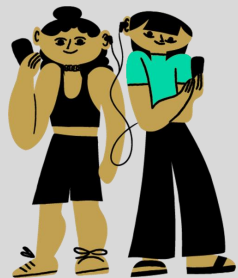


# Consent-based services – what's in it for cities?

City staff guide to modern municipal services

Helsinki





# Index

Summary

Key terms

How to read this document?

Consent and city services

What's happening with residents?

What's happening with legislation?

What's happening with technology?

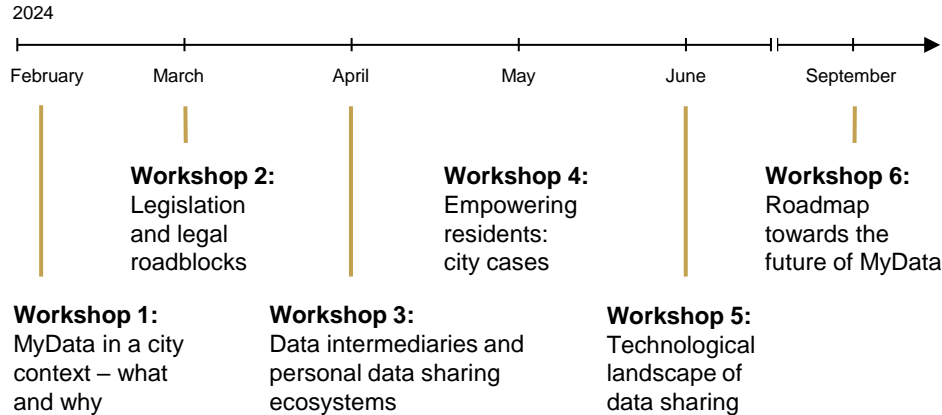
What's happening with city practices?

Current obstacles

Proposal for next steps

# Basis of this report

This report is part of a task force under the **Cities Coalition for Digital Rights** workshop series coordinated by the **City of Helsinki**. The document compiles themes that emerged through the process.



**6**  
Workshops

**55**  
Participants

**11**  
Countries

This report was created as part of a task force under the Cities Coalition for Digital Rights (CC4DR), focused on helping cities navigate consent-based personal data sharing. The City of Helsinki led the initiative, coordinating the project from start to finish.

A total of 55 participants from 11 countries contributed to the project through a series of six online workshops. These workshops brought together experts from legal, technological, and governance backgrounds to share knowledge, best practices, and address challenges cities face when adopting consent-based services.

Throughout the project, the goal was not only to discuss theoretical frameworks but also to develop practical, actionable guidance for cities. Now, with the collective expertise and experiences shared, this report offers insights that we hope will be useful to cities around the world as they explore consent-based, human-centric services.



# Summary

This report examines the shift toward consent-based data management in municipalities, with a focus on empowering residents, navigating legislation, leveraging technology, and exploring city practices. The report is designed for those involved in developing city services, offering a global perspective while primarily addressing a European audience.

**Consent-based services** give individuals control over how their data is used, but cities face challenges in implementing these systems due to fragmented practices and varying interpretations of legal requirements like the GDPR. While some cities are pioneering innovative data-sharing solutions, many struggle with technical and legal complexities, particularly around when consent is required for public services.

From the **residents' perspective**, the demand for data privacy and control is growing. However, consent remains a new concept for many, often causing confusion and mistrust. Concepts like data altruism, where residents voluntarily share anonymized data for the public good, present new opportunities but require clear frameworks to build trust.

The **legislative landscape** is evolving, with new laws such as the Data Governance Act and the Data Act aiming to balance privacy with data-driven innovation. These laws promote frameworks like data intermediaries and data spaces, which can help cities manage data responsibly while ensuring compliance with privacy regulations.

On the **technology** front, cities face challenges in integrating older systems with new technologies, and the absence of unified standards adds to the complexity of personal data management. To ensure data flows smoothly across organizational silos and municipal borders, cities should focus on creating interoperable systems. These systems would enable data to be used effectively in broader data ecosystems, supporting collaboration and efficient data sharing between municipalities.

**City practices** reveal a range of approaches, from early-stage experimentation to more developed models of human-centric data management. By focusing on interoperability, resident empowerment, and collaborative ecosystems, cities can improve public services while protecting privacy.

The report also highlights several **obstacles** to implementing consent-based data management, including technical limitations, the complexity of regulatory requirements, and low resident engagement.

**Proposals for next steps** include creating clearer legal frameworks, fostering collaboration between municipalities and technology providers, and improving resident education to build trust and increase participation in data-sharing initiatives.

# Key terms

## ***Consent-Based Services***

Services that require individuals to give explicit permission before their personal data is collected, shared, or used. Unlike website cookie consents, consent-based services use personal data from other contexts to improve service experiences. They empower individuals to control how their data is used, offering greater transparency and personalization.

## ***Self-sovereignty***

A principle where individuals have full control and ownership over their personal data, including how it is accessed, used, and shared. It involves managing one's own digital identity and data independently, without relying on centralized authorities.

## ***MyData***

A human-centric approach to personal data management that empowers individuals to control and share their data while ensuring privacy. MyData emphasizes transparency and trust in data use.

## ***Personal Data Management***

Systems and practices, such as data intermediaries and personal data pods, that allow individuals to control and manage their personal data. This includes the ability to decide who can access their data and how it is used.

## ***Interoperability***

The ability of different information systems, devices, and applications to access, exchange, integrate, and cooperatively use data in a timely and coordinated manner across organizational boundaries.

## ***Data intermediaries***

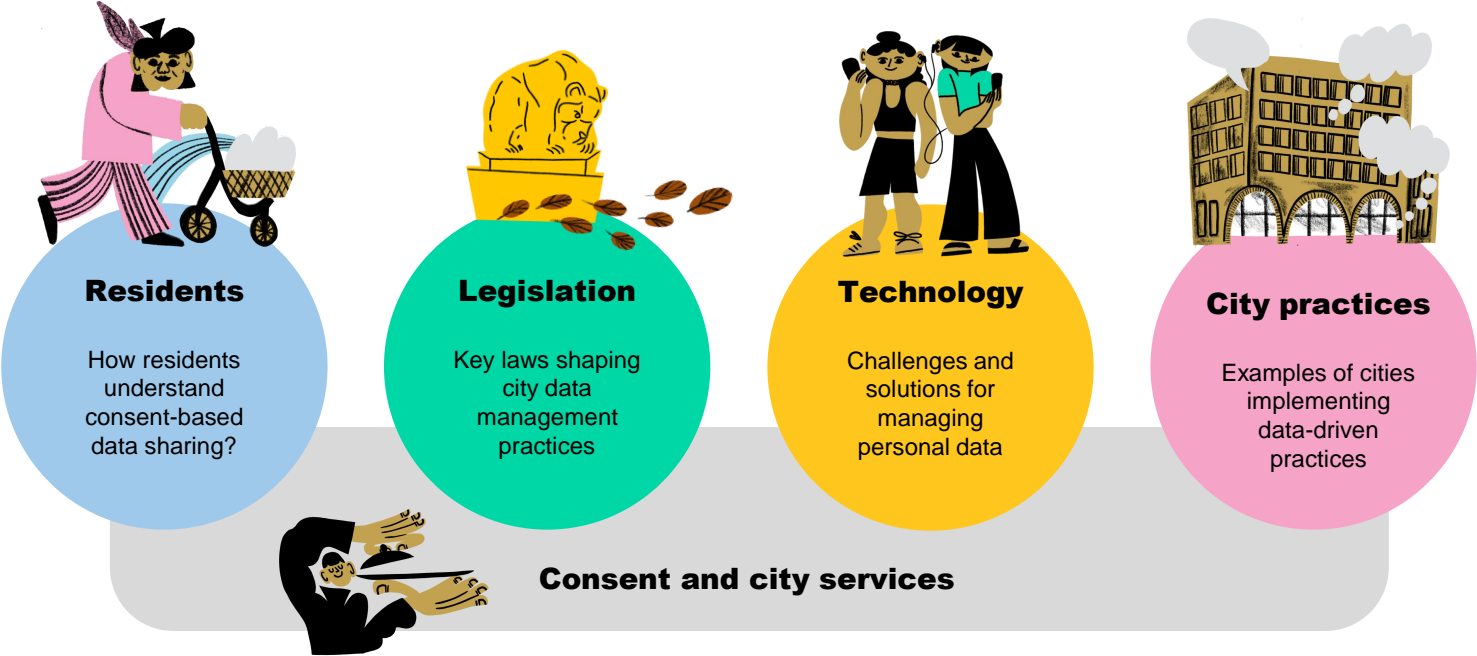
Neutral third parties that facilitate the secure sharing of data between individuals and organizations, ensuring that data is used only with the proper consent and privacy safeguards in place.

## ***Data spaces***

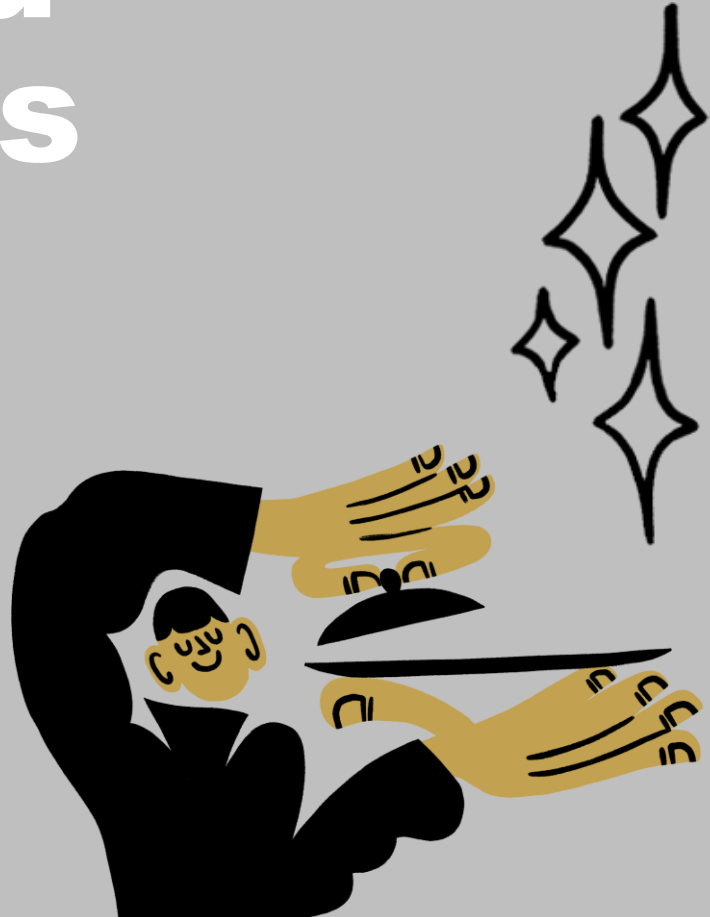
Secure environments where data can be shared between multiple stakeholders, typically across sectors and borders, under strict privacy and security standards.

# How to read this document?

This report explores several perspectives on data management in cities, each offering a unique viewpoint. The key perspectives covered are: residents, legislation, technology, and city practices. To make navigation easier, each perspective is color-coded throughout the report. You can quickly identify the focus of each section by its designated color, helping you follow the different themes as you progress through the document.



# Consent and city services



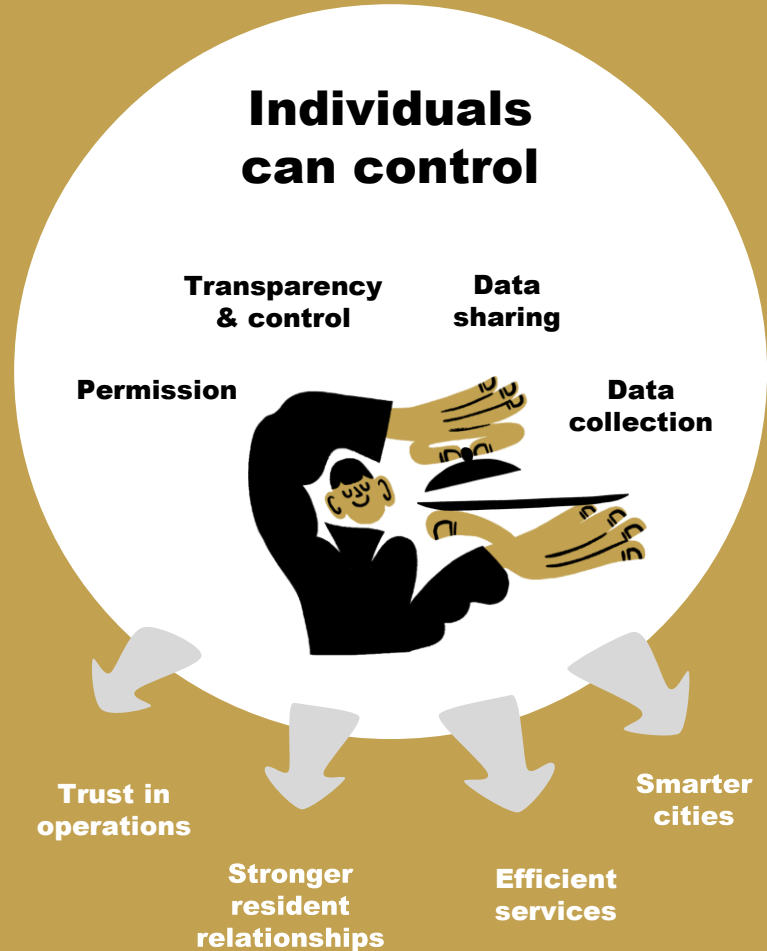
# What are consent-based services?

A consent-based approach means individuals have control over how their personal data is used.

In consent-based systems, individuals must give explicit permission before an organization can collect, share, or use their data. This requires organizations to transparently explain what data is collected and how it will be used. By putting individuals in control, this approach builds trust and fosters stronger relationships between organizations and individuals.

This approach is grounded in human-centric data management principles, such as **self-sovereignty** and the **MyData movement**. Self-sovereignty allows individuals to fully govern how their data is accessed, creating a user-driven system for sharing information. In the MyData philosophy, individuals take center stage in managing and sharing their data, moving away from traditional organizational control. These principles have gained traction over the past decade and are also reflected in European legislation, particularly the General Data Protection Regulation (GDPR), though in a slightly different form.

The growing demand for data transparency has made the consent-based approach more relevant than ever. It pushes also cities to adapt their services to meet these evolving expectations.





# Consent in municipal data services


Consent offers cities a valuable but optional approach for managing personal data in certain services.

For cities, consent-based services mean respecting individuals' autonomy – within legislative boundaries – to decide how their data is used across various municipal functions. This approach often aligns with cities' broader strategic goals of creating smart, efficient, and resident-friendly urban environments.

However, it's important to note that while individuals should have control over their personal data, this cannot fully apply to municipal services. **Cities do not need consent to provide statutory services**, as they are already permitted to handle personal data necessary for delivering these services. Additionally, residents cannot request the deletion of data held by public services when data management is legally required.

That said, cities can use consent for **voluntary services** that add value to residents or the city. These services are often aimed at achieving long-term benefits or preventing undesirable outcomes. The adoption of consent-based frameworks also marks a shift toward more ethical and secure data handling in the public sector, transforming how services are delivered.

Some forward-thinking cities have already begun exploring consent-based frameworks and developing tools to collect and use personal data that residents have consented to share.



**Consent is not required for statutory services like essential public functions.**



**Consent is used for voluntary services that offer additional benefits.**



**Consent allows residents control over how their data is used within legal limits.**

# From digitization to consent-driven services

Consent-based services can be seen as a natural next step in the ongoing digitalization of cities.

Cities began laying the foundation for digital services in the 1980s, when computing was first introduced to municipal organizations. During this period, the focus was primarily on digitizing basic administrative processes. Systems were largely internal, aimed at improving efficiency within city departments rather than enhancing public-facing services.

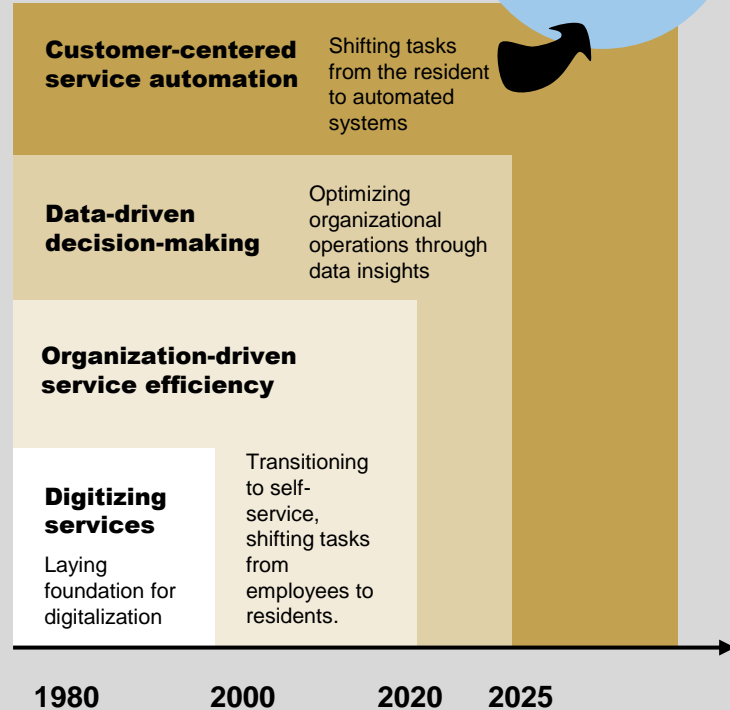
After the turn of the millennium, cities began transitioning from manual, employee-driven tasks to self-service portals. This shift empowered residents to complete tasks like submitting forms online, which significantly reduced the workload on city employees.

As data collection grew in cities, they began to harness its power to optimize internal operations. Data analysis became central to organizational decision-making, further improving operational efficiency and resource allocation.

Today, the focus is shifting toward automating services through AI and other technologies, with the goal of reducing the burden on residents. Automation allows services to anticipate residents' needs, benefiting users who no longer need to perform tasks themselves.

## Evolution of the use of data in cities

Empowering residents with access to their data without increasing control or surveillance



# Benefits of consent-based systems for all

**Ideally, consent-based services benefit all the parties involved.**

**For cities**, a consent-based approach enables the introduction of innovative, data-driven services that enhance residents' quality of life. It allows cities to gather more accurate personal data, leading to more efficient resource use and improved outcomes for communities. Importantly, these systems also help ensure compliance with privacy regulations such as GDPR, which mandate the responsible use of personal data.

Consent-based systems also promote clear processes for data collection, storage, and usage. With proper safeguards in place, cities can manage the personal data they collect more effectively, reducing the risk of misuse or unauthorized access. However, the success of these systems still depends on responsible data management practices.

**For residents**, consent-based services provide greater control over their personal data that is used in voluntary services. Consent is documented and can be withdrawn at any time, fostering transparency and building confidence in city services. This transparency encourages more active participation from residents.

**Private businesses** also benefit from consent-based systems. With secure access to consented data, companies can develop personalized services and products that meet real customer needs, creating opportunities for growth while adhering to privacy regulations.

## Examples of consent-based city services:

- **Smart waste management**  
Residents can share data on waste habits to e.g. receive personalized recycling incentives.
- **Health and wellness services**  
By sharing their data, residents can get e.g. alerts on air quality.
- **Social services support**  
Residents can share personal data for more tailored or timely assistance from social services.



**Creating  
smarter services  
by respecting  
resident data  
choices**



**Enhancing  
city planning  
and driving  
innovation with  
accurate data**

## EXAMPLE

# How consent unlocks services



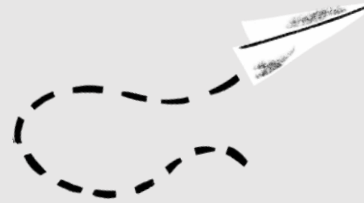
### Data registration at the source

An individual is accepted into an educational institution, and their student status and enrollment details are registered in the official educational database.



### Consent to use data is requested

The individual applies for a student discount in the public transportation app. The app requests their consent to verify their student status through an official educational database.



### Data is securely fetched with consent

The individual gives permission for the public transportation app to access their student status and enrollment details directly from the official database.



### Eligibility is confirmed and discount applied

Once the student's status is verified, the individual becomes eligible for the student discount and can immediately proceed to purchase the discounted ticket within the app.

# What's happening with residents?



# Rising awareness of data privacy

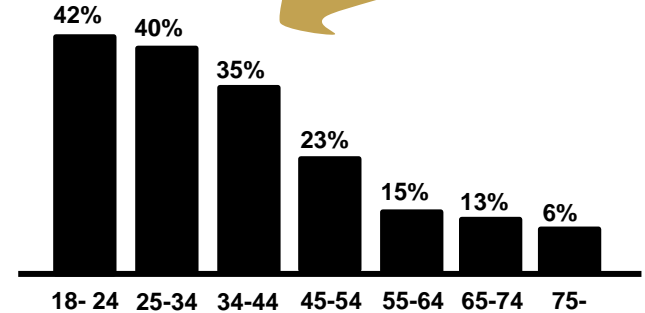
Residents are becoming increasingly conscious of how their personal data is being collected and used.

High-profile data breaches, privacy scandals, and the growing digitization of services have made people more cautious about how their personal information is handled. Many now question how much control they have over their data and are wary of how organizations collect, store, and share their personal information.

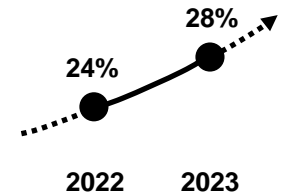
Simultaneously, there is a growing movement for stronger data rights, particularly among younger generations who are more informed about their digital rights. These individuals are demanding greater control and transparency, such as the right to access, correct, and decide how their data is shared. In fact, a 2023 survey by Cisco revealed that younger people are the most active in exercising their data rights, with a notable rise in Data Subject Access Requests globally (see the image for reference).

Cities find themselves at the heart of these changes. As public services increasingly rely on personal data, cities need to address these privacy concerns. This push for transparency and accountability is reshaping how cities manage personal information and build trust within their communities.

## Young people exercise their data rights most actively (2023)



## Growing number of people requesting to see their data



Source: Cisco Consumer Privacy Survey (2023): Survey included over 2 600 consumers from 12 countries worldwide.

# Understanding consent: A complex shift

**Consent is a powerful but confusing new mechanism.**

Consent-based services represent a major shift in how cities manage personal data. By asking residents for explicit permission before using their personal information, cities provide a more transparent and accountable approach to data management. However, this shift can also pose challenges, particularly when residents are unfamiliar with the concept of consent and its role in data-sharing practices.

A survey conducted in Espoo, Finland, revealed four distinct attitudes toward consent-based services, ranging from cautious to trusting. Some residents are happy to share their data, while others are willing as long as they retain control over how it is used. Some want a deeper understanding of the concept, and for others, the mere idea of being asked for consent raises concerns. This lack of understanding around data privacy rights and the consent-based approach can even lead to mistrust. The accompanying image illustrates these four attitudes.

Clear communication is essential for addressing the varying concerns residents have about consent-based data sharing. Cities should provide simple, accessible explanations and actively involve residents in designing these services to build trust. By directly addressing these different attitudes, cities can reduce confusion and foster confidence in how personal data is handled.

*I need to know exactly what my data will be used for before I agree to anything.*



**Aware but concerned**

*I want to control my data but share it to improve services!*



**Carefree but aware**

*I don't want the city knowing too much about me – and use that data against me.*



**Concerned and uninformed**

*I don't know how my data is used, but I don't mind if it helps.*



**Carefree and trusting**

# Data altruism: Sharing for the common good

Data altruism encourages residents to voluntarily share anonymized data.

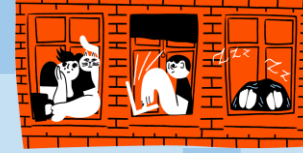
Data altruism is an emerging concept, supported by the EU's new legislative frameworks, that encourages individuals to voluntarily share their anonymized data to contribute to societal initiatives without concerns about personal data exposure. Unlike approaches focused solely on data privacy, data altruism emphasizes the collective benefits of shared information.

For example, residents might choose to share health data to support public health efforts or provide mobility data to improve urban planning. The recipients of this voluntarily shared data can include municipal organizations, national health authorities, research institutes, or even private businesses.

A practical example of data altruism is the daycare air-cleaning research project in Helsinki, Finland. Parents voluntarily shared welfare data through a city-operated consent platform, allowing researchers to study the effects of air-cleaning operations in daycare buildings. The findings can lead to measures to improve indoor air quality for the wellbeing of children and daycare staff.

In practice, data altruism is often facilitated by data intermediaries – trusted third parties that ensure safe data sharing – and data spaces, which are secure environments for sharing data across sectors. These mechanisms will be further explained later in the document. However, data altruism can also occur directly between individuals and organizations.

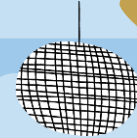
## How data altruism can work in practice



Individuals voluntarily share data for a specific purpose.



A data intermediary validates the residents' consent and anonymizes the data.



Data flows into a data space.



Members of the data space can utilize the data according to the agreed and communicated terms.



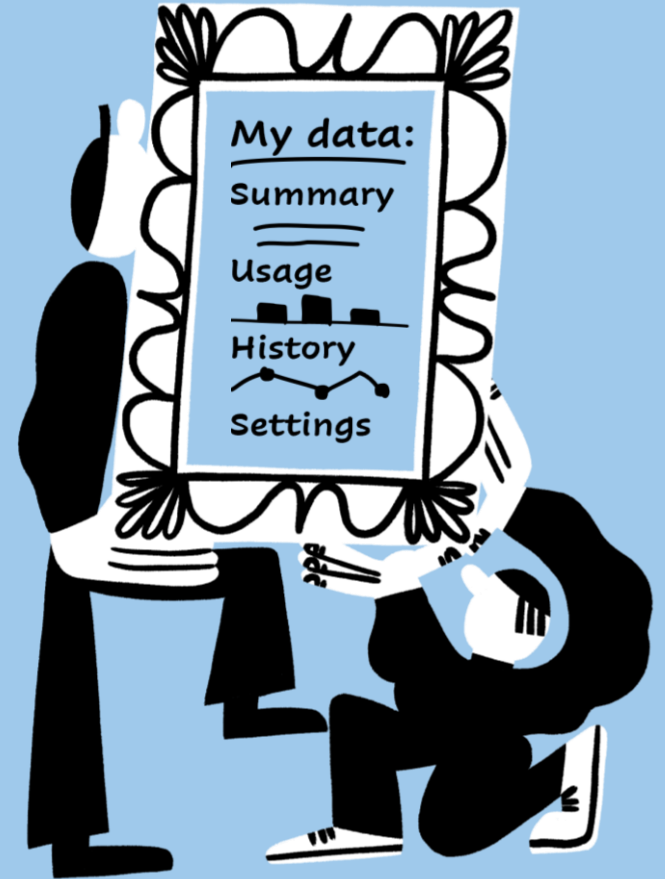
# Educating residents on data practices

Education can help residents in understanding new data practices.

Consent and data altruism are just two of the new concepts that a rapidly evolving digital society requires residents to understand. As cities become more data-driven, the way personal information is managed is undergoing significant transformation. For many, the pace of these changes and their underlying significance may be difficult to understand.

Cities play a crucial role in clarifying these concepts and simplifying processes related to them. By providing clear and accessible information about consent and data-sharing, cities can help residents feel more confident about how their personal data is managed. Transparent communication is essential for explaining privacy rights, consent choices, and the benefits of data-sharing for improving public services.

One practical solution for increasing understanding is the use of real-time dashboards, where residents can see what data is collected and how it's used, as well as adjust their consent preferences. For instance, a dashboard could show residents how their shared mobility data is being used to optimize city traffic flow in real time, while offering them the option to change or withdraw consent at any time.



# What's happening with legislation?



# Global shift toward personal data control

Countries around the world are embracing citizen control over personal data.

In the early 21st century, the rise of digital services, social media, and global data flows highlighted how easily personal data could be easily misused, leading to privacy violations, identity theft, or even mass surveillance. This created an urgent need for legislation on how personal data should be handled.

The European Union's introduction of the General Data Protection Regulation (GDPR) in 2016 laid the groundwork for stronger data rights, transparency, and user control. Countries like Canada, Brazil, Argentina, Mexico, Japan, and South Korea, as well as California in the U.S., have followed suit with laws that prioritize individuals' rights in the digital age.

These data protection laws set clear guidelines on how personal data should be handled legally. Whether collected for commercial purposes, public services, or research, organizations are now required to follow strict standards for gathering, storing, and using personal information. This legal framework ensures that data is processed transparently, giving individuals the right to access, correct, or delete their data when necessary.

## Regions of global adoption of personal data control regulations



# Navigating consent in municipal services

Using consent in municipal services isn't always straightforward.

The General Data Protection Regulation (GDPR) outlines six lawful bases for processing personal data. These bases include consent, contract, legal obligation, vital interests, public task, and legitimate interests, each defining when and how personal data can be lawfully processed.

In the context of municipal services, consent is not required for statutory services. Cities can process personal data necessary for providing essential services based on legal obligations or public tasks. However, when cities aim to introduce new services or develop innovative, data-driven processes, consent may be the only viable option.

For consent to be valid, it must meet four key criteria: it must be freely given, specific, informed, and unambiguous. This means consent cannot serve as the legal basis if residents feel pressured to agree due to fear of losing access to the service, or if the service cannot be provided without it. This dynamic creates a potential imbalance of power between the individual and the municipality, making consent inapplicable in such cases.

When residents have true freedom of choice, consent becomes a valuable tool for offering enhanced services without undue pressure. These services typically aim to improve the resident experience while maintaining ethical standards.



## Rights

Requires explicit consent for data collection.



## Transparency

Mandates detailed data processing information and access to data.



## Consent

Includes the right to be forgotten, allowing individuals to request the deletion of their data.



## Legal Obligation



## Consent



## Contract

Six lawful bases for processing personal data in the European GDPR



## Vital Interests



## Legitimate Interests



## Public Task

# New EU laws for secure data-sharing

The EU introduced new laws to enable more secure data-sharing.

After years of focusing on data privacy, the EU is now prioritizing innovation in the data-driven society – while maintaining privacy protections. Following the publication of the EU's Data Strategy in 2020, several laws related to data and digitalization have been introduced. This legal package aims to create an environment where data can flow securely across organizations, sectors, and countries. Central to this effort are the Data Act (DA) and the Data Governance Act (DGA).

The Data Act (DA) promotes competition by preventing data monopolization, ensuring that data is accessible across sectors. For cities, this means gaining access to more diverse data sets that can improve services such as urban planning and public health.

The Data Governance Act (DGA) introduces data spaces and data intermediaries – neutral third parties that facilitate secure data-sharing transactions. These mechanisms are designed to give cities confidence when engaging in data-sharing initiatives, ensuring resident data remains secure.

As these regulations take effect, data intermediaries are expected to play a key role in enabling self-sovereignty. Meanwhile, other technical solutions – such as Self-Sovereign Identity (SSI) systems and blockchain-based approaches – remain outside the current legislative spotlight.

## Core elements of the Data Act and Data Governance Act

### Data Act (DA)

- ✓ Promotes data sharing across sectors
- ✓ Prevents data monopolization
- ✓ Enables access to diverse data sets
- ✓ Supports innovation and competition

### Data Governance Act (DGA)

- ✓ Introduces data spaces for secure data-sharing
- ✓ Establishes data intermediaries as neutral entities
- ✓ Focuses on privacy safeguards
- ✓ Empowers self-sovereignty

# Balancing innovation with privacy laws

**The new legislative shift presents both challenges and opportunities for cities.**

As cities strive to innovate using shared data, they must balance data-driven service development with privacy protections. While new EU laws like the Data Act (DA) and Data Governance Act (DGA) provide frameworks for securely accessing and using data, uncertainties remain – particularly around how these laws align with existing regulations like the GDPR.

Cities find themselves navigating this evolving legal landscape. On one hand, the DA grants more rights for sharing data, encouraging its use for improving services. On the other hand, under the GDPR, it remains unclear whether public organizations can initiate data-sharing requests for non-legislative services without risking an imbalance of power. This ambiguity can slow down innovation, as cities need to ensure that data is either anonymized or processed with explicit consent, raising concerns about compliance and appropriateness.

As a result, cities must adapt their data management strategies to meet these regulatory challenges. At the same time, they should experiment with real-world use cases to explore how these principles work in practice and find a balance between innovation and privacy.

## Future possibilities unlocked by secure data use



### Personalized Public Services

Residents could receive tailored services, like healthcare recommendations, by sharing health data while retaining control over their information.



### Smarter Urban Planning

Cities could use shared data to optimize services, such as traffic management systems that reduce congestion through real-time data.



### Enhanced Data Altruism

Residents could voluntarily contribute data to public projects, like urban sustainability research, with full transparency and control over their input.

# What's happening with technology?



# The struggle for data standards in cities

**Standards are needed for enabling new data-driven city services.**

Implementing human-centric principles like self-sovereignty and MyData requires technical solutions that give individuals control over how their data is shared and accessed. This demands data-sharing platforms, consent management mechanisms, and identity management systems.

However, all of this can be achieved in numerous ways. Multiple players are developing their own solutions, but without a clear standard, there's no agreement on which path to take. We've seen similar battles with a number of new technologies, such as VHS and Betamax, where competing systems vied for dominance before a standard emerged.

Though one-size-fits-all solutions may not be feasible due to varying city needs, some level of standardization is crucial. The current fragmented landscape forces cities to develop isolated solutions, limiting their ability to share best practices or adopt common platforms. As a result, interoperability – the ability for systems to communicate and exchange data seamlessly – has been hindered. At least some level of standardization would improve consistency in personal data management and also strengthen resident trust.

## Elements of human-centric data management system

**Ownership**  
over personal data

**Access control**  
to personal data

**Consent management**  
granting and withdrawing consent

**Transparency**  
in how data is used  
and shared

**Data portability**  
moving data between  
systems





# Interoperability drives smart city collaboration

Interoperability is key to helping cities collaborate more effectively.

Europe is already making efforts to create standardized approaches for secure data sharing. One key initiative is the MIM4 (Minimum Interoperability Mechanism 4). It's a set of **technical guidelines that help cities share and manage personal data across different systems seamlessly**. It focuses on making sure that personal data can be exchanged between various platforms, even if they are built by different vendors, while ensuring the privacy and control of that data remains with the individual. MIM4 achieves this through standardized tools like APIs and data models.

MIM4 is part of a broader set of Minimum Interoperability Mechanisms (MIMs), each addressing a specific aspect of smart city data management. MIM1, MIM2, and MIM3 focus on other areas like data discovery, exchange formats, and real-time data handling. By following MIM4, cities can avoid building isolated data systems that don't communicate well with others.

Another important initiative is SIMPL, which works closely with MIM4 to make data-sharing easier for cities. While MIM4 sets the technical standards for interoperability, SIMPL simplifies the process by offering practical tools to integrate different systems. It focuses on reducing the complexity of data exchanges. SIMPL helps cities implement MIM4 more efficiently, fostering collaboration across various data platforms.

## Four key requirements of MIM4

### 1 Verify identities through trusted network

Ensure users are authenticated via secure, trusted networks before accessing personal data.

### 2 Create clear data-sharing agreements

Establish transparent, digital agreements for data-sharing, with the option for users to adjust consent.

### 3 Use secure APIs and personal data platforms

Facilitate data exchange using secure APIs or personal data stores, with user consent.

### 4 Standardize personal data models

Adopt uniform data formats to ensure seamless data sharing across systems.

*MIM4 is developed in collaboration with Open and Agile Smart Cities (OASC) and Living-in.eu, with support from the European Commission.*

# Two models for managing personal data

Cities can manage personal data using two primary approaches.

Among the various solutions for data sharing, two key models for handling personal data between organizations stand out: the "streaming data" and "digital memory stick" approaches. Each model has its own strengths and challenges.

The **"streaming data"** approach allows personal data to **move between organizations**, with residents actively managing their consents and controlling who can access their data. This model requires a robust infrastructure for consent management, encryption, and tracking systems to ensure secure and transparent data flow. Tools such as APIs (Application Programming Interfaces) and blockchain technology enable this model. APIs facilitate real-time data sharing between systems, while blockchain can provide a secure, immutable record of transactions, though its suitability for managing personal data is often seen as problematic due to inherent limitations.

The **personal data storage** approach can be likened to a "digital memory stick." It typically involves a secure cloud-based system where individuals store their data, and organizations request access as needed. This storage often contains the original data that individuals have received and can share. This model simplifies consent management, allowing individuals to control access from a single point, such as a consent wallet. Data can also be shared in minimal forms, such as a simple proof of eligibility. However, the stored data may not always be up to date, depending on the update cycle or if it's duplicated in the storage.

## Comparing the two data management approaches



### Streaming data

- Data flows between organizations
- Residents manage consent
- APIs enable data mobility

#### Pros

Real-time data sharing  
Resident control over data  
Transparent with blockchain  
Cross-organization collaboration

#### Cons

Complex and costly infrastructure  
Higher security risks  
Resident burden to manage consents  
Interoperability challenges



### Personal data storage

- Cloud or central storage hub
- Like a digital "memory stick"
- Data stored in one location
- Organizations request access
- Simplified consent management

#### Pros

Centralized data management  
Simplified consent process  
Lower security risks  
Easier to implement

#### Cons

No real-time access  
Dependence on centralized system  
Potential privacy concerns  
Less flexibility for complex services

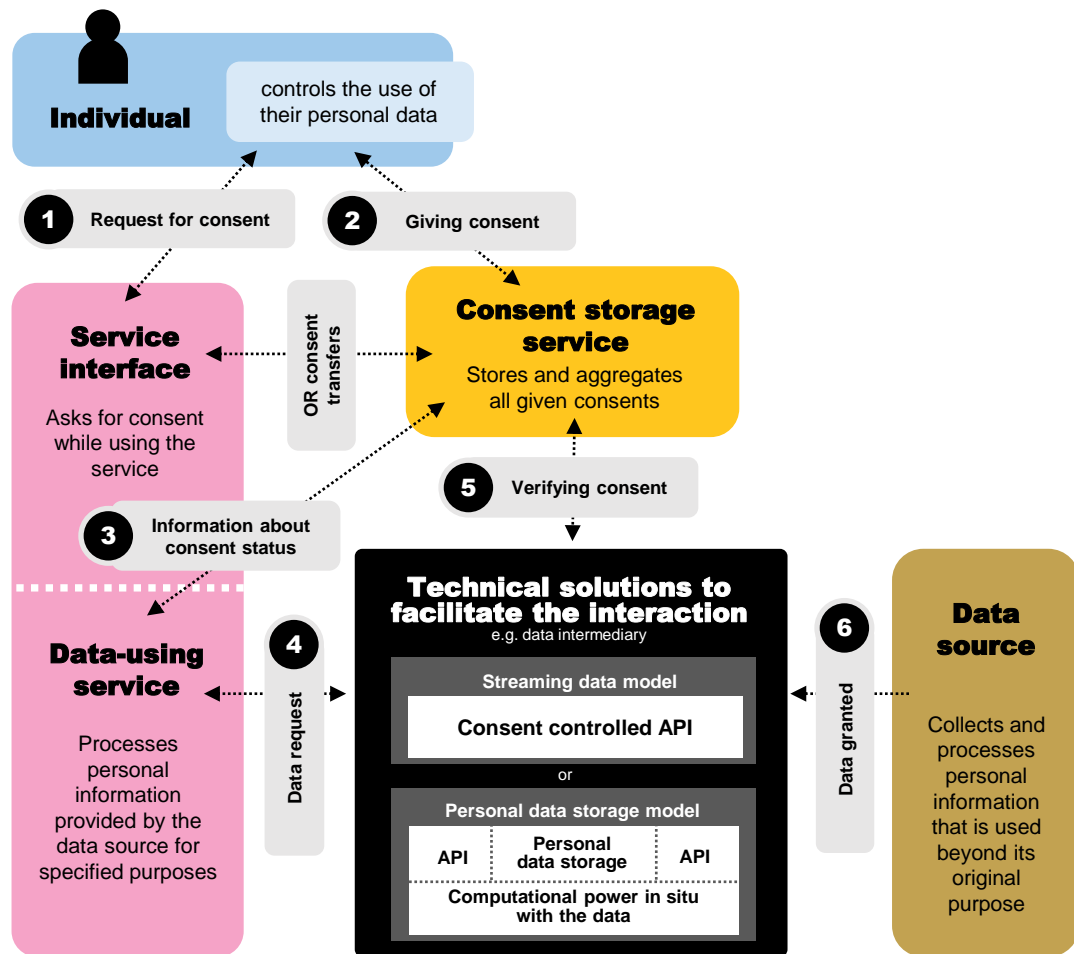
# How the consent process works

Regardless of the technological approach, the consent process typically follows the steps outlined in the image.

When a user interacts with a service, they are prompted by the **interface** (either from the service or the **consent storage service** such as a wallet) to provide consent. Once given, the consent is stored in the wallet, which manages all consents across various services.

The service then uses a technical solution to securely transfer the data, either fetching it from the original source (streaming data) or handling it through personal data storage. This system ensures data is accessed and processed only for user-approved purposes.

Users can later update their consent preferences through the wallet.



# Data intermediaries: Europe's trusted connectors

**Data intermediaries are central to Europe's vision for secure, transparent, and human-centric data sharing, underpinned by the Data Governance Act (DGA)**

**We facilitate data flows securely by handling only metadata, ensuring privacy and trust in every transaction.**

*Jaana Sinipuro,  
CEO, Data Space Europe*

In the EU, data intermediaries are envisioned as crucial players in managing secure data flows between individuals, businesses, and organizations. They enable bilateral or multilateral exchanges of data by making personal (or non-personal) data available for potential data users.

These neutral entities ensure that data is shared only with proper consent, aligning with Europe's regulatory framework aimed at empowering citizens and businesses while protecting data rights. By acting as trusted connectors, intermediaries help create a seamless flow of data across sectors and borders.

The Data Governance Act mandates that intermediaries operate with strict neutrality, meaning they cannot profit from the data they manage. This requirement builds trust by ensuring there is no conflict of interest between data intermediaries and the parties they serve.

Data intermediaries can have different operating logics such as data cooperatives, data trusts, data marketplaces or personal information management systems. MyData operators and personal data storages, for example, are possible types of intermediaries. These systems foster collaboration, boost innovation, and open new markets, while ensuring that all actors, from individuals to large enterprises, have more control and transparency over data exchanges.

*European data intermediaries are listed in the EU registry, ensuring compliance with strict neutrality and conflict-of-interest requirements.*

# **Decentralized data sovereignty with built-in control through Linked Web Storage**

**Linked Web Storage is a decentralized data storage standard designed to give users full control over how their personal data is stored, shared, and managed, ensuring that individuals retain ownership and control over their data across various services.**

**Linked Web Storage enables people to store their data in a portable space on the Web, and contextually share parts of it with applications, services, and others at their convenience, and with full transparency.**

*P J Łaszkwicz, Chair at Omnifi Foundation*

Solid, co-founded by Sir Tim Berners-Lee alongside a community of collaborators, is part of the W3C standards track, Linked Web Storage. It provides decentralized data control, allowing individuals to store their data in personal data stores, or pods. This ensures that only authorized services or individuals can access the data, providing individuals with full control over permissions.

The solution works by separating data from the applications that use it. Individuals store their data in pods, which can be hosted by a range of providers, maintaining ownership or visibility of their data. This approach provides an alternative to traditional centralized services where data is stored across various proprietary platforms.

A key feature of Linked Web Storage and Solid is the use of Linked Data principles. Data can be stored in pieces, connected across various pods and applications. This enables individuals to share only relevant data with various services, whilst keeping other personal information private. For example, an individual could grant a fitness app access to their health data stored in one pod, whilst restricting access to financial and social data in other pods.

*Naamio, a global, non-profit solution founded in Finland, is interoperable with Linked Web Storage and Solid, providing a secure and decentralized platform for managing personal data.*

# **MyData Operators: Securing personal data sharing**

**MyData Operators enable individuals to manage and share their personal data securely, while ensuring privacy and transparency.**

**The operator ensures that data flows only with valid permissions, safeguarding both privacy and interoperability.**

*Jami Haavisto,  
ID Solutions Manager, Vastuu Group*

MyData operators are designed to provide the infrastructure needed for human-centric personal data management, acting as intermediaries that facilitate secure data sharing between individuals, data sources, and services. Their primary function is to ensure that personal data is only accessed when explicit permission is granted, giving individuals full control over how their data is shared and used.

MyData operators are adaptable, reflecting the diverse needs of different regions and sectors. Their focus areas and business models can vary: some operators may focus solely on managing permissions for personal data, while others also store and govern the data themselves. To enable this, MyData operators offer various applications and tools that allow secure data exchange while ensuring accountability through data logs.

These operators help enforce interoperability at technical, informational, and governance levels. Their role aligns with broader efforts in Europe, such as the Data Governance Act, which seeks to establish trusted data intermediaries that ensure transparency and control for individuals. This shared infrastructure supports cities and organizations in handling personal data more responsibly, facilitating collaboration while respecting privacy and data rights.

*Over 40 MyData Operators worldwide are helping individuals manage their personal data, ensuring secure sharing with explicit consent and full transparency.*

# Building human-centric data management through technology



## User interfaces

E.g. digital wallets

## Data exchange operating models and governance

APIs, data intermediaries (such as MyData operators), personal data stores and their governance models and rulebooks

## General governance models and interoperability standards for personal data sharing

MIM4 personal data sharing standard, other standards and models

## Regulation and general principles related to personal data sharing

For example: MyData principles, data protection legislation (GDPR), other data legislation (DGA, DA)

Human-centric data management relies on a multi-layered system that integrates both technical and regulatory components. Each layer plays a crucial role in ensuring transparency, privacy, and control over personal data, while supporting the technological infrastructure needed to share and protect that data.

From user interfaces like digital wallets to the underlying data-sharing frameworks and technical standards, each layer ensures compliance with human-centric principles. This visualization demonstrates how technical solutions, such as APIs and data intermediaries, align with regulations like GDPR to enable secure, transparent data management.

# What's happening with city practices?





# Early lessons from pilot projects in cities

**Forerunner cities are already dipping their toes into human-centric data management.**

A few early-adopter cities have launched pilot projects to explore how to create value with consent-based services. However, most of these pilots remain in the experimental phase, as cities encounter significant challenges in scaling the projects into fully functioning systems. One of the biggest hurdles is that these cities may be slightly ahead of their time – the broader audience may not yet be ready for such solutions.

Another major obstacle has been the strict interpretation of GDPR by some national authorities, which limits how cities can handle personal data and creates uncertainty around consent requirements. This legal ambiguity has made cities hesitant to proceed without clearer guidance.

Despite these challenges, pilot projects have provided valuable insights into the technical, legal, and practical needs required for success. Cities have learned the importance of involving key stakeholders early, including legal experts, developers, and residents. They've also gained a better understanding of how to secure consent in a way that is transparent and easy to comprehend. To scale these systems effectively, cities will need clearer regulations, stronger resident engagement, and continuous feedback to refine their approaches using real-world data.

## Human-centric data management in practice

### 1. Data Collection

Data is collected with residents' consent.

### 2. Data Management

Residents can access and control their data through city-managed platforms

### 3. Data Sharing

Data sharing is done transparently and ethically.

### 4. Feedback

Residents can provide input on data practices.



# Scaling reveals hidden challenges

Scaling up reveals the real challenges beneath the surface.

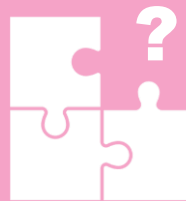
Many forerunner cities report that the technical foundation for scaling consent-based services is lacking, either due to the quality of the data or the state of the surrounding technical infrastructure. Pilots can be arranged using test data, temporary platforms, or manually governed data, but transitioning from pilot to full deployment is challenging, involving complex implementation and high costs.

The biggest infrastructure issue is fragmented systems and a lack of standardization, preventing seamless data sharing across systems and organizations. Addressing this requires significant investment in modern systems, leaving cities with the realization that advancing consent-based services will only be possible during larger technical renewal projects. By that time, cities should have gained enough experience from piloting consent-based services to ensure that any system renewal supports these initiatives.

When it comes to data usage, cities face three main issues: missing data, missed use of data, and misuse of data. The first two are often the result of siloed, outdated systems, reinforcing the need for technological upgrades. Misuse of data, on the other hand, tends to occur when data management practices are poor.

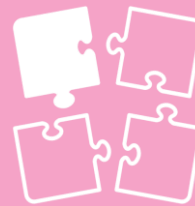
## Key challenges in city data management

### Missing data



Limited data collection

### Missed use of data



Missed opportunities

### Misuse of data



Mistrust and disengagement

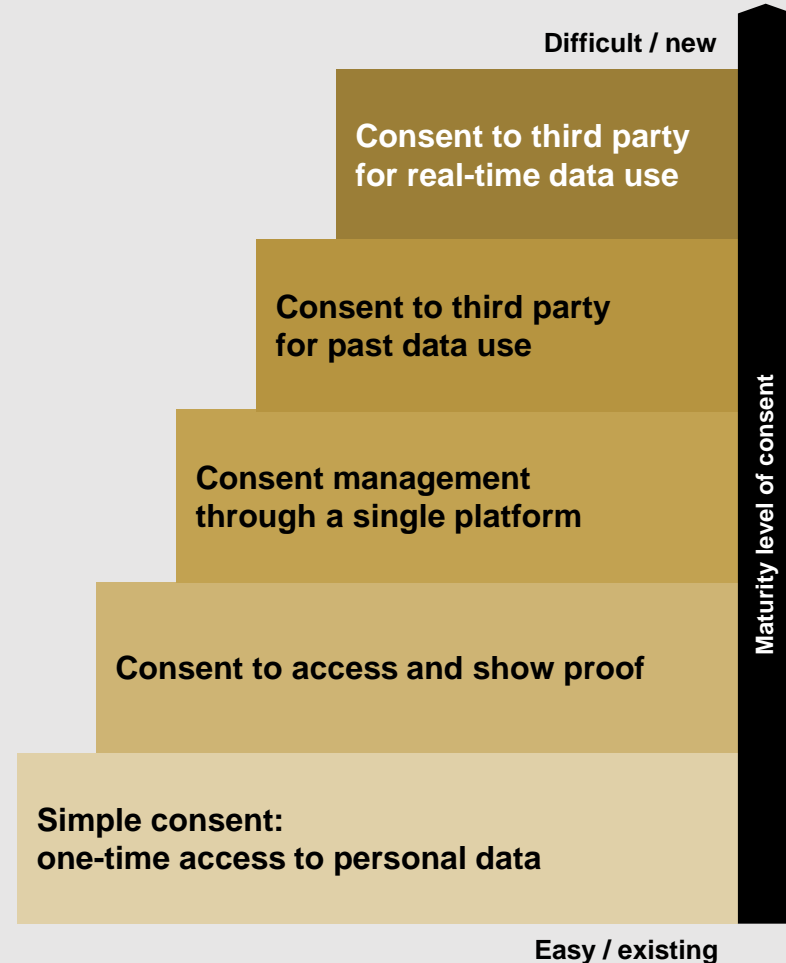
# Understanding the spectrum of consent mechanisms

## Consent comes in many forms.

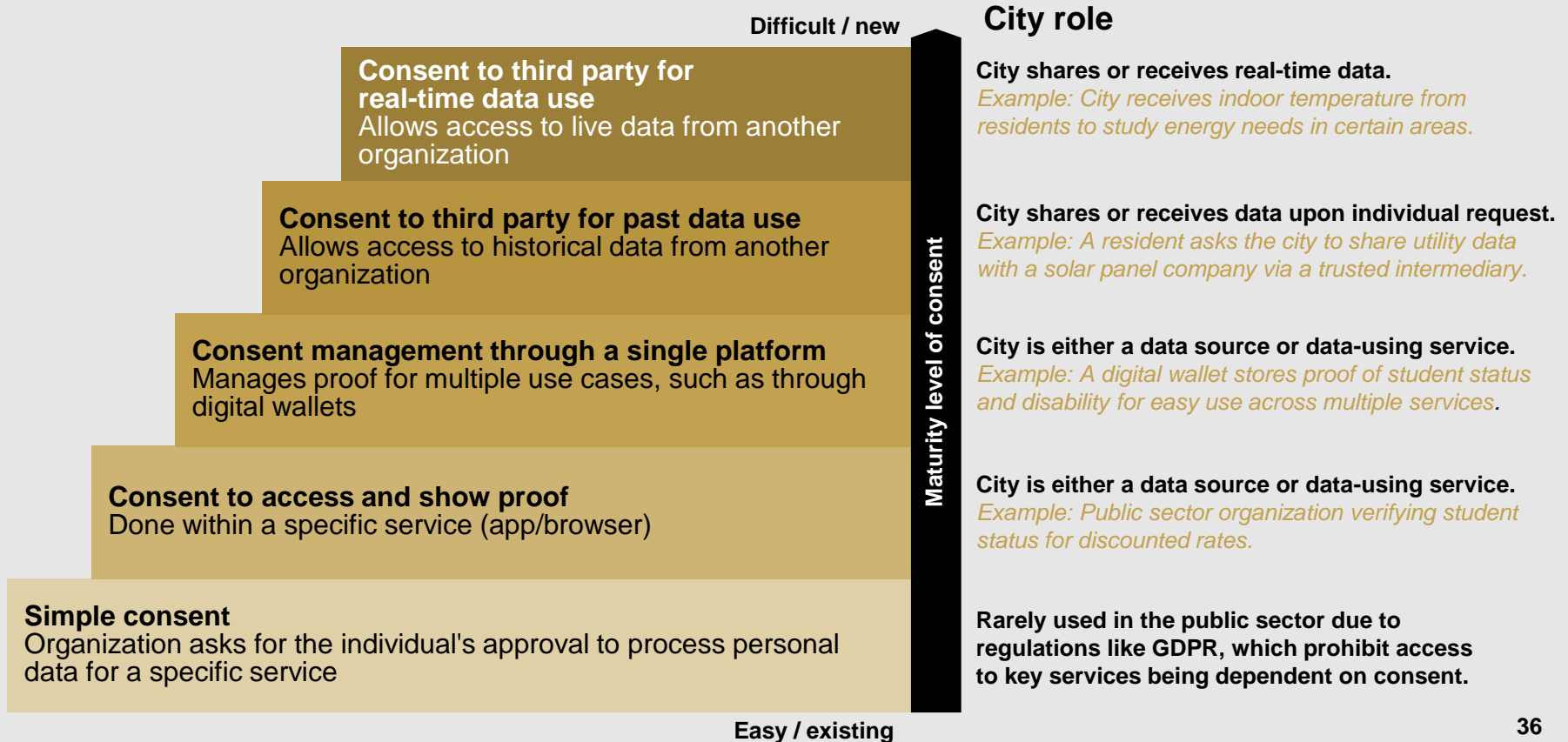
As cities talk about consent-based services, it's important to recognize that not all consent mechanisms are equal. Consent can range from basic forms, where individuals give one-time approval for data use, to more advanced models that involve dynamic, ongoing data use. The accompanying image shows how consent-based systems evolve from simple to more dynamic forms. It helps cities clarify the type of consent they are referring to when discussing with, for example, lawyers.

Cities' roles can vary across different levels of consent. European cities rarely engage in the most basic forms of consent because GDPR prohibits access to key services from being dependent on consent. In more mature forms of consent, a city can act either as a data-using service or a data source, and can receive or share data either upon unique requests or continuously. At the most advanced level of consent-based services, data flows in real time.

The following page explains the levels and city roles in more detail.



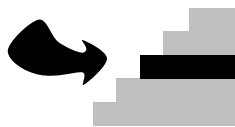
# Maturity levels of consent



# Lyon: Empowering resident access to personal data and services

Lyon has been exploring MyData solutions since 2016. The city's goal with this approach is to provide citizens with the highest level of control over their data and improve public policies through the collection of anonymized data.

**In this case, consent management is facilitated through personal cloud storage.**



Over the years, Lyon has ideated and piloted several services that promote data sharing between residents and the metropolis administration. The exploration began with *EcoIyo*, a service that provides citizens with information about their water, electricity, and gas consumption, along with tips to reduce usage.

The approach then shifted to a service that helps citizens organize, manage, and securely share their administrative documents. This service, called *Mes Papiers*, was launched in 2023 in cooperation with Cozy Cloud. It is an app that centralizes access to important documents from various institutions and includes features such as bank management and access to personal tax accounts, social services, and more. It also offers residents 5GB of free personal cloud storage.

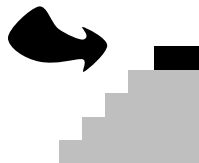
While feedback has been very positive, the number of users has grown quite slowly. Scaling up the service is the metropolis's next big challenge.

*Métropole Grand Lyon:*  
1,4 inhabitants  
The 3rd most populated city in France  
58 municipalities  
9500 workers

# Stavanger: Using crowd-sensing to improve urban planning

Norwegian city Stavanger has been exploring innovative crowd-sensing solutions to improve urban planning and public health. The project aimed to gather data through wearable activity trackers to provide insights into recreational activities and public space use.

**The consent maturity level in this project is high. Consent is used to allow third-party access to real-time data.**



Stavanger's approach focused on collecting non-sensitive health data through wearable activity trackers provided to citizens. The data, including GPS activity, was shared with the municipality to help inform urban planning, public health policies, and recreational space design. The aim was to use this data to map and analyze public health trends in a way that benefits citizens while ensuring compliance with GDPR regulations.

A key part of the project involved developing a consent management tool, which allows participants to choose the types of data they share, such as heart rate or GPS location. The municipality faced initial reluctance due to concerns about GDPR and data sensitivity, but the use of clear consent processes helped address these challenges.

Feedback from participants was positive, with users appreciating the ease of use of the system, though there were concerns about privacy and data surveillance. However, scaling the project to a larger user base remains a challenge for the city.

*Stavanger region (consisting of Stavanger and Sandnes):  
230 000 inhabitants  
The 3rd largest metropolitan area in Norway  
9,000 employees*

# The power of shared data in cities

**Collaborating across organizations in data-sharing ecosystems is key to addressing complex challenges that cities can't solve alone.**

Currently, efforts to develop consent-based services are often led by cities, with other organizations acting as data providers. However, the real potential lies in deeper collaboration. By building collaborative data ecosystems, cities can move beyond isolated innovations and create services that truly benefit residents while addressing larger societal challenges. Data-sharing across sectors – whether in transportation, education, or environmental issues – helps build smarter, more responsive communities.

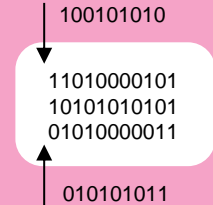
A key component of these ecosystems is the ability to securely share data between organizations. Cities need interoperable systems to ensure seamless data flow across platforms. But technology alone isn't enough; aligning goals and practices across organizations takes time and effort, requiring orchestration for effective collaboration.

Through effective, well-functioning partnerships, cities can address complex challenges they couldn't solve on their own. Issues like youth inactivity or neighborhood segregation require a holistic approach and data from multiple sources. By collaborating and sharing data with other organizations, cities gain better situational awareness and can develop innovative, sustainable solutions.

## Evolution of data ecosystems

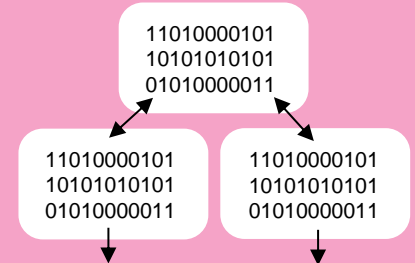
1

The organization uses both its own data and external data sources, as well as open data.



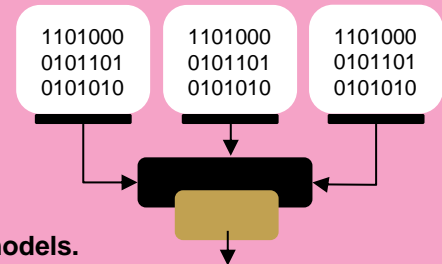
2

The organization forms a loose network for sharing data with other stakeholders.



3

The organization provides services as part of a closely-knit ecosystem with common operating models.



# Obstacles to a data-driven future

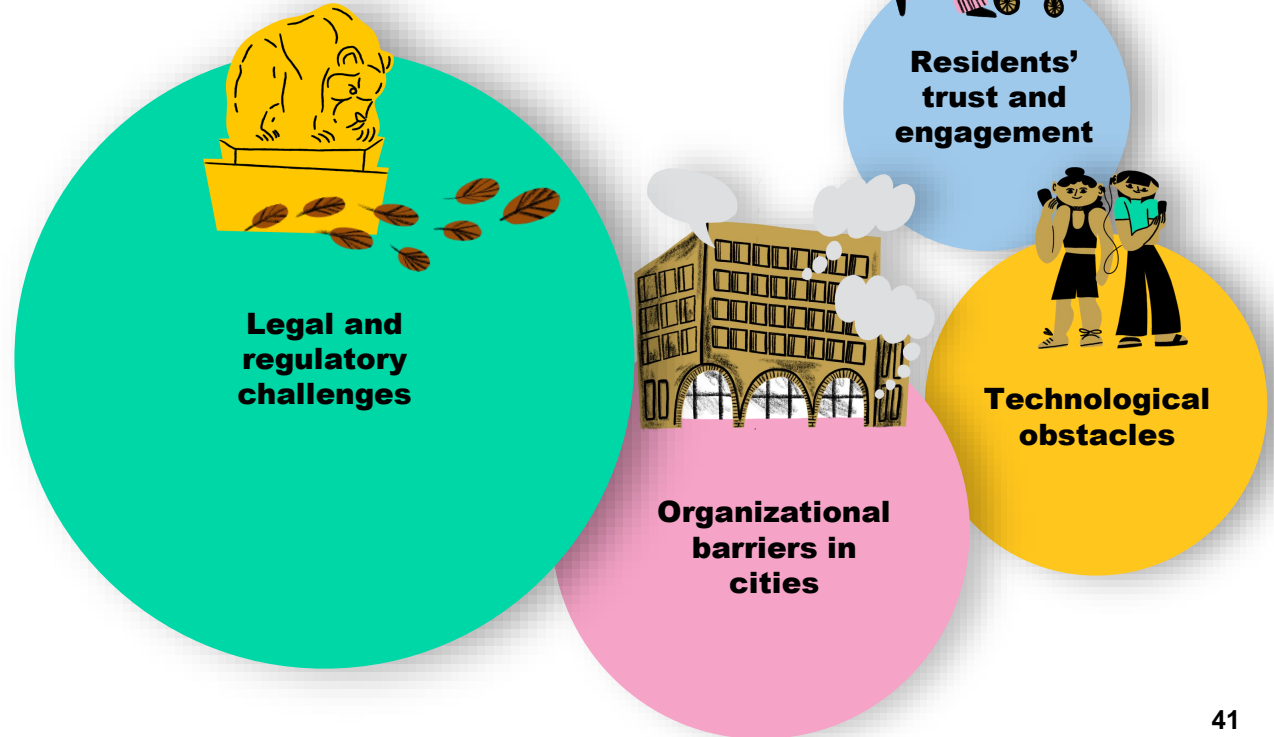




# Barriers slowing the adoption of consent-based city services

Previous sections have highlighted the various challenges cities face when implementing consent-based services. This section brings those issues together, grouping them under the key themes of the report.

While all these challenges need to be addressed, not all are equally pressing. Feedback from cities leading the development of consent-based services suggests that legislative hurdles and financial constraints are the most urgent. These two issues are widely regarded as the main barriers to effectively scaling consent-based services.



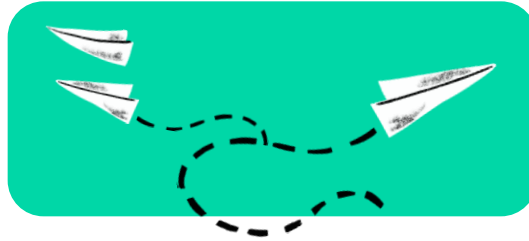
# Legislation: difficult to navigate



## Lack of awareness and understanding

Municipalities face uncertainty about when consent is required and how to comply with GDPR, leading to fears of legal consequences. Regulations like GDPR provide broad principles but lack detailed instructions for real-world application, especially when combined with other national or EU legislation.

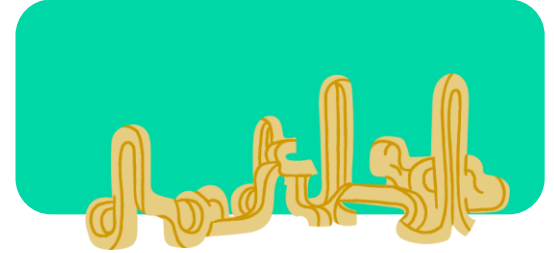
To overcome this, cities should lobby high-level authorities to allocate resources for creating practical guidelines and to collaborate with municipalities to share clear, tailored strategies for compliance.



## Varying interpretations

Varying interpretations of regulations like GDPR can lead to inconsistent compliance across municipalities, complicating efforts to create standardized practices.

To address this, municipalities should not only collaborate with each other and with legal experts to share best practices, but also advocate for better national and cross-border alignment to ensure shared understanding of how EU regulation should be implemented.



## Complexity of compliance

Keeping up with evolving regulations like GDPR, the Data Governance Act, and the Data Act poses a challenge. Cities must maintain compliance with complex laws, which requires continuous training and resources.

To mitigate this, cities should establish dedicated compliance teams and collaborate with other municipalities to share best practices for managing regulatory changes.

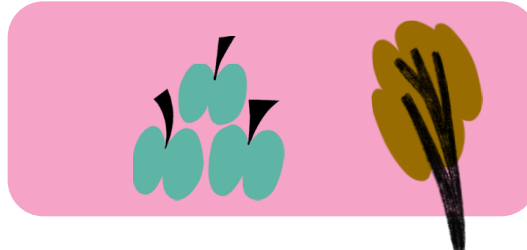
# Cities: financial and operational barriers



## Resistance to change and lack of expertise

Shifting from traditional practices to consent-based models requires a significant cultural shift, often met with resistance from employees who may be uncomfortable with new technology or fear increased workload. Additionally, many municipalities lack the in-house expertise in data privacy and digital services, making the transition even more difficult.

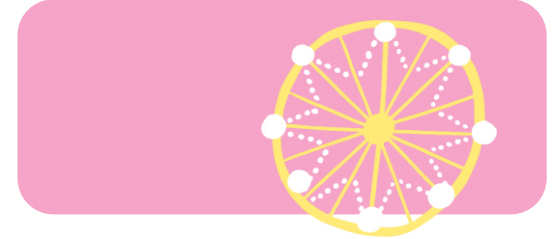
To address both, strong leadership, ongoing training, and external partnerships are essential for building competence and confidence.



## Budget constraints and uncertainty around ROI

Budget limitations and high entry costs are significant barriers especially for smaller cities. Upfront investments in IT infrastructure and training for consent-based systems can be difficult to justify, especially when the immediate financial returns are unclear.

To address this, cities can begin by launching pilot projects to demonstrate value on a smaller scale. Phased implementation also helps spread costs over time. Exploring public-private partnerships or cost-effective solutions like cloud services can further ease the financial burden.



## Coordination and siloed departments

Implementing consent-based systems requires collaboration across multiple departments, each with its own data practices and priorities. A lack of coordination can slow progress, making it crucial to develop cross-departmental teams and standardized procedures for data governance.

Aligning efforts across departments helps ensure a unified approach and smoother implementation of new systems.

# Technology: fragmented and outdated



## Legacy systems and interoperability challenges

Many cities rely on outdated IT infrastructure that lacks interoperability, making it difficult to support consent-based services. The absence of clear standards for data-sharing further complicates upgrades, leaving cities unsure how to ensure future compatibility.

To overcome this, cities could upgrade systems gradually, focusing on critical areas first, and adopt cloud-based solutions. Aligning with emerging interoperability standards will help ease transitions and future-proof systems.



## Risky data management

Many cities already store large amounts of personal data in systems that are not secure. These risky systems pose a significant challenge when transitioning to consent-based frameworks, as the existing data must be properly managed before new technologies can be implemented.

Cities should prioritize securing existing data by auditing current systems and investing in cybersecurity upgrades. Implementing data governance frameworks and ensuring proper encryption and access controls can mitigate risks.



## Slow procurement processes

The procurement processes in cities are often slow and cumbersome, delaying the acquisition of new technologies. This makes it difficult for municipalities to experiment with or adopt new solutions quickly, hindering innovation and slowing progress.

Streamlining procurement procedures by adopting more flexible and agile approaches can accelerate the adoption of new technologies. Cities can explore faster procurement options, such as pre-approved vendor lists or innovation-focused procurement programs.

# Residents: low awareness and trust



## Lack of awareness and understanding

Many residents are unaware of how their data is collected, used, and shared by municipal services. This lack of awareness often leads to disengagement or skepticism toward consent-based services.

Municipalities can address this issue through public education campaigns and by providing accessible, up-to-date information on how residents' data is being used. Additionally, residents should have access to a platform where they can ask questions or voice concerns.



## Low trust and privacy concerns

Public trust in how municipalities handle personal data can be low due to concerns about data breaches. Stories of misuse by other organizations can further deepen these concerns, leading residents to be more cautious or even refuse to share their information. This hesitancy impacts the adoption of consent-based services.

To improve trust, cities may need to implement robust data-security measures, communicate heavily about data security measures, and openly share how personal data is used.



## Perceived complexity of consent processes

Residents may find the consent processes associated with data sharing to be complex and difficult to navigate. Long forms filled with legal jargon can deter people from giving informed consent, as they may not fully understand what they are agreeing to.

Simplifying these processes and making them more accessible is essential to increase engagement and ensure residents feel comfortable sharing their data.

# Proposal for next steps

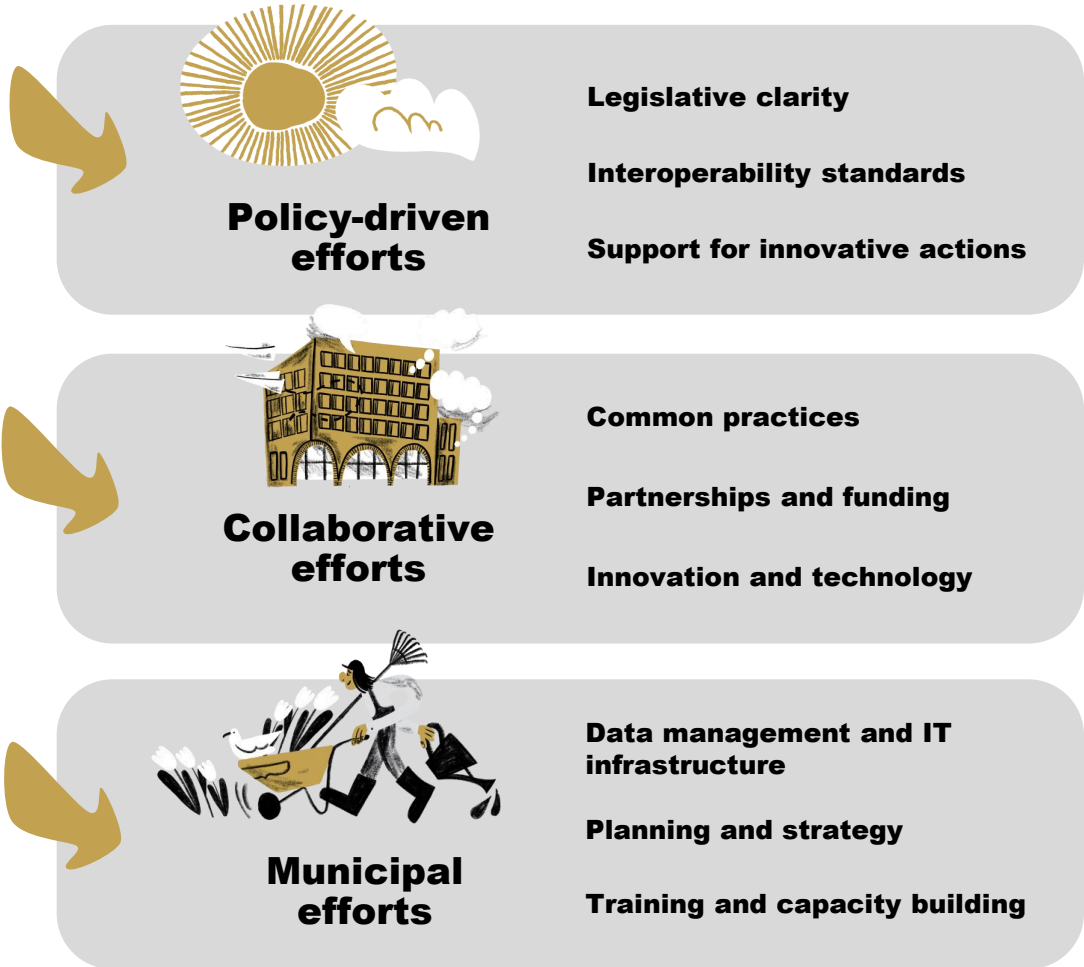


# How to tackle the obstacles?

To overcome the obstacles and successfully implement consent-based data services, municipalities must undertake a range of actions, independently, collaboratively, and through policy-driven efforts.

On their own, cities can focus on enhancing data governance, upgrading IT infrastructure, and building internal capacity through training and strategic planning. Collaborative efforts with other cities and partners are essential for sharing best practices, securing funding, and driving innovation. Additionally, policy-driven efforts from national or regional authorities are necessary to provide clear guidelines, allocate resources, and ensure regulatory compliance that supports the implementation of consent-based services.

These are further elaborated on the following pages.



# Policy-driven efforts to tackle the obstacles



## Legislative clarity

- Cities need clear **guidance from legal authorities** on new regulations, such as GDPR and the Data Act, to ensure they remain compliant while driving innovation.
- EU and national level authorities must **allocate sufficient resources to advisory services** to ensure that new regulation can be implemented fluently across different use cases. Currently, authorities focus primarily on monitoring compliance, which does not support innovation.

## Interoperability standards for cities

- Cities need to be **acknowledged as key players** in renewing and developing public services as well as in managing public data, alongside other public entities.
- Cities require **international interoperability standards** that take into account diverse approaches, such as wallets, personal data pods, and ecosystems with real-time data exchange, to streamline collaboration across services and systems.

## Support for innovative actions

- Cities must receive strong support for **innovative projects**, including access to funding and skill development programs.
- **Innovation and implementation programs like Horizon Europe** (or its successor FP10) **and the Digital Europe** program should support cross-border collaboration and data initiatives in this field with the role of cities in mind.
- There should also be **broad educational programs** to promote data literacy, as well as skills in data and AI.



# Collaborative efforts to tackle the obstacles



## Common practices

- Develop consistent and standardized **data policies** and practices that align with legal requirements like GDPR, DMA, and DA.
- Collaborate with forerunner cities to create **clear guidelines** for unified consent-based municipal services.
- **Establish forums** to share experiences related to consent-based data services to adopt proven strategies quicker and to avoid common pitfalls.

## Partnerships and funding

- **Form partnerships** with universities and private companies to access advanced technologies, expertise, and financial resources.
- Jointly **seek alternative funding** sources, such as government grants or international funding programs, to support the development and maintenance of consent-based data services.

## Innovation and technology

- Collaborate on **pilot projects** that demonstrate the value of consent-based models.
- Jointly develop **interoperable tools and platforms** for consent-based services to create solutions that can benefit multiple cities and become industry standards.

# Municipal efforts to tackle the obstacles



## Data Management and IT Infrastructure

- Establish centralized data governance
- Implement robust cybersecurity measures
- Consider shifting technological strategy towards flexible IT systems
- Prioritize investments in interoperable technologies
- Adopt cloud-based solutions
- Regularly update security protocols
- Utilize advanced compliance tools
- Implement new systems in phases

## Training and capacity building

- Provide continuous staff training
- Form strategic partnerships with universities or companies
- Develop cross-departmental teams to align efforts and facilitate collaboration
- Launch public education campaigns with clear communication
- Engage residents in decision-making
- Create simple consent processes
- Maintain transparency on data policies

## Planning and strategy

- Together with legal experts, form clear guidelines for consent-based services
- Support shift to data-based services with strong leadership
- Start demonstrating the value of data-based services with pilot projects
- Create feedback platforms
- Inform residents on data usage



**Wishing you success in creating city services that are more efficient, transparent, and trusted!**

**City of Helsinki: Jasmin Repo, Mika Leivo  
Futurice: Ida Rainio**

