CHAIR
DATA PROTECTION
ON THE GROUND

in partnership with BNP PARIBAS FORTIS

Personal data protection in smart cities

Roundtable report

September 2019

www.dataprotectionontheground.be

ABOUT THE CHAIR ON DATA PROTECTION ON THE GROUND

The VUB Chair "Data Protection On the Ground" (DPOG) promotes the investigation into actual practices of data privacy in organizations and the dissemination of best practices.

The focus of its research is on developments in smart cities, health, media, and banking. For this the Chair compares practices in public sector organizations with those in the private sector, and organizations experienced in personal data protection with beginners. In lectures, workshops, roundtables and other events, the Chair brings experts and practitioners together to stimulate the discussion of best practices.

The Chair is coordinated by the research center imec-SMIT (Studies on Media, Innovation & Technology) in collaboration with the research group LSTS (Law, Science Technology & Society), and supported by BNP Paribas Fortis. For more information, please visit the Chair's website at www.dataprotectionontheground.be.

Contact
The analysis for this report was conducted by researchers Jonas Breuer (VUB), Athena Christofi (KU Leuven) and Ine van Zeeland (VUB).

For questions about this report, please contact Ine van Zeeland, ine.van.zeeland@vub.be.
For questions about the DPOG Chair, please contact dataprotectionontheground@vub.be.

Contents

Abstract

This report describes the results of a roundtable session in June 2019, that brought different stakeholders together to discuss challenges and solutions for (personal) data protection in smart cities. The most discussed topics during the roundtable were: a) The roles and responsibilities of data controllers and processors; b) Skills and resources of data controllers, public authorities and data subjects; c) Legal bases for the processing of personal data; d) Power imbalances between different actors; e) Role of public authorities; f) Protective measures; g) Data re-use and sharing.

Recommendations for different relevant actors in the field of smart cities, resulting from the discussion of challenges and solutions, are provided at the end of the report, alongside directions for further research.

1. Introduction

In smart city projects, a variety of interests come into play: the interests of citizens, authorities, technology vendors, regulators, researchers and lawmakers. These different stakeholders will also have different perspectives on what should happen with the data that are collected and processed in smart city projects, especially when those data are personal. The introduction of the European Union's General Data Protection Regulation (GDPR) has accentuated these different perspectives and emphasized responsibilities.

On Friday, 24 June 2019, 15 representatives from different stakeholder groups participated in a roundtable discussion on personal data protection in the smart city. Participants had been provided beforehand with a policy brief, containing recommendations for smart cities and government authorities, based on lessons learned in projects that the research center imec-SMIT had been involved in. However, participants were free to bring in any topics related to personal data protection in smart cities that they saw fit. In three rounds, roundtable participants discussed challenges and solutions for personal data protection in smart cities, and then evaluated both challenges and solutions. Three researchers analysed the notes from the roundtable, coding them with the help of the MaxQDA qualitative data analysis and research software. The analysis pointed to recurrent topics during the discussions.

The most discussed topics during the roundtable were: a) The roles and responsibilities of data controllers and processors; b) Skills and resources of data controllers, public authorities and data subjects; c) Legal bases for the processing of personal data; d) Power imbalances between different actors; e) Role of public authorities; f) Protective measures; g) Data re-use and sharing. This report aims to give an overview of particular issues raised by stakeholders within the seven broad aforementioned topics. We often use direct quotes from participants to better convey the vivid character and key messages from the discussions.

"One of the bigger problems of the GDPR is that the public doesn't give a shit. [We have] 1,6 million users in the system, and never get emails or requests on data protection. [...] the solution is to create a demand for privacy."

Participant quotes

2. Roles and responsibilities of data controllers and processors

A challenge that was mentioned repeatedly was the problem of deciding who is controller and who is processor for a certain data processing activity. In many cases, smart cities and technology vendors are both controllers, processing data for joint purposes or for their own purposes. It is therefore also difficult to distinguish between situations of joint controllership and separate controllership. A specific example given during the discussion of joint controllership in public-private partnerships, was that of smart traffic systems, in which cars should be able to communicate with smart traffic lights. Notably, participants emphasized that data collected in public space could not simply be freely exchanged between private and public partners.

In cases of joint procurement, when multiple municipalities close contracts with a single vendor, controllership is distributed (joint controllership). This may lead to practical problems, such as the question of who is the ultimate controller, or inefficiencies, as all parties have to conduct their own safety checks. In such situations, the vendor can become the bottleneck, facing demands from

different actors. Additional risk for personal data may arise when several decentralized controllers share the same processor for different data processing activities.

Participants indicated that smart cities cannot always effectively control processing activities, in particular when vendors do not accept the role of processor, or deny having a role as either processor or controller, i.e. deny having any responsibilities regarding the personal data they are processing. Another issue raised related to the powerful position of certain processors: sometimes, vendors in monopoly positions simply impose their own data processing agreements, or reduce the choices a municipality might have.

"As a city, we can't address Google.
If the European Data Protection Authority does it, it is fine."

A solution that participants put forward for these issues was to appoint an independent, central authority. This central authority could either control all personal data necessary for public institutions and manage access to it, or decide definitively on the allocation of roles. The latter would entail that this institution should decide, upon request, for each new data processing activity who would be controller(s) and who would be processor(s). Another suggestion was for cities to use data protection impact assessments to reclaim some control from vendors. One participant mentioned that the Flemish government is mulling what its coordinating role in smart city projects should be.

"It would be interesting if there could be one entity to have all the data there
but then there is a question of who controls that entity."

Another actor with a role in smart city projects is the citizen. As one participant pointed out, citizens can be their own controllers if they get sufficient information. Another participant suggested that citizens do not care about what happens with their personal data, and if they don't take an interest, smart city vendors won't either. This was countered by a reference to a study in the United Kingdom that showed that citizens do care, but they feel powerless to control what happens with their data.[1]

"As long as the people don't care, companies won't care either."

---

3. Skills and resources

Lack of skills, knowledge and awareness, commonly termed (digital or data) 'literacy', were recurrent themes in the discussions. Participants agreed that not only data subjects lack necessary literacies, but also those working 'on the ground' in public authorities and municipalities as data controllers. This leads to situations in which people are not able to understand their challenges or communicate their problems. An idea proposed was to involve government departments of education in the efforts around the implementation of the GDPR, because of its direct interdependency with digital literacy.

[1] In scientific literature, people's impression of powerlessness to control what happens to their personal data is also known as 'privacy resignation'. See e.g. Draper (2016), 'From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates', *Policy & Internet*, *9*(2), 232-251. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.142

"Education is not only for the citizens but also for the Government."

Especially smaller municipalities struggle with low digital maturity, a lack of expertise and manpower. It was suggested that while the municipalities have to deal with ever-increasing tasks and competences, their budget is not being adapted accordingly. As mentioned before, these organizations might only have a DPO assisting for a couple of days per week and are not able to build up the relevant knowledge themselves, which is not conducive to good data stewardship. Participants suggested that higher levels of governments should provide subsidies, additional workforce and guidance concerning the often abstract GDPR. Interestingly, it was pointed out that allocation of resources itself is negatively impacted by the lack of literacy. As a result, the importance of education, not only for citizens but also for government officials and public servants was highlighted.

"The discussion [about GDPR] reveals broader problems, like illiteracy. It's all linked."

Regarding the citizens as data subjects, participants explained that the Flemish government, for instance, is aiming at providing sufficient help and proper information to increase critical literacy. There are decisive challenges here. Participants have mentioned, for example, that such efforts aiming at increasing literacy often do not reach minorities and vulnerable groups. Also, in order to understand your rights, you have to be aware of the matter in the first place, and take an interest in it, too. Some mentioned that a majority of the public is not aware and/or does not care about privacy, which makes it more difficult to raise awareness and provide education. It was suggested that a demand for privacy has to be created, and once the public demands it, institutions and companies will follow. In this context, also 'privacy fatigue' or 'GDPR sickness' were mentioned. These arguments were countered, stating that many people actually do care. Inaction, it was argued, is not caused by indifference but by incapability to act. These two opposing views hint at a classical chicken-egg conundrum.

"It's actually about awareness. People don't know they are monitored, it's good to tell them [...] so that they don't freak out."

Participants discussed the idea of templates, in particular in the context of controllership agreements. Such templates are "relatively easy to make" and can be provided by a central authority or shared between peers. Other participants put forward that these templates do already exist. This might hint back at the lack of literacy, that people are not aware of such documents because they are not able to find them. Moreover, participants discussed the sharing of resources by municipalities, in particular as a reaction to the increased demands towards them as mentioned above: local municipalities can (and do) share IT centres, for example, and develop shared services as they often have the same kind of data, the same obligations and problems. They can channel manpower and use expertise more efficiently in such an environment. It was also mentioned by a participant that these initiatives are more often than not driven by the municipalities themselves.

"To exchange knowledge is ok, but not to exchange data."

4. Legal bases for the processing of personal data

Participants raised the issue of legal bases to ground the processing of personal data smart city projects. This issue is crucial, as the need to have an appropriate legal basis for the processing is essential to ensure a project's legality. Using consent as the legal basis was viewed as particularly challenging in the smart city context. Participants questioned how one can obtain consent in the smart city, given that data collection happens in a public space and is not freely given. When explaining the challenges with consent, the phrases "public space", "opt-out" and "objection" were used. One participant mentioned that giving information about the collection of data can prevent people from getting upset, while another pointed out that the practice of informing individuals is more a transparency obligation rather than actual consent. Overall, participants had different views on whether and how consent can be used in the smart city, and what other legal bases can be used instead of consent.

"Consent is a nice idea but it is unworkable" […] "It gives a false sense of power."

A participant considered that the choice of technology impacts whether or not consent can be used.

"It depends on technology, not all of them allow opt-out. For example, with wi-fi tracking you could say that you can opt-out by switching it off, but again, opting out is not the same as consent."

To address the difficulties with consent in smart cities and the unclarity over what other legal bases ('namely legitimate interest' or 'public task') can be used instead, a participant suggested that delegated legislation can be adopted at national level to explain the conditions for processing. Adopting a culture of 'extreme transparency' where every sensor is registered and its purpose is discoverable in a transparent way was also mentioned by a participant as something that could potentially improve the trouble with consent, but it cannot solve it.

5. Power imbalances between different actors

The interrelations and power imbalances between public sector organizations and private companies were a recurrent theme beyond the roles and responsibilities of data controllers (see above). Vendors often seem to be in a position to exploit their power, for example regarding their rights to re-use data. In particular smaller organizations do not have the market power to enforce their requirements. Several solutions were put forward in this regard. Bundling the power of public organizations through cooperation, for instance, or stimulation of competition. Integrating GDPR requirements in tendering procedures was put forward as a means to standardise ways of working and to support smaller companies in joining the market. One participant confirmed that he experienced this working successfully in practice. Questions of interoperability and standards are broader than the GDPR but can address some of the core issues. Public sector driven standards in combination with procurement can stimulate and change the market.

"You need a standardised way of working. Otherwise it will be difficult for smaller companies."

Challenges faced in smart cities are clearly not limited to data protection, including also issues such as competition. Smart cities can also be locked in with a certain vendor, for instance, when there is only one vendor for a certain technology, or when switching vendors is prohibitively expensive or impossible because the vendor will not hand over data or because the vendor's offer is inextricably integrated in the internal procedures of organizations. Such a power imbalance or market failure also makes it difficult for smart cities to effectively control the data processing activity. Vendors even sometimes charge more to make their technology or software GDPR-proof and cities have no option but to comply. Collaboration among different (public) authorities was mentioned as a solution.

" [...] are the only vendors for public entities. There is no choice. It is almost impossible to change. This is not just about data, it is broader."

6. Public authorities

The role and responsibility that public authorities (e.g. regulators, supervisory authorities and local authorities) should have to safeguard data protection in the smart city was mentioned on several occasions. Participants underscored that cities or even all public authorities should consider themselves as 'data stewards' or 'data protectors', taking up the main responsibilities to keep data safe and implement good data governance. This entails that smart city staff should command the skills necessary for comprehensive data governance, as was discussed above. Cities should also avoid that third parties get access to personal data, for instance by only providing aggregated or de-identified data for outsourced processing. Participants acknowledged that this also may create barriers to sharing data for publicly useful purposes.

"If I am a mayor, I'm in a position to protect my citizens."

'Extreme transparency', as mentioned above, is another idea for how public authorities can take responsibility. For example, all sensors in the public space can be registered to provide citizens with all information required in Article 13 of the GDPR (purpose of processing, recipients of the data, contact details of the controller a.o.).

"Every sensor should be registered, its purpose must be discoverable in a transparent way."

7. Protective measures

Participants raised several other possible protective measures to (further) protect personal data in the smart city, which can be classified into: i) (further) regulation; ii) technological measures such as privacy by design; iii) values and ethics and; iv) anonymisation. Regulation was considered by some participants as a possible means to increase protection, drawing from lessons from the past and/or other countries. A participant mentioned that in Belgium there were a lot of discussions on security cameras in the past. Faced with a situation where everybody was trying to set up its own system, eventually, national legislation was adopted to solve the issue. Participants considered that there is scope for states to use national/delegated legislation to explain and specify conditions for processing where needed. An example raised from regulatory measures beyond the EU is the ban on using facial recognition in AI in the US. This is because "it is something concrete, the GDPR, for most citizens is represented with cookies and clicks".

"The recent ban on AI face recognition in California had a bigger impact on my family than the GDPR. The GDPR has done a lot, but it has no face."

Concerning technological measures, participants considered that a solution can be to make technology as 'privacy by design' as possible and to keep data separated, not combined. Others questioned whether solutions to enhance data protection can rely mainly on technology and suggested that values and ethics need to play a role.

"Maybe we should place the solution on values and ethics, not that much on technology."

Finally, the potential for anonymisation was also discussed. However, some participants remained critical expressing doubts on whether users can really remain anonymous in environments with a lot of data, which can be combined and reveal behavioural patterns.

8. Data re-use and sharing

The discussions revealed that the sharing and re-use of personal data are particularly challenging for smart city stakeholders. One mentioned that when an entity wanted to take certain data from a federal service for a project that would benefit the public, it was proved impossible as there are secrecy and confidentiality requirements. A federal service could give the data to the federal government but not the local government. Overall, it is unclear who can obtain access to data, and how, and there seems to be hesitance to share after the GDPR, even though the law's intention has been to restrict unlawful sharing practices and not data sharing in general (in the words of one participant: "But.. the GDPR in fact allows sharing if it's lawful!"). Participants considered that there are a lot of barriers to access even if one wants to do useful things with such data. As mentioned by a participant from a public authority:

" Sometimes we are the party that COULD give data, but it's very difficult because there are a lot of procedures. We are in between the two, we want to help but we cannot."

At the same time, participants emphasized that data collected in public space could not simply be freely exchanged between private and public partners. Data governance policies are important to prevent unwanted sharing. For example, some stakeholders explained that they try to avoid that third parties get access to personal data by giving them access to 'events' (aggregated data) rather than to raw personal data. Another participant called for different regimes on access and use for data that has "a public interest". France was mentioned as an example as there is a debate on public interest data. Such data can also be gathered by private companies, but they should be open to serve in the public interest.

"There should be a difference between data with a public interest and data that is for private purposes, even where both are collected in public spaces."

9. Other challenges

Other challenges mentioned during the roundtable include data ownership and smart city ownership, the application of principles like transparency and proportionality, participation and notions of public space and surveillance. Even though discussion on these topics was less dominant than discussions on

the issues we presented in more detail in previous sections, this is not indicative of their importance. Rather, it could be an indication of their complexity and that there are not many solutions yet.

10. Conclusion and recommendations

The solutions described in this report are aimed at different stakeholders and different levels of action. Summarized, these are the recommendations given for different actors in the smart city environment:

Cities and municipalities

- Develop data protection impact assessment (DPIA) methods that help reclaim control from technology vendors.
- Provide extreme transparency on smart city implementations and technologies.
- Involve education departments in internal GDPR implementation efforts (i.e. train staff).
- Share resources, such as IT departments and experts.
- Integrate GDPR requirements in tendering procedures.
- Seek standardization and interoperability[2] by collaborating with other smart cities.
- Limit access by third parties (commercial actors) to publicly held personal data.

Regulators

- Provide guidance on distinguishing controllers and processors.
- Provide guidance on conditions for (re)use between public and private partners.
- Provide templates for partnerships.

(National or federal) governments

- Appoint or designate an independent, central authority to provide or supervise access to publicly held personal data. This authority can also decide on the allocation of controller/processor roles.
- Provide more resources (subsidies, staff, guidance) to cities and municipalities to protect personal data.
- Set up projects to improve awareness and data literacy among citizens, including minorities and vulnerable groups.

Lawmakers

- Introduce delegation legislation to explain conditions for processing personal data.
- Introduce legislation on sensor registration.

Technology vendors and service providers

- Implement privacy by design wherever possible.
- Separate personal data from different sources.

Overall, the participants in the roundtable issued a clear call for public authorities to take up their role as 'data stewards', to take responsibility for the protection of the personal data of citizens.

Subsequent research

Based on the challenges and solutions highlighted in the roundtable discussion, subsequent research will be focused on data protection impact assessments, transparency, data literacy of staff within smart cities, and the legal basis of consent in public space. These research efforts will be conducted within the frameworks of the SPECTRE project and the research chair Data Protection On The Ground.

[2] See e.g. the Datum Future report: 'Data Portability: What is at stake? (July 2019), https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf

The SBO research project SPECTRE supports stakeholders, and particularly public institutions, in implementing the GDPR in their smart city realities. A focus here is on data protection impact assessments, from a participatory, a cost-benefit and a legal perspective. This work is conducted in an interdisciplinary team composed of the research center imec-SMIT, scholars in the field of economics from the BUSI-APEC research group at the Vrije Universiteit Brussel, and legal experts from the CITIP research group at the Katholieke Universiteit Leuven.

The VUB Chair on Data Protection On The Ground will also gladly support stakeholder discussions for policy development. Its research is focused on daily practices of personal data protection.