AUTORITEIT
PERSOONSGEGEVENS

Smart Cities

Investigation Report on the Protection of Personal Data in the Development of Dutch Smart Cities

July 2021

About the Dutch Data Protection Authority
Everyone has right to careful handling of their personal data. The Dutch Data Protection Authority monitors compliance of the legal rules regarding the protection of personal data and advises on new regulations.

Foreword

Increasingly more municipalities are collecting personal data in public spaces through the use of smart city applications. With the term smart cities, I often linger on the word 'smart', because what does a smart city actually entail? For what purpose and for whom should a public space be smart? Using technology can help municipalities understand the use of public space or create new ways to guide the use of public space. That is why it is important to consider the price you and I pay when we find ourselves within a smart city. How does the collection of our personal data in public space relate to our freedom? Data can be inaccurate, ambiguous, or may even discriminate. There is a risk that dataism and digital solutionism will gain the upper hand: the belief that everything can be understood through data and technology. Especially in the public space, where the number of people is as large as they are diverse, it is questionable whether this can be represented by data let alone be controlled by it. There is a danger that we are headed towards a surveillance society where you cannot walk freely on the street anymore. It is for these reasons that we are also calling for a ban on facial recognition in public spaces.[1]

With this report we stress the importance of a public space where citizens can move freely and unobserved. We call on directors and civil servants to reflect on the rights and freedoms of citizens, and to truly consider them at every step in the development of a smart city. And to be aware that a municipality cannot simply infringe on the fundamental right citizens have to data protection, in order to do this, a legal basis or free consent from citizens is required. Let privacy be the starting point of innovation, not the end point.

To municipal council members, I would like to specifically ask you to pay close attention to the (ethical) framework of each technological proposal and to consider whether that proposal respects the rights and freedoms of citizens. Also, ask advice from the Data Protection Officer. Make sure that when you come to a decision, you have considered it carefully, fully, and from a multitude of perspectives. Not just to have checked off the GDPR-checkbox, but because you want the best for your residents and visitors of your municipality and because you want to stimulate responsible innovation. In the end, it is not the technology but the human who makes the public space smart.

Monique Verdier
Deputy Chair of the Dutch Data Protection Authority

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-pleiten-voor-verbod-op-gezichtsherkenning

Table of Contents

1. Summary

The public space is increasingly subject to the use of technology. Think of Wi-Fi and Bluetooth tracking, (mobile or body) cameras or sensors that collect traffic or sound data. Municipalities are increasingly using this technology to gain a better understanding of the public space in order to optimize, influence or better manage it. These smart city applications can process personal data in or about the public space. The altering of intentions, resources, and thus, the use of personal data for purposes other than those originally intended, occurs regularly and poses a potential threat to the fundamental rights of people entering a public space. There is also a risk that knowledge about a public space will be exchanged for data about the public space; data that can be inaccurate, ambiguous, or discriminatory. The Dutch Data Protection Authority (DPA) has therefore carried out research into the protection of personal data in the development and use of smart city applications by municipalities.

The DPA notes that there are significant differences in the use of smart city applications. While a group of municipalities is at the forefront of the development of smart city applications, there are also municipalities that employ limited or do not (yet) use smart city applications in the public space. This difference seems to be strongly influenced by specific issues as well as by the size, urbanization, and population density of the municipality. The differences between municipalities is reflected in both the number of applications and the innovative nature of the technology chosen for the applications. Most of the applications focus on mobility and (traffic) safety, ranging from measuring visitor and traffic flows to monitoring entertainment areas.

In order to develop smart city applications responsibly, almost all municipalities need to develop more knowledge and focus on specific municipal frameworks as well as raise awareness about the impact of smart city applications on citizens' rights and freedoms, including the protection of personal data. The use of measuring personal data in public spaces is subject to strict requirements. It is not always the case that the determination of whether the processing operations related to the smart city application are lawful is sufficiently substantiated or documented. This starts with the question of whether the collection of personal data in the public area by a municipality is lawful. In doing so, municipalities must also properly record and update their considerations regarding the processing of personal data in smart city applications, for example, through the use of DPIAs. Only when the question of legality has been answered positively, is it wise to consider the ethical issues as well.

A smart city is more than just the sum of its applications. While one smart city application alone does not seem worrisome or risky, the entirety of the applications can certainly create bigger or new risks. Clear municipal policies, democratic control, and the involvement of citizens can help mitigate risks and the development of responsible smart city applications. Transparency is necessary for this purpose. The use of technology in public spaces is a major decision in which all aspects need to be carefully considered. After all, not everything needs or can be solved with technology or data. In order to ask the right questions and put citizens at the heart of defining the purpose of smart city applications, an ethical framework can be helpful. The research showed increasing attention for ethics in the development of smart city applications, for example, by appointing an (ethical) committee. However, this must form part of the development process in a concrete way, otherwise there is a risk that the public will not be aware of these well-intentioned discussions.

Based on this study, the DPA highlights the following points of interest for municipalities:

- The basic principles of the GDPR must be in order. Determine whether the way personal data is being processed is lawful. What is the concrete purpose of using a smart city application and what legal basis is there for the data processing? And is it really necessary to process personal data to achieve its purpose? If there is no legal basis for the processing or if the data processing is not necessary for the specified purpose, the smart city application should not be used. Altering the purpose poses a real risk that could harm citizens' rights and freedoms.
- DPIAs as a process. The execution of a DPIA is an important process to assess whether the processing of personal data in smart city applications is lawful and fair, which risks there are, and to internally and externally account for the choices made. The implementation of a DPIA for smart city applications that process personal data is often mandatory. There are areas of improvement for municipalities when it comes to drafting DPIAs. Municipalities could publish DPIAs more often with regards to smart city applications to account for the collection of data in public spaces.
- Getting a grip on smart cities. Instead of defining data protection (and ethics) frameworks per smart city application, municipalities should develop policies for the deployment of smart city applications. These also need to be translated into concrete tools to be used in practice, which does not always happen. Moreover, municipalities also have a role to play regarding gaining insights into the sensors placed by third parties in public space. Municipalities may explore the possibility and desirability of imposing municipal conditions prior to the use of sensors by third parties in public areas.
- Municipal councils as a counterforce. Digitalization and the use of smart city applications deserve greater attention from municipal councils. Municipal councils must be given sufficient knowledge and information to carry out their democratic task properly. Involving experts can help in asking the right questions.
- Privacy as a basis. Many municipalities still do not organize enough privacy in the execution of their work. Mobilizing sufficient people and resources, and properly positioning privacy professionals in the organization is essential. In particular, attention should be paid to the DPO, who has a specific role and set of tasks that is protected in order to ensure the performance of their function. This contributes to a positive climate of development in which applications are developed according to the privacy by design principle.
- Solution or problem. Municipalities, especially those who do not have sufficient knowledge regarding the processing of personal data, occasionally hastily partner with suppliers of 'beautiful solutions'. Be critical of any supplier's statements regarding compliance with the GDPR or the statement that no personal data is being processed.
- Civilians as brains. Real knowledge of a public space lies with its users. Citizens not only know the problems, but often see other risks associated with the processing of personal data in or about the public space. In the case of high-risk smart city applications, the DPA does not believe that a municipality can map out all the risks in advance without the involvement of citizens. Involving citizens in smart city applications seems to be the key to success, but it is one that is rarely implemented.

Only when these aspects are addressed is responsible further development of smart cities possible. By not paying attention to these aspects, the Dutch smart city runs the risk of losing sight of the citizen and even threatening the rights and freedoms of the individual. This risk applies particularly in the public space; the place where citizens should be able to feel free and unobserved.

2. Introduction

The Dutch Data Protection Authority (DPA) has identified digital government as one of the three focus areas in the 2020-2023 Focus. Smart cities is an important area of attention because of the growing use of data-driven applications that process personal data in public space. These applications are often still in the development or growth phase, where the questions about the protection of personal data also play an important role.

The DPA decided to launch a study on smart city applications by municipalities in order to map the handling of personal data in the Dutch smart city. In doing so, the DPA aims to stimulate sustainable innovation, ensuring the privacy of affected citizens in smart cities. Through this research, the DPA aims to gain insight into the use of personal data by smart city applications, the use of Data Protection Impact Assessments (DPIAs), the role of the Data Protection Officer (DPO), and the experience of municipalities and experts. To this end, the DPA requested documentation from 12 Dutch municipalities and sent out a questionnaire. Interviews were also held with councilors, DPOs, officials, and experts who were involved. The aim of this research was not to detect possible violations, but to gain insights into this topic and share these findings in order to stimulate sustainable innovation. Through this report, the DPA aims to share its insights obtained through the research.

In this report, we discuss the design of the research, the relevant basic principles of the General Data Protection Regulation (GDPR) in the context of smart cities, the DPIAs that the DPA has studied in the context of this research, the ways in which the municipal council and its board can get a grip on smart cities and the role of citizens, the importance of the organization of privacy within municipalities, Mobility as a Service, and finally, we conclude with recommendations and concluding remarks about the state of data protection in Dutch smart cities.

2.1 Defining Smart Cities

The DPA understands the term, smart city application, as the collection and processing of (personal) data about or in public space through the use of sensors, technology or other applications to gain insight into, or obtain analytical capabilities about public spaces, or to enable the control of a public space. There is a wide range of smart city applications that may fall under this definition. Examples include the use of Wi-Fi and Bluetooth tracking, the use of (mobile or body) cameras, or sensors that collect traffic or sound data. The DPA uses smart city as an umbrella term under which all public spaces in The Netherlands fall, including villages, nature areas, and agricultural zones.

2.2 Purpose of the Research

The purpose of this investigation is multifaceted. Based on the research, the DPA aims to:

- gain insights into the processing of personal data within smart city applications;
- examine and encourage the use of the DPIAs as a tool, and thereby, also highlighting the use of prior consultations as understood under Article 36 of the GDPR;
- collect and share best practices on smart city applications;
- examine the role of the DPO in the development of smart city applications;
- stimulating privacy-friendly innovation throughout the entirety of the smart city application development process;
- raise awareness among municipalities that smart city applications can pose major risks to the rights and freedoms of the individual.

The research focused on smart city applications in which the municipality acts as the data controller. In addition, as part of this research, we also paid attention to the regulation of smart city applications by municipalities (e.g. private parties that use sensors in public spaces) and partnerships.

2.3 Approach

In order to achieve the aforementioned objectives, 12 municipalities in two groups were investigated. The first group concerned five municipalities in more urban areas. The second group concerned seven municipalities with a more diverse location and composition in The Netherlands. It was decided to have one group of municipalities that were selected because they profiled as a smart city or as having smart city policies, and another group of municipalities where this was not present and were either a small or medium-sized municipality. Smart cities are commonly associated with the big cities or the Randstad, but it is also prevalent in smaller municipalities in the Netherlands. An overview of the smart city applications as well as the corresponding DPIAs, were requested from the 12 municipalities, and each of municipalities was asked to complete a questionnaire, which can be found in the annex to this report. Based on the response, follow-up questions were asked in a number of cases and interviews with councilors, civil servants, and DPOs were held. Also, a few scholarly and practical experts were interviewed about specific issues regarding the intersection of technology, ethics, and governance in smart cities.

The first phase of the survey concerned five municipalities and lasted from September 2019 to February 2020. The second phase of the survey concerned seven municipalities and lasted from March 2020 to August 2020. Meetings and interviews were held between April 2020 and November 2020; the completion of the investigation was delayed due to the impact of COVID-19 on the organization.

2.4 Cooperation with the Investigation

Municipalities are obliged under the GDPR and the General Administrative Law Act (Awb) to participate in an investigation of the DPA.[2] During this investigation, the DPA requested information on several occasions and in once instance, had to conduct a norm-addressing conversation with a municipality that did not cooperate sufficiently with the DPA's request and ordinance. Public organizations must protect the interests and fundamental rights of citizens, act transparently, and therefore, also comply with the requests and ordinance of the supervisory authority. This is especially applicable in this case as the requested information should be largely available by municipalities on the grounds of the accountability obligations of the GDPR.

2.5 Reflecting on the Research and Dutch Smart Cities

To encourage discussion between all parties, the DPA asked a number of experts to write an independent reflection based on this report and their views on elements related to smart cities. These experts were given access to the draft report and were asked on the basis of their expertise to write a reflection which had no impositions regarding its content. The DPA has included the entirety of these reflections without any editing or changes in order to ensure independent reflection. No remuneration or compensation was given to the writers or organizations. The content of these reflections was written independently and was not reviewed or approved by the DPA and, therefore, it should not be read as such.

[2] Article 5:20(1) Awb in conjunction with Article 31 GDPR.

3. Basic principles of the GDPR for Smart Cities

Cities, urban areas, and municipalities are increasingly seeking smart solutions to issues such as mobility, energy, security, and housing. These smart solutions are found in sensors and data. Supported by technologies such as machine learning, municipalities can collect data or combine data on, for example, visitor flows, traffic, or security. Through the use of this data, residents can be 'lead' to better choices and municipalities can optimize the use of public space.

The deployment of smart solutions in public spaces undeniably affects a number of fundamental rights. For example, the use of data to classify or exclude (groups of) people based on behavior or external characteristics can lead to discrimination. The processing of personal data is by definition a breach of the right to data protection. The development of smart cities also touches on ethical aspects and societal issues. Questions that municipalities can ask themselves in this context are, for example, the following: Can problems in complex ecosystems such as cities be solved with data when the data collected is by definition limited and non-objective? Does the use of data exclude alternative solutions? In a smart city, will you still be able to feel free or demonstrate nonconforming behavior?

In order to stimulate sustainable innovation where the fundamental rights of the individual are taken seriously and the citizen is at the center, each municipality must have a set of basic elements for each process in order to be able to process data lawfully. This infringement should not be taken lightly. The use of data processing in public spaces is subject to strict requirements. The processing of personal data can only take place lawfully if it is based on a legitimate basis. In that light, it is therefore important to consider some of these basic elements before we go into the results of this study.

3.1 Legality

The GDPR determines, on the basis of open standards, in which cases the processing of personal data, such as through smart city applications, is lawful. Data processing is lawful if at least one of the legal principles mentioned in the GDPR is complied with. The purpose of the processing shall determine which basis applies. Therefore, prior to the start of the data processing, it is necessary to determine the purpose of the smart city application and whether the processing of personal data for that application is lawful. If there is no legal basis for the processing of personal data, the smart city application cannot be used. Even if an application´s purpose is not the processing of personal data, if it still does process personal data then it is an infringement of a fundamental right.

A legal basis that is specifically for municipalities who process personal data in public areas is 'the performance of a task carried out in the public interest or in the exercise of official authority' (Article 6(1)(e) GDPR). In other words, municipalities may only process data in order to exercise their duties if they have been given the proper authority by law. For example, municipalities have the public task of managing the public space. However, this general task alone is not sufficient enough to substantiate the processing of personal data for this purpose. The GDPR requires that the legislation which is the legal basis for the processing, to be sufficiently concrete and foreseeable. Municipalities must therefore be able to demonstrate a legal basis that is precise; general terms of reference are often insufficient for this purpose. What is meant by 'sufficiently foreseeable' will have to be considered on a case-by-case basis. In the public

space, it is almost impossible to ask for the consent of individual citizens. Therefore, the legal basis of consent is practically inapplicable to smart city applications.[3]

In order to determine whether there is a legal basis for the processing, a municipality must also be able to demonstrate that the processing of personal data is necessary for the pursued purpose. In order to do so, the municipality must consider whether there are less intrusive alternatives, and whether the infringement outweighs the objective being achieved (elaboration will be provided further on in this chapter). This requires proper consideration, which must be executed (and documented) before the processing of personal data starts.

Only when there is a legitimate basis can a municipality process personal data. Without lawful data processing, smart city applications cannot be developed or applied. This also applies to pilots. However, the mere fact that the processing is lawful does not mean that a smart city application can simply be used. There are also various other obligations under the GDPR that the processing of personal data must comply with. The main obligations are addressed in this report.

Recommendation: Before you start any smart city application, determine whether personal data is being processed and whether the processing of personal data is lawful. Without lawful data processing, smart city applications cannot be developed or applied.

3.2 Purpose Limitations

In smart city applications, it is not rare that they are initially used as a solution for a particular purpose, but are later also seen as 'convenient' for the solution of other (policy) goals. This is at odds with the purpose limitation principle. Purpose limitation consists of two elements: the purpose must be clearly defined, delineated, and justified and data should not be further processed in a manner incompatible with that initial purpose. An example of this is the use of cameras for enforcement purposes, images are taken for the purpose of enforcement but later, the same images are used for pressure measurements. This can only be done if the new purpose is compatible with the original purpose for which the data was collected and processed. Any new purpose, process or deployment of new technology will have to be re-evaluated by the municipality or the new purpose must fit the municipality's original goals. The expectations of citizens will also play a role in this; the less it is determined as reasonable that their personal data will also be processed for another purpose, the less likely it will be that the new processing is compatible with the original purpose.

3.3 Necessity

The processing of personal data can only be necessary if the smart city application actually contributes to the predefined, concrete purpose and the objective pursued is proportionate to the nature and amount of personal data processed for it (proportionality). No alternative that infringes the GDPR less in order to achieve the same objective should be available (subsidiarity). This should be documented with clear and verifiable arguments in the DPIA, which should also be sufficiently up-to-date. Any processing of personal data that is not deemed necessary cannot comply with the GDPR.

[3] For further information regarding legal bases, please see: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf, p. 20 et seq. Moreover, consent from government organizations is generally not an appropriate legal basis because consent must be given 'freely'. In the relationship between government and citizen, there is a power asymmetry, which means that consent cannot always be given freely.

The Rathenau Institute found in a study on smart cities that it is essential that municipalities clearly define trial projects with clear start and end dates, (measurable) objectives and indicators, and moments of evaluation. However, this does not always happen in practice.[4] The DPA recognizes these findings and stresses that also for smart city applications that are already 'in production', setting concrete goals and monitoring effectiveness is essential to be able to comply with the GDPR. For example, as a part of this study, a DPIA regarding pilots with bodycams that was sent in by a municipality mentioned the objective of 'enhancing safety and their sense of security in the performance of primary tasks. And that in certain situations, bodycams can have a de-escalating effect". Following this, it is stated that the results of the pilot at the end of a three-month period are 'to be broadly evaluated'. It is positive that the DPIA specifies a clear start and end date, as well as the obligation to evaluate. A point of improvement is that the submitted documentation does not clearly indicate which indicators are used to measure the objectives and what criteria is used to determine whether or not the pilot will go into production. This is of importance especially when it comes to establishing 'soft' objectives such as improving 'the sense of security'.

Recommendation: Determine which goals the smart city application will contribute to. Make these objectives as concrete and measurable as possible to determine the effectiveness of the smart city application. General purposes such as 'safety' or 'liability' must be further specified. Also, identify what the next steps will be if a smart city application is unsuccessful or has unwanted side effects.

3.3.1 Subsidiarity

Municipalities will consistently have to determine whether there are alternatives that infringe less to achieve the same goal prior to the deployment of smart city applications. Occasionally (human) interventions or other technical solutions are equally as effective in achieving the same goal, and process less or even no personal data.[5] Therefore, many of the 'solutions' offered by the market must be considered critically. Data processing in smart city applications should be a supportive action and not an end in itself. When purchasing or developing smart city applications, municipalities must always motivate why alternative solutions that process less personal data or no data do not, or insufficiently, contribute to the solution of the objective pursued. The DPA may also ask municipalities for this justification.

Especially in times of Covid-19, there has been a trend in the development of all kinds of technical solutions. Municipalities will have to regularly ask themselves whether they actually contribute or continue to contribute to, for example, the regulation of crowds and whether other solutions are possible.

Recommendation: Prior to the deployment of smart city applications, check if there are alternative solutions to achieve the same goal where no or less personal data is processed. Think from the perspective of the problem and not from the provided solution.

3.4 Transparency

Citizens must be fully informed about the collection of personal data in a public area that they cannot avoid. The DPA has observed that transparency in the development of smart city applications and smart city policies still needs to be improved. Transparency is necessary to ensure that the municipality is accountable for smart city applications that it develops and deploys with the aim of keeping citizens in control of their personal data and giving them the opportunity to exercise their rights if necessary. The incorporation of transparency should not be disregarded in smart city policies. Transparency starts in the

[4] Report Voeten in de Aarde, p. 6.
[5] See also in this context:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf, p. 24 and 25.

way decision-making takes place, how problems that are eligible for technological or data-driven solutions are identified, and in the processes a municipality has when starting a new development. During the development, citizens can play an important role in the process of identifying general and target-specific risks and highlighting other issues (this will be elaborated on later in the report).

After the roll-out of smart city applications, there is a danger of creating a patchwork of various applications within a municipality, making it hard for a citizen to gain an overview of these applications. The DPA sees this as a very important challenge that is being tackled by a number of municipalities through the examination of instruments such as a public sensor registers (more about this in the chapter, 'Regulation by Municipalities and Sensor Registers'). These initiatives build upon the principles of the GDPR, including the mandatory registration of processing operations. Also, the privacy statement of municipalities deserves more attention in order to ensure that all target groups are properly informed. Not only can language play a role in this – e.g. an English translation for tourists or temporary residents – but also accessibility, a privacy statement should be understandable to a reasonable extent by people who are illiterate or do not know the legal jargon.

4. DPIA

During the research, the DPA paid a lot of attention to the role of the DPIA. A DPIA is intended to be a process used to assess the lawfulness and fairness of the processing *prior* to the data processing, identify available alternatives and risks and, if possible, mitigate those risks by taking appropriate measures. Moreover, a municipality must be able to demonstrate both internally and externally why certain choices have been made. A DPIA can also act as a guiding document during the data process in order to monitor the data protection risks and allow for changes in the process, for example, when the purpose of the processing changes. Therefore, in the context of investigations, the DPA regularly requests DPIAs because the content and quality of it can be an important indicator for the DPA.

4.1 DPIA Obligation

Performing a DPIA is mandatory if the risks of data processing are 'high' for the data subject. The European privacy authorities have jointly developed nine criteria to assess whether the intended processing of personal data poses a high level of privacy risk to data subjects. As a rule of thumb, the execution of a DPIA is mandatory if the processing fulfils two or more of the nine criteria.[6] In the context of smart cities, the categories of 'evaluation or scoring', 'systemic and large-scale monitoring', 'large-scale data processing' and 'use of new technologies' are particularly relevant. Projects within the smart city framework will typically fall under two or more of these categories, meaning that the execution of a DPIA is mandatory.

In addition, the DPA has created a list of processing operations for which the execution of a DPIA is mandatory. This applies, inter alia, to the following processing operations:

- Large-scale processing and/or systematic monitoring of personal data generated by devices connected to the Internet that may transmit or exchange data via the Internet or otherwise (*Internet of Things*). Think, for example, of sensors that systematically follow the crowds in public space.
- Sharing personal data in or through partnerships in which municipalities or other public authorities exchange special personal data or personal data of a sensitive nature with other public or private parties. Information nodes are an example of this.
- Large-scale processing and/or systematic monitoring of publicly accessible spaces with cameras, webcams, or drones.
- Large-scale and/or systematic use of flexible camera surveillance, such as bodycams.
- Large-scale processing and/or systematic monitoring of location data from or traceable to natural persons. For example, (scan) cars, telephones, or processing of passenger location data on public transport.

4.2 Implementation of a DPIA

The research showed that a number of municipalities work with so-called 'pre-DPIAs'. A questionnaire is used to determine whether it is mandatory to carry out a DPIA for a given processing operation. While a questionnaire may be a good and easily accessible tool, as a DPO pointed out to the DPA during a discussion, the implementation of such a pre-DPIA should not disregard the needed considerations when it comes to data protection even if it turns out that a DPIA is not required. The responsibility to establish appropriate safeguards and to be accountable applies even if a DPIA is not required.

[6] For more information, see: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

Another point of attention is that DPIAs should be periodically reviewed or updated. For example, one of the DPIAs that the DPA received was a document from 2016 which contained incomplete action points, such as the finalization of a processing agreement and consulting the works council. Once these actions have been fulfilled, the DPIA should also be updated. Also, in the event that the risks which have been identified, change, it is important to periodically review and update the DPIA. Technology used in smart city projects also develops over the duration of the project. Especially now with the COVID-19 measures, the weight of the risks may be change in a number of months or years. In general, it is advisable to periodically monitor and, if necessary, revise a DPIA in order to address existing and possible new risks. A good example of this is, due to a three-year revision deadline drafted by the municipality for DPIAs, a municipal DPO indicated that they were currently reviewing a number of DPIAs which were implemented just after the GDPR came into force.

Recommendation: Keep DPIAs up-to-date in order to be able to demonstrate the current risks of the processing operation. Incomplete action points in an outdated DPIA or failure to document technical adjustments of the processing does not comply with the accountability duty of controllers. Have policies that ensure DPIAs are periodically reviewed and/or updated.

4.3 DPA´s Overview of Received DPIAs

For this research, the DPA requested DPIAs for smart city applications. From the smaller municipalities in particular, the DPA received very few or even no DPIAs. The first explanation is that these municipalities simply do not use smart city applications or only use smart city applications that do not process personal data (for example, when measuring air quality, filling rates of containers, detection loops, etc.). A second reason is that it is often a processing operation that was already applied before the GDPR and has not changed since the GDPR has come into force (examples are registration plates for various purposes, camera surveillance in public spaces, etc.). Thirdly, municipalities indicated that the risks of the project in question do not qualify as 'high' and, therefore, no DPIA was required.

4.3.1 Missing DPIAs?

However, there were a few cases where the DPA questioned the justification of why no DPIA had been executed. This was the case firstly for smart city applications that were started and tested in a pilot format before they were rolled out more widely. Personal data is occasionally already processed during the pilot phase. The DPA stresses that processing of personal data in a pilot or trial must also comply with the rules of the GDPR, including the DPIA obligation. The DPIA should describe the purpose of the pilot and the legal basis along with the possible outcomes and associated risks. A municipality which states that 'to examine whether the public order task under Article 151c of the Municipal Act is also useful as a legal basis' with regards to the use of (mobile) cameras as a pilot does not meet these requirements. In addition, it should be made clear when a pilot has been successful and what happens, for example with the data, if the pilot does not meet the requirements and expectations. It is also necessary to establish how any (un)foreseeable risks are going to be dealt with. This pre-determination will provide a clear framework in which the pilot can then take place. The evaluation of (pilot) projects is also of great importance in order to ensure purpose limitation of (future) projects.

Recommendation: Smart city applications that are in the pilot phase must also meet the requirements of the GDPR if personal data is processed.[7] Therefore, in pilot and trial projects, check whether these projects are GDPR compliant and, if necessary, carry out a DPIA.

[7] See also: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#is-de-avg-van-toepassing-bij-pilots-testen-en-proefprojecten-8161.

Secondly, some municipalities indicated that in the context of certain smart city applications, anonymous data is being used, while the description of the application occasionally suggested otherwise. For example, a municipality indicated that, through a particular app, user location data is processed for a traffic light system, but that 'these cannot be traced back to a person or a specific smartphone' and 'all data collected is anonymous'. Data can only be considered anonymous when a party uses reasonable means (for the designated purpose), to make it unlikely that a person can be identified.[8] This is nearly impossible, especially for location data.[9] Also, correct application of the technology is necessary to ensure anonymity.[10]

Recommendation: Be critical when assessing the anonymity of the data that is being processed; data can only be considered anonymous when a party uses reasonable means (for the designated purpose), to make it unlikely that a person can be identified.

A third point of attention that the DPA would like to highlight is the use of partnerships. A smart city application is often used for several different purposes in collaborations and falls under multiple legal frameworks because the data is shared with different parties within and outside the municipality. This could include partnerships with the police and private actors such as housing corporations. In order to be able to exchange data, it must be sufficiently clear in advance whether the exchange is lawful and under what conditions the parties may process and record the data.[11] This includes, for example, determining which actor may process which data on the basis of which legal basis, for what purpose and for how long this data may be retained. Too often it seems to happen that municipalities and other member parties want to 'explore' these kinds of issues during a pilot. The DPIA is not always present or completed at the start of the processing in a number of municipalities where partnerships have been established. In addition, some DPIAs show that there are uncertainties about the responsibilities of the different parties involved in the smart city application and that the DPIA (therefore) is missing. The DPA stresses the need to clearly invest and document responsibilities *prior* to data processing in a smart city application so that the data exchange takes into account the protection of personal data 'by design'. After all, parties need to know who is responsible for what and citizens need to know where they can exercise their rights; transparency about the processing for citizens and stakeholders is, therefore, essential.[12]

Recommendation: In the case of partnerships, prior to the start of the processing, identify who is the controller or processor. Be transparent about this for citizens as well.

4.3.2 Quality of DPIAs

The DPIAs received by the DPA proved to be of varying design and quality both between and occasionally within municipalities. The difference in quality was evident, for example, since in a number DPIAs the impact of the data processing on the rights and freedoms of the data subjects was missing as well as an analysis of what safeguards there are in order to minimize the risks. Also, not all DPIAs, a clear description of the data processing operation in the smart city application was given, merely a reference to the

[8] There are many misunderstandings regarding anonymization. This short factsheet created by the privacy authorities, describes common misunderstandings and explains them in further detail: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.
[9] See also: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimiteit_en_geaggregeerde_telecomdata.pdf
[10] See also: https://autoriteitpersoonsgegevens.nl/nl/nieuws/techblogpost-praktische-problemen-bij-het-afknippen-van-hashes
[11] See also the 'Cooperation' section of this report.
[12] The European Data Protection Authorities have provided (revised) guidelines ('Guidelines 07/2020 on the concepts of controller and processor in the GDPR') on the concepts of controller and processor. These can help allocate the division of roles in partnerships.

operation in the smart city application was provided. The European privacy authorities have established criteria that municipalities can use to assess whether a DPIA has been executed properly enough to comply with the GDPR.[13] In general, older DPIAs appeared to be of lesser quality than the more recent ones. Firstly, this can be explained because the GDPR has established clearer requirements for the content of DPIAs. In addition, the continued level of growth of 'privacy maturity' of municipalities has also played an important role in the quality of the DPIAs. A mature organization in which citizens' privacy is a well-known and embedded concept and that has seriously taken this into account in the development process, greatly contributes to the quality of a DPIA and its application. See also chapter 8 of this report for more information about the organization of privacy in the municipality.

4.4 Prior Consultation

The DPA has learnt through different channels a number of smart city applications that are in start-up or pilot phases that have been associated with possible high (residual) risks. The DPA points out that a DPIA must be carried out prior to the processing of personal data. If, as a result of the DPIA, the municipality determines that there are high risks that cannot be limited to an acceptable level ('high residual risks'), a prior consultation should be submitted to the DPA as understood under the GDPR.[14] Until then, the processing of personal data (and, therefore, the smart city application) cannot start. The DPA has a maximum of 8 weeks to assess a prior consultation and possibly provide advice.[15] For complex processing operations, an extension of the time limit by 6 weeks is possible. If parties are bound by deadlines, for example, because the smart city application is to be deployed in scheduled events, it is important that parties identify the risks in a timely manner through a DPIA. The DPO can advise whether a prior consultation should be submitted to the DPA.

Recommendation: Do not delay executing the DPIA, try to do so as early as possible in development of smart city applications. This is particularly important for scheduled events or other applications with deadlines. This will allow for the timely consideration of whether the processing may need to be submitted to the DPA for prior consultation. Involve the DPO as early as possible, so that they can provide advice in a timely manner.

[13] Guidelines for data protection impact assessments and whether processing is likely to constitute a high risk as stated in Regulation 2016/679

[14] The processing of police data is subject to a lower threshold when submitting for a prior consultation. Prior consultation is also mandatory if the nature of the processing, in particular using new technologies, mechanisms or procedures, poses a high risk to the rights and freedoms of the data subject (Article 33b(1)(a) of the Police Data Act). This may be of interest in partnerships involving the processing of police data.

[15] For more information, see: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#hoe-beoordeel-ik-of-er-een-restrisico-is-6808

When is there high residual risk?
The DPA is regularly asked what is considered to a high residual risk. There is no definite answer to this; the risks will have to be identified per data process. It is the responsibility of the controller, who has the knowledge regarding the context of the case, to classify the risks. Those risks should be mitigated by organizing the processing operation in such a way that the risks are minimized through reasonable means and measures have been taken to reduce both the likelihood of, and the impact of, a breach of the right to personal data protection. A description of the procedure when a risk does occur in practice (and, for example, results in a data breach) must also be included. With the help of a number of guidelines, it is possible to assess whether the risks still qualify as 'high' after these measures. The controller will have to assess whether these are still high residual risks.
In practice, processing operations with a high residual risk are (large-scale) processing operations which are already subject to the DPIA obligation because the risks are inherent to the process and are, therefore, generally assessed as high. Think, for example, when the data or technology used has such large inherent risks that the effects will also be large or unforeseeable. Especially in the case of government processing operations, which concern a large group of people, the effects will quickly be large. A residual risk is also present if the opportunities or effects are foreseeable, but insufficient measures are in place to address them. A possible residual risk is, for example, the risk of false positives in the deployment of algorithmic systems and the stigmatizing consequences that this may have when using a particular technology.

4.5 Publication of DPIAs

Accountability should be provided not only to the DPA, but more importantly, to the citizens whose personal data is collected (transparency) and to other interested parties. The DPA, therefore, welcomes the disclosure of (parts of) the DPIA on smart city applications, precisely because smart city applications are used in public spaces. As a municipality by providing more insight into the personal data that will be processed, the technology that will be used, the possible risks of the processing and the measures that will be taken to do so, can contribute to growing confidence in the applications used. If desired, the disclosure of the DPIA may omit possible sensitive information that may affect, for example, the security of the processing. In practice, we see that most DPIAs are often not made public. It is advisable not only to consider the publication of DPIAs on an ad hoc basis, but, also, to develop policies or balancing frameworks regarding this. This also applies to DPIAs not related to smart city applications.

Recommendation: Publish as many DPIAs as possible of smart city applications and develop policies on the publication of DPIAs.

4.6 Involvement of Citizens

The GDPR states that, when implementing a DPIA, "where appropriate, the controller shall seek the views of the data subject or their representatives on the intended processing".[16] During the research, the DPA therefore asked the municipalities whether they involved citizens and if they did, how did they involve

[16] Article 35(9) GDPR.

citizens in the development of smart city applications. The research has shown that municipalities often do not involve citizens in the development of smart city applications.

The DPA believes that citizens are more likely to be involved when the legislation provides a less clear framework regarding the violation of the rights and freedoms of data subjects, for example, because the law does not specifically determine which data may be processed and what safeguards should be applied. When the data processing of a smart city application is based on laws and regulations that are less foreseeable, while the level of breach by the citizen can be perceived as high or poses high risks to citizens' rights and freedoms, it will be more likely to involve citizens. Especially in smart city applications, it seems intuitive to involve citizens. Due to the (municipal) laws and regulations, municipalities have broad tasks, therefore, not every use of a smart city application can be expected in advance.[17] Moreover, for example, the tracking of human behavior through the use of smart city applications could be considered as intrusive and may even lead to a *chilling effect*, where people start to behave differently or refuse or even fear using public space.

With complex, innovative smart city applications, it seems almost impossible to understand the possible breaches of the rights and freedoms of all the various individuals whose personal data are being processed. In order to identify these risks in the context of the mandatory DPIA, the opinion of the citizens concerned is of great value. The GDPR provides a very suitable starting point for municipalities to make citizens part of the smart city they live in. In view of the fact that Article 35(9) GDPR relates to the DPIA, it is recommended to include in the DPIA whether and how the municipality asks the data subject for their opinion. This will make it possible to raise awareness of the implementation and to account for the extent to which citizens (and other stakeholders) have been asked for their views. A good example is a municipality that has included in the DPIA as a standard question whether the data subjects (or their representatives) have been asked to give their perspective on the processing activities (including justification of the choice) and how follow-up was given to the input (and a justification if this has not been done).

Recommendation: Pay attention in the DPIA to whether data subjects have been asked for their views and how these opinions have been followed up. The higher the possible risks are, the more unclear the legal basis is, or the higher the degree of perceived infringement, the more likely it will be to involve citizens.

[17] It could even lead to the conclusion that processing does not meet the legality criteria (see the chapter 'Legality').

5. Reflection: Participatory DPIAs and administrative law mechanisms in Smart Cities

Authors: Athena Christofi†, Jonas Breuer, Olia Kanevskaia†, Ellen Wauters†*
*Organization: † CiTiP, KU Leuven; * SMIT, Vrije Universiteit Brussel*
Functions: Researchers, Smart-city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem (SPECTRE) Project[18]

We warmly welcome this report and the opportunity it provides to understand smart city practices in the Netherlands and reflect on the future. The challenges cities face in becoming smart are similar throughout Europe and the attention and recommendations of the DPA can facilitate learning beyond the Netherlands.

In the following paragraphs we reflect on two issues emerging from the report that we find particularly worthwhile for smart cities and data protection in the EU.

Participatory DPIAs
We welcome the emphasis on the role of citizens in the development of smart-city applications. Citizen participation has a fruitful tradition in other domains and shows promising potential for assessing impacts of data processing in public space. We hope that this emphasis brings together relevant authorities, cities and umbrella associations to collaboratively develop best practices tailored for DPIA methodologies. Guidance is much needed.

Considering the richness of fundamental rights in the European legal tradition, assessing risks of a processing operation to individuals' rights through DPIAs could be a powerful legal tool to enable what is often described as ethical smart-city development. To account for the plurality and complexity of rights at stake, DPIAs should include multi-perspective risk exploration, and become participatory: Article 35(9) GDPR enables -if not requires- this. Participation in DPIAs is important because rights are not static - their meaning and reasons justifying their limitations are evolving with socio-technological change. Citizens may also perceive risks to their rights differently: in a smart city, one might fear being observed or nudged in public space. Couldn't this amount to a curtailment of privacy, or freedoms of expression and association? Citizens' perceptions are vital to enable municipalities to anticipate and address risks. Citizens involvement can also provide further democratic legitimation for decisions of city officials and councils: such legitimation is particularly important when legal bases and processing purposes are unclear.

Still, municipalities often do not - or are not able to - directly involve citizens in complex discussions about technologies, risks and rights despite the potential of Article 35(9).

They face important challenges. How to operationalise diverse input of those affected by smart-city applications? How to assess concrete risks of an application before its implementation or development? Participation may take additional time and money, and may disturb development processes and the goal

[18] Project funded Research Foundation – Flanders (FWO S006318N). This reflection gives the views of the authors and does not present the position of the research centres/universities or the funding organisation.

to provide innovative solutions. Also, representativeness is as crucial as it is challenging. How to sample a group that mirrors the heterogeneity of affected individuals/groups? How to discuss complex topics with groups that have no prior knowledge (or language skills)? And, if participation cannot be representative, is it even useful? We are convinced it is, and note that Article 35(9) also enables the involvement of '*representatives*' of data subjects. Civil society groups, public bodies and entities with mandates to represent certain groups do exist in cities and may represent citizens who may have no interest in being involved. Methods and tools to facilitate public participation are abundant but remain separated from DPIAs due to, e.g., abstract legal provisions, vague guidelines, compliance-oriented controllers, the complexity of technologies. We hope that the DPA's attention in this report will launch efforts to answer the many open questions, as a lot more is still needed to realise participatory DPIAs in (smart) cities: clear guidelines, support and incentives for different actors involved.

Leveraging administrative law

Supporting data protection with administrative law measures could also enhance the protection of citizens' rights. The initiative to register sensors in public spaces is a positive step in this direction. The report rightly notes that it can improve transparency over data processing in the city. But also, it may enable a more strategic risk assessment that could be desirable and necessary to support long-term decision-making. Smart cities are nowadays a patchwork of different projects, and proportionality and risks are examined within the boundaries of specific projects. Little attention is given to possible impacts from the combined effects of the different interventions that slowly aggregate in public space and urban governance (Edwards, 2016, 52-53). Yet, perhaps the most difficult questions concern projects' accumulation. How much privacy loss is acceptable for the urban dweller? At which point could datafication transform the city into an alien environment for digitally illiterate citizens? Administrative law could create participatory processes requiring the mapping and strategic assessment of impacts - inspiration may be drawn from environmental law, which includes processes aimed to assess cumulative impacts. Administrative law could also institutionalize the involvement of democratically-elected city councils, by requiring them to discuss and approve the purchase and use of data processing technologies in smart cities (Galič, 2019, 353).

More attention should also be given to public procurement's role in smart cities. As technologies are designed and deployed by private vendors, the relationship between them and municipalities should ensure that control and accountability for protecting citizens' rights primarily rest with the latter. There are evident links between public procurement and data protection, but operationalizing them is difficult. Procurement is tailored for objectives like open competition and sound procedural management, so inserting participation and fundamental rights considerations in highly bureaucratic processes can be challenging (Mulligan and Bamberger, 2019). Is/should there be space for participation and public hearings during the procurement process? What are the necessary requirements to introduce in tendering documents and contracts to protect citizens' rights? Smart-city tailored data protection standards could possibly facilitate the selection of suitable partners, yet certification and codes of conduct under the GDPR are at their infancy. While procurement could be used strategically for a rights-respectful city, the aforementioned raise pertinent questions that deserve more attention by smart city research and practice.

Recommendations

We would like to conclude with three final recommendations for cities. First, leverage Article 35(9) GDPR. While guidance is still needed and DPAs could have a more active role in (co)developing such guidance, cities could only learn by doing. Second, it is important to educate city councils about the possible challenges of smart cities for fundamental rights, and how these may be addressed, for instance through training and workshops. Increasing council members' digital literacy can lead to better decision-making and more democratic control over smart cities. Third, we recommend cities to increase cooperation between the data protection and procurement departments, e.g. by establishing regular consultations or the co-drafting and -negotiation of contracts.

References

Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 2 Eur. Data Prot. L. Rev. 28 (2016)

Maša Galič, Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space. Optima Grafische Communicatie (2019) <https://pure.uvt.nl/ws/portalfiles/portal/31748824/Galic_Surveillance_19_11_2019.pdf>

Deirdre K. Mulligan and Kenneth A. Bamberger, 'Procurement As Policy: Administrative Process for Machine Learning' Berkeley Technology Law Journal, Vol. 34, 2019

6. Getting a Grip on Smart Cities

Digitalization of society is more than just the protection of personal data, which often focuses on the rights of the individual. Smart cities also call attention to social and democratic values such as data ownership and fundamental rights. These values touch upon the collective and long-term developments and effects of smart city applications. Data protection should therefore not be seen as an isolated element in digitalization and smart cities, but as part of a wider playing field where other, occasionally conflicting, interests also play a role. The use of technical possibilities should be part of a broader discussion within municipalities where the inclusion of these social and democratic values is essential. Therefore, the DPA payed attention not only to the GDPR, but also to policy-making around smart cities, ethics, the role of politicians and citizens as well as sensor registers.

6.1 Smart City Policies

The Dutch smart city has come to a turning point where it should grow from a patchwork of small-scale projects to a broader vision of how technology and data should be utilized in the public space. Developing policies around digitalization and smart cities, using the frameworks of the GDPR, is crucial.

Through policies municipalities can define their core principles, such as the protection of personal data, thereby creating frameworks that will determine the future development of all smart city applications rather than having to specify the procedure per project or development. Through the use of standard frameworks, conflicting choices made in different smart city applications can be avoided which is an occurrence that is not rare in practice. Moreover, it demonstrates accountability towards citizens about the principles/values that the municipality applies, such as the protection of personal data.

The research has shown that mainly the larger municipalities indicate that they have policy documents regarding digitalization/the digital city. Also, they regularly refer to the 'Principles for the Digital Society' published by the VNG, which has been signed by all municipalities.[19] Smaller municipalities, on the other hand, often do not have a specific policy regarding smart cities.

Principles and policies do not always provide sufficient guidance for practice. Further development of these principles is therefore necessary in order to be able to apply them effectively. An example of this is the application of privacy by design by municipalities: it is important not only for a municipality to apply *it*, but above all to develop *how* it applies it to matters such as retention periods, security technologies (including anonymization), and the rights of data subjects. Therefore, we encourage 'leaders' to (continue to) play a role in further elaborating and sharing knowledge about this topic, so that smaller municipalities can also benefit from this.

Recommendation: Define policies and principles around smart cities/digitalization that respect the frameworks of the GDPR and implement them through concrete instructions for the workplace. Make use of existing knowledge and experience so that it can be shared with other municipalities.

6.2 Ethics and Smart Cities

Laws and regulations are often described as 'tangible ethics'. However, ethics cannot be replaced by a set of laws and regulations. This became clear in the municipalities the DPA researched. Many municipalities call for an ethical framework that is broader than the applicable laws and regulations such as the GDPR,

[19] https://vng.nl/artikelen/principes-voor-de-digitale-samenleving

which focuses mainly on the rights and freedoms of the individual. In many cases, this need is reinforced by citizens and municipal councils who want to know not only whether new projects comply with legal frameworks, but also whether it is appropriate to use technology in this way and at this place. Part of this 'is it right' question is addressed by the GDPR and its accountability obligations. When these obligations are completely and properly fulfilled and followed up, then an important part of the ethical questions are already addressed and the ethical considerations are clarified. The need for a comprehensive ethical framework is understandable, but when processing personal data in smart city projects, the municipality should start with a suitable and high-quality DPIA where a part of these questions are already addressed. Needless to say, this can be complemented in later stages by an ethical framework that addresses themes that are not covered by the DPIA, and the DPA encourages this. The GDPR also requires, in several respects, that not only the right to data protection should be considered but also other fundamental rights.[20]

The DPA has observed that councilors and municipalities want to conduct a dialogue about the ethical questions regarding smart cities. Conducting a broad dialogue such as that is advisable. A broad dialogue with a wide range of stakeholders could address questions about the technical, legal, organizational, and ethical aspects of the use of technology by and within a municipality. Also, questions about transparency towards citizens and about the inclusion of citizens in developments can be a part of that discussion. This may result in a framework or vision of the municipality on digitalization in general, and smart cities in particular. Some municipalities are already working with ethical frameworks or have an ethics committee that is involved early in the developments in this area. In municipalities where this is present, it is considered to be valuable and the municipal council is also seen as a place where questions about ethics should be asked and discussed. The DPA considers this to be a positive development.

Recommendation: Ethics cannot be replaced by adopted laws and regulations. Therefore, start by executing a DPIA in order to address questions regarding data protection. For questions that are broader than the GDPR, an ethical framework can be developed and applied.

6.3 A Democratic Smart City

The public space must be at service of society as a whole. The deployment of smart city applications should therefore focus on citizens. This calls for ways of involving citizens, giving insight into and a degree of control over the technology and data collected and used in public spaces. Smart city applications appear to be to a large extent technology- and data-driven in The Netherlands, and mainly for municipal and private interests, such as maintaining public order and commercial purposes. Only in a number of cases are municipal smart city applications focused on engaging the citizen, facilitating the needs of residents or strengthening the democratic system. There is a danger that *Dataism*, the belief that data is a solution to all problems, might hinder data sharing that respects the rights and freedoms of the individual and thus, make responsible and sustainable innovation impossible. In order to ensure that the deployment of smart city applications is implemented more democratically where citizens also have a (indirect) say, the DPA calls upon the municipal council and board. The DPA sees this as an important task for the municipal council and board, as well as for civil servants to involve citizens and residents of smart cities in the deployment and decision-making of smart city applications.

[20] For example, in the context of the DPIA, the EDPB guidelines determine: "(...) the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion."

6.3.1 Role of the Municipal Council and Board

Municipal councils play a crucial role in the development of, and debate around, smart cities. They have the role of supervising the Board of Mayors and Councilors. The municipal council is the democratically elected representation of citizens in a municipality who deserve explanation, transparency, and the possibility to influence the board. The DPA believes that the municipal council can play an important monitoring role in smart city and digitalization aspects. For example, the municipal council can ask questions about the realization of policy objectives of a pilot, the options for alternative, "non-technological" solutions, and the needed safeguards for a smart city application.

We notice that smart cities are not on the agenda yet in all municipal councils. Digitalization and its social impact are rarely the subject of discussion.[21] The lack of knowledge among councilors does not help. When municipal councils are not sufficiently aware of the specificities regarding smart cities and its relationship with the GDPR, then they are not in position to ask the right questions. In addition, this may inadvertently lead to motions from municipal councils that cannot be properly implemented because they appear to be in conflict with laws and regulations or ethical frameworks or policies of the municipality. In some municipalities, we see councilors taking initiatives to educate their municipal councils about issues related to privacy, ethics and the more technical side of smart cities. Also, in a few cases, there is good collaboration between the municipal council and the DPO. These are developments that the DPA welcomes.

The DPA advises municipal councils and political parties to gain more knowledge about the digital world, in order to strengthen their capacity for effective control and enable them to ask good questions about new initiatives. In the end, more substantive discussions will take place, which benefits the considerations taken about smart cities. A framework like the one created by the Rathenau Institute can be a tool to discuss not only data protection, but also ethical and societal aspects in the council.[22] Due to its supervisory role, the DPO can also play an informative role in informing the council about specific data protection issues. The board, municipal councils and DPOs, can also make use of the input of civil rights movements, since they also think critically about these issues, so that the rights and freedoms of citizens are carefully considered in a good and timely manner. This will make it easier to consider problems more in depth and ask critical questions about the current plans.

A municipality should not only talk *about* citizens, but also *with* citizens. Especially when smart city applications continue to affect the rights of citizens, it is important, and in some cases even obligatory, to involve them in the discussion so that their perspective can be taken into account in development and risk analysis.[23] Moreover, the municipal council could ask citizens about their views on particular smart city applications, if the municipality has not already.

Recommendation: Ensure that the municipal council is more informed about the deployment and process of smart city applications by the municipality, so that there is more debate on the topic. There should be adequate knowledge about digitalization and technology within the municipal council. If necessary, the municipal council can be informed by experts, such as the DPO, civil rights movements and (municipal) experts.

[21] Raad weten met digitalisering, pg. 18 et seq.
[22] Raad weten met digitalisering.
[23] See also the section 'Citizens and Solutions' of this report.

In addition to the monitoring role of the municipal council, the DPA also researched the role of councilors. In practice, we see that not every municipality has a councilor who deals with digitalization and smart cities. The responsible councilor will therefore differ per executed application. This is not a problem in itself, but the effect may be that digitalization and the deployment of smart city applications from different sectors are addressed with a limited perspective, despite that the effects are cross-sectoral. Therefore, it can have added value to make a councilor specifically responsible for digitalization. In the municipalities where this is the case and that the DPA has spoken to for the purpose of this research, this is perceived to have a positive impact on the management of digitalization developments. This councilor preferably has knowledge of the subject and can help determine the frameworks of the municipality in relation to digitalization issues, including smart cities. By have a specifically appointed councilor, the municipal council has a (specialized) point of contact and this councilor can gain an overview and ensure that the entire municipal organization works with the same principles. Even when they touch upon the 'classical' domains such as the environment, mobility, and safety, that are the responsibility of other councilors and the mayor.

Recommendation: Explore the possibility of appointing a specific councilor who deals with digitalization or make agreements about who within the board oversees cross-sectoral digitalization issues.

6.3.2 Involvement of Citizens

Data is only a facet of reality. In order to gain a real understanding of a public space, it is always necessary to keep an eye on the underlying cultural, political, and social aspects. Solutions to certain (social) problems can be found elsewhere and do not only need to be found in data and technology. Technology is also not neutral; data is generated and displayed on the basis of choices made by people. These choices can be, for example, which data is collected, which locations are used, and how the data is visualized. The real knowledge of a public space lies with its users: the citizen. Therefore, when determining the desirability, possibilities, and risks of collecting data in and about a public space, it is important in many cases to ask for their opinion at an early stage (such as when performing a DPIA). While doing this, special attention should be paid to the diversity of the citizens involved.

The fact that citizens are more often not involved in the decision-making and development of smart city applications is partly due to the fact that many smart city applications are top-down solutions, where the municipality determines how technology is used for certain problems and not the citizens. Citizens are involved more when municipalities choose to develop smart city applications through a 'bottom-up' approach (i.e. more initiation and influence from the citizens). A notable observation in this context is that projects revolving around new technology are in many cases given priority to projects that promote transparency or strengthen the democratic process. For example, projects that make sensors and data comprehensible, give citizens a role in the process or strengthen the democratic process. The growth of initiatives to facilitate this is clearly falling behind, despite the fact that these projects would give back power to the citizen and actually make the city smart.

When citizens are involved by municipalities, there is no clear form or approach to it. Some municipalities indicate that citizens are already indirectly involved, for example, through the elected representatives of the municipal council. None of the municipalities that were a part of this research have worked out when citizens will be or will not be involved in initiatives. This is mainly determined on an ad hoc basis. Well-known forms of involvement have been mentioned by a number of municipalities, such as citizen panels, residents' evenings and information sessions. In addition, more and more municipalities seem to explore opportunities for online civic participation, where citizens are able to provide input about (intended)

municipal developments through online channels. Although these tend to involve developments other than specific smart city applications. In general, municipalities that involve citizens seem to have positive experiences with this process since the support of smart city applications grows. Some municipalities indicate that they want to involve citizens, but are still struggling with how to execute this in practice. When citizens are asked for their opinion, municipalities tend not ask citizens about privacy issues regarding smart city applications. Municipalities that involve citizens on privacy issues indicate that representation of the questioned group is an important point that still needs improvement.

In addition, it is not always necessary to actively involve citizens, for example, when the risks associated with certain smart city applications are limited. However, when personal data is processed in a public space, it usually means that there is large-scale processing which has its associated risks. Since citizens do not have a choice when it comes to these types of processing operations and cannot always foresee the consequences, the involvement of citizens in smart city applications should, therefore, be necessary in most cases. What the most appropriate form of engagement is needs to be carefully assessed.[24] When citizens are asked for their opinion about an intended process, it is interesting to question them not only about their individual perspective, but also, as a representative of (a part of) society. Due to the fact that smart city applications concern the public space, the perspective of all groups, including that of minorities, should be taken into account in order to involve a broader range of society in the development of a smart city.

Recommendation: Consider in which cases, when and how citizens will be involved in the development of smart city applications. Consider in particular the role of citizens in determining the desirability, possibilities and risks of collecting data in and about public spaces. Explicitly address the privacy aspect of smart city applications.

6.4 Regulation by Municipalities and Sensor Registers

In addition to municipalities, private parties can also use sensors to collect (personal) data in public spaces. The use of data processing by private parties in the public space is subject to strict requirements and is in many cases prohibited. The processing of personal data in the public area is primarily the responsibility of, or must have been made possible by, the (legislative) government. A private party like a company usually has no authority there.[25]

When sensors are present in a public space, a citizen will primarily address the municipality that manages and controls the public space. Even though municipalities are not the controller of these sensors as understood under the GDPR, they cannot remain on the sidelines as the authority of the public space. Certainly not if the use of sensors is contrary to municipal policies and principles. At the moment, we see that municipalities do not properly map the processing of personal data by private parties in the public space. The DPA, therefore, sees this as a task for municipalities to examine how to control these sensors and other applications of private parties that process personal data, either through regulation or not. It is important for municipalities to maintain a grip on the sensors in public spaces and its associated data collection in order to be able to govern them and to provide transparency.

A number of municipalities work with sensor registers. In those (public) registers kept by the municipality, citizens can consult which sensors or other applications (such as cameras) are used in public

[24] The so-called 'participation ladder' could help provide an answer to this question.
[25] However, this does not mean that personal data may never be processed by private parties in a public space. See also: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq.

areas. This concerns not only sensors and other applications of the municipality, but also private parties. The DPA welcomes these initiatives. A sensor register can be a tool to increase transparency, involve citizens, hold actors accountable, and control developments both within the public and private domains of public space. Until now, these registers are kept mainly on the basis of voluntary cooperation. Municipalities indicate that they lack (legal) possibilities to understand which sensors and applications are in the public space, who is responsible for it and what these sensors do exactly and what data they process. The municipality of Amsterdam intends to introduce a notification obligation for sensors in the APV[26] and the municipality of Utrecht has a policy that requires that all cameras in the public space to be registered.[27] A first step in this respect could be the introduction of a register so that citizens can be informed about these sensors. Whether or not these are linked to observable characteristics that make sensors recognizable.

A second step could be to examine, in the long term, whether it is possible and desirable to attach conditions to the use of sensors and collection of data in public spaces, for example, through a licensing system. Municipalities can then impose conditions on private parties, such as mandatory use of open source technology, requirements on how to inform the public, for example, through the use of signs, the storage of data in the EU or the Netherlands, etc. It is advisable (with regards to the VNG) to further explore whether, for example in the Municipal Act, there should be an explicit possibility of being able to create rules regarding the placement of sensors in public spaces by private parties. Moreover, the question remains whether the collection of data by private parties is permitted under the GDPR or is even desirable; a licensing system does not exempt parties from complying with the GDPR. Municipalities can gain a better understanding of the collection of data in public spaces by linking conditions and applying further restrictions if they are breaching the GDPR and/or municipal policy.

Recommendation: Research what ways municipalities can gain an insight into the sensors that are placed in public space by third parties if these process personal data. Share information about these sensors with citizens, and if possible, through a central location such as a sensor register. Consider (together with other municipalities) the possibility and desirability for municipalities to establish conditions that must be fulfilled prior to the use of sensors in a public space, so that citizens can continue to move freely in the public space.

[26] https://bekendmakingen.amsterdam.nl/bekendmakingen/publicatie/inspraak/inspraak-sensoren/
[27] https://www.utrecht.nl/bestuur-en-organisatie/privacy/cameras/

7. Reflection: Beyond Participation, Put Citizens at the Heart of Smart Cities

Author: Judith Veenkamp
Organization: Waag
Judith Veenkamp works for Waag, a Future Lab for Technology and Society, and leads the team that researches the role of citizens in innovation and digitalization. From groups of citizens who measure air quality themselves to patients and caregivers who design their own care solution.

With the child benefits scandal and its aftermath still fresh in our memory, no one will contradict you if you argue that technology should be developed and used on the basis of public values. The same applies to the technology used in the so-called Smart City. The technology and data used in Smart Cities are a means to address societal issues. Not only the design and development of the technology, but also the context in which these applications are subsequently used, is currently undergoing an intense debate. The ideas of Herman Tjeenk Willink in 'Groter denken, kleiner doen'[28] are being rediscovered and revived. The call for a new culture of governance where the position of the citizen in relation to the government is reshaped is increasingly becoming louder. This is also apparent from the `Adviesrapport Betrokken bij het klimaat' (Advisory Report Involved with the Climate) of the advisory committee, Brenninkmeijer, and the publication of the report `Grote opgaven in een beperkte ruimte' (Big Challenges in a Limited Space) by PBL Netherlands Environmental Assessment Agency, where explicit attention is paid to the need to involve citizens. But we really need to take a step further: not only involve citizens, but make sure that citizens' initiatives **from** society get their rightful place to influence policies and direct Smart City applications.

Even though the public debate on technology in the city is shifting and the role of the citizen is regularly mentioned, the reflex of optimist tech solutionism remains strong, a belief that sees technology as the solution, without knowing exactly what for. This is why I was surprised by the fanaticism with which, at the beginning of the coronavirus crisis, camera cars were used by the municipality of Rotterdam to maintain the 1.5 meter rule in public space, without thinking carefully whether this means exceeded its purpose. There are blatant questions to be asked about the way the technology of a camera car determines whether or not the 1.5 meters is being adhered, but what is especially remarkable is that in a crisis situation, the possibility to speak to each other about the necessity of keeping distance is completely dismissed. A method that is many times more human and has a more direct effect than when the camera images are viewed live from a control room. In my opinion, proportionality/subsidiarity was missing here. The importance of this is discussed in this DPA report. Would this measure also have been used if residents had been able to think along about ways to incentivize or enforce compliance with the 1.5 measure?

Also in less acute crisis situations, such as the energy transition, housing, and the nitrogen crisis, innovation and technology are regarded with hope. Around me I see the same administrative reflex emerging around the concept of the *digital twin*. The *digital twin* is a digital representation of our living environment that runs on data collections and predictive models. With a digital twin, you can calculate and simulate the impact of certain interventions. Also here, the temptation is high to see the *digital twin* as the Holy Grail, causing goal and means to get confused. Private parties work together with governments to

[28] Willink, Herman Tjeenk (2018). *Groter denken, kleiner doen.* Amsterdam: Prometheus

develop this instrument, practically a dashboard 2.0. First of all, it is good to keep in mind that this is always a representation of reality and, thus, not reality itself. The people who develop the technology, often working for private companies or the government, determine which data is or is not taken into account and write the algorithms that run the predictive models. Secondly, there is a real risk that also in this tech innovation, the citizen will ultimately act as the subject of discussion, rather than be a part of it. Not only do they have the right to know what relevant data is collected, they should also have an equal place at the table when the *Digital Twin* is developed and applied. There it will determine which data is collected, linked, and used and under what conditions. Then they can have a say, can co-design, and co-decide.

After more than a decade of experimentation and *pilots*, the Dutch smart city has come to a turning point. There is a need for a broad vision of the use of technology and data to shape, maintain and control public space. A vision where technology strengthens democracy rather than crumbles it, and effort is made to have *smart citizens* rather than *smart cities.* Residents are by definition experts with knowledge and experiences of their own neighborhood. By giving them an equal place at the drawing table from the very beginning of a Smart City application, they can play a valuable role in co-designing the technology and deploying their knowledge and expertise about their own neighborhood to take the Smart City application to a higher, more democratic level. Only through this way will it be possible to embed public values and build checks and balances so that technology does not harm the democratic system but instead strengthens it.

This report shows that some municipalities are working towards greater transparency with public sensor registers and processes in which technological applications in public space must be reported to the municipality by third parties. However, it seems that there is still a lot of work that needs to be done. Thus, it is very interesting to do the mandatory DPIA (Data Protection Impact Assessment) together with citizens. The DPIA then becomes a tool to start the process of having a timely conversation with the resident and/or users about a social issue and how technology can provide support. It is important that there is a competent process supervisor who can oversee this and who can create space for the citizen and protect it. The Data Protection Officer can play an important role in this.

But to truly create a new culture of governance where you as the government and citizen tackle issues together and determine the way forward with the help of technology, it will be necessary to show more ambition. Participation and “engagement of citizens” seem to be the magic words in the land of government. However, this is still often about the government who creates the frameworks that allows citizens to participate. The municipality devises where and when citizens’ input is desired and organizes a participatory evening, design session or, if necessary, a citizen’s consultation. The same applies to DPIAs in which citizens have a say. The residents are thanked, the municipality withdraws into its establishment and will brood over policies, programs and interventions. It is time for the municipality to look in the mirror and critically scrutinize its own way of working. Let go of your own system and go into the communities. As a municipality, join existing citizens’ initiatives where there is already a lot of energy and expertise and where concrete societal issues are worked on wholeheartedly. Challenge yourself to let this be the starting point of the development and deployment of technology in public space. Only then will Smart City applications be created that are at service of society.

9. Organization of Privacy in the Municipality

The fundamental right to data protection cannot be just be understood in theoretical terms, but must also be implemented in practice. This requires a strong foundation of data protection in the municipal organization. A well-developed smart city therefore requires mature organization of privacy. A municipality that acts as a reliable and steadfast entity can optimally protect citizens' rights and take advantage of the opportunities that exist to democratize technology and data and to give power back to citizens. Therefore, in this chapter we also pay attention to the organization of privacy in the municipality.[29]

9.1 Privacy as the Basis

The design of the organization of privacy depends on the character and size of the municipality. In several municipalities, this organization is still under construction and in different stages of maturity. Many municipalities still do not organize enough privacy in the execution of their work. The function and role of the DPO is not always sufficiently addressed and too often the obligations under the GDPR are seen as a legal obligation that seems to have little effect in practice. Privacy must be at the heart of the organization, especially in a public organization such as a municipality where a lot of citizens' personal data is processed.

Organizing privacy requires municipalities to free up enough people and resources. These conditions are far from being met by all municipalities. Good positioning of people in the organization is also important. For example, some municipalities have appointed decentralized privacy officers. This is beneficial to the municipality because decentralized knowledge of practice is often necessary to provide a good assessment of specific issues. Especially when smart city applications arise from decentralized organizational components, such as traffic or enforcement.

In addition, it is necessary that the discussion about the importance of the right to data protection is held within the organization (in a timely manner). Too often, data protection is seen as a right that hinders other interests, such as security. This creates uncalled for polarization, because the right to data protection is not an absolute right that goes beyond other rights, nor does it apply to, for example, the right to security. We have seen that the excuse that 'nothing can be done because of the GDPR' usually comes back when data protection has not been taken into account from the beginning of discussion. It is by involving aspects regarding data protection at an early stage that polarization can be avoided.

Recommendation: Provide sufficient personnel and resources to organize privacy within the municipality, so that data protection is given sufficient attention in the organization and can be included in the process in a timely manner.

9.2 Data Protection Officer (DPO)

The GDPR mandates that a municipality must appoint a DPO and has ascribed to this position a set of tasks, independence and protection in order for the DPO to be able to perform their function. The DPO plays a key role in the organization of privacy within a municipality. The role and position of the DPO are

[29] In the context of this study, the DPA did not explicitly question the organization of privacy within municipalities, but asked a number of questions regarding this topic in the interviews. The findings of this report were made on the basis of external signals and contacts the DPA maintains with stakeholders, municipalities and DPOs.

taken into account in the supervision of the DPA in the context of responsibility and accountability. The DPO cannot be dismissed or punished for the performance of their duties. Protecting the municipality from missteps and protecting the citizen is an important task for a municipal DPO. A board that relies on its own organization must take the role and position of the DPO seriously and give sufficient resources and capacity to fulfil this.

A misunderstanding that is still common in practice is that the DPO is responsible for the drafting of and compliance with the GDPR. That is not the case: the Board of Majors and Councilors is responsible for this. The DPO provides advice regarding compliance with the GDPR within the frameworks of the organization and municipal practice. The DPO advises how processing can take place lawfully, fairly, and transparently, in accordance with the principles of *privacy by design*. Therefore, the DPO should be involved in the development of applications and policies in a timely manner. The DPO also functions as an internal supervisor who is aware of GDPR-related developments and can identify possible problems because they have an overview of ongoing development and bring these to the attention of the responsible person. The DPO should therefore also have access to the board. The DPA also observes that the DPO is often held responsible for carrying out DPIAs, but this is not its role; the DPO provides advice. The DPO can also be an important source of information for the municipal council in its decision-making.

In practice, the DPA sees a varying picture regarding the role of the municipal DPO. The performance of this role depends on the size of the municipality and the associated nature of work and processing. Therefore, it may be that municipalities where the number of processing operations are limited can achieve the proper implementation of this function by means of a part-time DPO. However, we note that the number of processing operations in municipal practice is growing and many municipalities still struggle to integrate and comply with all GDPR obligations in its organization. The DPA would like to emphasize that the DPOs play an important role in managing the development of, among other things, smart city applications, but do not always have the means, resources, or ability to from the municipality. The reason for this can differ from organizations that are still developing into a mature organization and, therefore, do not make the best use of the DPO or burden it with wrong tasks, to municipalities that do not fully use the DPO or do not allow for proper execution of the role. This is an important cause for concern for the DPA.[30]

Recommendation: Make sure that the DPO can fulfill their function independently and in accordance of all the requirements. The DPO is not responsible for policies and should not be positioned as such in the organization. Access to the board is essential in order for the function to be executed properly. Ensure that the DPO has and is able to gain knowledge of processes and municipal practice in order to be able to provide optimal advice and supervision. The DPA has made recommendations regarding the positioning of the DPO.[31]

9.3 Cooperation

Municipalities have a challenging and comprehensive set of tasks. No municipality indicates that it can carry out all its tasks completely independently. Many municipalities outsource tasks or work together with other municipalities in cooperation. With regards to smart cities, technological developments are going very fast. It is almost impossible for municipalities to be fully informed and stay fully informed of all of these technological developments. This often involves cooperation with other, including private actors,

[30] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verzwaart-toezicht-op-gemeente

[31] See also the DPA's recommendations regarding the positioning of the DPO: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht

who, for example, develop a smart city application on behalf of a municipality or together with academic and educational institutions, citizens, or other governmental institutions (such as ministries, regional associations, provinces, police, etc.). Cooperation can take many different forms, such as general policy-making for smart cities, knowledge sharing and the joint development and implementation of smart city applications.

Cooperation and the sharing of knowledge offers many opportunities. Municipalities often encounter the same questions in the context of smart city applications. For example, when answering legal issues (e.g. about the legal basis or risks), policy questions (e.g. which smart city applications are effective in addressing a particular problem and how can citizens be involved) and implementation issues (e.g. formulating purchasing conditions). In addition, joint purchasing pathways could, for example, help to establish a stronger position vis-à-vis influential market players. In particular, smaller municipalities with fewer resources can benefit greatly from support from other larger municipalities, academic organizations, or umbrella organizations such as the VNG. The DPA welcomes these forms of cooperation.

However, working together on the development of smart cities should not turn into negligence. The municipality is and will continue to be responsible for the smart city applications it uses, including those used in a collaborative relationship. Municipalities should therefore always reflect critically on the propagated solutions offered by smart city applications to determine whether they are appropriate for the municipality concerned. A smart city application in one municipality does not necessarily have to be successful in another municipality if it does not meet the specific objectives and problems in the municipality. This may even be contrary to the GDPR (see also the chapters Purpose Limitations and Necessity). It is therefore essential that municipalities continue to think about the problem that the application would contribute it and not about the solution provided.

There is a lack of critical reflection within the municipal organizations, for example, in the case of contracting or issuing of permits. Simply indicating that a contractor must comply with the laws and regulations, and thus with the GDPR, is of course necessary, but given certain specific activities, occasionally additional measures are required. Especially when the contractor starts processing data on behalf of the municipality, the GDPR has additional requirements. Therefore, municipalities are advised to introduce more in-depth requirements and safeguards in both procurement and permit procedures. We illustrate this in the context of smart cities, namely *Mobility as a Service* (MaaS) in the next chapter.

Recommendation: Seek cooperation to address common issues around smart cities. Let 'leaders' take a leading role in this. At the same time, remain critical of the deployment of smart city applications, even if they are widely shared and applied; a smart city application in one municipality does not necessarily have to be successful in the other municipality when it does not meet the specific goals and problems of the municipality.

10. Development in Practice: MaaS

Traffic and mobility within and around a municipality are important points of interest for municipalities, which translates into projects that are characterized as smart city applications in many municipalities. Municipalities are seeking, individually and in cooperation, opportunities to make mobility more sustainable, a better use of capacity, but also, sufficiently flexible to meet the needs of the inhabitants. These mobility projects are covered by the term *Mobility as a Service* (MaaS). In order to do this, mobility services that are offered through a platform are used. These services are very diverse and try to respond to the customer's needs, such as a reserving a shared vehicle, or an app offering several types of transport in a single package. In addition, there is a desire not to build cities fill with roads and parking facilities. Therefore, research has also been carried out on the use of digital means. MaaS is therefore being researched by many municipalities because it makes it possible to optimize the use of transport. MaaS often has several parties that participate. For transport questions regarding greater distances between municipalities, these projects often require data to match supply and demand. Especially if the transport demand cannot be fulfilled by one provider, but by, for example, a combination of bus, tram and/or train. In addition, municipalities, often united through regional connections, are responsible for public transport concessions in that region. Data collected by concessionaires on transport can therefore be useful for MaaS. Municipalities also often play a role in issuing licenses to providers of shared transport such as shared scooters and shared bicycles. The movement of people is remarkably useful to identify people. Misuse of such data thus entails risks to the protection of personal data.

Therefore, it is advisable to explicitly consider when issuing a license whether and how a MaaS provider processes personal data, for example, by assessing a provider's accountability documentation. When, for example, a provider is unclear about the purpose and necessity of processing in a privacy statement, it is not sufficiently accessible to data subjects, has an unclear privacy statement or has not taken measures to give effect to the right of removal, a municipality should take this into account when deciding to issue a permit. Next to, for example, the physical security of users of these services, the protection of personal data of users should also be an important element in the assessment.

Requirements for the protection of personal data are also necessary with regard to concessions and contracts. These procedures occasionally require an exchange of data between the parties. Information can also be exchanged with the municipality itself. These requirements are often met by referring to commonly used industry standards. Standards that have come from outside the EU or are less recent are not always the most privacy-friendly. Even though the GDPR requires solutions that meet the requirements of privacy by design. Insufficient attention to these aspects may result in excessive processing of personal data and is, therefore, contrary to the GDPR. Critical analysis is desirable here too.

On occasion, municipalities encourage citizens to use or install technology, whether or not this is subsidized by the municipality. This raises questions about data protection. We mention only one aspect here, namely when municipalities are determining their choice of supplier, have they considered whether the product or service that is processing personal data actually complies with current laws and regulations that are in force in Europe. In the interviews, one municipality indicated that it would carry out a basic check on the processing of personal data before entering into a relationship with that party or using or promoting the services of that party within the municipality.

Consideration should also be given to whether the agreements and requirements agreed on in the permits and contracts are still up-to-date and relevant. Technology and its associated risks are constantly changing and developing. Permits and contracts often apply for a longer period of time, and during the periodic evaluation of these agreements, it should also be considered whether they still comply with the GDPR.

Recommendation: When drawing up the program of requirements for contracts, or the conditions applicable to a license, explicitly include requirements regarding the processing of personal data. Periodically determine whether the agreed requirements are met, and whether the requirements themselves are still in line with the GDPR.

11. Recommendations

11.1 Basic principles of the GDPR for Smart Cities

- Before you start any smart city application, determine whether personal data is being processed and whether that processing of personal data is lawful. Without lawful data processing, smart city applications cannot be developed or applied.
- Determine which goal(s) the smart city application will contribute to. Make these objectives as concrete and measurable as possible to determine the effectiveness of the smart city application. General purposes such as 'safety' or 'liability' must be specified. Also, identify the next steps if a smart city application fails or unwanted side effects occur.
- Prior to the deployment of smart city applications, check if there are alternative solutions that process less or no personal data to achieve the same goal. Think from the perspective of the problem and not from the provided solution.

11.2 DPIAs

- Keep DPIAs up-to-date to demonstrate the current risks of the processing. Incomplete action points in an outdated DPIA or failure to document technical adjustments to the processing do not comply with the accountability obligation. Have policies that mandate that DPIAs are periodically reviewed or updated.
- Do not delay executing a DPIA, do so as early as possible when developing smart city applications. This is particularly important for scheduled events or other applications with deadlines. This will allow for the timely determination of whether the processing may need to be submitted to the DPA for prior consultation. Involve the DPO as early as possible, so that they can provide advice in a timely manner.
- Publish as many DPIAs of smart city applications as possible and develop policies on the publication of DPIAs.
- In the DPIA pay attention to whether data subjects have been asked for their opinions and how these opinions have been followed up. The higher the possible risks, the more unclear the legal basis or the higher the degree of perceived infringement, the more likely it will be to have to involve citizens.
- Smart city applications that are in the pilot phase must also meet the requirements of the GDPR if personal data is processed. Therefore, in pilot and trial projects, check whether these projects are GDPR compliant and, if necessary, carry out a DPIA.
- Be critical when assessing the anonymity of the data being processed; data can only be considered anonymous when a party uses reasonable means (for the designated purpose), to make it unlikely that a person can be identified.
- In the case of partnerships, prior to the start of the processing, identify who is the controller and processor. Be transparent to citizens about this as well.

11.3 Getting a Grip on Smart Cities

- Define policies and principles around smart cities/digitalization that respect the frameworks of the GDPR and work out them in concrete instructions for the workplace. Make use of existing knowledge and experience so that they can be shared with other municipalities.

- Ethics cannot be replaced by adopted laws and regulations. Therefore, start by executing a DPIA to address data protection issues. For questions that go beyond the GDPR, an ethical framework can be developed and applied.
- Ensure that the city council is more informed about the deployment and process of smart city applications used by the municipality, so that there is more debate around this topic. Ensure that there is sufficient knowledge about digitalization and technology within the city council. If necessary, the municipal council can be informed by experts, such as the DPOs, civil rights movements and (municipal) experts.
- Explore the possibility of appointing a specific councilor who deals with digitalization or make agreements about who within the board oversees cross-sectoral digitalization issues.
- Consider in which cases, when and how citizens will be involved in the development of smart city applications. Consider in particular the role of citizens in determining the desirability, possibilities, and risks of collecting data in and about public spaces. Explicitly address the privacy aspect of smart city applications.
- Research what ways municipalities can gain an insight into the sensors that are placed in public space by third parties if these process personal data. Share information about these sensors with citizens, and if possible, through a central location such as a sensor register. Consider (together with other municipalities) the possibility and desirability for municipalities to establish conditions that must be fulfilled prior to the use of sensors in a public space, so that citizens can continue to move freely in the public space.

11.4 Organization of Privacy in the Municipality

- Provide sufficient personnel and resources to organize privacy within the municipality, so that data protection is given sufficient attention in the organization and can be included in the process in a timely manner.
- Make sure that the DPO can fulfill their function independently and in accordance of all the requirements. The DPO is not responsible for policies and should not be positioned as such in the organization. Access to the board is essential in order for the function to be executed properly. Ensure that the DPO has and is able to gain knowledge of processes and municipal practice in order to be able to provide optimal advice and supervision. The DPA has made recommendations regarding the positioning of the DPO.[32]
- Seek cooperation to address common issues around smart cities. Let 'leaders' take a leading role in this. At the same time, remain critical of the deployment of smart city applications, even if they are widely shared and applied; a smart city application in one municipality does not necessarily have to be successful in the other municipality when it does not meet the specific goals and problems of the municipality.

11.5 Mobility as a Service (MaaS)

- When drawing up the program of requirements for contracts, or the conditions applicable to a license, explicitly include requirements regarding the processing of personal data. Periodically determine whether the agreed requirements are met, and whether the requirements themselves are still in line with the GDPR.

[32] See also the DPA's recommendations regarding the positioning of the DPO: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht

12. Annex: List of Definitions

Smart city application
The collection and processing of (personal) data about or in public space through the use of sensors, technology or other applications to gain insight into, or gain analytical capabilities about, public space, or to enable the control of public space. For example, Wi-Fi and Bluetooth tracking, deployment of (mobile or body) cameras, or sensors that collect data on traffic applications or sound.

GDPR
The General Data Protection Regulation (GDPR) is the main rules for the handling of personal data in The Netherlands. Previously, this was the Personal Data Protection Act (Wbp). The GDPR has been in force since 25th of May, 2018. Since this date, the same privacy laws have been applicable all throughout the European Union.

UAVG
The GDPR is directly applicable in The Netherlands. The parts of the GDPR that allow for national choices regarding the implementation of the GDPR are filled in by the GDPR Implemention Act (UAVG).

Personal data
The General Data Protection Regulation (GDPR) indicates that personal data is any information relating to an identified or identifiable natural person. This can be information that is either directly about someone, or can be traced back to a person.

Processing of personal data
When personal data is processed this can be, for example, the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination, restriction, erasure or destruction of data.

Controller
A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In municipal practice, the board of the mayor and the councilors are the controller under the GDPR. In specific cases involving security situations, it may also be that the Mayor is a controller.

Processor
A natural or legal person, public authority, agency or other body which processes personal data for the purposes of the controller.

Data Protection Officer (DPO)
A Data Protection Officer (DPO) is an independent internal supervisor who monitors GDPR compliance of the controller. The controller is responsible for drafting and implementing the privacy policy. The DPO monitors compliance and advises on the risks posed by existing processing operations and new products and services. The DPO also ensures that the rights of the data subject can be exercised effectively. The DPO can provide advice on the DPIA and act as the point of contact for the supervisory authority. The municipality must provide the DPO with means and access to all information and councilors. The DPO shall not receive instructions or be punished or discharged for the performance of its duties.

DPIA
Under the GDPR, organizations may be required to carry out a Data Protection Impact Assessment (DPIA). This is a tool used to identify the privacy risks of a data processing operation in advance. And can then be used to take measures to reduce the risks.

Prior consultation
If a DPIA shows that an intended process poses a high risk and insufficient measures can be taken to mitigate the risks, then the DPA must be consulted before the start of the processing. This is called a prior consultation. In the prior consultation, the DPA advises on how the risks associated with your intended processing might be mitigated. If these measures are carried out, processing may start. It might also be the case that the DPA advises to completely refrain from using the intended process.

MaaS
Mobility as a Service (MaaS) are mobility services that are offered through a (digital) platform. For example, private vehicles that can be reserved through a smartphone app, but also digital platforms, where multiple types of transport are offered in a single package, fall under the term MaaS.

Accountability
Under the GDPR, a municipality must be held accountable for the processing of personal data. This means that a municipality must fulfil a set of obligations in order to make this possible which are known as the accountability obligations. Examples of these obligations include, having a register of processing operations, executing a DPIA, and being transparent about the processing of personal data.

EDPB
The Dutch DPA is a member of the European Data Protection Board (EDPB). This is an independent body where all EU national privacy regulators cooperate. The EDPB ensures that privacy legislation is consistently applied in the EU. For example, by publishing opinions, decisions, and guidelines that provide explanation about the GDPR.

13. Annex: Municipality Questionnaire

1. Overview of smart city applications

First, we request that you provide an overview of all smart city applications starting from 1 January, 2015, in particular the smart city applications where your municipality processes personal data and acts as data controller. We would like to ask you to provide in your overview at least the following data regarding the smart city applications:

- Name of the application;
- Start date;
- End date (if applicable);
- Subject (e.g. mobility, safety, etc.);
- Description of the application, including, at least in general terms, a description of:
    - The purpose of the application;
    - The (personal) data processed;
    - (Technical) information regarding the means of obtaining and processing the data.
- DPIA executed yes/no (if yes: please send it along with this questionnaire).

2. Questionnaire

In addition, we ask you to answer the following questions:

1. At what moment do you involve your Data Protection Officer (DPO) in the development and deployment of smart city applications?
2. To what extent do you involve ethical questions and dilemmas in your smart city applications?
3. Does your municipality have specific policies regarding smart city applications? (If yes: please send us a copy)
4. Are there other parties such as knowledge centers, resident groups, expert groups, etc. involved in the development of smart city applications? If so, which ones, and what role have they played?
5. Are you aware of other smart city applications in your municipality where you are not the (only) controller? Can you give examples of this and indicate who (else) is controller for these applications?
6. Are there smart city applications where you work together with other municipalities? If so, how does this cooperation take place?
7. In your role as legislator, has your municipality regulated or plan to regulate the use of sensors, cameras or other technological data collection methods in the public space?

3. DPIAs

Finally, we request that you to send the DPIA(s) for the smart city applications where your municipality was controller and where a DPIA was mandatory, starting from 1 January 2015. Any personal data in the DPIA(s) you can delete.

14. Concluding Remarks

Technology is becoming intertwined with our cities, and therefore, also with our lives. With this report, the Dutch DPA hopes to promote a holistic approach to the Dutch smart city with attention to the GDPR. This report cannot answer all of the questions, that is the task of the controller, but provides guidance in the search for responsible innovation in public space. Even though there are many concerns about the level of knowledge and focus on data protection, there are also positive developments where things are headed in the right direction. Here data protection is often seen as a challenge by developers, which fits our Dutch knowledge economy. We therefore call upon municipalities to take responsibility and develop applications within responsible frameworks. There must also be room for reflection on the desirability and significance of smart city applications in society. Also, dare not to do things occasionally. This is a complex task, but ultimately, it results in sustainable innovation that improves the public space for all citizens without the need for citizens to give up their fundamental rights. In this regard, it is important to involve citizens in the development; they have indispensable knowledge about their living environment that can contribute to the sustainable development of public space. We hope that this report will lead to a constructive dialogue about the application of technology and data in our public space. The reflections in this report are a first step towards this. We thank the writers for their independent reflection and contribution to the discussion about sustainable development of the Dutch smart city.

On behalf of the researchers:

- Anna Maj Drenth
- Gerald Hopster
- Arjan Kapteijn
- Celina Romijn
- Maxine Moleman
- Krijn Wijnands

Questions about the General Data Protection Regulation

On our website www.autoriteitpersoonsgegevens.nl, you can find information and answers to questions about the General Data Protection Regulation (GDPR). Are you unable to find an answer to your question on our website? Then you can contact the Information and Privacy Notification department of the Dutch Data Protection Authority through this number 088-1805 250.