care Insurance Act, etc.
Energy	Electricity Business Act, etc.
Communication	Radio Act, etc.
Agriculture	Agricultural Land Act, etc.
Administrative procedures	Digital Procedure Act, etc.
Urban development	City Planning Act, Road Act, River Act, Urban Parks Act, etc.

Source: Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2, Phase 2, Big-data and AI-enabled Cyberspace Technologies/Smart City Architecture Development/Smart City Architecture Design and Promotion of Related Verification Research "Smart City Reference Architecture White Paper"

In addition to the relevant laws, it is also essential to consider guidelines, etc. formulated by government agencies and industry organizations. Due to the recent fast pace of technological innovation and the difficulty of keeping pace with this at the legal level, there are many examples where governance frameworks are used, predicated on the voluntary regulations by corporates known as soft laws. Therefore, it is also important to research and examine which soft laws are relevant in the project field of smart city.

For instance, representative soft laws would include METI and MIC's "Guidebook for Utilization of Camera Images Ver. 3.0" for the project using camera images and MLIT's "Guidelines for MaaS-related Data Linkage Ver. 2.0" for transportation data. There are also independent soft laws, mainly created by corporates, such as LBMA Japan's "Guidelines on the Usage of 'Device Location Data' in Position Information, etc."

Table 5-3 Examples of soft laws to be taken into consideration

Data used, etc.	Soft laws
Camera images	METI/MIC "Guidebook for Utilization of Camera Images Ver. 3.0"
Position information	LBMA Japan "Guidelines on the Usage of 'Device Location Data' in Position Information, etc."
Transportation	MLIT "Guidelines for MaaS-related Data Linkage Ver. 2.0"
Health information	MIC/MLHW/METI "Basic Policy on Handling Medical Examination Information from Private-Sector PHR Businesses"
Medical information	MHLW "Guidelines on Safety Management of Medical Information Systems Ver. 5.2." METI/MIC "Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information"
Smartphone apps	MIC "Smartphone Privacy Initiative"

5.3. Risk analysis

Based on organizing the project overview and relevant laws, it should be considered whether risks are present in the data life cycle during project implementation. The following six focal points for risks would be important with reference to the "Implementation Guidance for Platform Data Handling Rules Ver. 1.0" of the Digital Agency and Cabinet Office Intellectual Property Strategy Headquarters.

Three focal points (Compliance with relevant laws and regulations, Privacy protection in the data life cycle, Ensuring security) are explained below.

Table 5-4 Focal points for risks in smart cities

Focal points	Overview
Compliance with relevant laws and regulations	Have the relevant laws and regulations including soft laws been suitably understood? Is the project in compliance with their contents?
Privacy protection in the data life cycle	Has appropriate consideration been given when handling personal data so as not to cause feelings of unease and discomfort among stakeholders with regard to the handling process?
Respect for intellectual property and confidential information	Is there suitable protection for the intellectual property and information to be kept confidential belonging to the organizations participating in the smart city?
Ensuring security	Is there safety management ensuring that there are no problems such as information leaks or service falsifications?
Appropriate operation	Is there any risk that the smart city services will negatively impact fairness, safety and economy for citizens and others?
Maintenance of overall governance	Is the governance system working for mitigating the above risks with regard to the overall stakeholders who comprise the smart city services?

(1) Compliance with relevant laws and regulations

It is relatively simple to handle aspects of compliance with relevant laws in smart cities that are explicitly stated in the law. However, parts that depend on soft laws, precedents, etc., are less easily judged and may lead to risks, mostly concerning privacy violations. Successful legal action by a group of residents based on privacy violations may result in an order to pay compensation (demand for compensation for damage based on torts (Civil Code Article 709)) to residents or to cease doing business (injunction based on violation of personal rights). Careful examination of existing smart city plans indicates three issues likely to involve privacy violation problems: 1) use of facial recognition cameras; 2) use of location data; 3) use of education data.

1) Use of facial recognition cameras

Regarding the photography of humans with cameras and the use and release of the information photographed, legal precedents have made it clear that in certain cases, infringement of image rights and privacy will incur compensation and injunctions. Many of these include police security cameras and mass media reporting. Photography with facial recognition cameras is done to extract features; because features are numerical representations of image shapes, they are sometimes considered not applicable to image rights infringement. However, in general, photography with facial recognition cameras is considered a possible source of image right infringement.

The courts have thus far indicated strict standards regarding police photography, with conditions for legality such as “when a crime is recognized to be in progress or to have just taken place, and when evidence preservation is both necessary and urgent, and when the photography takes place with methods not exceeding the limits of those generally permitted.”[10] While this is an extremely stringent standard, police photography should be distinguished from photography conducted within the scope of smart city by non-police administrative organizations. Photography by municipalities or shopping districts within the scope of smart city can be considered similar to photography by private-sector businesses as long as there is no special reason requiring the photographic data to be provided to the police.

While there are few court precedents on private-sector security cameras, those on convenience store security cameras can be referenced. A representative case heard by the Tokyo District Court on September 27, 2010 (*Precedent Times* Vol. 1343 p. 153) debated whether the act of photography by convenience store security cameras itself could be considered illegal as a violation of image rights and privacy.[11] The verdict provided criteria for illegality as below.

> The security camera in this case indiscriminately recorded customers selecting and buying products, without their individual consent, and it was therefore considered to be at risk of violating customers’ personal interests[12] and privacy as above. Therefore, with regard to the security cameras in this case, the question of whether recording customers in the store and publishing the images via provision to the media is illegal or not, should be determined based on the criterion of whether the violation of personal interest and privacy exceeds the socially acceptable limits. Consideration should also be given to the overall context such as the purpose, necessity, and method of the photography and of the provision of images, image management methods, and so on based on weighing the benefits of publishing against those of not publishing the images photographed as above.

This case addressed both photography and provision without permission. With regard to photography alone, the verdict took the purpose, necessity, and method of the photography, along with the method of image management, into overall consideration to determine whether a violation of privacy and image rights had taken place, serving as a reference for judgments of legality in facial recognition camera photography overall.

From the perspective of this kind of overall judgment, the following points require caution to avoid violations of privacy and image rights.[13]

- The purpose of use must be legitimate, and the photography must be required in connection with the purpose of use. Inappropriate examples include use for discriminatory purposes without a legitimate reason or the acquisition and use of camera images with an unclear purpose of use such as “for purposes needed by regional

[10] Supreme Court, December 24, 1969, Kyoto Student Union Incident (*Precedent Times* Vol. 242 p. 119, *Precedent News* Vol. 557 p. 18). However, note that there are convincing opinions that this standard is a case verdict and that it does not apply to general police photography (Supreme Court verdict exegesis, *Criminal Cases* Vol. 62 No. 5 p. 1398, April 15, 2008).

[11] For a similar case, see the Nagoya District Court of July 16, 2004 (*Precedent Times* Vol. 1195 p. 191).

[12] Citing the Supreme Court’s Kyoto Student Union Incident (see note 10 above), the term “personal interest” is used rather than “image rights.”

[13] Created based on page 12 of the “Guidebook for Utilization of Camera Images Ver. 3.0”

store business."

- The methods, means, and use of photography must be appropriate. Inappropriate examples include the use of excessive photography methods affecting privacy (for instance, long-term, large-scale tracking without the permission of the subject), acquisition of data within an unnecessarily broad scope of photography, storage of data outside the required period, or photography using methods in which the subject does not realize they are being photographed (sneak photography, etc.).
- The images photographed must be suitably managed. Inappropriate examples include storing data on the subject such that it can be easily used for unrelated purposes.

Reference

Report of the Council of Experts on the Use of Camera Images for Preventing Crime and Ensuring Safety (Draft)

Guidebook for Utilization of Camera Images Ver. 3.0

2) Use of location data

Location data provides information not only on place of existing but also, over a minimum period of acquisition, on home addresses, schools, places of employment, etc. Sensitive information on beliefs, health status, etc., can also be inferred from visits to churches, political party offices, hospitals, and so on. Elsewhere, location data is currently acquired and used by many smartphone apps.

Among court cases on location data and privacy, the N-system[14] incidents serve as a reference. While there are multiple precedents related to the N-system, recent case criteria for illegality are as below.

> Overall judgments should be made based on (a) the nature of the information acquired, stored, and used, that is, whether it relates to individual ideology, beliefs, behavior, etc.; (b) the legitimacy of the purpose for which the information is acquired, stored, and used; (c) the legitimacy of the methods of acquisition, storage, and use; (d) the rigor of the information management methods; and so on.

The verdict above evaluates (a), the nature of the information, as below, clarifying that it involves a degree of sensitivity and privacy.

> When information on the travel of a vehicle is accumulated in large quantities and in detail, it is undeniable that it can serve as a basis for inferences regarding the behavior of the individual driving the vehicle. Further, as argued by the plaintiffs, as the problem of monitoring citizens' behavior may arise, the information obtained by the N-system etc., is also clearly outside the scope of information that may be gathered, whether in terms of purpose or method.

This judgment is notable for the court's recognition that the accumulation of "large quantities of detailed" location data in fragments may lead to an understanding of individual behavior.

We should also note that the criteria used here are similar to those regarding camera photography above. That is, an overall judgment is composed of four elements: the three camera elements plus (a) above - the nature of the information acquired. From the perspective of this overall judgment, the following points require attention to prevent violations of privacy or image rights.

- First, regarding the use of location data in emergencies or for disaster prevention or mitigation, even if we

[14] Officially the "Automatic Vehicle Number Recognition System." This system photographs the number plates of vehicles in motion and automatically references them against vehicles being sought by the police, unlike Orbis, which only photographs vehicles exceeding the speed limit.

assume that the information is sensitive with regard to (a) the nature of the information, there is a high likelihood of such use being deemed legal in terms of the legitimacy of (b) the purpose of acquisition and use. By contrast, when using location data for commercial purposes to recommend content or target ads based on behavior, there is a lower level of legitimacy of (b) the purpose of acquisition and use, and therefore, (c) the method of acquisition and use must be stringently examined. Basically, it is impossible to eliminate the risk of privacy violation without obtaining effective consent from the subject.

- Next, when obtaining location data from facial recognition cameras, the reasonableness of (c) the method of acquisition and use comes into play. Position information can also be obtained by other methods, such as finger vein authentication, which is less likely to violate rights. When location data in smart city plan can be acquired by other means, such as finger vein authentication, (c) the method of acquisition and use may be judged to be unreasonable.
- Further, regarding the N-system, note that the courts consider the "accumulation of large amounts of detailed" location data, even in fragments, to lead to understanding and monitoring individual behavior. Given this view on the part of the courts, it is significant that even when the location data is the same, the vehicle travel information acquired by the N-system is entirely different in precision from, for instance, the location data of a smartphone app GPS. In the case of N-system, vehicle travel is just one part of the movement within an individual's life overall; its precision is reduced by the inclusion of information about family members and others apart from the individual in question, thus making it less likely to lead to "behavior monitoring." Smartphone GPS dada clarifies the entire scope of movement within an individual's life, and because generally each smartphone is used by one person, eliminating the inclusion of information about others, it enables high-precision monitoring; compared with the N-system, it caries a notably high risk for privacy violations. Based thereon, when acquiring and using smartphone GPS data, in an overall judgment of (b) the purpose of acquisition and use, (c) the method of acquisition and use, and (d) the method of managing the information acquired, each element must be judged stringently.
- In addition, the final element of the overall judgment ((d) the method of managing the information acquired) calls for safety management; when the project plan lacks safety management, obtaining location data is likely to be considered a violation of privacy.

3) Use of educational data

The use of the educational data possessed by the municipality must be human-centered (i.e., child-centered), as the Guidelines emphasize. In addition, as seen in the article "failure of the road map to utilization of educational data"[15], that road map publicized by the Digital Agency, the "unified management" of educational data is a source of lasting unease in society. Therefore, careful consideration is required for unified management with data in other fields or data stored for long periods involving observation of children. Elsewhere, educators have repeatedly emphasized that the use of educational data should be for "children's benefit"; if operators of institutions such as cram schools make use of educational data for profit purposes, it must be highly effective for the children at the same time.

The judgment standards for privacy violations in terms of acquisition, listed above ((a) the nature of the

[15] DIAMOND online "Hardly started, and yet...Why the Digital Agency's 'utilization of educational data' went up in smoke," January 28, 2022.

information acquired; (b) the purpose of acquisition and use; (c) the method of acquisition and use; (d) the method of managing the information acquired), are also effective here. In terms of making an overall judgment with consideration for the special characteristics of educational data as above, the following precautions are required to avoid privacy violations.

- (b) The purpose of acquisition and use must be for the children's benefit; whatever the overall judgment, any project lacking in this aspect is not suitable.
- In particular, careful consideration is required regarding (c) the method of acquisition of use in relation to concerns about "unified management" with data in other fields and long-term data storage.
- The prevention of delinquency and other deviant behavior is an important issue in school education; predicting the potential for delinquency by recording and analyzing the changes in students' educational history and overall lifestyle at school is highly rational in terms of (b) the purpose of acquisition and use of data. However, problems remain in relation to (c) methods of acquisition and use. First, data must not be gathered in contexts subject to the problem of "inaccurate labeling" of students, which arises due to low-precision predictions, as this can lead to unjust discrimination and disadvantaging of students. In addition, even with sufficiently improved prediction precision due to the outcomes of machine learning, it is entirely possible that children with attributes statistically likely to lead to delinquency will not in fact become delinquent based on their individual beliefs, thinking, etc. The effect of judging such students as being "at risk of delinquency" in spite of this is a denial of their individual autonomy.[16] Rejecting the possibility that students with attributes prone to delinquency will overcome them based on their own strength of will indicates that data-based prediction of delinquency lacks rationality in terms of (c) methods of acquisition and use, risking violation of privacy.
- In addition, the final element in an overall judgment ((d) the method of managing information acquired) requires safety management; if smart city project is lacking in this regard, the use of educational data may prove a violation of privacy.

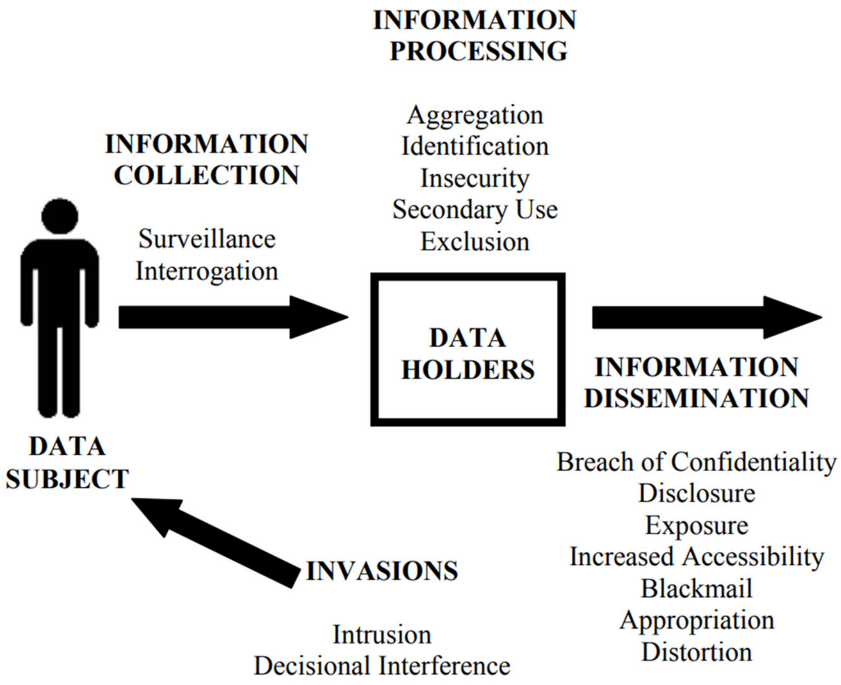
(2) Privacy protection in the data life cycle

The section on "Compliance with relevant laws and regulations" discusses the risks of privacy violation based on soft laws, precedents, etc. When realizing a human-centered smart city, it is essential to consider risks over a wide range of perspectives, including those of citizens and other stakeholders. For example, when handling data even in situations other than (1), the risks associated with privacy protection may be examined from perspectives like those in Fig. 5-2. Compiled by the US privacy scholar Daniel Solove, this fig. shows the risks that can arise within the data life cycle (collecting information from the data subject (individual), processing it, disseminating (diffusing) it, and invading (providing feedback) to the individual) and serves as a reference for anticipating potential risks. (See Appendix for details)

As noted above, when considering the human-centered smart city, the extent to which citizens will accept the use of data differs by region. Therefore, risk analysis also requires a grasp of the regional stakeholders' awareness.

[16] Yamamoto Tatsuhiko's *Privacy no kenri wo kangaeru [Considering the Right to Privacy]* (Shinzansha, 2017), p. 102, takes a similar position, albeit with regard to crime prediction.

Fig. 5-2 Privacy risks



Source: Daniel Solove "A taxonomy of privacy"

(3) Ensuring security

In smart cities, it is necessary to pay attention to the increasing security risk as information breach in addition to the violation of the relevant laws and rights to privacy. The reason security risks are higher in smart cities is that data are shared among diverse stakeholders.

Data linkage necessitates ensuring not only the security of the information communication network required for the linkage but also that there is a sufficient security level on both the data provider's side and the data user's side. In addition, because data are shared among multiple stakeholders, handling incidents becomes more complex. For example, when data brech from a given organization, the effects extend not only to that organization but all the organizations linking with its data throughout the smart city, meaning that collaboration is required in handling incidents.

In addition, smart cities would make and maintain their data platforms, such as the city OS. Because these platforms are effective as data linkage hubs that accumulate various data, it is important to note that security issues there may lead to serious adverse consequences.

As noted above, given that data itself circulate in linkage among organizations as the bloodflow of the smart city, major risks arise when its accuracy and authenticity are not ensured. If the data quality is not ensured, results may include failures in AI development or the inability to create the benefits that ought to result from smart city services.

Reference

MIC | Press Release | Result of Appeal for Opinions on Draft Smart City Security Guidelines (Edition 2.0) and Release of Finished Smart City Security Guidelines (Ver. 2.0) (soumu.go.jp)

5.4. Rule design

A data policy (rules) must be created for smart city projects from the perspective of risk mitigation. Here the rules exist at two levels: the overall framework for the smart city as a whole (the promotion organization) and the individual services (benefits) (i.e., each program).

The rules for the smart city as a whole indicate the basic approaches to and principles for data handling, with points in common with the rules set for individual projects. These rules also stipulate the organizations and decision-making processes for setting rules for individual projects.

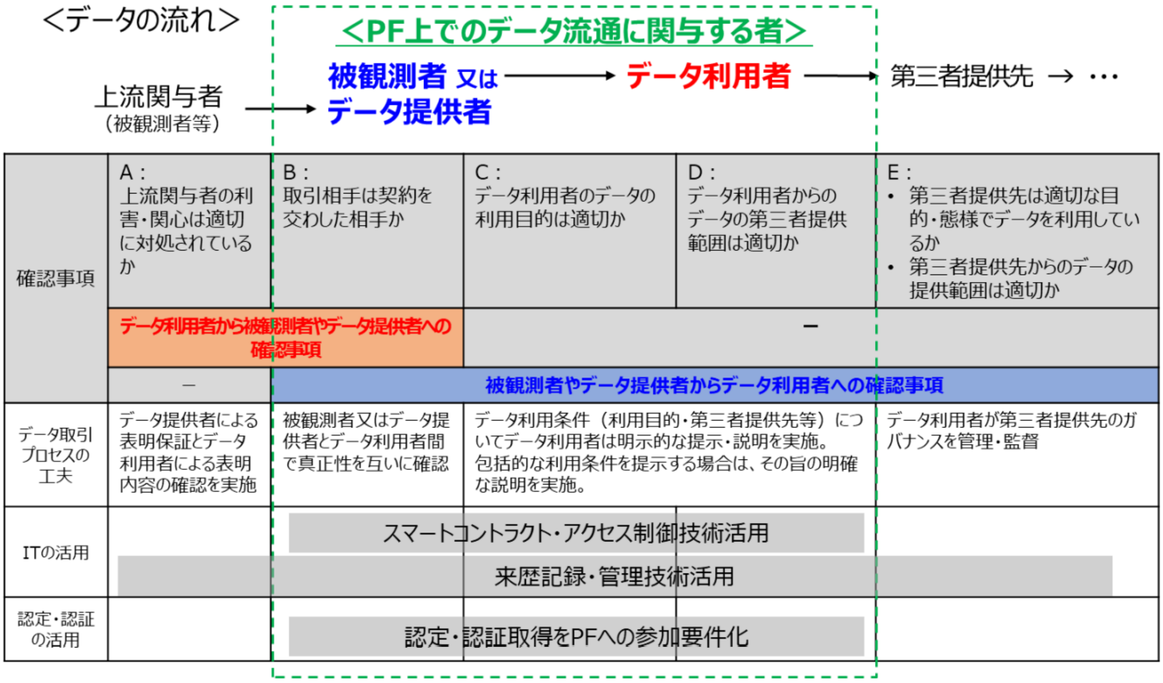
Elsewhere, rules for each program must be examined individually based on service (benefit) content, program field relevant laws, regional characteristics, etc., so that data handling is regulated more specifically.

It is important to consider the following in rule design at either level.

(1) Data controllability

The basis of data governance is to ensure data controllability with regard to data handling in smart cities, regardless of whether it be data on individuals (personal data) or on corporations, the environment, etc. (non-personal data). Therefore, based on the data provider (the individual, in the case of personal data), data users, third parties, data distribution, life cycle, etc., the planning of countermeasures for risk mitigation in each case is itself the process of rule design. Fig 5-3 depicts the points to confirm and confirmation methods for ensuring controllability on platforms as shown in “Implementation Guidance for Platform Data Handling Rules Ver. 1.0” of the Digital Agency and Cabinet Office Intellectual Property Strategy Headquarters. The purpose of designing rules is to regulate those items. In addition, in the case of personal data, the individual from whom data are being obtained is subject to observation, i.e., the target of observation is the data subject. Some forms of non-personal data (weather data, for instance) do not have any target of observation; others include data created from the activities of organizations, such as warehouse data or machine tool operating information have the target of observation as organizations themselves.

Fig. 5-3 Points to confirm and confirmation methods for ensuring controllability on platforms



確認事項	A： 上流関与者の利害・関心は適切に対処されているか	B： 取引相手は契約を交わした相手か	C： データ利用者のデータの利用目的は適切か	D： データ利用者からのデータの第三者提供範囲は適切か	E： • 第三者提供先は適切な目的・態様でデータを利用しているか • 第三者提供先からのデータの提供範囲は適切か
	データ利用者から被観測者やデータ提供者への確認事項		−		
	−	被観測者やデータ提供者からデータ利用者への確認事項			
データ取引プロセスの工夫	データ提供者による表明保証とデータ利用者による表明内容の確認を実施	被観測者又はデータ提供者とデータ利用者間で真正性を互いに確認	データ利用条件（利用目的・第三者提供先等）についてデータ利用者は明示的な提示・説明を実施。 包括的な利用条件を提示する場合は、その旨の明確な説明を実施。		データ利用者が第三者提供先のガバナンスを管理・監督
ITの活用	来歴記録・管理技術活用	スマートコントラクト・アクセス制御技術活用			
認定・認証の活用		認定・認証取得をPFへの参加要件化			

Source: Digital Agency and Cabinet Office Intellectual Property Strategy Headquarters, “Implementation Guidance for Platform Data Handling Rules Ver. 1.0”

(2) Rules on personal data

While all data handling must be founded on ensuring controllability, personal data in particular calls for handling that respects individual privacy and dignity, making it important to examine rules from the perspectives below. Naturally, as in 5.3 (1), this is premised on compliance with the Act on the Protection of Personal Information and the Civil Code’s rules on privacy violations.

○ Sufficient notification and publicization

When using personal data, it is absolutely essential to inform individuals of its purpose of use. In smart cities, this will include new uses of data, many of which individuals may not be able to imagine. Therefore, it is important to notify individuals as carefully and clearly as possible, with attention to their level of awareness. [17]

For example, it can be difficult to obtain consent for the use of camera sensor data or the secondary use of personal data previously collected. In these cases, as in 5.3 (1), implementation may be legal even without individual consent based on an overall judgment of (a) the nature of the information acquired; (b) the purpose of acquisition and use; (c) the method of acquisition and use; and (d) the method of managing the information acquired[18]. Nonetheless, efforts must be made to publicize the purpose of use as much as possible. For example, when AI cameras (from which the images were immediately deleted, with only attribute data such as age, gender, race, etc., being used) were installed in Kashiwa-no-ha Smart City, in addition to noticing by physical posters, privacy policy was posted on the website, and resident briefings were held for explaining about that.

○ Guaranteeing safety

Diverse stakeholders are likely to be involved with projects in smart cities. Even when stakeholder involvement is required to create benefits (services), expanding data accessibility can also mean expanding risks. Therefore, to ensure the safety of personal data, access to the data must be controlled. Rules must be created to guarantee the safety of the individual stakeholders with access. Further, with regard to individual data, the consent of the individual to stakeholder access is required on principle based on the Act on the Protection of Personal Information (Article 27 (1)). [19]

○ Transparency and independent information control

Smart cities are notorious for cases in which data acquisition was prioritized to a problematic degree. Therefore, the framework of data flow and usage, including citizen benefits, must be made as public as possible, enhancing

[17] When acquiring personal information requiring consideration or providing personal information to a third party, consent based on the Act on the Protection of Personal Information is required. Consent may also be required so as to avoid violations of image rights or privacy.[18]As in the above note, consent is required in some cases. For secondary use, methods such as anonymization or removing personal information from the data may be used when obtaining consent is difficult.

[18] As in the above note, consent is required in some cases. For secondary use, methods such as anonymization or removing personal information from the data may be used when obtaining consent is difficult.

[19] When sharing personal information or providing it to a third party with consent, the Act on the Protection of Personal Information required organizational, human, physical, and technical safety management measures. In addition, when dealing with contractors, their safety management measures must be guaranteed as well.

the transparency of the promotion process itself. In addition, to gain citizens' trust, it is important to make them aware of how their data are being used and, if necessary, enabling them to independently implement information control for themselves by personally stopping its use or correcting the data.

○ Minimum acquisition principle

Concerns about smart cities include the acquisition and integration of personal data without governance and violating personal privacy. To assuage with these concerns, unnecessary data acquisition or name aggregation should be avoided. In addition, data usage methods with the greatest possible consideration for privacy must be examined.

For example, if using individual medical data for public health purposes, in some cases at least, data enabling individual identification is not required. In those cases, usage with greater consideration for privacy, such as anonymization, should be examined.

(3) Rules on security

As noted above, data linkage may take place among diverse stakeholders in smart cities, in which case rules must be drawn up to ensure a suitable security level. Arrangements to guarantee the reliability, etc., of data are also necessary to build trust and enable effective operation in smart cities. Specifically, the items below may be involved in setting rules for data linkage among stakeholders.

・Security control actions (organizational, human, physical, technical) required in organizations involved in data linkage

・Methods and approaches for ensuring transparency, such as storing data linkage logs

・Methods to ensure the accuracy and authenticity between data providers and data users

Smart cities in particular are likely to involve data linkage across fields, requiring attention to differing security levels. For example, when using medical information for regional public hygiene and health promotion, private-sector services are required to have security levels equivalent to those of medical institutions. When designing rules, it is also important to pay attention to the need for tougher security regarding platforms like the city OS, which are characterized by aggregating data and serving as data linkage hubs. Further, for smart cities to realize the necessary services (benefits), it is very important to guarantee data accuracy and authenticity on which the suitable development of AI is predicated, with rules therefor also essential. With reference to the "Report on Data Provision Contracts on AIDC Platforms" produced by the AI Data Consortium, along with determining compliance items, etc., for data providers and users, methods of log management, etc., premised on cross-organizational participation should also be decided upon.

Rules for handling security incidents must also be determined and agreed upon among stakeholders. Specifically, rule formation may involve items such as the following.

・In the event of an incident, information is to be immediately shared among stakeholders

・Methods and contact points, etc., for handling incidents and sharing information

・Points for demarcating responsibilities in data linkage, etc.

・Handling audits by third parties or smart city management bodies as needed

Reference

[Report on Data Provision Contracts on AIDC Platforms (aidata.or.jp)]

(4) Individual benefits and public interests

Rule design must also include the relation between individual benefits (those directly benefiting individuals) and public interests (those benefiting the region or community as a whole). Smart city initiatives do not always provide direct benefits to the individual alone; rather, they may also create benefits within the larger frameworks of societies or communities. Therefore, rule design must include incentives, among which are those enabling citizens to cooperate for public interests.

For example, studies have found that the COVID-19 Contact-Confirming Application COCOA is used in expectation not only of its individual benefit (i.e., preventing infection for oneself) but also of the publicly beneficial effects of preventing infection for families and communities as a whole. Given that even policies like this in which individual benefits and public interests coexist may not be accepted universally, greater consideration for citizens is required in rule design for smart city initiatives centered on public interests where individual benefits are unclear.

This consideration might include an objective framework guaranteeing the public interests (e.g., inspection by a committee of experts), information release guaranteeing transparency, and making the public interests more readily understandable.

(5) Incentive design

To achieve compliance with rules designed in the context of data governance, the design of incentives is also important. While it is important to clarify smart city services' influence on and benefits for stakeholders, it is also essential to receive consent from stakeholders with regard to the rules that need to be observed to reap these benefits. Possibilities include screening the participation qualifications of service providers, monitoring the extent to which rules are being implemented, and taking measures to implement such screening and impose penalties in the case of rule violations. As a complement to penalties, other effective incentive designs would include positively evaluating and publicizing stakeholders who appropriately observe the rules and contribute to smart city operation to enhance their reputations.

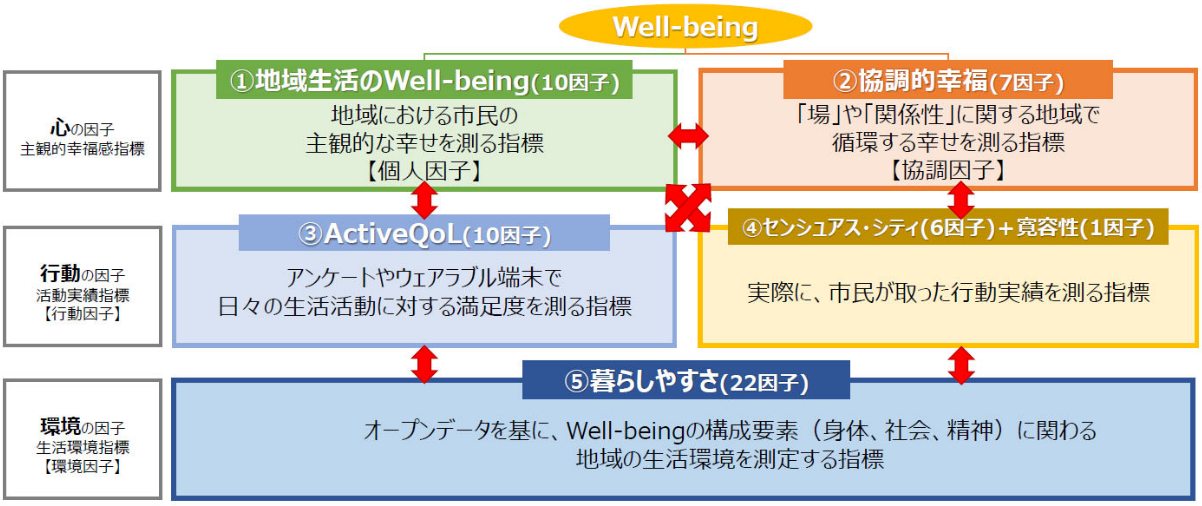
5.5. Implementation and evaluation

Once designed, the rules are then implemented in practice within the smart city and evaluated to determine whether they are functioning suitably.

It is important to bear in mind that the smart city operation and evaluation take precedence, with rule implementation and evaluation occurring within the context of the smart city.

Normally, it is effective for project realization to set KPIs and so on for the evaluation of an initiative's progress and effects to establish a PDCA cycle. In smart cities as well, when deciding on the regional ideal to be attained through services (benefits) and the qualitative indicators to be configured, the Liveable Well-Being City indicators developed and made available by the Smart City Institute Japan (SCI-Japan) can be referenced as evaluation indicators.

Fig. 5-4 Liveable Well-Being City Indicator System


Well-being
心の因子
主観的幸福感指標
①地域生活のWell-being(10因子)
地域における市民の
主観的な幸せを測る指標
【個人因子】
②協調的幸福(7因子)
「場」や「関係性」に関する地域で
循環する幸せを測る指標
【協調因子】
行動の因子
活動実績指標
【行動因子】
③ActiveQoL(10因子)
アンケートやウェアラブル端末で
日々の生活活動に対する満足度を測る指標
④センシュアス・シティ(6因子)+寛容性(1因子)
実際に、市民が取った行動実績を測る指標
環境の因子
生活環境指標
【環境因子】
⑤暮らしやすさ(22因子)
オープンデータを基に、Well-beingの構成要素（身体、社会、精神）に関わる
地域の生活環境を測定する指標

Source: Digital Agency, Smart City Institute Japan "LWC Indicator Usage Guidebook"

Reference

Smart City Institute Japan｜Liveable Well-Being City Indicators: Introduction and Use (sci-japan.or.jp)

Based on an evaluation of the degree of achievement of smart city services (benefits) and its ideal form, the rules are likewise implemented and evaluated. If the smart city is not making the expected effects, evaluation of whether the rules are the cause for that is also required. Rule implementation and evaluation should also have evaluation indicators such as KPIs. For example, the following indicators might be used.

- Number and content of complaints, etc., from citizens
- Status of rule compliance (number and content of violations, etc.)
- Work required for rule implementation
- Rule-related education activities (number of training sessions held, etc.)

If the results of evaluation indicate that the rules are excessive or not being observed appropriately, their content and the framework itself must be revised. The rules must also be revised on occasion in accordance with changes in the social environment. If the relevant laws and regulations are amended, if the framework itself changes along with technological progress, or citizens' awareness undergoes changes, various fluctuation factors must be considered and the rules must be revised through implementation and evaluation process.

Appendix: Privacy risk content

Data collection	Surveillance	Is continuous monitoring causing feelings of anxiety or discomfort for individuals?
	Interrogation	Is information being extracted from individuals under pressure? Are individuals feeling compelled to answer invasive, anxiety-inducing questions?
Data processing	Aggregation	Have the expectations of an individual been betrayed due to the collection of fragmentary information about this individual, leading to the revelation of new facts about them that they would previously have been unable to imagine?
	Identification	By linking all data to individuals, have any individuals been linked to harmful information, causing them anxiety or dissatisfaction?
	Insecurity	Have personal data been insufficiently protected, disadvantaging individuals?
	Secondary use	Have data been used for other than the original purpose in a deceptive manner without obtaining individual consent?
	Exclusion	Have individuals been deprived of the right to disclose and correct data or of the ability to control important decisions?
Data dissemination	Breach of Confidentiality	Have individuals felt betrayed by the disclosure to other companies of personal data acquired within a specific relationship of trust?
	Disclosure	Has disclosure of personal data to third parties led to further privacy issues in relation to secondary use?
	Exposure	Due to the exposure of aspects of their lives to others, have individuals experienced embarrassment that places obstacles in their capacity for social participation?
	Increased Accessibility	Has the accessibility of personal data expanded to other parties, increasing risks of "disclosure"?
	Blackmail	Is a blackmailer forcing their victim into a power relationship, dominating them, and controlling them based on threats of exposure or disclosure of their personal data to others?
	Appropriation	Is anyone using another individual's identity or personality for their own purposes, depriving them of control over how they present themselves to society, and interfering with their freedom and self-development?
	Distortion	Is anyone manipulating the way another individual is perceived and judged, creating a false persona or misunderstandings, and exposing them to shame, stigma, or reputational damage? Have any individuals' ability to control their own information and how society perceives them been limited? Have any individuals' self-identity as well as the evaluation and character essential to their ability to participate in public life been distorted? Are any individuals at risk of deliberate and inappropriate distortion of social relationships?
Direct invasion of	Intrusion	Have any individuals' everyday habits been disrupted or resulted in anxiety and discomfort caused by excessive contact (email, phone calls, etc.)?

individual privacy	Decisional Interference	In the use of AI for important decision making in individual lives, have any individuals suffered a chilling effect due to opaque decision-making methods?

Source: METI “Guidebook on Corporate Governance for Privacy in Digital Transformation (DX) Ver.1.2”