

---

# No Standardization Without Participation

Designing better information relations between  
citizens, government, and the housing market

Danny Lämmerhirt  
Isadora Dullaert

January 2025

waag  futurelab

---

## No Standardization Without Participation

Danny Lämmerhirt  
Isadora Dullaert

With support from: Alain Otjens, Aris Ham, Pourya Omid, Marit Hoefsloot, Jikke van den Ende, Sylke van Duijnen, Sander van der Waal, and Simone van der Burg

© Waag Futurelab, january 2025

This document uses the Creative Commons license  
Attribution-NonCommercial-ShareAlike Int. 4.0



# Executive summary

This report focuses on the experiences of tenants and homebuyers with sharing personal data in the housing sector. Waag Futurelab has conducted this research to define recommendations for data sharing standards. The report builds on earlier research by Waag which found that the Netherlands lacks a coherent and standardized approach that enables citizens exercise control over sharing their personal data between government data sources and the services receiving this data. In our new research, we found that it is often unclear to citizens why they are asked to share particular categories of data, which parties have access to this and how tenants or buyers are selected based on this data. Our key proposal is to develop **public standards** for data sharing: these are technical and legal agreements that incorporate citizen preferences and protects them from harm. This research was conducted with financial support from the maatschappelijke coalitie Over Informatie Gesproken.

## Research goals and research approach

The goal of this research was twofold: 1) to develop a method that allows tenants and home buyers to articulate their opinions and preferences about current and future data sharing practices, and 2) to derive a list of recommendations that inform future standard making processes. To do so, we organized three focus group meetings (n=18 participants) with tenants in the free housing market, housing aid recipients, and home buyers. In addition, we interviewed housing corporations and researchers working on discrimination in the housing sector.

## Results

We find that participants perceive data sharing within the context of unequal power relations as a requirement to access housing. For them, data sharing is not act of individual choice and control. Our report shows that participants have nuanced ideas about different aspects of data sharing standards. They deem specific data irrelevant or sensitive, including historical data or birthplace. A significant finding is the common experience that existing data sharing setups, including gates and wallets, are perceived as opaque. Neither the involved actors, nor the data processing for housing applications are understandable to citizens. Our participants prefer more control options for their data and, if they would need to choose between data intermediaries, gave preference to a government wallet as opposed to a commercial gate app.

- **Data:** Participants deem certain data as sensitive, such as identity data revealing someone's nationality or status as foreigner, medical data that could be shared in the future with housing corporations, and data of relatives. Historical data such as past income or address history is considered to be irrelevant for finding a house.
- **Actions:** Participants wish to have control options when sharing data, including the ability to see what exact data they are sharing, the ability to limit data access to a short time frame and the ability to provide data step-by-step and only for specific purposes. Participants want to have clarity on the relationship between government data sources and commercial data intermediaries.
- **Actors:** Participants are skeptical about using a commercial data sharing service and prefer a government-issued wallet. Not all participants support the use of intermediaries and instead would prefer submitting data themselves. However, several participants consider intermediaries as a way to standardize data sharing within the housing sector.
- **Purposes:** Most participants agreed that the data use in the housing sector is highly opaque. They were concerned with how they are being selected for housing based on their data, and the fairness of selection. Participants expect future data sharing mechanisms to have high transparency standards. This includes making criteria for selecting tenants and buyers transparent and defining clear regulations concerning the use of data by third parties.

## Recommendations

Based on these results, we conclude that the government has a responsibility to develop technical and legal infrastructure that protects the interests of citizens. We argue that it is crucial to involve the public in creation of standards for this infrastructure. **Public standards** are based on the needs of citizens and translate these needs into concrete requirements for data sharing and reuse. It is also important to involve other key stakeholders in the field, such as policy makers, public service providers acting as data sources, research institutes and citizen rights organizations, commercial developers of data intermediaries, and data recipients. In short, we need an integrated regulatory and design approach.

For citizens, not only data sharing is important, but they are also concerned about data use, whether data is used in their interest and who has access to their profiles. These topics are splintered across different policy areas. For example, the Law for Digital Government regulates access to data sources such as the BRP, while the eIDAS Regulation considers different aspects of data intermediaries (wallets). Finally, data reuse in the housing sector is regulated by housing laws, such as laws within the housing market stipulating the non-discriminatory selection of tenants. This means that our

recommendations are relevant for different public policy areas. These areas will have to be aligned in a comprehensive data sharing framework.

On the basis of our findings, we make the following recommendations:

- **Continuous involvement of citizens, sectoral researchers and tenants' rights representatives is important, instead of primarily involving industry representatives.** Citizens and their representatives can provide advice on the potential harms and data sharing requirements in different sectors, including the housing sector.
- **The Ministry of Interior and Kingdom Relations should develop an integrated framework for personal data sharing.** This framework should regulate access to governmental data sources (as part of the Law for Digital Government) and define requirements for the sharing of data by intermediaries (as part of the Dutch EUDI-framework). This has also been recommended by ICTU, that called for an integrated framework that combines the abovementioned policies.
- **This integrated framework should recognize the crucial role of government data sources to grant citizens control rights to their personal data.** The Ministry of Interior and Kingdom Relations should involve citizens in defining structured access to personal data. Based on our report, structured data access should provide citizens with granular control options and minimize data access at the source. This can include granting highly modular access to individual data points, or consider using attribute-based credentials. The goal should be to limit the interpretability of data to specific use purposes at the source.
- **To minimize data processing, different parties should be assigned specific processing purposes to avoid conflicts of interest.** In the housing sector, this can mean that a dedicated data intermediary provides identity checks for the purpose of identity verification or fraud detection, whereas housing corporations can use income data for selecting tenants.
- **The Ministry of Interior and Kingdom Relations should further develop the public NL-wallet as a standard, government-issued data sharing mechanism.** A government-issued wallet can provide a standardized data sharing mechanism for citizens who are required to share personal data with different commercial (housing) platforms and other digital services. This can be done by mandating the adoption of a public NL-wallet by commercial providers as ID management and data sharing system within the Dutch EUDI-framework.

- **The ICTU should test the evolving technical standards for the public NL-wallet with citizens.** The tests should go beyond isolated technical mechanisms, and consider how citizens perceive them in relation to concrete use scenarios. To do so, ICTU can implement the insights and apply the methods presented in this report.
- **The Ministry of Interior and Kingdom Relations should not only consider personal data sharing, but also permissible data uses and transparency requirements thereof.** In the housing sector, public involvement is important considering recent proposals to include medical data as novel data category to be processed, as well as calls for more transparent selection criteria for tenants. This requires interministerial collaboration with bodies such as the Ministry of Housing and Spatial Planning.

# Table of contents

<b>Executive summary</b> .....	<b>3</b>
Research goals and research approach .....	3
Results .....	3
Recommendations .....	4
<b>Table of contents</b> .....	<b>7</b>
<b>Introduction</b> .....	<b>8</b>
<b>1 Background: Public standards for personal data sharing</b> .....	<b>9</b>
1.1 Personal data sharing in the context of a more open and responsive government	10
1.2 Better information relations require standards .....	11
<b>2 What are standards for personal data sharing?</b> .....	<b>14</b>
2.1 Designing information relationships: why do standards deserve our attention? ....	14
2.2 What are standards for data sharing? .....	16
2.3 The status quo of standard setting for person-related data in the housing market	18
<b>3 Why public standards for data sharing?</b> .....	<b>21</b>
3.1: How does public standard making differ from existing user research? .....	22
3.2 Our method: Documenting people’s concerns around personal data sharing .....	24
<b>4 Results: Experiences with personal data sharing</b> .....	<b>26</b>
4.1 Experiences with existing personal data sharing mechanisms .....	26
4.2 Scenarios of data sharing alternatives .....	32
Scenario 1 (Tenants and social housing aid recipients) .....	32
Scenario 2 (Tenants and social housing aid recipients).....	35
Scenario 3 (Buyers).....	37
Scenario 4 (Buyers).....	38
<b>5 Conclusions and recommendations</b> .....	<b>40</b>
<b>6 Literature</b> .....	<b>45</b>
<b>Appendix: Scenarios</b> .....	<b>47</b>
Scenario 1 (Tenants, free market and social housing) .....	47
Scenario 2 (Tenants, free market and social housing).....	48
Scenario 3 (Buyers) .....	49
Scenario 4 (Buyers) .....	50

# Introduction

This report focuses on the experiences of tenants and homebuyers with sharing personal data in the housing sector. Waag Futurelab has conducted this research to define recommendations for data sharing standards. The report builds on earlier research by Waag which found that the Netherlands lacks a coherent and standardized approach that enables citizens exercise control over sharing their personal data between government data sources and the services receiving this data. In *No Standardization Without Participation*, we show that it is often unclear to citizens why they are asked to share particular categories of data, which parties have access to this and how tenants or buyers are selected based on this data. Our key proposal is to develop **public standards** for data sharing: these are technical and legal agreements that incorporate citizen preferences and protect them from harm. This research was conducted with financial support from the maatschappelijke coalitie Over Informatie Gesproken.

This report proposes a method to involve the public in discussions over data sharing in the housing sector. It presents findings from focus group discussions (n=18) with tenants in the free market, home buyers, and rent subsidy recipients. The findings discuss how participants experience existing ways to share data in the housing market and the desirability of data sharing via a wallet and consent mechanism. We are asking the following research questions:

1. What interests and expectations do citizens attach to sharing their data with different services in the housing sector when using data sharing tools?
2. What requirements for a public data sharing standard arise from citizens' interests and expectations?

Our report shows that citizens have nuanced ideas about different aspects of data sharing standards. People deem specific data irrelevant or sensitive, including historical data or birthplace. A significant finding is the common experience that existing data sharing setups, including gates and wallets, are perceived as opaque. Neither the involved actors, nor the data processing for housing applications are understandable to citizens. Our participants prefer more control options for their data and, if they would need to choose between data intermediaries, gave preference to a government wallet as opposed to a commercial gate app.



# 1 Background: Public standards for personal data sharing

Data sharing has become a key priority for the Dutch national government. Through data sharing, person-related data that government holds and processes about its citizens shall be made usable by external (commercial) third-parties and citizens. To enable data sharing, the Dutch government has initiated legal, political, and technological developments to help citizens enact their right to data portability. The right to data portability is not only enshrined in the GDPR but also made part of past policy programs such as the program “Control over Data” (Dutch: Regie op Gegevens). One objective of the program is to enable citizens to request copies of their person-related data from government institutions and share it with others. In the recent report “Grip op Eigen Gegevens”<sup>1</sup>, we researched at Waag Futurelab (in the following: Waag) what technical instruments are available to help citizens enact their right to data portability. The report found that these instruments are primarily developed by a private market of personal data intermediaries, including gates (a form of a consent mechanism that transfers data from server to server) and wallet apps that enable citizens to consent to accessing and sharing various data such as identity data, salary data, labor history data, and others with (commercial) parties. Our report laid out how government and market parties distribute roles and responsibilities: the Dutch government and public service delivery organs act as a data source for personal data and determine policies for data sharing, while private market parties develop the technical infrastructure. We found that this constellation causes problems because legal and technical infrastructures for data sharing do not align between government and market: Dutch base registers and public service providers lack APIs to structure data access. Waag and the Dutch Data Protection Agency<sup>2</sup> have argued that the Dutch infrastructure for data sharing currently does not adequately protect the rights of citizens and broker (unequal) power relations between government, citizens, civil society, and market parties.

In this report, we argue that the development of data sharing infrastructure requires standards for data sharing and that these must be developed together with the public. Because the circulation of personal data affects citizens, they have to be involved in discussions about what “good” data sharing means for them. This is especially important because there are multiple initiatives in Europe and the Netherlands underway to develop a data infrastructure for the circulation of personal data held by public institutions. This

---

<sup>1</sup> See Lämmerhirt, Danny, and Julia Jansen. 2024. “Grip Op Eigen Gegevens.” Waag Futurelab. Available at: <https://grip-op-eigen-gegevens.waag.or>

<sup>2</sup> Autoriteit Persoonsgegevens. 2024. “Brief AP aan BZK over datadeler-apps | Autoriteit Persoonsgegevens.” August 27, 2024. Available at: <https://autoriteitpersoonsgegevens.nl/documenten/brief-ap-aan-bzk-over-datadeler-apps>.

report offers two broader insights: a) it describes how citizens experience existing arrangements to share person-related data held by different government institutions, including identity data, income data, work history data, educational data, and others; b) it develops the notion of “public standards” as a conceptual framework and related methods for facilitating structured debates about important component parts of a data sharing standard. In contrast to past studies commissioned by the Ministry of Interior and Kingdom Relations which studied people’s opinions on data sharing, our report explores how citizens can meaningfully debate existing data sharing infrastructure and how their experiences can be translated into requirements for infrastructural standards.

By doing so, we respond to calls by other Dutch researchers who pointed out a lack of citizen involvement in the development of information infrastructure<sup>3</sup> and the development of standards for public ICT infrastructure.<sup>4</sup> After providing context on data sharing infrastructure for data sharing in the Netherlands, we explain why public involvement in the development of standards for data sharing matters and present findings from three workshops with 18 participants searching housing in the free sector, the home ownership market, and the social housing sector. In our conclusion, we summarize our findings and present recommendations that public sector officials and developers of data intermediaries can use to design data sharing setups.

## 1.1 Personal data sharing in the context of a more open and responsive government

Enabling citizens to exercise control over the data they share with others is also a priority of several political parties and public sector institutions. Since the Dutch benefits affair, the Dutch public information infrastructure has become a focal point for organizing good and just relationships between citizens and public institutions. This has included calls for better information management, the simplification of contact points and interactions between government and citizens, as well as a turn towards more control by citizens over the data government stores about them. As a response, the Control over Data program stated three distinct policy goals: providing citizens insight into the data held about them by government, enabling them to make corrections to data, and requesting copies of data held by public institutions such as the Base Register for Personal Data. With the right to data portability, public institutions extend access to personal data to outside parties, including data intermediaries and commercial parties providing services to citizens. Some of the Dutch political parties have supported more citizen control over personal data. The People’s Party for Freedom and Democracy (short: VVD) argued for instance that citizens must have control over their data by being

---

<sup>3</sup> See Van Zoonen, Liesbet. 2020. “Data Governance and Citizen Participation in the Digital Welfare State.” *Data & Policy* 2. <https://doi.org/10.1017/dap.2020.10>.

<sup>4</sup> Driessen, M, M Van der Koppel, D Hollander, S Milan, J De Vos, and N Ten Oever. 2024. “Publieke Waarden Rondom Digitale Technologieën.” NWO. [https://in-sight.it/assets/IN-SIGHT\\_Publieke\\_waarden\\_rapport\\_NL.pdf](https://in-sight.it/assets/IN-SIGHT_Publieke_waarden_rapport_NL.pdf).

enabled to view the data that the government stores about them and by managing data in a digital wallet. The party New Social Contract (short: NSC) also supports developing a digital wallet with which citizens can have as much control as possible over their data. It argued in its party program<sup>5</sup> that citizens must have easier overviews of who processes which data for which purposes and advocated for a “once only” principle based on the Estonian model: personal data of citizens shall only be stored once in one government database, instead of multiple databases. This database shall register and report any data requests to the citizen who gains insight and may file a complaint about it, if necessary.

How are these policy ambitions translated into practice? Our report “Grip op Eigen Gegevens” found that the Dutch government offers citizens a vast number of instruments and that these do not provide standardized experiences and functions for citizens. The existing instruments usually only focus on selected rights, for instance providing citizens information about what data is held by government, or the right to correct data. At the same time, many of the instruments we found provide citizens with different actions on different kinds of personal data. For instance, citizens can request different overviews of the government institution that have accessed someone’s data from different institutions via different processes. Data intermediaries enabling data portability, on the other hand, are primarily developed by industry and research institutions, while the Ministry of Interior and Kingdom Relations, as well as public institutions play a role as provider of data sources and as rule-maker for data sharing policies. Our report stated that the current landscape of data intermediaries is not coordinated enough and lacks standards for data sharing. As an outcome of this current patchwork, some data intermediaries operate in a legal grey area and may violate the rights of citizens. They also may increase the complexity for citizens to understand how data is being shared and reused. With upcoming implementations of the Law for a digital government (Wet digitale overheid, part 2) as well as the Dutch implementation of the European eIDAS regulation, the Dutch government has ambitions to develop a government-own data wallet and to develop standards for making personal data shareable with third-parties upon the consent of citizens. We concluded that citizens remain confronted with a complex landscape of instruments that raises serious concerns whether citizens can actually enact their rights to data and improve their position towards government.

## 1.2 Better information relations require standards

In the Grip op Eigen Gegevens report, we noted that the public policy goal to enhance personal control over data is only effective if it leads to more personal control over one’s own life (e. g. by improving a citizen’s access to public services), and if it is accompanied by an infrastructure of laws and technology that works in the interest of citizens. This raises the question what data sharing infrastructure is desired by citizens

---

<sup>5</sup> [https://storage.googleapis.com/groep-pieter-website/NSC\\_verkiezingsprogramma\\_2023\\_v3.pdf](https://storage.googleapis.com/groep-pieter-website/NSC_verkiezingsprogramma_2023_v3.pdf)

and how can it change their power position to the better. In this report, we argue that giving citizens more control over their data and their lives also requires a “good” data sharing infrastructure that can broker between the interests of citizens and data recipients. We argue that the sensitivity of data, and interests in data, are relative to existing social environments in which people are asked to share personal data. By extension, they also influence how people think about the sharing of their data and what kind of control they want to exercise.

As a case study, the report focuses on personal data sharing within the housing sector. We select this sector, because intermediaries for data portability already exist and are being used by this sector. In addition, the housing sector provides a concrete example that virtually all citizens are affected by. Our broader arguments are applicable to other sectors in which people receive (public) services upon sharing data about themselves. The Dutch housing market relies on all kinds of personal data – from in-person introduction meetings, to online application forms requesting data about someone’s financial situation, family status, job history, nationality, but also hobbies and lifestyle that may be included in landlord statements. Because using personal data can lead to discrimination, the Dutch housing sector is regulated by multiple laws that regulate what data may be processed that is classified as “relevant data” by law and that can be for purposes such as verifying someone’s identity. Discriminatory practices, such as forbidding someone housing based on their family status, gender, religion, or nationality, are forbidden.

Yet, even relevant data can do harm. Recent studies on the Dutch housing market suggest that also the use of “relevant data” can lead to discrimination and institutional racism.<sup>6</sup> Based on anecdotal evidence, such research suggests that certain identity data, such as a person’s name, birthplace, and nationality could enable landlords to indirectly discriminate against tenants, for instance by not selecting them for a house viewing. Even in a highly regulated sector, discussions about what data should be shared, with whom, for what purposes, persist.<sup>7</sup>

Our report asks citizens what they think good data sharing arrangements look like in the housing sector and develops recommendations for standards for data sharing of person-related data. With these recommendations, we want to sensitize government and data intermediary developers for the development of public standards: standards that can respond to and accommodate the concerns of citizen groups affected by the use of a standard. By doing so, we follow recent research on people’s perceptions of data

---

<sup>6</sup> Van der Tuin, Inte, and Milynn Koene. 2021. “Sterke Vermoedens, Maar Geen Bewijs. Discriminatie-Ervaringen van Woningzoekenden in Rotterdam.” Rotterdam: Radar voor gelijke behandeling tegen discriminatie.;

See also Hoogenbosch, Arwen. 2022. “Institutioneel racisme bij woningverhuur.” Utrecht: Kennisplatform inclusief samenleven. <https://www.kis.nl/online-publicatie/institutioneel-racisme-bij-woningverhuur>.

<sup>7</sup> Given the focus of our study, we are unable to provide a detailed review of these debates. We direct interested readers to expert literature on this topic.

sharing, showing that people's willingness to share depends on the data, the recipients of the data and their trustworthiness, and its (imagined) use purposes.<sup>8</sup> Standards for sharing personal data therefore cannot stop short at discussions about data, but must consider the broader social environment people share data within.

Public standards for personal sharing data must put the interests of citizens central. We describe a method to involve citizens in conversations about data sharing scenarios and derive recommendations for their development. Thereby, we address a persisting gap in the development of participatory methods for standards.<sup>9</sup> In this report, we therefore address the following research questions:

1. What interests and expectations do citizens attach to sharing their data with different services in the housing sector when using data sharing tools?
2. What requirements for a public data sharing standard arise from citizens' interests and expectations?

---

<sup>8</sup> Urban, Monika. 2022. „Toll. Ich bin froh dabei zu sein“. Studie zur Spende digitaler Körperdaten in der Corona-Krise.“ *ZQF – Zeitschrift für Qualitative Forschung* 22 (2). <https://www.budrich-journals.de/index.php/zqf/article/view/39525>;

Van Zoonen, Liesbet. 2016. “Privacy Concerns in Smart Cities.” *Government Information Quarterly*, Open and Smart Governments: Strategies, Tools, and Experiences, 33 (3): 472–80. <https://doi.org/10.1016/j.giq.2016.06.004>.

<sup>9</sup> Brandusescu, Ana, Michael Canares, en Silvana Fumega. 2020. “Open Data Standards Design behind Closed Doors?” *Open data standards design behind closed doors? ILDA (blog)*. August 21, 2020. <https://idatosabiertos.org/en/diseno-de-estandares-de-datos-abiertos-a-puertas-cerradas/>.

# 2 What are standards for personal data sharing?

Standards are a key defining aspect of modern life that is usually not noticed and taken for granted. Whether it is about what power outlets we use, what side of the street we drive our cars on, or the size and form of fruit in our supermarkets: standards shall streamline procedures, regulate behavior, and predict results.<sup>10</sup> In this report, we understand standards as agreements that are reusable by different stakeholders to solve more or less defined problems and to structure daily behavior. Standards organize our world into concepts, languages, rules, and results to be agreed and followed. Often, these standards are shaped by governments and industries, sometimes with involvement by civil society, but very rarely with citizens affected by these standards.

We speak of standards in the plural, because a standard usually does not function on its own. Instead, it requires other standards to work. For instance, when we write an email to a government official, we rely on standardized email exchange protocols, an email user interface that allows standardized actions, but also standards for appropriately talking to each other. As we will describe below, this nested character of standards makes defining rules for data sharing complex: standards for the sharing of personal data may apply to data categories (e.g. our date of birth and nationality) that can be nested in data schemas (e.g. grouping our data of birth under an identity data group), data structures (such as XML, JSON), and data file formats (such as .xls or .odt), which can furthermore depend on legislation that defines what personal data is allowed to be shared or not.

Even though standards take a stable form, people can experience them differently. For instance, standards for working hours or age vary in their cultural meaning. Identity verification through a standard passport is probably perceived as benign for most citizens registered in the EU, but it can present bureaucratic problems for people without official citizenship status. Standards are one person's helpful tool, and can be another person's nightmare.

## 2.1 Designing information relationships: why do standards deserve our attention?

The Dutch public sector increasingly relies on data to interact with citizens. Standards for data access, sharing, and use govern how citizens are documented, made legible, and provided with services. They structure the relationship between citizens and

---

<sup>10</sup> Lampland, Martha, and Susan Leigh Star, eds. 2009. *Standards and Their Stories*. Ithaca: Cornell University Press.

government by manifesting norms. The ideal is that standards can provide guidance on how to deal with different lived realities. But as the sociologists Susan Leigh Star and Martha Lampland point out, “perhaps the most intriguing aspect of standards is their always already incomplete and inadequate [...] character”.<sup>11</sup> We see this point reflected in discussions about the inadequacy of the Dutch information system and public service delivery to match the lived realities of citizens. Peeters and Widlak for instance have shown how the Dutch base registers can exclude people who do not fit into the categories of the base register, or the public service procedures relying on these categories.<sup>12</sup> Likewise, the report *Grip op Eigen Gegevens* by Waag found that Dutch public services lack technical standards for sharing data and that there are multiple approaches to data sharing. They reflect different norms and values regarding security, data protection, fraud detection, and the degree of control over data that standard developers want to grant citizens.

Considering the incomplete nature of every standard, we therefore do not advocate for the development of one standard alone. Rather, with this report we present what requirements citizens themselves see important when sharing data, and what recommendations for standards we can derive that put the interests of citizens center stage. By providing recommendations, we want to support standards development that is sensitive to different meanings of “good” data sharing for citizens, that may depend on different situations in which people share data.

Data sharing in the housing market is a particularly useful example. Not only do applications for personal data sharing exist in this sector. The housing market also deals with many personal data which influence whether people are getting access to housing or not. The housing market also consists of many social interactions and relations: we can find housing via friends and acquaintances, we can apply for lottery in the free market, search for housing targeting particular professions, rent with a partner or alone, ask relatives to vouch for us financially – the relations are many. As earlier research found, these relationships may also matter for how data sharing is perceived. What data counts as sensitive and how people want to share their data, depends on many things: the rules and technologies handling data, the types of data (and how sensitive they are for people), the actors involved (e. g. some people may mistrust commercial parties), and the goals and purposes for processing data. Before we explain what a public development of such standards could look like, we explain what a data sharing standard entails.

---

<sup>11</sup> Ibid, p. 14.

<sup>12</sup> Peeters, Rik, and Arjan Widlak. 2018. “The Digital Cage: Administrative Exclusion through Information Architecture – The Case of the Dutch Civil Registry’s Master Data Management System.” *Government Information Quarterly*, 35 (2): 175–83. <https://doi.org/10.1016/j.giq.2018.02.003>.



## 2.2 What are standards for data sharing?

We consider standards for personal data sharing as *agreements* that organize how people and organizations can access, share, and reuse data. In this report, we focus on personal data that is held by public service providers or traditionally used for public services, including the BRP, public service providers like the UWV, the DUO, or the Tax Office. In the Netherlands, several laws and policies outline possible elements of a data sharing standard. The Control over Data program stipulates that citizens should be able to share personal data (as defined in the GDPR) from government data sources with private service providers. To do so, it has developed a vision for a reference architecture<sup>13</sup> that includes control applications. These applications shall distribute control actions between government, third parties, and citizens, as well as so-called “interaction patterns” between government data sources, citizens, and private service providers. In policy and industry, these interaction patterns are also called data flow models, data routes, or data sharing setups.<sup>14</sup> These include three models:

- “Safe model: in this model, the citizen retrieves the required personal data from the government and places them in a digital personal environment that he manages himself (e. g. an app). He can also place data from third parties there (whether or not authenticated), but he can also add his own data. Every time he wants to use a service from a service provider, he can provide the required data from his digital personal environment to the service provider or (if the environment provides for this) give a service provider access to (part of) his data.
- Gate-model: in this model, the service provider makes a digital personal environment available with which the service provider (after permission from the citizen) can directly retrieve personal data from a government registration and place it in that personal environment.”
- Source-model: in this model, the government creates a digital personal environment for the citizen. The citizen gives the government permission to make the relevant personal data available to the service provider if a service provider requests this. This permission therefore takes place (and is registered) at the source, in conjunction with the government.”<sup>15</sup>

What could be relevant standards for these models? To answer this question, we suggest it is best to split each model into its component parts. Recent research suggests that we can distinguish and classify data intermediaries by considering how their individual components are designed, such as the authorization mechanism, the consent protocol,

---

<sup>13</sup> See: [https://www.noraonline.nl/wiki/Referentiearchitectuur\\_Regie\\_op\\_Gegevens](https://www.noraonline.nl/wiki/Referentiearchitectuur_Regie_op_Gegevens)

<sup>14</sup> See Sharma, S. 2024: “Proeftuin Regie op Gegevens met Zorgeloos Vastgoed”. Available at: <https://rog.pleio.nl/attachment/entity/56db3a5a-06f5-409a-9bee-09c494f16ceb>

<sup>15</sup> Sharma, Shane Arjun, and Rocco Langeweg. 2024. “Proeftuin Regie Op Gegevens Met Zorgeloos Vastgoed.” Available at: <https://rog.pleio.nl/attachment/entity/56db3a5a-06f5-409a-9bee-09c494f16ceb>



the data schema used, or the services provided.<sup>16</sup> Therefore, we argue that we must distinguish data intermediaries by the component parts they are built from, and how these parts are combined into a data sharing setup.

Element	Component parts	Relevance for citizens
Data	Data schemata (including standard data categories, units, and aggregation levels); Data structures (e. g. JSON, XML); File formats (.xls etc.); Data standardization services	Citizens attribute different degrees of sensitivity to different data types. <sup>17</sup>
Actions	Authentication (e. g. via the OAuth 2.0 protocol or DigiD); Consent management / authorization (e. g. definitions of permission scopes); Data access management (e. g. definitions for permissible actions)	Citizens have nuanced ideas about what data they share in relation to specific services and data requests. <sup>18</sup>
Actors	Standardized categories of actors who may request data (e. g. defined in ad hoc standards for data partnerships or via existing legal categories)	Citizen willingness to share data is influenced by the data recipient or reuser. <sup>19</sup>
Purposes	Usage policies for data; Permissible use purposes as defined by legal frameworks	Citizens have nuanced ideas about what happens with their data that influence if they want to share data. <sup>20</sup>

Table 1: Overview of possible data intermediary standard components and their relevance for citizens

Another important point is that we focus on the flow of data between an entire data sharing setup. Beyond a data intermediary service, this includes (government) data sources, and data re-users. To connect the development of standard components with

<sup>16</sup> Schweihoff, Julia, Anzelika Lipovetskaja, Ilka Jussen-Lengersdorf, and Frederik Möller. 2024. "Stuck in the Middle with You: Conceptualizing Data Intermediaries and Data Intermediation Services." *Electronic Markets* 34 (1): 48. <https://doi.org/10.1007/s12525-024-00729-9>.

<sup>17</sup> Bijlsma, Michiel, Carin van der Cruijssen, and Nicole Jonker. 2024. "Not All Data Are Created Equal - Data Sharing and Privacy." *Applied Economics* 56 (11): 1250–67. <https://doi.org/10.1080/00036846.2023.2175777>.

<sup>18</sup> Urban, Monika. 2022. "„Toll. Ich bin froh dabei zu sein“. Studie zur Spende digitaler Körperdaten in der Corona-Krise." *ZQF – Zeitschrift für Qualitative Forschung* 22 (2). <https://www.budrich-journals.de/index.php/zqf/article/view/39525>.

<sup>19</sup> Ajana, Btihaj. 2018. "Communal Self-Tracking: Data Philanthropy, Solidarity and Privacy." In *Self-Tracking: Empirical and Philosophical Investigations*, Btihaj Ajana (ed.), 125–41. Cham: Springer International Publishing. [https://doi.org/10.1007/978-3-319-65379-2\\_9](https://doi.org/10.1007/978-3-319-65379-2_9).

<sup>20</sup> Kennedy, Helen, Hannah Ditchfield, Susan Oman, Jo Bates, Itzelle Medina Perea, Monika Fratzczak, and Mark Taylor. 2024. "How People Connect Fairness and Equity When They Talk about Data Uses." *Big Data & Society* 11 (4): <https://doi.org/10.1177/20539517241303162>.

the requirements of citizens, we focus in this report on selected component parts that are characteristic for data intermediaries and that have been shown to influence people's perception of data sharing setups (see table 1). To gather responses from citizens on these component parts, we will discuss them in two data sharing scenarios that draw on the gate and the wallet models. We deliberately exclude other important standardized components such as encryption standards or sector-specific standards for handling specific data such as financial information.

### **2.3 The status quo of standard setting for person-related data in the housing market**

At the moment, the Dutch government and private parties are developing and adopting different standard components for personal data sharing. Each of these components regulate different aspects of data sharing. Some of these standards are laid down by Dutch legislation, other standards are implemented by private actors who design their data intermediaries within these laws. This nestedness of standards for data sharing, and their uneven development and adoption makes the design of data sharing setups complex.

Regarding the development of wallets for personal data sharing, the Ministry of Interior and Kingdom Relations is tasked with transposing the European recast of the eIDAS Regulation of 2021 into Dutch legislation. This includes developing a Dutch EDI framework, as well as a public NL-wallet that co-exists alongside a marketplace of private wallets regulated by the EDI framework. Currently, first user tests are being conducted with the public NL-wallet, and technical experts at the ICTU are continuing conversations on the technical standards and protocols that should underpin such a wallet.<sup>21</sup> On the European level, key aspects of wallets are further negotiated, including permissions, interoperability, and data sharing standards via wallets.

Regarding access and data sharing from government databases, the Ministry of Interior and Kingdom relations is working on the two-part Digital Government Act (WDO), with the first section being in effect since July 2023. The second part of the law will address the sharing of digital personal data between government and non-government entities. A central feature of this is the updated Federated Data System, which centralizes data storage in one location, preventing data from being copied or transferred. This concept is further outlined in the Data at the Source Action Plan, which focuses on enhancing government information management, increasing transparency, and promoting both data quality and minimization.

---

<sup>21</sup> See <https://edi.pleio.nl/>

Commercial parties, on the other hand, have played a role to define standards for data access and data minimization as data is being processed and transferred to a receiving party. As Waag has shown earlier, private third-parties develop filter mechanisms for data to comply with governmental data minimization requirements. They also define what control options citizens have, and how data flows from a government data source to a data recipient in the housing market. Waag and the Dutch data protection agency argued that instead Dutch government should provide structured access to data sources via an Application Programming Interface (API), in order to define rights and responsibilities between citizens, data intermediaries, and data receivers.<sup>22</sup>

Data sharing setups increase in complexity when applied to a sector. Data sharing and use in the Dutch housing sector is heavily regulated by several laws. These laws define what data landlords, financial service providers, housing corporations, and housing brokers may process. An important policy goal is to balance data access with avoidance of potential discrimination. Discrimination is not permitted under the General Equal Treatment Act (Awgb), the Equal Treatment Act on the grounds of disability or chronic illness (Wgbh/cz), the Criminal Code, and the Good Landlord Act (Wgv). Under the Good Landlord Act (Wgv), landlords are required, among other things, to use only objective selection criteria and to apply a transparent working method. Generally, data receivers such as landlords may only request data necessary for a specific purpose, such as for making a viewing appointment or for signing a rental agreement. For instance, while someone may request a name and telephone number for viewing appointments, employer statements or income documents may only be requested if the potential tenant is probably going to sign a rental agreement.

While this sounds straightforward, in practice data that is classified as relevant can be put to harmful purposes. Both, data and processing practices raise questions. Landlords may use objective and relevant criteria, such as income, family composition or rent payment history, provided that these criteria have a legitimate and objective justification. For example, an adapted home may be reserved for people with a physical disability, or a room in a private home may be rented to someone of the same sex. However, the use of objective criteria may indirectly lead to discrimination if they are used to achieve a discriminatory aim or if they disproportionately exclude certain groups in practice. A recent study<sup>23</sup> on the Dutch housing market suggests that relevant identity data such as someone's nationality or place of birth can be problematic. Usually, this data is being used to verify the identity of a tenant and prevent fraud. The report suggests that birthplace data may lead to discrimination, if landlords decide against tenants with origin from certain countries. The study pointed out that the selection criteria for tenants must be made more transparent and proposed a possible data sharing setup whereby identity

---

<sup>22</sup> See <https://autoriteitpersoonsgegevens.nl/documenten/brief-ap-aan-bzk-over-datadeler-apps>

<sup>23</sup> See: Hoogenbosch, A. 2022. "Institutioneel racisme bij Woningverhuur". Available at: <https://www.kis.nl/online-publicatie/institutioneel-racisme-bij-woningverhuur>

data is only shared with identity verification services, while other relevant data is shared with landlords.

Data sharing in the housing market is therefore a useful case because debates about what data should be used to select tenants and home buyers are not settled. Data and its use are strongly regulated with multiple existing frameworks governing what data can be accessed and circulated. At the same time, the housing market faces open questions regarding the efficacy of legislation in practice to prevent discriminating behavior, for instance by considering the opacity of selection criteria that landlords and housing corporations use to choose candidates. Furthermore, data sharing in the housing market is a lived reality for virtually anyone, making it a tangible example for citizens to discuss their perceptions of data sharing.

# 3 Why public standards for data sharing?

How can we involve the public in the design of data sharing infrastructure and data sharing standards? Standard-setting is a highly technical activity that many Dutch people are not aware of according to a recent survey on people's awareness of standardization procedures for internet infrastructure in the Netherlands.<sup>24</sup> Public involvement in standard-setting usually takes the form of participation by experts and professional organizations with differing degrees of openness of such processes.

In contrast to this kind of public involvement, in this section we present our proposal for the development of public standards. **We define a public standard by its ability to recognize and accommodate the concerns of groups that are directly or indirectly affected by the standard.** Because these concerns cannot be adequately grasped without involving affected groups, the development of public standards must by definition also be public and participatory. We argue that public standard making is important to address a key problem for standards: the tension of balancing their general design with situation-specific problems people may encounter. Importantly, a public standard for data sharing differs from an open standard. Open standards are reusable agreements that make it easier for people and organizations to publish, access, share and use better quality data. A key defining criterion of an open standard is its availability for anyone to access, use or share.<sup>25</sup> The difference between a public standard and an open standard is therefore the orientation towards the concerns of affected groups. A public standard can be open if it is openly licensed and aims to be reusable, but it does not necessarily have to be open. Our concept of public standards reflects Waag's approach to public research, which is oriented towards addressing public problems and concerns together with members of the public.<sup>26</sup>

---

<sup>24</sup> See also: Driessen, M, M Van der Koppel, D Hollander, S Milan, J De Vos, and N Ten Oever. 2024. "Publieke Waarden Randon Digitale Technologieën." NWO. [https://in-sight.it/assets/IN-SIGHT\\_Publieke\\_waarden\\_rapport\\_NL.pdf](https://in-sight.it/assets/IN-SIGHT_Publieke_waarden_rapport_NL.pdf).

<sup>25</sup> The ITU, the United Nations specialized agency for information and communication technologies, provides the following definition of open standards: "Open Standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus-driven process". Available at: <https://www.itu.int/en/ITU-T/ipr/Pages/open.aspx>

<sup>26</sup> We also take inspiration from similar work, such as: Gray, J., & Lämmerhirt, D. 2019. "Making Data Public? The Open Data Index as Participatory Device". In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good Data*. Amsterdam: Institute of Network Cultures. Available at: <https://zenodo.org/records/5515197>

Ananny, Mike. 2024. "Making Generative Artificial Intelligence a Public Problem. Seeing Publics and Sociotechnical Problem-Making in Three Scenes of AI Failure." *Javnost - The Public*, January. <https://www.tandfonline.com/doi/abs/10.1080/13183222.2024.2319000>.

### 3.1: How does public standard making differ from existing user research?

It is important to mention that there has been a significant amount of research regarding data sharing preferences in The Netherlands. Some of this research was conducted in the context of the Control over Data program, while other research stems from academic research. This research has primarily explored citizen attitudes towards data sharing in the context of The Netherlands, how citizens perceive data sharing mechanisms in the context of applying for a mortgage<sup>27</sup>, and citizens' views on using an app to share data when applying for a rental property<sup>28</sup>. Here, we briefly explain the insights from this research, the lessons for our work, and how our method for public standard making differs from existing research.

In a survey using three 'interaction patterns' for data sharing (a wallet, a gate and a source pattern) Van de Poll et al. assess which model for data sharing respondents would prefer. The study focused on home owners with a mortgage. Respondents were asked to pick the two most and two least important aspects of data sharing from a list consisting of nine aspects. This quantitative research design makes it possible to generalize findings but limits the possibility for respondents to add their own concerns, or reflect on their experiences. Being a qualitative study, our approach leaves more room for placing concerns and preferences in context. For example, Van de Poll et al. (2021: 10) conclude "that trust and safety are crucial" in the context of data sharing, but offers little context as to why respondents find this important. What is more, the report does not reflect on the types of data that respondents feel comfortable sharing. By asking workshop participants about their experiences with the sharing of personal data in the housing market, one of our main findings was that buyers do not only want the data sharing process to be safe, but they also want more transparency in regard to why different types of personal data are required and how decisions (e. g. about granting a mortgage) are made on the basis of this data. The possibility to provide context during the conversation was important in this regard, as these concerns surfaced while participants were reflecting on different data sharing scenarios.

User research by Mare has focused on data sharing in the context of housing. Their qualitative research design (interviews) allows for a more in-depth assessment of respondents' views. However, this research mainly focuses on citizens' experiences with one concrete data sharing app (MyQii), rather than asking how people think about data sharing more generally, or how people's perceptions about data sharing differ between parts of the housing market, such as the free market, the real estate market, or social

---

<sup>27</sup> Van de Poll, Machiel, Petra Immerzeel, and Dylan De Mots. 2021. "Digitaal delen persoonsgegevens van burgers." Rapport. Ministerie van Algemene Zaken. October 13, 2021. as well as Van de Poll, Machiel, and Dylan De Mots. 2022. "Regie op gegevens: Welke burgers zien het digitaal delen niet zitten, en waarom niet." Rapport. Ministerie van Algemene Zaken. October 13, 2022.

<sup>28</sup> Mare. 2021. "Evaluatie Gebruikeronderzoek Qii - in Opdracht van Mens Centraal." Amsterdam.

housing. While some of our findings align with those of the Mare report, e. g. DigiD being perceived as a marker of trust, we find that citizens hold more nuanced views when it comes to the sensitivity of data. For example, the Mare report states that, after having submitted their data through the MyQii app “citizens do not question what happens to their data afterwards, or who is responsible for managing or updating them”. In our research, we found that citizens are actually more critical: they often wondered where data is stored and which parties have access to it. What is more, they hold nuanced views about which categories of data they feel comfortable sharing and for which purposes.

The Ministry of Interior and Kingdom Relations has recently financed legal and technical research into the feasibility of personal data sharing in collaboration with the ICTU and the Zorgloos Vastgoed Foundation. This project has built on earlier research to argue that personal data sharing from governmental data sources should safeguard privacy and ensure ease of use.<sup>29</sup> The project advised against conducting further user research and relied on fictitious user personas to develop a technical concept for a data sharing architecture. The final report advises to further develop a data intermediary and the data rights it grants different stakeholders, as well as to include update upcoming legislation such as the second part of the Law for Digital Government (Wet digitale overheid). Effectively, this would mean that citizen perspectives are excluded from further developments. We show that this would foreclose important concerns citizens have when sharing data.

---

<sup>29</sup> See Sharma, S. 2024: “Proeftuin Regie op Gegevens met Zorgeloos Vastgoed”. Available at: <https://rog.pleio.nl/attachment/entity/56db3a5a-06f5-409a-9bee-09c494f16ceb>

## 3.2 Our method: Documenting people's concerns around personal data sharing

As mentioned earlier, people's data sharing preferences are relative. They depend on the actors who may process data, the actions that are possible on the data, and the broader use purposes of data processing. Existing research either considers data sharing preferences to be stable, or it only considers some aspect of data sharing (e. g. general perceptions of data sharing). We propose a method that considers all four aspects, combining a focus group setting with the scenario method.

We assembled focus groups with 18 participants, including tenants in the free housing market (group 1, n=6), the social housing sector (group 2, n=6) and home buyers (group 3, n=6). To begin our discussions, we asked all participants to individually reconstruct and document their data sharing experiences when looking for a house in the last 2 years. Afterwards we had a discussion about what they felt comfortable and uncomfortable with. This provided insights into how people currently consider data sharing in the housing sector. We closed this discussion with individual reflections by our participants on the three most important requirements they have when sharing personal data.

Afterwards we wanted to understand people's opinions about existing data sharing apps and their broader data sharing setups, using the scenario method. The scenario method is a well-established qualitative research method. It uses (often written and fictitious) descriptions of an event that are related to the research topic and that can gather responses by research participants. Participants are asked to respond to these scenarios in order to understand their perspectives on the scenario and their values. In our case, we developed two fictitious scenarios for tenants and for home buyers that included:

- Data being accessed and processed
- Actions on data (such as filtering, scraping, copying to receivers)
- Actors (such as government data sources and data receivers)
- Purposes (the overall context for which data was used, such as a tenant lottery)

All scenarios can be found in the appendix. We based the scenarios on existing data sharing apps (a gate and a wallet app for the Dutch housing sector), existing data that is being processed by these apps, as well as existing use purposes. We designed the scenarios in such a way, that they can reflect a common experience of our participants and so that they allow for discussions of concrete data sharing experiences and data being shared. In each workshop we asked participants three questions:

- What are your first reactions when reading this scenario?



- What aspects of the scenario align with your personal requirements for data sharing?
- What aspects of the scenario conflict with your personal requirements for data sharing.

By following this approach, we found that using scenarios can create awareness among participants about how data sharing works and whether they support the arrangement or not. While many participants told us that they do not think about data sharing in the moment, they changed their opinion about data sharing when they were asked to reflect on their experiences and our scenarios. This is reflected in statements such as “Now that I know how it really works, I don’t like it”. We also found that people are able to uncover issues with past data sharing activities. Because we asked people to search for data they had shared through different submission forms and portals, we found that these portals often still store data about people.

# 4 Results: Experiences with personal data sharing

## 4.1 Experiences with existing personal data sharing mechanisms

In the following we present the experiences of our three user groups with data sharing when searching for a house. All three groups perceive that data sharing is opaque and that it was unclear what happens to their data after they submitted it, who can access it, how long it can be stored for, and how it is being secured. Tenants reported to share a wider variety of data with landlords and housing corporations, while home buyers reported more uniformity in terms of categories of data shared. For example, buyers all submitted data such as their identity document, paychecks for the past three months and an employer's statement. The group of housing aid recipients differed primarily with regards to eligibility rules for social housing.

### **Personal data sharing: currently not an act of control, but a requirement to access housing**

Tenants do not see data sharing as an act of control, but as a requirement to access housing. All of our interviewed tenants were renting on the free housing market. The housing crisis and a scarce housing supply framed their perception of data sharing. A participant put it succinctly:

"I do have a lot of things where I thought, well really, what the fuck, that this has to be done. But I honestly didn't think twice about it. Because it's such a competitive world, [...] that I thought yeah, I have no other choice."

The structural power imbalance of the housing market, and competition among home seekers, influences people's perception of data sharing as a requirement. Therefore, a tenant and a subsidy recipient said that they would share more data than asked for (for example personal motivation letters) to be considered as tenant. They also reflected on the ability to "play the system": if you know how it works, it is easier to send additional information to help your application. An expat tenant remarked that this also puts them at a disadvantage: it is often unclear how the renting process works, or where to find particular data which is considered to be standard in the Dutch context. Some said that withholding data can be interpreted against one's favor because one could count as a "difficult tenant". Several participants mentioned that they share more data than they deem to be necessary. Some felt that mortgage brokers can easily ask for too much data because they know that prospective buyers really want a house. Some housing aid

recipients said that applying for a house is a stressful process, making them willing to submit all kinds of data:

“I wanted that house really badly. I was actually very scared that it would not happen. Because that had happened to me before with a house owned by a different cooperation [...]. So I was actually willing to... Well you can know everything about me, if I can have that house.”

As the example above illustrates, this can mean that people are willing to personal data out of fear that they will not be allocated their preferred home. People share data to create trusted relations with a landlord and to stand out among competitors. This means that participants data sharing is not a matter of individual choice. Participants may deprioritize concerns around data sharing out of enthusiasm for their prospective house, the necessity to stand out among others, and the simple difficulty to refuse sharing data. Therefore, people accept sharing “weird” data such as information about one’s wish to have children, personal reasons of moving to a new place, or the current civic and marital status. As one tenant said:

*“I just want to have a house and if this is necessary, I will do it. I did find a lot of things weird. So, for example that they asked things like ‘are you planning to have children in the next five years?’”*

Because data sharing is considered as a necessary means to access housing, many of our participants report that they do not question or take issue with data sharing in the moment of applying for housing. Participants often felt that they were in a position of dependence, as they were very eager to buy or rent a home, and actors like mortgage lenders or property developers are able to pick and choose from a large pool of applicants.

**Data: income data of relatives, historical data, ID data of birthplace and nationality particularly sensitive**

Most of our participants remarked that they thought about the issues with existing data sharing setups retrospectively in our workshop, rather than in the spur of the moment. Many of the participants pointed out data they found problematic to share when we asked them to reflect on them in hindsight.

In the tenant group, sharing data about people one has a close relationship with was considered to be sensitive. Particularly problematic was the sharing of income data from relatives who are vouching for one’s ability to pay rent. The participants were mostly in their early career and therefore had to share income data from their parents to indicate their ability to pay rent. Our participants considered income to be a taboo topic they usually do not speak about with relatives. This becomes especially an issue when data-

sharing channels enabled participants to access and see data from relatives. For example, one participant reported feeling uncomfortable sharing her father's payslips over email because then the data is also available for her to see.

In the group of housing subsidy recipients certain types of data were considered to be "normal" to ask. For example, one participant recalls having to submit identity data, where she rents at the moment, how long she has lived there for, whether there is any rent overdue and proof of "whether she is a problematic tenant", when looking for a new place to live. One participant mentioned that she needs to submit updated landlord statements (verhuurdersverklaring) and a BRP certificate every three months to keep receiving housing offers. Here, the issue were costs for requesting an updated BRP certificate, considering the financial circumstances of housing aid recipients falling into the 'low income' bracket.

### **Actors: A variety of platforms and data sharing media, little perceived control options for personal data**

When applying for housing, tenants and home buyers reported that they often share data with many different parties via multiple channels. They share personal data with individual landlords, housing corporations, and brokers through platforms such as Funda, Pararius, Woningnet, or Rentslam, but also by email, WhatsApp, and other communication channels. Our participants reported that they sometimes lost track of the different portals: there were too many to keep a good overview of where data ended up and how long it would be stored there. Because the landscape of data sharing technologies is perceived as scattered and involves many parties, participants were concerned where their data ends up, who has access to it, and what is being done with the data.

One problem is the need to submit data to multiple parties, for instance by creating unique personal accounts and profiles with each party, instead of using one central account. One tenant gave the example of the Rentslam platform which required her to create accounts with different housing providers, including housing brokers and corporations and had to leave her data in each account. When discussing this case, the participating tenants argued that this may increase risks of data leaks but it also makes it less easy to follow where one has submitted what personal data. Even though the buyers reported that they felt uncomfortable using channels like email and WhatsApp, they did not usually protest to using them. The reason for this was that they often felt that speed was of the essence in order to arrange a mortgage or participate in a lottery.

Another common problem was the loss of control over data when people are asked to submit sensitive data via communication media, such as email or chat apps like WhatsApp. Our participants said that they found it particularly problematic to submit sensitive data such as one's passport over these media. Participants thought that these media offer no control over the data once it is sent. One can only ask a recipient to delete the data but cannot be sure that this will actually happen. Our participating buyers

argued that they cannot be sure what happens to their information if it stays “in the back of someone’s inbox” and there are no means to remove this information or exercise control over what the recipient uses it for.

Some participating home buyers accept existing data sharing channels even if they are perceived as unsafe because they allow for quick reactions to real estate postings. Because of this, they sometimes noted feeling a sense of hypocrisy, as they did not always act in line with their values and preferences. For example, one participant remembers sharing personal data over email, even though he would prefer using encrypted channels. As he puts it: “I know how it should be. But I send lots of stuff through email. Because you want to do it quickly. You want speed, if you have the momentum”. Another person reported that she used the platform Rentslam to be able to respond to new house listings by sharing pre-filled data about herself as fast as possible.

Some participants think that sharing data through an ‘intermediary’ that enables control options is a better option. One option that was considered more trustworthy was a portal where people store personal data and can control who has data access. One participant argued that a portal would be a good alternative that allows for data sharing with several people and companies without the need to upload data anew and with time-limited access. Another example that participants mentioned was DocuSign. They used it as an alternative for physical contracts during the Covid-19 pandemic. The program felt more secure as the responsibilities were explained, and it was made clear that signing in this program had the same legal status as signing a physical document. In other words, more transparency about data flows, storage and usage could make buyers feel more secure.

Participants were concerned about the increasing number of parties that may process sensitive data in the housing sector and beyond. One particular concern revolved around the possibility that medical data could become part of the data used to allocate housing to people in the social housing sector. Some participants were particularly worried about a new legislative proposal<sup>30</sup> which would allow increased data sharing between housing corporations and healthcare providers and municipalities (which, in special cases, would be allowed to share medical data with a housing corporation). One participant was concerned that this could lead to more precise profiling and categorization. This means that the actors and permissible actions are not clear to participants and the expansion of data sharing parties in the housing sector is considered problematic by some.

### **Actions: long-term data storage as a problem**

Regarding the permissible actions on data, many participants remarked long-term data storage as a problem. Because we asked people to reconstruct their application process

---

<sup>30</sup> See <https://www.internetconsultatie.nl/gegevensuitwisselingwoningcorporaties/b1>

and find again the data they have shared with others, we found that many of our participants were able to find back data, sometimes several years after the application process. One tenant participant was surprised about this:

*“Yeah, I think so...if I really... I have to say, I haven't really thought about it lately. But if I really think about it now, I think it's a strange idea. Because there's really a lot of me in it.”*

When looking up the data they shared in the past, some participants were surprised to see that data is still available after several years. Another home buyer accessed the online portal that she used to upload data for her mortgage broker during our workshop. After two years, her personal data was still accessible to view. The participant remarked being shocked to see this, as she did not expect this still to be available, and she had used “her easiest password” for the online portal. Furthermore, she felt that the portal felt unsafe, as it did not have two-step verification and it looked dated, or, as she put it, “had a 2000s feel”.

In the housing subsidy group, one participant mentioned that his housing corporation stores a digital copy of a file about him that goes decades back, showing that he was two months behind on rent in 1986. While it did not affect his eligibility for housing today, this participant did feel uncomfortable that this information is stored for decades. One tenant shared an anecdote that she received invitations for house viewings long after she had found her most recent place. Sometimes, people’s worries over data storage are linked to security concerns, as the portals used to share the data did not inspire confidence. The participants want to have information on what happens with the data that is being stored there for so long.

Aside data storage, some participating tenants expressed their preference for data sharing in phases. They didn’t think it is nice that they are asked to submit various data before they know that they are eligible for a place. Others compared the house search process with a job application and said that they would like to receive a response from the organization one is applying with and also to learn what happened with the (sensitive) data after the selection process.

### **Purposes: Unclear about who receives what data, for what purposes**

Our discussions with participants show that they consider data to be sensitive in connection to concrete use purposes. Participants do not have sufficient information about these use purposes to say if data sharing is justified or not, such as a landlord’s selection criteria for tenants. Participating tenants asked why they have to share data that they cannot directly relate to renting, such as one’s civil status, or one’s level of education as documented on a diploma. One of the main issues that the buyers pointed out, is unclear why particular documents need to be submitted, and how they inform

decisions about receiving a mortgage or participating in a lottery. Having to submit information like full address history or degree certificates is not understood: participants feel that this information is irrelevant, and can easily abuse to unjustly select “desired” buyers. They remarked that, in their view, the only piece of information that should really count, is proof that the prospective buyer is able to afford the house. However, it turned out that even that is subject to various interpretations. One participant recalled asking two different banks for a mortgage, and feeling this was a very opaque process since both banks assessed her creditworthiness very differently.

Our participants were concerned with the fairness of selection criteria and argued that these should not unduly give preference to some group. If selection criteria are considered to be fair and objective, participants considered them to be less problematic. The tenant group for instance said that a lottery where everyone supplies the same data is considered fairer because people assumed that everyone is judged by the same standards and that the selection criteria are clear. By contrast people judged the requirement to earn four or five times the requested rent as unfair. They argued that it is not good to submit pay slips, because one might be rejected based on the salary. Sometimes, our participants thought that the multiple meanings of data can work against their interest because they allow for discriminatory use cases. The participants discussed housing history data and agreed that it is in itself not problematic to share this data, but that it is also not clear why sharing such data is necessary. Some people wondered if people are judged by the addresses where they lived and are more preferred, or whether they could be classified to have lived in a “problem neighborhood”.

Our participating housing subsidy recipients were unclear about how housing allocation works via platforms like Woningnet. They described these as opaque systems that does not make clear why particular housing options are presented to them to apply for. In response to the question what their data are used for on Woningnet, one respondent replied “I wish I knew. I will say control and selection criteria”, to which another participant replied “these data are also used to see which place you get. They are used for the algorithms on Woningnet”. Trying to understand the system, one participant mentioned contacting Woningnet asking how prospective tenants are categorized and offered housing they can apply for. The organization never replied. Another participant mentioned that he helped people who are not able to understand the language (“jargon”) used, or do not have internet at home. This makes it difficult to use Woningnet regularly, and it affects the ability of social housing applicants to collect points by reacting to social housing offers.

These examples indicate that there are concerns about decision-making processes on several levels. As some participants pointed out, while having more control over who accesses and uses their personal data would be desirable, it would not fundamentally shift the unequal power relations that opaque decision-making processes brings about. In other words, having control over the sharing of data alone, does not change the fact

that buyers do not know what their data is used for and how decisions are being made on the basis of it. It is important that participants are critical about data sharing if the use purpose is not obvious and may think that it supports unfair or discriminatory selection processes. Besides providing more information about decision-making processes and how data are relevant for these, standards for data sharing also need to provide confidence that data uses do not treat housing market participants unfairly.

## 4.2 Scenarios of data sharing alternatives

### Scenario 1 (Tenants and social housing aid recipients)

#### **Data: historical data, birthplace, and nationality are problematic to share**

When being asked about their opinion on the shared data, tenants found it problematic to share historical data like proof of income over the past year. They argued that this data is subject to change and may therefore no longer reflect someone's current situation, which can work to their disadvantage. One participant reflected: "what if I signed a permanent contract last week, and I suddenly receive an amazing salary. Well... then it should not matter what I earned over the past year". The housing aid participants agreed that nationality and place of birth are unnecessary categories of data in this context. They felt that this type of information could easily lead to discrimination. As one participant remarked:

"In every other thing you need to add your place of birth. I do not like that. Why do you have to do that? Is that applicable? What if I say, I was born in Paramaribo, and they say: 'oh no, we don't want that here'".

Participants also argued that sometimes *not* enough information was taken into account in the context of applying for social housing. One participant mentioned that it is sometimes problematic that people are asked for their income, but other factors such as personal savings are not taken into account. This can mean that tenants are not eligible for more expensive housing even though they would be able to afford it. In other words, people were not only concerned with submitting *less* data, but with submitting the right data that can adequately reflect their personal situation. By contrast, our participating tenants argued that a standard set of the same data would level the playing field, as this would make it harder to use certain circumstances (e. g. a personal relationship with the real estate agent, or sending additional information like a letter of motivation) to their advantage. While some participants supported the idea to be able to share additional data to reflect one's situation, others said that this could lead to unfair advantages.

**Actors: data intermediaries can lower costs, and control access to data, but commercial data intermediaries are less trusted**



Generally speaking, the involvement of a data intermediary was perceived positively, as this would mean that housing corporations do not have access to all data in government accounts. However, the participating tenants would prefer government-owned intermediaries over commercial ones. The main reason for this is that commercial apps are considered to be less trustworthy, as the participants do not know their business model and fear they may have a profit motive. One participant remarked: "I don't like the idea of this. I actually do not want a commercial party to have this kind of data. Or have access to it".

Housing aid recipients argued that it would be helpful if a data intermediary like DataSafe app would mean that tenants can access BRP certificates for free. They also supported the idea that housing corporations would use this app to request data. However, some participants felt that the purpose of the app was not made clear enough; they want more information about what it is and why it is necessary. Or, as one participant phrased it: "I am wondering what it is for; does it make easier, is it to save money or reduce staff costs? Yes, it reduces staff costs. But where does the data go? And how can we check this?" In addition, they would also like to know where the data go once removed; it should be made clearer how this works from the outset.

#### **Actions: Authorization of a third-party and scraping feel like loss of control**

Participating tenants found it problematic that the DataSafe app logs in on behalf of account holders. Participants felt uncomfortable with a system that was pretending to be them, and would prefer to upload their personal data themselves. The group of housing aid recipients also questioned the data access and sharing model of DataSafe app. Social housing tenants felt uncomfortable with linking different services, particularly different parts of MijnOverheid, as it is unclear which data are scraped, and which government accounts the app would have access to. The housing aid recipients wanted more control over the data, for instance by uploading the data themselves.

Similar to the other groups, the participants did not feel comfortable with scraping. One participant termed this "Big Brother", and argued that prospective tenants should be able to select the data that they are sharing. What is more, participants remarked that scraping made them feel vulnerable: they were wondering how safe this process is, and what would happen if the app got hacked. They were concerned that hackers could copy and save their data.

#### **Actions: Authentication via DigiD suggests trustworthiness, but may mislead users**

Relatedly, they remarked that this set-up could also be misleading to users, as DigiD is perceived as a marker of trust: participants feel that they can trust this system, because it is a government portal. However, they speculated that prospective tenants could mistakenly put their trust in the app, because - if the role of DataSafe is not made clear - they could incorrectly assume that it is also a government app. One participant said: "Yes, we know it is a commercial app. Maybe other people don't know that because they

log in with DigiD. I think that's just a... Yes, or you have to make that very clear". They therefore think it essential that future data sharing set-ups should make the different parties involved visible.

**Actions: Authentication via DigiD may suggest mistrust in users**

A third issue with this set-up was that some participants felt that this conveyed a lack of trust in tenants. As one participant put it: "I just think it is very annoying that they have to check my DigiD to believe me based on my documents, which I can also send myself. Because that is what this is actually about: what they want to know here are minimal data that I can easily send myself, but apparently they don't trust me enough. So they want to verify through my DigiD". In other words, they felt that the need for verification reveals a lack of trust in tenants, as it presupposes they might not speak the truth or purposefully submit false documents.

**Actions: Seeing and choosing what data is being transmitted is desirable**

Participants felt that the filtering process of the DataSafe app is very opaque: it was unclear how this mechanism works, why all data need to be scraped before they can be filtered (rather than only uploading the necessary data in the first place) and which data are actually necessary for the housing corporation's verification process. The tenants argued that it should be made clear which categories of data can and cannot be accessed by the DataSafe app in their personal accounts.

Others suggested the need to share a set of basic personal data: "a minimal set of data where it also makes sense to the user why this is necessary". This could improve the trust of tenants in the system, as becomes clear to them why certain data is necessary. In relation to this, one participant mentioned that she would feel more comfortable if different categories of data were to be assessed separately and step by step, rather than a landlord reviewing them all at once to generate a profile about her. Here, the uploaded data can fulfill base criteria - e. g. proving that one earns enough to afford the rent – without connecting this to their identity as a tenant. In addition, some participants felt that this way of asking for data is too rigid: it does not leave enough room for nuance, as people are not able to adjust the data themselves (as the data are extracted automatically). As such, they would prefer if corporations would ask them for the data directly, specifying what is needed and for which purposes.

## Scenario 2 (Tenants and social housing aid recipients)

### **Data: historical data are seen as unnecessary**

In terms of data, participants were adamant that a complete address record and employment history are unnecessary, as they feel this is irrelevant and could be used to someone's disadvantage. Similarly, nationality and place of birth were considered to be unnecessary and "weird". As one participant reflected with reference to place of birth: "who cares? I could accidentally have been born in an airplane [...] I find this very weird".

Among housing subsidy recipients, participants understood the need to provide some sort of proof that they would be able to pay rent. However, they felt that a complete address history is not relevant, as they did not see what this would prove. They also considered bank transactions were unnecessary, because it was not clear to them why and how these would be used. Some also felt uncomfortable an employer's declaration (werkgeversverklaring), because this means that their employer would know that they are looking for a new place to live. In other words, it is important that the data that tenants need to submit feels necessary in light of their application.

### **Actors: government app is preferred because it is not associated with profit motives**

Participating tenants supported that the MyData app was provided by government. They assumed no "monetary relation" between the app and VGW Housing Group, which makes them trust the process more. Another participant mentioned finding it "annoying" when an intermediary (like in scenario 1) is "earning money off my data", and trusts that the government does not have this motivation. The tenants were wondering, however, whether the app is used by all different housing groups. If the same app could be used for all applications, they remark, it would be very efficient.

### **Actions: control by uploading data oneself and by limiting data access over time**

The tenants preferred this scenario over scenario 1, with some of them pointing out that this is "a great scenario". They felt that uploading their data themselves is better - as one participant put it: "you're actively involved. You are performing the action yourself. This also gives one the feeling of still being in control. Instead of it all being submitted automatically".

All tenants agreed that the fact that data can only be checked for 14 days is a good option, particularly when this is communicated from the start: this feels transparent, and reassured the participants that their data would not be used for other purposes. For them, the MyData app feels safer than using channels like email, particularly because the app puts limits on the amount of time the data is available for, which is not the case when sending information over email.

Among the housing subsidy recipients, participants did not trust that VGW housing group would really only be able to read the data for 14 days. They mentioned, for example, that there was no way for them to check whether this is indeed the case, and some were afraid that the housing cooperation would still be able to copy the data. One participant mentioned that it is unclear what “safely stored” entails, and that an explanation is required.

“Very often it says, when you call an institute or something asking to what extent the safety of data is guaranteed [...] ‘No, you don’t need to be afraid, we are storing it safely’. But if I ask ‘how do you do it?’, they don’t know. [...] But I want to know why!”

### **Actions: proof of oversight over data intermediaries is desirable**

Some of the housing aid recipients thought that the organization that is responsible for storing the data should provide responsive customer service, also via phone, to be able to explain to users what they do with their data: “I need to have trust in the organization [...] That if I phone them up, they can say how it works, ‘yes, your data has been removed, no, we can’t see anything anymore’”. One participant made a comparison with job platforms, which send an email at the end of the year, asking whether the person who applied is still happy for the platform to store their data; a similar mechanism would increase their trust in the system. Other participants said that there should be proof of oversight (such as via the Autoriteit Persoonsgegevens) that is actually checking whether data is indeed only stored on the app. They mentioned they would feel more comfortable if they had more assurance that their data is safe.

### **Purposes: tenant selection via lottery is controversial**

In terms of the lottery process, one participant remarked that it is important that all applicants submit the same set of data (rather than, as she put it, having the opportunity to add additional or ‘fake’ data), so that the process is fair. In other words, a standardized data sharing process is seen as a way to render access to opportunities more equal. In contrast to the other group of renters, some of the housing aid recipients felt that a lottery is not objective: they were afraid that desirable candidates would be pre-selected. Interestingly, several participants compared this process to a state lottery:

“Look, a house is not a state lottery...where you either win the grand prize or you don’t. So I am against that. And based on an income check, that is also only beneficial for the landlord. And they can pick who they want...well they select based on income. So they will only want working people who have an income.”

They felt that a house should not be a prize and agreed that the selection criteria for the lottery are unclear which could lead to discrimination. In addition, as the quote above also shows, several participants argued that this system is tailored to the interests of housing corporations rather than citizens. This, they argued, is because they are requested to

submit their personal data upfront, while it is not made clear what these data are used for, and what happens to the data of those that are not eligible to participate in the lottery. Therefore, they suggested that there should be several data sharing moments; where some data should only be shared after someone has been selected (e. g. through the lottery system).

### Scenario 3 (Buyers)

#### **Data: minimizing data access only to those data needed for a specific purpose**

Within the buyers group, people argued that data should not be shared if it can be interpreted in multiple, and potentially discriminatory, ways. For example, one of the participants suggested that the selection criteria for a mortgage could be made more objective by limiting the data in such a way that multiple interpretations from the data are prevented. “If an application uses the right data points, you can create objectivity by...leaving out certain matters. If I had not been born in the Netherlands, for example. Someone is looking at this information. They will think something about this. This person was born in the Netherlands. This person is not”. Then, this participant argues, the mortgage broker makes a decision coming from their own perspective – even though nationality should not be a relevant factor. Therefore, he suggested that data that can be interpreted in multiple ways, should be avoided.

#### **Actions: scraping and filtering of data post-retrieval feel like a lack of control**

Similar to the two tenant groups in scenario 1, the buyers reviewing this scenario remarked that it is unclear how the scraping and filtering process works. They did not understand what exactly is being filtered, and did not like the fact that an algorithm could do the filtering. Rather, they would prefer to submit the data themselves. Buyers reported not knowing what scraping entailed, but once our researchers explained the mechanism, they felt uncomfortable with this process. This suggests a lack of knowledge and awareness around data sharing mechanisms, which impacts people’s ability to make informed decisions about data sharing.

#### **Actions: automated data retrieval is interpreted as distrust against users**

Another similarity was that some buyers interpreted the automated access to source data as a sign of distrust, as they felt that they were not trusted to speak the truth (which would translate into uploading the data themselves). What is more, they feel that this conveys a lack of transparency, as they are not being told what the real purpose of the app is. In other words, they perceived this verification process - in which they do not have an active role - as not being seen as trustworthy. This flips around the narrative that people do not trust the app: rather, they think that the app (and recipients of the data) does not trust them.

#### **Actions: preference for step-by-step data sharing, only for specific purposes**

Some participants supported the idea that instead of gathering all data, the app could gather and submit data step by step. This would be in accordance with the processing purposes of verifying someone. Here, it would be preferable to upload a minimal set of data to check eligibility, before asking to submit more detailed data.

**Actors: Fear of data sales by commercial intermediary, preference for a government-owned app**

The participants considered it to be problematic that a commercial intermediary would have access to key government portals and people's accounts. Similarly to the two tenant groups, people were concerned about the profit motives of a commercial data intermediary. The participating buyers would prefer using a government-owned app. While they liked the fact that the mortgage broker could only access the data for three months, it was unclear whether the DataSafe app would be able to store the data for longer. Some participants imagined that the app could sell the data. This arguably shows that a lack of transparency about the workings of data-sharing processes leads to speculation about possible underlying data processing motives.

Scenario 4 (Buyers)

**Data: historical data are considered to be irrelevant**

One thing that stood out to the buyers, was the requirement to submit two year's worth of bank transactions. They felt very uncomfortable with that as it was not clear to them why this information was necessary, and did not want the parties involved to have access to all their transactions. When our researchers explained that transaction data only refer to income from an employer, they considered the scope of two years irrelevant. Furthermore, participants agreed that education certificates, address history and work history were irrelevant. Particularly education certificates were a point of discussion; participants questioned the value of judging a person based on their academic degree, pointing out that this does not guarantee a high income. This shows again that participants tend to imagine possible reasons and justifications for data use when it is unclear how the data-sharing or decision-making process works.

**Actors: preference for government app**

The buyers agreed that the MyData app is preferable app was developed by the government (as opposed to a commercial actor). One participant did ask why they need to upload it themselves at all, considering this is a government app. One of the questions that came up was whether all involved parties (e. g. mortgage broker, housing projects) use the same app to request the necessary data. They suggested that, for efficiency reasons, it would be helpful if all parties could use the same channel, and that for privacy reasons, the app should only grant access to the data necessary for a specific purpose.

**Actions: Self-upload of data and read-only data access are seen as positive**

In general, the participants agreed that the fact that the mortgage advisor can only read personal data for 14 days, was positive. Some remarked that this adds some pressure on the side of the mortgage advisor, and could therefore contribute to speeding up the process. One participant, however, was skeptical as they felt that this would give the advisor too little time and this would only result in prospective buyers having to upload their information multiple times. The participants agreed that generally speaking, uploading data themselves would be better than the data being scraped. However, one person mentioned that this does presuppose a lot of trust in the devices (e. g. phones) that are used to download the data from government portals.

# 5 Conclusions and recommendations

In this study, we asked how citizens can gain a voice in the definition of standards for personal data sharing. We proposed the idea of **public standards** as a framework for translating people's concerns about data sharing into concrete requirements such as data sharing standards. Using personal data sharing in the housing market as a case, we asked the following research questions:

1. What interests and expectations do citizens attach to sharing their data with different services in the real estate sector when using data sharing tools?
2. What requirements for a public data sharing standard arise from citizens' interests and expectations?

Developing public standards together with citizens is important for several reasons. As our findings show, citizens perceive data sharing within the context of unequal power relations as a requirement to access housing. Within this context, most respondents said they are in a position of dependence and must provide data. Our report shows that participants have nuanced ideas about different aspects of data sharing standards. They deem specific data irrelevant or sensitive, including historical data or birthplace. A significant finding is the common experience that existing data sharing setups, including gates and wallets, are perceived as opaque. Neither the involved actors, nor the data processing for housing applications are understandable to citizens. Our participants prefer more control options for their data and, if they would need to choose between data intermediaries, gave preference to a government wallet as opposed to a commercial gate app.

Below, we summarize these experiences and connect them to relevant aspects of data sharing standards. Afterwards, we provide recommendations for actions that policy-makers and IT-developers can take to respond to our conclusions.



Element	Experiences of citizens	Recommendations for data sharing standards
Data	<ul style="list-style-type: none"> <li>- Historical data are seen as irrelevant to determine housing eligibility</li> <li>- ID data: place of birth and nationality are considered to be particularly sensitive and may enable discrimination</li> <li>- Personal data of relatives are sensitive</li> <li>- Data access should be minimized only to those data needed for a specific purpose</li> <li>- Medical data is seen as particularly sensitive</li> </ul>	<p>Implement data schemata at the data source that require querying personal data points individually (e. g. "birthplace" instead of "ID data") and only for limited time-frames;</p> <p>Define data schemata that minimize risks of harmful interpretation, for instance by using attribute-based credentials;</p> <p>Communicate not only what data is being accessed, but also how data is being used, for instance to select prospective tenants.</p>
Actions	<p>Building a relationship of trust is important:</p> <ul style="list-style-type: none"> <li>- It should be clear to users if an app is run by government or a commercial party. Commercial data intermediaries are less trusted</li> <li>- The relationship between DigiD and a data intermediary app should be clear to avoid misleading users</li> <li>- Users can interpret the need to identify themselves via DigiD as mistrust</li> <li>- Users can interpret automated data retrieval as mistrust</li> </ul> <p>Third parties should not be able to:</p> <ul style="list-style-type: none"> <li>- Scrape and filter data from (government) portals as this feels like a loss of control to citizens</li> <li>- Store data long-term</li> </ul> <p>Citizens see more control options over data, provided that they are able to:</p> <ul style="list-style-type: none"> <li>- Have access to copies of personal data (such as BRP certificates) at no cost</li> <li>- See and choose what data is being transmitted;</li> <li>- Upload data oneself;</li> </ul>	<p>Provide information about the ownership of a data intermediary and the relationships between government data source and intermediary</p> <p>Provide a point of contact that can explain how data is being processed;</p> <p>Provide information why identification/ authentication via DigiD is being used;</p> <p>Define API access with modular permission scopes (see recommendation on data schemata above) that enable citizens to give access to specific data points;</p> <p>Provide users with options to limit data access to a specific time-frame or by giving read-only access to data;</p> <p>Decouple data uses from one another (e.g. ID-verification; proof of income) and provide data access step-by-step and only for each specific data use</p> <p>Provide users with the option to download/upload data manually;</p>

	<ul style="list-style-type: none"> <li>– Have a proof that data intermediaries are adhering to regulations and oversight;</li> <li>– Be able to submit data step-by-step, in connection to specific purposes</li> </ul>	Define accessibility requirements for no-cost access to BRP data, including certified digital copies.
Actors	<ul style="list-style-type: none"> <li>– Involving a variety of platforms and data sharing media limits citizens’ sense of control over personal data;</li> <li>– Some participants saw data intermediaries as a means to standardize data sharing on existing housing platforms;</li> <li>– Other participants questioned the need of an intermediary and preferred sharing data themselves without a middleman;</li> <li>– Being able to use government apps for data sharing is preferred, because these are not associated with profit motives</li> </ul>	<p>Government should provide citizens with options to use a government-owned data intermediary service, or share data manually;</p> <p>A standardized data intermediary should be implemented by housing platforms to avoid usage of multiple accounts and a multiplication of data across systems;</p> <p>Involve citizens in legal procedures of redefining which actors are enabled to process different personal data (including medical data in the context of housing).</p>
Purposes	<ul style="list-style-type: none"> <li>– The selection criteria for choosing tenants and home buyers were opaque to all participants.</li> <li>– The opacity of selection criteria leads citizens to mistrust data sharing and speculate about harmful data use.</li> <li>– People are concerned about the objectivity and fairness of selection processes.</li> </ul>	Alongside defining data use policies, develop transparency requirements for data processors. In the housing sector, data receivers (incl. landlords, mortgage brokers, housing corporations) should provide information on how they select tenants.

Table 2: Summary of recommendations for data sharing standards

## Recommendations

The further development of personal data sharing infrastructure requires the continued involvement of the public and collaboration between policy makers (also across policy domains), public service providers acting as data sources and service providers, research institutes and rights organizations studying the societal impact of sectoral data uses (e. g. in the housing market), as well as commercial parties developing bespoke data

intermediaries and offering services to citizens. Good data sharing arrangements require standards that regulate data sources, data intermediaries, and data reusers and therefore call for a comprehensive and integrated regulatory and design approach.

Citizen concerns regarding data sharing are not limited to the process of data sharing itself, but also relate to what data is being handled in the first place. This is a relevant topic for the governance of data sources such as the BRP (touching upon policies within the Law for Digital Government) and data intermediaries potentially filtering and cleaning source data (concerning policies within the Dutch EDI framework). Furthermore, citizen concerns relate to the opacity of data processing purposes which can be governed by sectoral laws, such as laws within the housing market stipulating the non-discriminatory selection of tenants.

On the basis of our findings, we make the following recommendations:

- **Continuous involvement of citizens, sectoral researchers and tenants' rights representatives is important, instead of primarily involving industry representatives.** Citizens and their representatives can provide advice on the potential harms and data sharing requirements in different sectors, including the housing sector.
- **The Ministry of Interior and Kingdom Relations should develop an integrated framework for personal data sharing.** This framework should regulate access to governmental data sources (as part of the Law for Digital Government) and define requirements for the sharing of data by intermediaries (as part of the Dutch EUDI-framework). This has also been recommended by ICTU, that called for an integrated framework that combines the abovementioned policies.
- **This integrated framework should recognize the crucial role of government data sources to grant citizens control rights to their personal data.** The Ministry of Interior and Kingdom Relations should involve citizens in defining structured access to personal data. Based on our report, structured data access should provide citizens with granular control options and minimize data access at the source. This can include granting highly modular access to individual data points, or consider using attribute-based credentials. The goal should be to limit the interpretability of data to specific use purposes at the source.
- **To minimize data processing, different parties should be assigned specific processing purposes to avoid conflicts of interest.** In the housing sector, this can mean that a dedicated data intermediary provides identity checks for the purpose

of identity verification or fraud detection, whereas housing corporations can use income data for selecting tenants.

- **The Ministry of Interior and Kingdom Relations should further develop the public NL-wallet as a standard, government-issued data sharing mechanism.** A government-issued wallet can provide a standardized data sharing mechanism for citizens who are required to share personal data with different commercial (housing) platforms and other digital services. This can be done by mandating the adoption of a public NL-wallet by commercial providers as ID management and data sharing system within the Dutch EUDI-framework.
- **The ICTU should test the evolving technical standards for the public NL-wallet with citizens.** The tests should go beyond isolated technical mechanisms, and consider how citizens perceive them in relation to concrete use scenarios. To do so, ICTU can implement the insights and apply the methods presented in this report.
- **The Ministry of Interior and Kingdom Relations should not only consider personal data sharing, but also permissible data uses and transparency requirements thereof.** In the housing sector, public involvement is important considering recent proposals to include medical data as novel data category to be processed, as well as calls for more transparent selection criteria for tenants. This requires interministerial collaboration with bodies such as the Ministry of Housing and Spatial Planning.

# 6 Literature

- Ajana, Btihaj. 2018. "Communal Self-Tracking: Data Philanthropy, Solidarity and Privacy." In *Self-Tracking: Empirical and Philosophical Investigations*, Btihaj Ajana (ed.), 125–41. Cham: Springer International Publishing. [https://doi.org/10.1007/978-3-319-65379-2\\_9](https://doi.org/10.1007/978-3-319-65379-2_9).
- Ananny, Mike. 2024. "Making Generative Artificial Intelligence a Public Problem. Seeing Publics and Sociotechnical Problem-Making in Three Scenes of AI Failure." *Javnost - The Public*, January. <https://www.tandfonline.com/doi/abs/10.1080/13183222.2024.2319000>.
- Autoriteit Persoonsgegevens. 2024. "Brief AP aan BZK over datadeler-apps | Autoriteit Persoonsgegevens." August 27, 2024. <https://autoriteitpersoonsgegevens.nl/documenten/brief-ap-aan-bzk-over-datadeler-apps>.
- Brandusescu, Ana, Michael Canares, and Silvana Fumega. 2020. "Open Data Standards Design behind Closed Doors?" *ILDA (blog)*. <https://idatosabiertos.org/en/disenio-de-estandares-de-datos-abiertos-a-puertas-cerradas/>.
- Bijlsma, Michiel, Carin van der Crujisen en Nicole Jonker. 2024. "Not All Data Are Created Equal - Data Sharing and Privacy." *Applied Economics* 56 (11): 1250–67. <https://doi.org/10.1080/00036846.2023.2175777>.
- Driessen, Milan, Maartje van der Koppel, Dewi Hollander, Stefania Milan, Jeroen de Vos and Niels ten Oever. 2024. "Publieke Waarden Rondom Digitale Technologieën." [https://in-sight.it/assets/IN-SIGHT\\_Publieke\\_waarden\\_rapport\\_NL.pdf](https://in-sight.it/assets/IN-SIGHT_Publieke_waarden_rapport_NL.pdf).
- Gray, Jonathan, Danny Lämmerhirt. 2019. "Making Data Public? The Open Data Index as Participatory Device." In *Good Data*, Angela Daly, Devitt Kate, and Monique Mann (eds.) 174–88. Amsterdam: Institute of Network Cultures.
- Hoogenbosch, Arwen. 2022. "Institutioneel racisme bij woningverhuur." Utrecht: Kennisplatform inclusief samenleven. <https://www.kis.nl/online-publicatie/institutioneel-racisme-bij-woningverhuur>.
- Kennedy, Helen, Hannah Ditchfield, Susan Oman, Jo Bates, Itzelle Medina Perea, Monika Fratzak, and Mark Taylor. 2024. "How People Connect Fairness and Equity When They Talk about Data Uses." *Big Data & Society* 11 (4): <https://doi.org/10.1177/20539517241303162>.
- Lämmerhirt, Danny, and Julia Jansen. 2024. "Grip Op Eigen Gegevens." Waag Futurelab.
- Lampland, Martha, and Susan Leigh Star (eds.) 2009. *Standards and Their Stories*. Ithaca: Cornell University Press.
- Mare. 2021. "Evaluatie Gebruikeronderzoek Qii - in Opdracht van Mens Centraal." Amsterdam.
- Peeters, Rik, and Arjan Widlak. 2018. "The Digital Cage: Administrative Exclusion through Information Architecture – The Case of the Dutch Civil Registry's Master Data Management System." *Government Information Quarterly*, 35 (2): 175–83. <https://doi.org/10.1016/j.giq.2018.02.003>.
- Schweihoff, Julia, Anzelika Lipovetskaja, Ilka Jussen-Lengersdorf, and Frederik Möller. 2024. "Stuck in the Middle with You: Conceptualizing Data Intermediaries and Data Intermediation Services." *Electronic Markets* 34 (1): 48. <https://doi.org/10.1007/s12525-024-00729-9>.

Sharma, Shane Arjun, and Rocco Langeweg. 2024. "Proeftuin Regie Op Gegevens Met Zorgeloos Vastgoed."

Urban, Monika. 2022. "„Toll. Ich bin froh dabei zu sein“. Studie zur Spende digitaler Körperdaten in der Corona-Krise." *ZQF – Zeitschrift für Qualitative Forschung* 22 (2). <https://www.budrich-journals.de/index.php/zqf/article/view/39525>.

Van de Poll, Machiel, Petra Immerzeel, and Dylan De Mots. 2021. "Digitaal delen persoonsgegevens van burgers." Rapport. Ministerie van Algemene Zaken. October 13, 2021. <https://doi.org/10.13/digitaal-delen-persoonsgegevens-van-burgers>.

Van de Poll, Machiel, and Dylan De Mots. 2022. "Regie op gegevens: Welke burgers zien het digitaal delen niet zitten, en waarom niet." Rapport. Ministerie van Algemene Zaken. October 13, 2022. <https://doi.org/10.13/regie-op-gegevens---welke-burgers-zien-het-digitaal-delen-niet-zitten-en-waarom-niet>.

Van der Tuin, Inte, and Milynn Koene. 2021. "Sterke Vermoedens, Maar Geen Bewijs. Discriminatie-Ervaringen van Woningzoekenden in Rotterdam." Rotterdam: Radar voor gelijke behandeling tegen discriminatie.

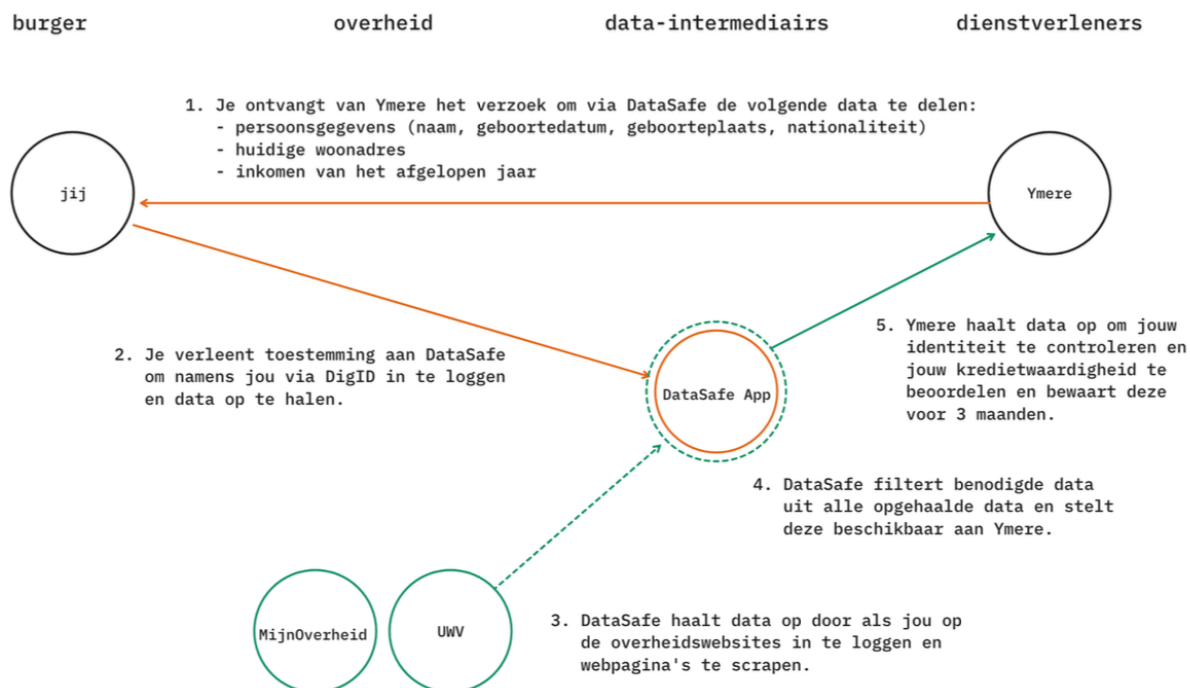
Van Zoonen, Liesbet. 2016. "Privacy Concerns in Smart Cities." *Government Information Quarterly*, Open and Smart Governments: Strategies, Tools, and Experiences, 33 (3): 472–80. <https://doi.org/10.1016/j.giq.2016.06.004>.

Van Zoonen, Liesbet. 2020. "Data Governance and Citizen Participation in the Digital Welfare State." *Data & Policy* 2. <https://doi.org/10.1017/dap.2020.10>.

# Appendix: Scenarios

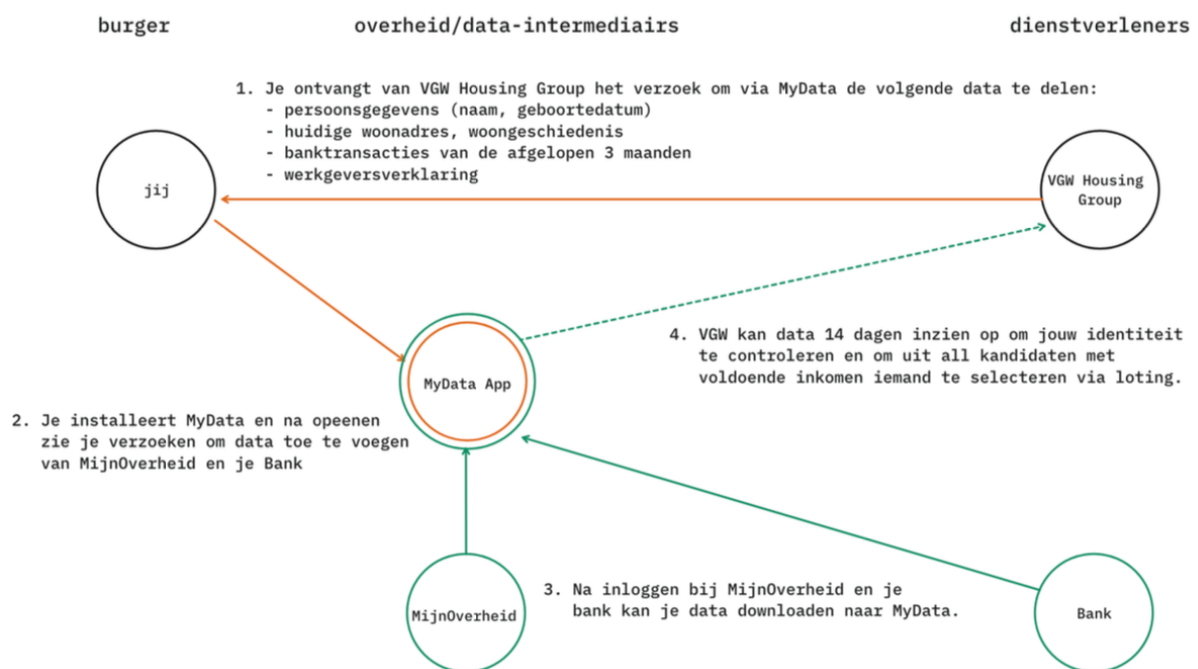
## Scenario 1 (Tenants, free market and social housing)

“Je bent werknemer en op zoek naar een woning. Je vindt online een appartement van de woningcorporatie Ymere. Je wilt je inschrijven voor een middensegmentappartement. Deze appartementen zijn beschikbaar voor mensen met een inkomen tot 62.500 euro. Om je in te schrijven voor het appartement, vraagt Ymere je om via een commerciële app, de DataSafe-app, gegevens over jezelf te verstrekken. Nadat je de app op je telefoon hebt geïnstalleerd, vraagt DataSafe je om met je DigiD in te loggen op je accounts bij Mijn Overheid en UWV. Eenmaal ingelogd, kan DataSafe al je persoonlijke gegevens inzien die op deze portalen zijn opgeslagen. De app maakt eerst een kopie van deze gegevens en filtert vervolgens irrelevante gegevens eruit voordat deze naar Ymere worden verzonden. Ymere ontvangt de volgende gegevens: identiteitsgegevens incl. naam, geboortedatum, geboorteplaats, nationaliteit, huidige woonadres, jouw inkomen van het afgelopen jaar. Ymere bewaart de gegevens 3 maanden op hun servers en zegt de gegevens te gebruiken om je identiteit te verifiëren, en je kredietwaardigheid en je inkomen te beoordelen.”



## Scenario 2 (Tenants, free market and social housing)

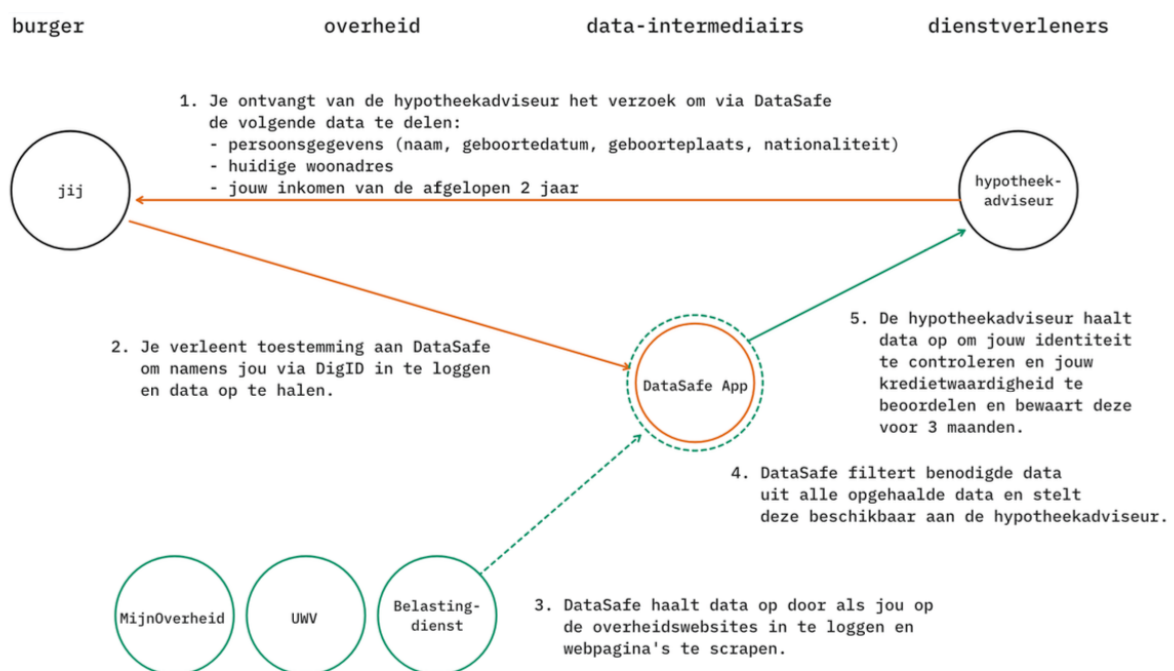
“Je bent werknemer en zoekt via de VGW Housing Group naar een woning. Je wilt een vrije sectorappartement aanvragen dat beschikbaar is voor mensen ongeacht hun inkomen. Om je aan te melden voor het appartement, moet je de nieuwe overheidsapp “MyData” gebruiken. Nadat je de app op uw telefoon hebt gedownload, wordt je gevraagd om in te loggen op jouw account bij Mijn Overheid (via DigiD) en uw bankrekening om identiteitsgegevens en inkomensgegevens te verstrekken. Na het inloggen moet u gegevens uploaden naar MyData waar ze “veilig worden opgeslagen.” VGW Housing Group kan de gegevens alleen na je toestemming gedurende 14 dagen uitlezen. VGW leest de volgende gegevens uit: identiteitsgegevens (naam, geboortedatum), huidige woonadres, woongeschiedenis, inkomen van de afgelopen 3 maanden (banktransacties). Daarnaast vraagt VGW Housing je om een werkgeversverklaring via de MyData-app te verstrekken. VGW Housing zegt dat het de gegevens gebruikt om uw identiteit te verifiëren en om geschikte huurders te selecteren via een loterij, op basis van een inkomenscontrole.”





## Scenario 3 (Buyers)

“Je bent werknemer met vastcontract en op zoek naar een koopwoning. Je vindt op Funda een appartement en doet een aanbod bij de makelaardij Beter Wonen. Om het hypotheekproces te versimpelen, vraagt Beter Wonen je om de commerciële app “DataSafe” te gebruiken. De app deelt je gegevens met een hypotheekadviseur. Nadat je de app op je telefoon hebt geïnstalleerd, vraagt DataSafe je om met je DigiD in te loggen op je accounts bij Mijn Overheid, UWV en de Belastingdienst. Eenmaal ingelogd, kan DataSafe al je persoonlijke gegevens inzien die op deze portalen zijn opgeslagen. De app maakt eerst een kopie van deze gegevens en filtert vervolgens irrelevante gegevens eruit voordat deze naar de hypotheekadviseur worden verzonden. Hij ontvangt de volgende gegevens: identiteitsgegevens incl. naam, geboortedatum, geboorteplaats, nationaliteit, huidige woonadres, jouw inkomen van de afgelopen 2 jaar (UWV). De hypotheekadviseur bewaart de gegevens 3 maanden op zijn servers en zegt de gegevens te gebruiken om je identiteit te verifiëren, en je kredietwaardigheid en je inkomen te beoordelen.”



## Scenario 4 (Buyers)

“Je bent werknemer met een tijdelijke contract. Je zoekt via de VGW Housing Group naar een koopwoning. Gelukkig - jouw aanbod werd geaccepteerd! Nu wil VGW Housing dat je persoonsgegevens deelt met een hypotheekadviseur middels de nieuwe overheidsapp “MyData.” Nadat je de app op je telefoon hebt gedownload, wordt je gevraagd om in te loggen op jouw account bij Mijn Overheid (via DigiD) en jouw bankrekening om identiteitsgegevens en inkomensgegevens te downloaden. Daarna kun je de gegevens uploaden naar MyData waar ze “veilig worden opgeslagen.” VGW Housing Group kan de gegevens alleen na je toestemming gedurende 14 dagen uitlezen. VGW leest de volgende gegevens uit: identiteitsgegevens (naam, geboortedatum, BRP), huidige woonadres, woongeschiedenis, inkomen van de afgelopen 2 jaren (banktransacties), de laatste aanslag inkomstenbelasting (Belastingdienst), je diploma’s (DUO) en je werkgeschiedenis (UWV). De hypotheekadviseur zegt dat hij de gegevens gebruikt om jouw identiteit te verifiëren en om je kredietwaardigheid op basis van een inkomenscontrole en je werkgeschiedenis en opleiding te controleren.”

