Transparency versus security of privacy sensitive data

Ensuring the right balance – an example for the Netherlands' Cadastre

Rindert VOS and Gerard DABROEK, The Netherlands

Key words: Ethics, Cadastre, Legal, Privacy, Transparency

SUMMARY

In recent years there have been calls for more transparency in (geospatial) data, especially when it comes to data owned by governments, as it promotes accountability and protects citizen's rights (e.g. the right to privacy). On the other hand, with the increasing dissemination of (geospatial) data and a growing risk of privacy violations, data misuse, and cyber-attacks, the importance of robust data security is underlined. However, the right to public access to data and the right to privacy are apparently at odds with each other. Public access to data requires transparency, while privacy requires restraint or even secrecy. This paper explores the intricate balance that (public) organizations should strike to safeguard sensitive data while maintaining transparency of the same data based on experiences and best practices from Kadaster.

The tension between transparency and security of data creates a challenge which also applies to the Netherlands' Cadastre, Land Registry and Mapping Agency (Kadaster). Kadaster is developing a system to deal with this challenge to counter several issues, such as: How do we ensure that Kadaster is transparent about the personal data that they have provided about someone?; How does Kadaster ensure that the personal data of people who are threatened do not end up on the street?; Are the measures that Kadaster takes for this purpose legally and ethically justified?; What is Kadaster allowed to do and what are obliged to do as a government organization?

Kadaster organizes its data systems in such a way that the above issues can be addressed and at the same time unauthorized consultations, irregularities, and abuse can be detected. In this paper, we delve into the evolving landscape of privacy-sensitive data, and we offer insights and best practices how Kadaster organizes its systems to deal with the tension between transparency and security.

1. INTRODUCTION

In recent times, there seems to be a rising discourse that governments should be seen as open data suppliers which share information across governments, businesses, and the public. This movement is called 'Open Government Data' which is a philosophy that promotes transparency, accountability, and value creation by making government owned data available to all (OECD, 2020). The right to access information is one of the driving factors behind this movement as it allows all individuals to obtain information held by public authorities or entities. Especially transparency generates economical and societal value because it encourages businesses and citizens to use, reuse, and distribute government owned data. In addition, it fosters accountability and increases citizen access to government decision-making.

Transparency, in the context of government-owned data refers to the openness and accessibility of information held by public authorities (Buijze, 2013). It involves making government data available and easily understandable to the public. Transparency is a fundamental principle and an important value as it not only enables citizens to assess their administrators, it also forms the basis for trust between citizens. For example, when doing business with partners with whom you are not familiar.

However, to what extent should this apply to government owned personal data such as address information, date of birth, or marital status? Although the notary, civil servants or depth collectors can rightfully use this privacy-sensitive data, there is a danger that it is being misused. When personal information falls into the wrong hands, criminals can take the opportunity to profit from it. Using your identity, a criminal can commit fraud in your name. Worse still, personal information or that of loved ones can be used to intimidate, bribe or physically attack others. Especially politicians, celebrities and people with important positions (e.g. judges) are more prone to these risks. In recent years, the Netherlands was shocked by several serious incidents such as the murders on Dutch lawyer Derk Wiersum and on crime reporter Peter R. de Vries which prove this is not just theory anymore.

It goes without saying that in these cases transparency has its limits to make sure not everyone has to know everything about each other. Privacy of this data turns out to be of, in some cases, lifesaving importance. The right to privacy protects an individual's personal space, autonomy, and the ability to control their personal information (EDPS Euro, 2016). This right is recognized in various (inter)national frameworks and is considered a fundamental human right.

While transparency is essential, it should be balanced with the protection of the privacy of individuals. Sensitive and personal information should be managed responsibly, and measures should be in place to prevent the unauthorised disclosure of private data. However, the right to access information and the right to privacy are apparently at odds with each other. Public access to data requires transparency, while privacy requires restraint or even secrecy. The key for government organisations is to ensure that there is an appropriate balance between these two rights which aligns with the legal requirements, ethical standards and the ambitions of an open government.

The tension between transparency and privacy of data creates a challenge which also applies to the Netherlands' Cadastre, Land Registry and Mapping Agency (Kadaster). This paper explores the intricate balance that (public) organisations should strike to safeguard sensitive data while maintaining transparency of the same data based on experiences and best practices from Kadaster. Kadaster is developing a system to deal with this challenge to counter several issues which will be addressing in this paper, such as: How does Kadaster ensure the transparency of the data it provides? How does Kadaster protects sensitive personal data from the public? And in which way are the measures taken by Kadaster legally and ethically acceptable? Finally, this article focuses on raising awareness of the challenges and opportunities in advancing both data transparency and privacy.

2. ENSURING TRANSPARENCY IN PROVIDING PERSONAL DATA

The position of Kadaster in land registration and real estate transactions is crucial because every deed, transfer, and mortgage is preserved in the Public Registry. Essential information is extracted from the deeds and is recorded in the 'Basis Registratie Kadaster' (Kadaster Base Register, BRK) that can tell exactly which persons have which legal rights to which property in the Netherlands. Data from the Public Registry and the BRK are both accessible to the public.

Kadaster strives for transparency of the personal data it provides based on three principles. First, Kadaster has the legal obligation to publish data in the Public Registry in order to guarantee the right to ownership as much as possible. The basic principle states: everything we register must also be able to be provided, with exceptions (see next chapter). Second, Kadaster complies with the right to access information, based on the General Data Protection Regulation (GDPR). As discussed in the introduction, the right to access information entails that every person has the right to know which personal data has been processed for which purposes and to which receiving parties it has been disclosed (GDPR Euro, 2018). Third, Kadaster aims to improve the accuracy and quality of its data. Transparency ensures that data is better understood and therefore contributes to a better service for all users.

To ensure transparency in the personal data provided, Kadaster adopted several measures. To comply with the legal task of providing data to the public, Kadaster operates based on various standards and models (e.g. Logius Framework). Almost all data that is shared is standardised, so that requesting and accessing data works in the same way. This allows the user to easily monitor how Kadasters' data is collected. The standardisation makes it possible to share all data cheaper, faster and easier. However, in exceptional situations, Kadaster offers customised products for its customers. In addition, Kadaster is affiliated with the website 'Mijn Overheid' (My government), which improves the connection between citizens and the Dutch government. It is a free tool that shows all personal information registered by Dutch authorities. For example, after logging in and selecting the option 'living', all personal data registered by Kadaster are visible.

Every Dutch citizen has the right to request from Kadaster to whom his or her personal data has been provided. In detail, everyone has the right to know who consulted and provided the data, when the transfer occurred, what personal data has been received, and for what purpose it was requested. Thereafter, Kadaster is obligated to inform the requestor on (1) which data have been provided to which non-natural persons and (2) the number of disclosures to natural persons (in accordance with GDPR article, paragraph 1c). Processing such requests is time and effort consuming because several departments, applications and data sources should be involved in providing the requested information. Moreover, Kadaster risks not being able to monitor all information distributions. In practice, it is impossible to execute a complete examination because several custom systems do not have logging of delivered personal data. Therefore, Kadaster is developing a central solution with a Data Analytics Platform, consisting of three components: (1) Auditing and monitoring data are stored on a central data platform, (2) Source data is accessed via events (Realtime) and/or via batch, (3) Auditing and monitoring via Data Analytics Platform.

The proposed solution provides for a generic provision for logging all data provision, both standard and customised, both individual deliveries and bulk deliveries, both to individuals and to organisations. This results in that every access or provision of data related to a natural person will be logged and therefore a GDPR request can be managed immediately, quickly and completely. This logging process should be as 'lean & mean' as possible because of the enormous amount of information being logged. This solution enables central governance and monitoring, and is extensible with more datasets for fraud detection, cyber security analytics and pattern recognition algorithms. Although it contributes to the Kadaster being more transparent in the data it provides, it should be mentioned that there are still hurdles to overcome (e.g. storage capacity, retention period).

Last, Kadaster aims to improve its data accuracy and quality by installing dashboards and focusing on making the data more accessible for its users. The data accuracy and quality are constantly monitored and shared to users with the intention to understand what Kadaster can do to improve the understandability of the data. In addition, data management systems are used to help users interpret data correctly by explaining the data with definitions and concepts in the correct context. All discussed measurements installed are aimed at ensuring the transparency of personal data owned by Kadaster.

3. PROTECTING PERSONAL DATA FROM THE PUBLIC

Securing privacy and protecting personal data has become increasingly more important due to digitalisation, regulatory compliance, the growing risk of privacy violations and data misuse. To address these challenges and to ensure that sensitive personal data is protected from the public, Kadaster installed several measures. The security of Kadasters data is ensured on various fronts. Through the established trajectory of working under architecture, information models are created in collaboration with the modelling agency, in conjunction with the Data Asset Manager. Within this collaborative triangle, meticulous care is taken to ensure that personal data is stored and made available uniformly and preferably centrally.

Services exchanging data are built upon Zero Trust principles. All traffic is encrypted and exchanged through authenticated and authorized APIs. Additionally, both internal and external chain tests are conducted to ensure the protection of sensitive information.

Specifically for the protection of sensitive personal data, Kadaster appointed privacy officers, a central data protection officer, and makes use of several risk analysis and audits. The main principle that Kadaster uses for protection of sensitive data is that of 'purpose limitation.' In Kadasters' web-shop, the public is allowed to type in an address or request a cadastral parcel to look up information about the owners. However, only authenticated professionals who are legally authorised to use personal data (e.g. notaries) are able to use Kadaster's informational systems to enter a person's name while searching for information on their properties. Therefore, Kadaster uses the principle of purpose limitation which makes it impossible for the public to search for information about a person at risk. Purpose limitation only gives legally recognized actors with a legally recognized purpose the right to access all information: "Your nosy neighbour is not entitled to your personal data, while your notary who drafts up the deed of sale of your home does" (Dabroek, 2023).

One of the main measures that Kadaster has installed to protect sensitive data from the public, is the 'APG-loket' (APG- counter). In order to implement data protection, it has been decided on the basis of Article 37a of the Land Registry Act that Kadaster is authorised to completely shield persons from the cadastral registration. This concerns persons who are on the supervision and protection list of the Public Prosecution Service, or persons with specific functions (e.g. judges) who are on the exhaustive list of the NCTV (National Coordinator for Security and Counterterrorism). To be shielded, the person in question must file a request for protection. Kadaster identifies this person and the registered property that he or she owns. After approval of the request, this person is protected in the KPR (Cadastre Person Registration) for 5 years. If someone wants to request data from this person during that period, they will receive a message that the data is not available, and they will be referred to the APG counter. If a request is received at the APG counter, after assessment of this request, the personal data will only be provided to the person himself and to business customers who are eligible for access to protected data (notaries, bailiffs and administrative bodies). The assessment is made based on the purpose limitation principle discussed above. Moreover, the person in question is always informed.

According to the Kadaster Enterprise Architecture, the protection of personal data is based on a number of principles and foundations. First, the shielding of persons is recorded exclusively in KPR, which is a link between the base registration of Kadaster and the base registration of persons in the Netherlands. Second, there is a shielding of both the current and the historical data provision. Third, the protection of a person concerns the protected person, the partner and other co-rights holders. Fourth, persons without rights in the BRK are not active in the KPR and therefore are not eligible for protection.

The process of shielding persons from the public is as follows. After checking the person in KPR, the system searches for the right person to mark them as protected. When a request for the provision of this data is received, the consultation system asks the central OR data services ('Openbaar Register' – Public Registry) whether this person has been shielded. The OR data services is a filter that connects different systems and allow them to talk to each other. It links the KPR to the various systems from which the data is supplied based on variables (e.g. place of residence, first name and date of birth). When providing material, text recognition is used to check whether there is a match between the people shielded by KPR and what is requested. If it is determined that the person is subject to shielding, no data will be provided, and the requester will be referred to the APG counter.

Although Kadaster is committed to protecting sensitive data, there are still challenges. For example, decentralized storage requires extra security because it is more difficult to secure. In addition, it is expected that there will be a significant increase in the number of requests for information about shielded persons, which will put pressure on employee capacity and the system. Emerging technologies offer opportunities to improve data security. An emerging trend in data management is the increasing focus on pseudonymization and data minimization. Pseudonymization involves replacing personally identifiable information with non-identifying data, while data minimization aims to limit the data collected to strictly necessary information. Together, these approaches represent important aspects of data protection. They focus on ensuring privacy and reducing risk by making it difficult to identify individuals and minimizing the amount of sensitive data stored.

4. LEGAL AND ETHICAL BOUNDARIES

As discussed in the above paragraphs, Kadaster has installed several measures to both ensure transparency and privacy of sensitive personal data. Constructing such measures should be paired with legal (what is allowed to do to ensure transparency and privacy?), technical (is it possible to do?) and ethical aspects (do we want it?). Especially when being a governmental organisation, it is important whether the measures taken are legally and ethically acceptable.

There are two main legislations on enhancing transparency that the Kadaster should adhere to. The Interoperability Act is a European law which is aimed at increasing the exchange of data between governmental organisations. When different government organizations are compatible to exchange data, data as a service becomes more accessible to the public which increases transparency on the specifics of the data are, how you can retrieve and use it. Kadaster complies to this legislation by adhering to the various regulations regarding the storage, access and processing of data. The Open Government Act and the Digital Government Act provide guidelines on the extent to which Kadaster may and can communicate about data. The Open Government Act aims to make government more transparent by increasing access to information, while the Digital Government Act focuses on promoting the digitization of government services and ensuring accessibility for citizens and businesses.

Developments in digitalisation and data misuse put an end to radical transparency. Various legislation gives Kadaster guidance how to guarantee the privacy of sensitive data. The most important legislation in this area is the General Data Protection Regulation (GDPR). Kadaster is obliged to comply with the GDPR and to adhere to legal requirements in the field of data protection and privacy. The goal is to anonymize and minimize data where possible, in consultation with the Data Asset Managers within the relevant domain. Kadaster is obliged to explain whether and how a facility fits the purposes for which the data was originally collected (this is also stated in the Land Registry Act, Article 2a). In addition, there are developments at the above-mentioned APG desk where legislation calls for the expansion of professional groups and the ordinary citizen as an exceptional position.

In order to take ethically responsible measures to guarantee both transparency and privacy, Kadaster has established an Ethics Committee whose aim is to provide reproducible ethical advice. The committee uses Kadaster's core values (reliable, open, relevant, driven) and the ethical values from the Codio Framework. This is a framework that indicates how a government organization should deal with ethics. Transparency is one of the values. The committee is also committed to increasing awareness among employees. As an organization, it is important to always look at the effect of the actions from Kadaster on the stakeholders and to communicate this to the relevant stakeholders.

5. CLOSING WORD

In recent years there have been calls for more transparency in (geospatial) data, especially when it comes to data owned by governments, as it promotes accountability and protects citizen's rights (e.g. the right to access information). On the other hand, with the increasing dissemination of data and a growing risk of privacy violations, data misuse and cyber-attacks, the importance of securing privacy is underlined. The tension between promoting transparency and privacy leads to the discussion whether the two are contradictory or can reinforce each other. Kadaster has introduced various measures to invest in both areas, without detracting from each other. As discussed in this paper, Kadaster aims to comply with the right to access of information by fostering transparency on the data it possesses. Making the data publicly available in an accessible manner contributes to the right that everyone can see who is requesting his or her data. In addition, Kadaster has taken various privacy and security measures to protect the sensitive personal data from the public. One of these measures is the legally installed APG counter. The APG protects people from trying to request information by using a filter. Based on the principle of purpose limitation, only authorised persons can request necessary information.

As a government organisation, Kadaster must comply with the various laws that the Dutch government installed such as the Open Government Act and several privacy legislations. To ensure being ethical acceptable, Kadaster uses an independent ethical commission which uses an ethical framework to assess measures taken. However, Kadaster still faces challenges to balance its ambitions, the technical possibilities and legal restriction to ensure both transparency and privacy in providing its data.

This paper concludes with the invitation to be aware that transparency and privacy are not mutually exclusive and are actually reinforcing each other. Consider using this insight to use in your own context, even with geodata.

CONTACT

Dhr. Rindert Vos
Kadaster Netherlands
Hofstraat 110, 7311 KZ
Apeldoorn
The Netherlands
Tel. +316-11234575
Email: rindert.vos@kadaster.nl
Website: https://www.kadaster.com/

REFERENCES

Buijze, A. (2013). Retrieved from https://dspace.library.uu.nl/bitstream/handle/1874/269787/buijze%2Bapp.pdf?sequen

EDPS Euro (2016). Retrieved from https://edps.europa.eu/data-protection/data-protection_en#:~:text=Privacy%20%E2%80%93%20a%20fundamental%20right&text=The%20right%20to%20privacy%20or,Fundamental%20Rights%20(Article%207)

GDPR Euro (2018). Retrieved from https://gdpr-info.eu/art-15-gdpr/

OECD (2020). Retrieved from https://www.oecd.org/gov/digital-government/open-government-data.htm