

Smart Parking

Best Practices for Image Recognition

The «smart parking» project launched in Frauenfeld (TG) constitutes an example of innovative use of artificial intelligence (AI) to optimise car park management in Swiss cities and municipalities. Through use of image recognition developed by the ETH spin-off Parquery AG, this project enables parking occupancy to be detected and analysed efficiently as part of the Innovation Sandbox for AI. The technology, which is based on anonymised camera images, not only improves urban traffic planning, but also contributes to residents' quality of life by reducing traffic caused by searching for parking. Particular attention is afforded to data protection: privacy-by-design measures, such as use of low-resolution images, ensure that facial and number plate recognition is avoided and the protection of personal data thus guaranteed. This project demonstrates how modern technologies can contribute to overcoming urban challenges, offering valuable best practice recommendations for other Swiss cities and municipalities as well.

Innovation Sandbox for Artificial Intelligence (AI)

This document was created within the scope of the Innovation Sandbox for Artificial Intelligence (AI). The sandbox is a test environment for the implementation of AI projects from various sectors. This broad-based initiative involving public administration, industry and research, is designed to promote responsible innovation by allowing the project team and participating organisations to collaborate closely on regulatory questions and enabling the use of novel data sources.

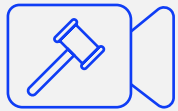
[More Information](#)



I.	Initial challenge: lack of data	4
----	--------------------------------------------	----------



II.	Technical solution: smart parking in Frauenfeld (TG)	5
-----	-----------------------------------------------------------------	----------



III.	Legal aspects: camera data from public spaces	10
------	----------------------------------------------------------	-----------



IV.	Technical measures: handling personal data	14
-----	-------------------------------------------------------	-----------



V.	Implementation: collaboration and transparency	16
----	-----------------------------------------------------------	-----------



VI.	Conclusions and recommendations	18
-----	--------------------------------------------	-----------

I. Initial challenge: lack of data



Public **car park*** management is an issue that many Swiss cities and municipalities face. On the one hand, advocacy groups and some political parties are demanding that there be less parking in downtown areas for the sake of increasing sustainability and improving the amenity value of urban spaces (e.g. by de-paving surfaces and planting new trees). On the other hand, associations and other parties are committed to preserving existing parking, e.g. to support local businesses. Irrespective of political discussion and differing stakeholder objectives, there is a notable lack of solid data on overall capacity, parking occupancy and parking duration to allow for informed decisions in relation to car park management. This makes it difficult for city authorities to optimise car park usage, minimise traffic caused by searching for parking, and to use traffic infrastructure efficiently.

In this AI Sandbox project, the city of Frauenfeld is testing the use of image recognition to improve public car park management. The AI technology is based on the automated analysis of camera data. The aim is to support public administration with traffic planning through supplying real-time data on city car park occupancy, and to provide citizens with information on available vs. occupied parking spaces. The technology has been made available by the ETH spin-off Parquery AG and is being tested in a one-year smart parking pilot project. This real-life example serves to build skills on how to handle image recognition in public spaces.

The technical solution of this specific case study will be described in the next chapter. Summaries of legal aspects, best practices and privacy-by-design measures will follow in the subsequent chapters, so that other Swiss cities and municipalities may build on the knowledge gained.

* The highlighted terms in the text are explained in the glossary.

II.

Technical solution: smart parking in Frauenfeld (TG)



Cities and municipalities primarily pursue two technological approaches to **car park** management in public spaces: the installation of in-ground sensors or use of cameras to collect image data. Both approaches have their pros and cons (see [this report](#) for sensor solution). Sensors tend to be less problematic data protection wise, as no personal data is collected. However, they are expensive to purchase and install (one sensor per **parking space**); they are also maintenance-heavy, susceptible to interfering signals and do not provide for any specific analysis to be conducted, e.g. with regard to vehicle types or parking fee billing. Use of camera data generally allows for broader and more efficient data collecting, given that larger car park areas can be captured with just one camera and the produced images offer greater potential for smart parking applications. That being said, the critical factor in this regard concerns collection of personal data on camera images or in video streams. In principle, a distinction can be made between two categories of image recognition:

- Examples of use that do not require any personal data (e.g. analysis of car park or individual parking space occupancy)
- Examples of use that rely on personal data (e.g. automated billing of parking fees based on number plates)

The example of use in this AI Sandbox project does *not require any personal data*. The project proposal was submitted to the Innovation Sandbox for AI by Parquary AG in spring 2022 and was selected for the pilot project based on public selection criteria. The

city of Frauenfeld subsequently agreed to implement the specific case study as a project partner.

«Our goal is to realise an efficient parking management based on intelligent technologies.»

Peter Koch, City of Frauenfeld

Choice of camera locations and installation

In order for car parks to be managed efficiently, car park administrators depend on the availability of comprehensive information on **parking space** occupancy. Whereas data on occupancy rates is often available for indoor private and public car parks, most cities and municipalities do not have any data on outdoor public car parks. The city of Frauenfeld is home to fourteen public outdoor and indoor car parks. The pilot project at hand is limited to five car parks with a total of approx. 500 parking spaces owned by the city. Since cost-benefit considerations are also relevant for choice of camera locations, the question as to whether it makes sense to install cameras at locations with only few parking spaces is merited.

The procurement and installation of cameras may prove to be time- and resource-intensive, given

* The highlighted terms in the text are explained in the glossary.

that clarifications will need to be sought with all of the property owners concerned. Supplying of electricity presents a further challenge as this would, ideally, need to be ensured 24/7. Cameras attached to “intelligent” lamp posts must, therefore, be additionally equipped with a battery that provides for 24-hour power supply as, in many locations, only off-peak electricity is available. There are no major requirements as to which type of camera should be used. Basically any camera will do provided the device can transmit information in real time via a SIM card, wireless or wired network connection to a server with Parquery’s software (see chapter 3 for legal aspects).

Data processing with the Parquery software is carried out either on premise on a local server, or in a cloud environment as a software as a service (SaaS). For on-premise operations, there is a choice between use of a server on the business premise or edge computing close to the camera using a small, high-performance computer. While this gives full data control to the operator, it also means that system maintenance and operations need taking care of. In contrast, a cloud solution tends to be easier to manage – however, the focus must imperatively be on ensuring data security. With both options, camera images can be deleted immediately after processing.

AI-based image recognition

The Parquery software analyses camera images to detect if a **parking space** is available or occupied. The occupancy time is also recorded using AI. Image recognition with AI is based on computer algorithms that learn by way of examples. This training, so to speak, enables the software to gradually recognise patterns, including learning from its own mistakes and allowing it to adapt to new situations, environments and tasks. This is very important given that visual perception is highly complex: while a human will deem recognising a vehicle to be a simple matter, the technology behind it is highly sophisticated. It would be impossible to program a computer system with every single rule on how cars look in their different shapes and sizes, from various angles and in variable lighting conditions. Therefore, AI based image recognition is used for this case study.

The camera images used are low resolution, yet sufficient for the software to detect **parking space** occupancy without rendering persons or number plates identifiable. The software recognises vehicles purely based on appearance and precise parking position; no identification is needed. As a further step to protect privacy, areas not needed for parking space recognition are rendered unrecognisable before processing. In this way, collection of metadata related to persons and vehicles is avoided.

Generating and analysing image data

No videos are recorded within the scope of this pilot project - just still images every two minutes. That interval is sufficient for calculating car park occupancy. The image data (see example below) is transmitted via mobile network to a Swiss cloud server, converted into numerical data and transmitted to an interactive dashboard (see figures 1 and 2 for screenshot examples of the dashboard).

Setting up the dashboard

Images are deleted immediately after processing so that the information can only be retrieved from the dashboard (**parking space** occupied: yes/no). The responsible administrators only have access to numerical data so that they can analyse availability, capacity and duration of occupancy of individual parking spaces anonymously. There is no access to original image data. The authorities responsible for car park management, e.g. department for civil engineering or the urban development office, can carry out individual statistical queries for reporting purposes – e.g. for a particular geographical area or timeframe (see figures 3 and 4).

Integration of “Regio” app

When using real-time data, the focus is on drivers travelling within the city of Frauenfeld. Foresightful trip planning with the help of real-time data enables drivers to find free parking spaces faster. The aim is to limit traffic caused by searching for parking and, inter alia, to reduce unnecessary noise and

II. Technical solution: smart parking in Frauenfeld (TG)

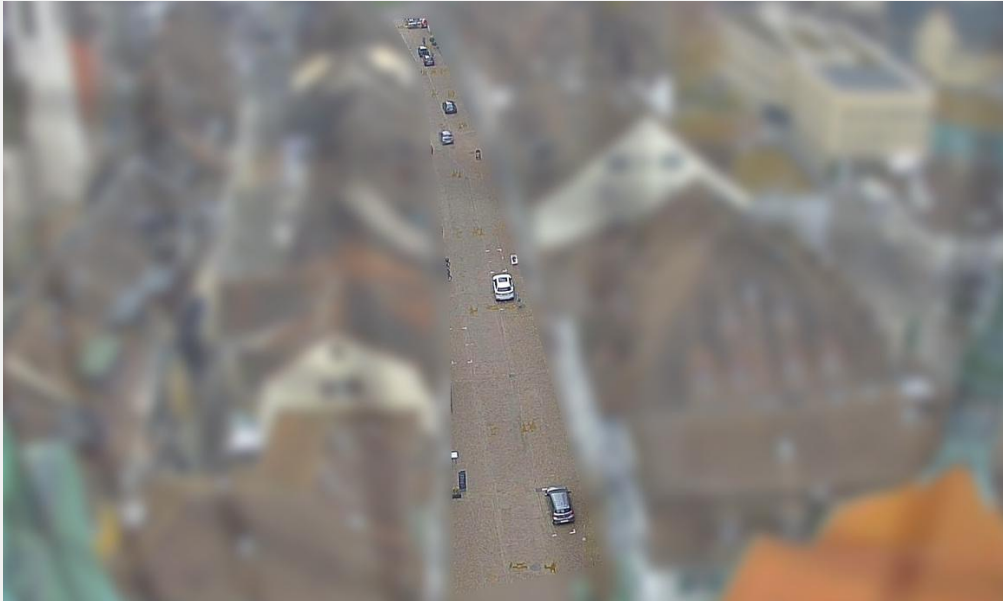


Figure 1: Exemplary image* with built-in privacy protection: the identification of vehicles and persons is avoided through high camera positioning (bird's eye view), low image resolution and the rendering unrecognisable of non-essential image areas. The images are deleted immediately after processing.

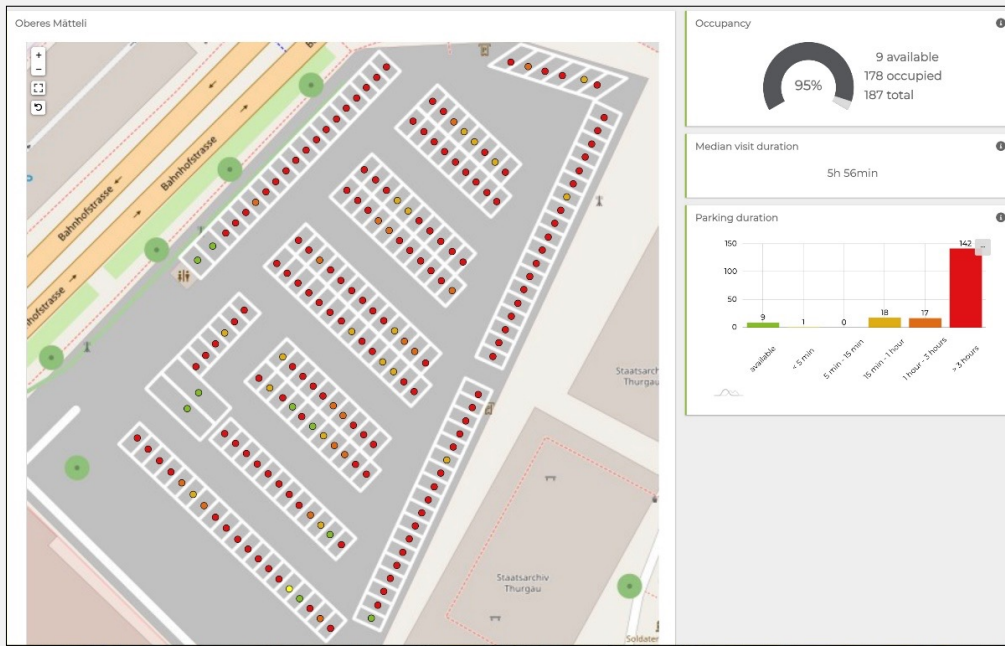


Figure 2: Exemplary image of a camera shot with built-in privacy protection:

- High positioning of camera (bird's eye view)
- Low image resolution (see yellow circled enlargement in the centre of the picture to render number plates and persons unrecognisable)
- Rendering unrecognisable of image areas that are not needed for detection

* The images shown above are illustrative examples, and exclusively for this report. In reality, images are neither stored nor displayed, but analysed automatically and deleted immediately thereafter.

II. Technical solution: smart parking in Frauenfeld (TG)



Figures 3 and 4: Picture of a dashboard for real-time analysis of car parks. Available parking spaces are marked with green dots. Depending on duration of parking, occupied spaces are displayed with yellow to red-hued dots on a map. At no time are camera images available; they are deleted as soon as the automated analysis has been completed.

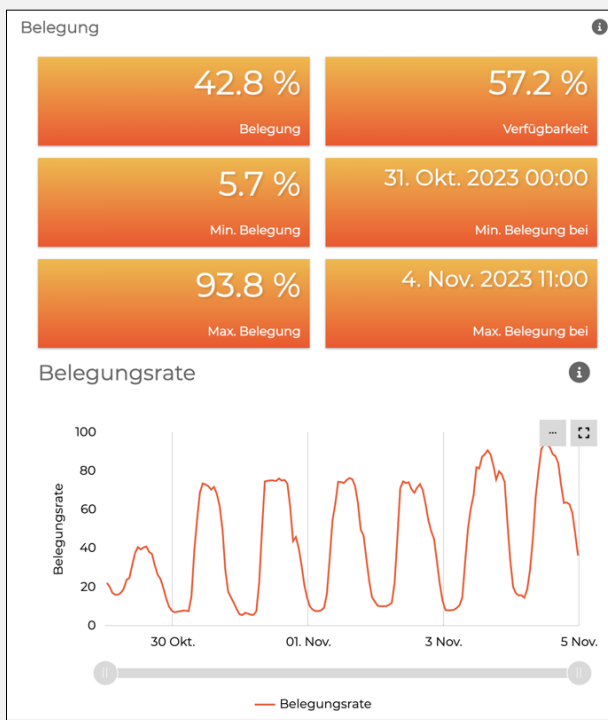


Figure 5: Picture of reporting for a particular car park location with statistics in relation to a particular week. Analysis options range, both time-wise and geographically speaking, from general overviews to specific details. For example, the entirety of locations can be analysed as a whole, or analyses can be performed for individual parking spaces.

environmental emissions. Drivers looking for parking can initiate route planning on a conventional web mapping platform (e.g. Google Maps) directly from the “Regio” app. Furthermore, in future, Frauenfeld’s car park data will also be available via Parkopedia interface in numerous navigation apps provided by car manufacturers.

Open data

In a next step, the numerical data is to be made publicly accessible by way of an open data approach, so that any interested party may perform further analyses – e.g. by combining parking data with other data sources, such as weather data, to gain new insights and potentially develop new offerings. Provision of open data in keeping with the ISO standard of APDS (Alliance for Parking Data Standards) is important in this respect.

Chapter 2 has provided an overview of key points in relation to the technical solution of the smart parking project in Frauenfeld. Chapters 3 to 6 are dedicated to describing general best practices in regard to legal aspects, technical measures and implementation with project partners.



III.

Legal aspects: camera data from public spaces

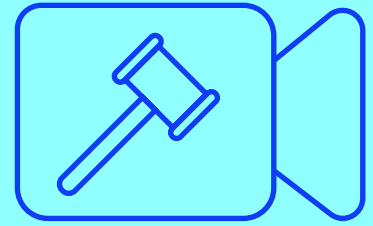


Image detection in public spaces is a legally sensitive topic. As a result, various legal questions arise in connection with the described technical solutions – questions which must be clarified ahead of any such project.

The following chapter provides an overview of the most important legal topics that need to be explored in greater depth for each case and summarises general recommendations on how to tackle the various challenges.

a. General

Legal questions regarding cameras on public property

The main questions in connection with cameras in public spaces concern data protection and personality rights. However, other areas of law may also be relevant, such as general administrative law, e.g. in relation to use of public property. Questions of contract law may also need to be addressed.

Important note – violation of personality rights through dummy cameras

Aside from legal factors, ethical questions also need to be taken into account. Even if a camera does not capture any personal data, individuals may assume that they were recorded by the camera. As a result they are restricted in their personality because a sense of “being under surveillance” can affect the behaviour of the person concerned. Therefore, this may result in a *breach of personality rights* for the person concerned.

Recommendation – it is important to inform the general public with clarity as to which data a camera is recording. If no personal data is recorded, this must be specifically indicated.

Inclusion of all parties involved

Because cameras in public spaces tend to make big waves, it is important to include all parties from the outset. As well as local residents, these parties may include civil society organisations and all of the public sector offices involved (transport, civil engineering, communications, etc.).

b. Data protection

Is data protection law applicable to every camera?

Cantonal and/or federal data protection law is applicable to *personal data*, i.e. to information relating to an identified or identifiable person. A person is identifiable if the identity of that person can be determined with reasonable effort by virtue of the data and additional information. Identifiability is relative, i.e. a person can be identifiable for another person who has additional knowledge, but not for a person without that additional knowledge. If data is personal data then the principles of data protection law must be adhered to when processing data. For public institutions this means, in particular, that processing is only permissible if there is a *legitimate basis* for doing so (principle of lawfulness, see below).

In the case at hand (see chapter 2), special

vehicles (company cars displaying brand lettering, luxury cars) may be conducive to conclusions being drawn about natural persons and, thus, qualify as personal data. Data of legal persons is not covered by data protection law. This means that recording company vehicles on camera is unproblematic from a data protection perspective provided no connection can be made to a natural person. The latter may, however, be the case for small enterprises. Given that the principle of law applies to all actions carried out by the state, data processing of legal persons would also require having a legal basis.

Recommendation – check your project for compliance with data protection law. In particular, technical measures should be taken so that, whenever possible, recording of personal data is avoided or at least rendered unidentifiable (see next chapter).

Applicable data protection law

Either cantonal or federal data protection law will apply depending on whether data is processed by cantonal/municipal institutions or by private persons. The Federal Act on Data Protection (FADP) is applicable for data processing by private persons or by federal authorities. As for data processing by cantonal authorities, there are specific cantonal (information and) data protection laws; the applicable law in the Canton of Zurich, for instance, is the law governing information and data protection [Gesetz über die Information und den Datenschutz (IDG)]. In addition to applicable laws, any ordinances as well as other provisions for implementation must be taken heed of.

The point of reference in terms of applicable law is the party responsible for data processing. A smart parking project will generally involve collaboration between private providers of an AI tool and a public body. However, in this constellation, the public body is the responsible party because the task in question, e.g. car park management, is a public task. Accordingly, public data protection law will generally apply to potential data processing. The FADP would apply if the AI tool provider were to carry out data processing for own purposes.

Responsibility

In the context of data protection, the question of who is responsible for the specific data processing is a very important one. Whichever person or entity is deemed responsible must ensure that data processing adheres to data protection rules and regulations. The person/entity responsible for data processing is the person/entity who determines the purpose and the means of data processing. In the case of a smart parking project, the responsibility generally rests with the public body using the data. The reason for use of the AI tool is to fulfil a public task, e.g. traffic or car park management. Therefore, the rights and duties of the employees of the responsible institutions must be taken into account. Third parties -including private persons- may be called on in order for public duties to be fulfilled.

The case may arise that these third parties – in the case at hand, the AI tool provider– will need to process personal data within the scope of the tasks assigned to them. In this case, third parties are not permitted to decide on the purpose and the means of data processing and, furthermore, are not permitted to carry out any data processing for their own purposes. This is referred to as commissioned data processing (“Auftragsdatenbearbeitung”).

Commissioned data processing requires a contract between the responsible public body and the commissioned data processor, i.e. the AI tool provider. The minimum content that needs to be included in commissioned data processing contracts is defined in the relevant data protection laws, the accordant ordinances and in the provisions for implementation. In accordance with the IDG that applies to the Canton of Zurich, commissioned data processing contracts must be in writing and encompass the entirety of information (not just personal data).

Recommendation – if services of third parties are drawn on to perform a public task and these third-party services involve processing personal data, this will generally qualify as *commissioned data processing* and will require concluding a *written contract* between the competent public body and the third-party provider.

Existence of a legal basis

A public body must always have a legal basis for data processing. *The principle of lawfulness* is already enshrined in the federal constitution and is also explicitly entrenched in the federal and in the respective cantonal data protection laws.

Prior to installing a camera in a public space, the public body must determine the relevant legal basis and verify whether it specifically covers the envisaged data processing. For example, some cantons have a video surveillance law for this. Data processing is not permitted without an accordant legal basis. Even if no personal data is recorded, at the very minimum a legal basis for the task concerned is required (e.g. legal basis for authority in the domain of car parks).

Recommendation – identification of the legal basis constitutes a fundamental step in a project and needs to be done at the earliest possible time.

Ensuring data security

Personal data must be protected by way of suitable, state of the art measures. The purpose of these measures is to ensure that the data is exclusively accessible to authorised persons (confidentiality), the data is available when needed (availability), the data is not changed without authorisation or unintentionally (integrity) and the data is processed in a traceable manner (traceability). In particular, the data must be protected from unauthorised access by third parties. This is to be done by means of suitable technical and organisational measures. In the case of cameras, particular attention needs to be paid to transmission paths making sure that transmitted signals cannot be intercepted by third parties.

Recommendation – the topic of data security needs to be addressed with utmost care. Every possible precaution must be taken, particularly when processing personal data, to avoid data access by unauthorised third parties.

Guaranteeing the rights of data subjects

If a person feels personal data relating to them has been collected, they are entitled to request information from the data controller, i.e. the competent public body. The right to information gives a person the right to find out whether and, if so, what data relating to them has been processed. Subsequently, the data subject may exercise further rights, e.g. the right to deletion. The Federal Act on Data Protection contains a –non-exhaustive– list of data that must be made available to the requester.

Recommendation – even if no personal data is recorded on camera, requests for information may still be made to the public body. It is advisable to have a response strategy in place for this eventuality.

Data storage abroad and in the cloud

AI tools often generate a large amount of data, which raises the question as to whether it is permissible to store the data in a cloud environment, or whether data must imperatively be stored “on premise” at the responsible public body.

The question as to whether and under what conditions public body data may be stored in a cloud environment is a heavily disputed one. If data is saved in a cloud environment unencrypted, i.e. the cloud provider could discern data content, then this is considered to be commissioned data processing and a contract must be concluded with the cloud provider. Cloud usage is less problematic if the data is stored in encrypted form. Most public bodies will have fairly detailed guidelines on data storage in cloud environments. It is advisable to clarify this question with the competent offices.

Additional requirements must be met if the cloud environment is located outside of Switzerland. Pursuant to the Data Protection Act data may only be disclosed to states whose legislation guarantees an adequate level of protection. A list of these states is provided in Annex 1 of the Ordinance on Data Protection (DPO). For instance, adequate protection is guaranteed in all EU member states, as well as in the United Kingdom, but not in the USA.

The question as to which project data can be stored in a cloud environment is contingent on how sensitive the data is. Data that has been rendered fully anonymous may be stored outside of Switzerland.

Recommendation – any envisaged storage of personal data in a cloud environment must be examined in-depth beforehand. If the cloud environment is located outside of Switzerland, additional clarification is needed as to whether the country in question guarantees adequate data protection. This is the case for all EU member states.

Access to data by other authorities

The question that always arises in connection with cameras is whether and, if so, which authorities may have access to the camera-recorded data, and under which conditions.

In principle, data may only be processed for the purpose that the data was collected. Use for a different purpose is only possible if there is a legal basis for doing so or if a data subject has given consent in a specific case. There are various legal bases at federal and cantonal level that, for instance, give permission to the police to conduct searches based on suspicion of certain (serious) offences.

In the case at hand, from the perspective of data subjects, access to data would, however, be unproblematic as the recorded images are deleted immediately after processing.

c. Locations – use of public ground and consent of private persons

If a camera is to be installed on public ground, the consent of the competent public body is required. This may be, but does not necessarily have to be, the same public body that wishes to implement the smart parking solution. In many cases, it may be a good idea to position cameras on private property. Doing so will require obtaining prior consent from the respective property owner.

Recommendation – clarification as to who or which body is responsible for giving consent should al-

ready be sought at the time of exploring suitable camera locations.

d. Legal regulation of collaboration

Collaboration often tends to be informal and agreed orally. That being said, a written agreement may be worth drawing up wherein the mutual rights and duties in relation to the respective project are defined. As part of a commissioned data processing relationship, it is imperative to draw up a written contract with certain minimum content (see “Responsibility” above). Apart from matters of data protection, other aspects are also worth taking into account, including costs, milestones and liability.

Defining the most important points of collaboration will help discern any potential friction points and differences early on and, ideally, allow these issues to be clarified. If they creep up later on and lead to unsolvable differences, this is likely to result in disadvantages for all project parties.

Recommendation – devising a basic document is recommended, at the very least with the most important rights and duties of the parties to the contract. In most cases, freely available standard contracts adaptable to a specific case are worth using.

IV.

Technical measures: handling personal data



Technical as well as organisational measures should be taken with regard to image recognition for smart parking solutions, so as to ensure that a project is implemented responsibly and in keeping with data protection law. The concepts **privacy by design** and **privacy by default** are stipulated, particularly in the context of the European General Data Protection Regulation (GDPR) for processing activities involving personal data. They also apply to Switzerland.

Commonalities:

- **Focus on data protection** – both concepts emphasise the importance of data protection from the outset and integrate it as a central element in systems and processes.
- **Proactive approach** – instead of having to react to potential data protection breaches, these should be avoided from the start through forward-looking measures.
- **Legal framework** – both privacy by design and privacy by default are central to compliance with data protection laws.

Whereas privacy by design pursues a holistic approach that integrates data protection into the entire development and implementation of a system or product from the outset, privacy by default refers specifically to the default settings of a system or service. This means that with the privacy-by-design approach technical as well as organisation measures to protect data are placed in the foreground, whereas the default approach focuses on standard technical and systemic configurations.

«Image recognition in public can be responsibly implemented through technical and organisational measures..»

Raphael von Thiessen, Head of Innovation Sandbox for AI

Chapters 4 and 5 of this document will elucidate technical and organisational best practices to illustrate that personal data –such as images of faces and number plates– is neither being processed nor stored and that the data collected is only available to the project administrators in anonymised form. Insight is provided into the methods and technologies used to meet both functional and data protection requirements for camera systems.

- **Individual images:** Rather than a continuous video stream that bears a higher data protection risk, individual photos should be taken e.g. every two minutes. This approach not only reduces the potential for further use of data for sensitive applications, e.g. gait analyses; it also increases social acceptance of image recognition systems.
- **Choice of angle:** To avoid identification of faces and number plates, cameras should, when possible, be installed at a height at which the camera angle is too steep for such details to be discernible.

- **Low resolution:** A low resolution should be chosen for car park image data, to avoid recognisability of faces, number plates and specific vehicle letterings.
- **Privacy masks:** Digital masking technology can be applied in camera images to mask or blur certain areas. In this way, sensitive areas that are not relevant for occupancy detection of parking spaces –such as pedestrian zones, ATMs or business and store entrances– can be rendered unidentifiable.
- **Conversion into numerical data:** Once the image data has been collected and processed, an automatic conversion into numerical data should be carried out, which is subsequently displayed on the dashboard. Access to the image data by administrative staff or other persons should be avoided.
- **Continuous deletion of image data:** All original image data should be deleted immediately after being converted. This will rule out any other use, making sure no personal information is kept stored. There is a clear difference to security cameras where image data often has to be stored for a predetermined period of time.
- **Swiss cloud:** The cloud solution should preferably be in Switzerland, as this offers additional security in regard to data protection standards. Secure transmission paths such as VPN (Virtual Private Network) may offer further added value.
- **Edge computing:** This technology makes sure that image data never even leaves the camera systems. This means that processing occurs directly at the place of data collection, thus further reducing any risk of unauthorised data processing.

It is important to note that no measure on its own is sufficient to ensure responsible and data protection-compliant handling of image data. Measures should, therefore, always be combined.

V.

Implementation: collaboration and transparency



The implementation of innovative smart parking projects requires detailed planning and inclusion of various stakeholders. This chapter discusses key elements and best practices that are essential for a successful project. This extends far beyond purely technical measures. Whether it be political coordinating or involving the general public and technology partners – a wide range of aspects need to be considered in order for a project to be implemented effectively and in accordance with the needs and expectations of all parties involved. Careful adherence to the steps and considerations below will help to ensure that smart parking projects are not only technologically advanced, but also socially and politically viable.

Political processes

- Any project of this size requires broad political backing. This means that both the respective municipal government and the municipal assembly should be included. The topic of smart parking must be locally relevant, politically desired and democratically legitimised.
- Embedding in political processes is key. A comprehensive car park management or parking guidance & information system requires, e.g., a government resolution (“Regierungsbeschluss”), especially in relation to discussing budgets or issuing service mandates.

Internal administrative processes

- It is important to include several municipal and cantonal offices, e.g. the civil engineering office, the urban development office and the department of security, from the start. This will allow for multifaceted needs to be duly considered and integrated into the solution.
- Involving the competent cantonal data protection authority early on is key to preventing data protection issues.

Involving the general public

- The focus from the outset should be on transparent communication. To that end, formats such as, or similar to, FAQ can be a useful way to present clear information that is easy to understand.
- Transparency should be assured by providing on-site information where the cameras are located (e.g. with QR codes at the recorded car parks). This will help the general public understand how the system works and why it was implemented.
- It is important to hold events that give residents the opportunity to discuss the project critically and to address any concerns, and that help to continuously improve the system.
- When communicating with the general public, the advantages of the system should be highlighted, e.g. less traffic caused by search for parking and the time saving factor.

Data usage and service integration

- The collected data serves not only for traffic planning, but should also be integrated into publicly accessible services, such as regional apps or websites.
- Publishing the collected data as open data offers numerous advantages: provision of data in an open format allows developers, researchers and interested parties to use the data to create their own applications, analyses or services. This, in turn, promotes the innovative capacity within a municipality and may lead to the development of new tools or services that are of direct benefit to citizens.

Site clarification

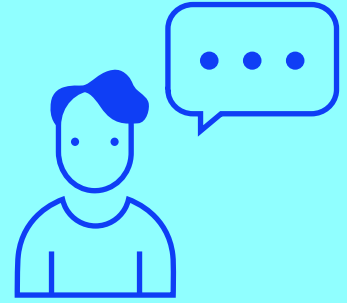
- Clarification with owners of public or private properties, as well as concerning placement of cameras on electricity pylons or other suitable locations, is critical to the project and must be planned and implemented with care.
- In addition to private owners, it is important to involve large property owners within the urban area (e.g. Swiss Federal Railways - SBB) to achieve broad coverage.

Supplier management

- A project of this complexity requires collaboration with several suppliers that offer different skills – ranging from electricity supplying and camera installing to AI image recognition solutions and communications. Hence, coordinated supplier management is key to implementing the project successfully.

VI.

Conclusions and recommendations



Managing car parks in urban environments involves numerous technological, social and political challenges. This project within the scope of the AI Innovation Sandbox has shown that it is possible to implement modern technologies –particularly image recognition– ethically and compliant with data protection law. The main findings and recommendations drawn from this project can be summarised as follows:

- **Responsible use of technology:** Best practices drawn from this report offer a solid foundation for other municipalities and cities in Switzerland, with a view to supporting their mobility initiatives with modern technologies. It has been clearly demonstrated that image recognition can be used responsibly for car park management.
 - **Data objectivity:** Solid data provides a neutral basis for decision-making irrespective of political or emotional position in regard to car park management. It offers the opportunity to reduce traffic caused by searching for parking and, thus, also traffic load. In so doing, it contributes to an improved quality of life and reduces environment emissions. That notwithstanding, it is important to consider the multilayered effects on private transport (e.g. increased traffic due to simplified search for parking) and to seek a healthy balance.
 - **Communication of relevant data protection issues:** Transparent and comprehensible communication on the handling of data is a key ingredient for the success of image recognition in smart parking initiatives. This concerns, in particular, data protection and data security. It is essential that citizens be informed as to which data is being collected, how that data is being processed and how long it is being stored. An open dialogue with the general public and consideration of any concerns and feedback can strengthen the trust in such technologies and contribute to broader acceptance in society.
- **Integration into comprehensive mobility offerings:** Smart parking should not be seen as an individual initiative, but incorporated into a broader mobility concept. This encompasses integration into programmes of public transport, bicycle and pedestrian initiative as well as other mobility solutions.
 - **Standardisation:** Clear efforts are being made to harmonise data standards at national and European level. This will not only facilitate use and integration of car park data, but also pave the way for future mobility solutions. Various stakeholders in Switzerland are already working in this direction, including: [Ausschuss Digitalisierung des Verbands ParkingSwiss](#) (digitalisation committee of the ParkingSwiss association) and [the federal mobility data infrastructure \(MODI\)](#) of the Federal Office of Transport. At international level, the [Alliance for Parking Data Standards \(APDS\)](#) has already developed an ISO standard.
 - **Future use:** The implementation of camera infrastructures harbours the risk of later use for purposes other than those intended. Defining clear processes and boundaries is crucial to ensuring that the technology remains democratically legitimised and is not used for undesired purposes

which were not intended at the outset (e.g. transformation into surveillance cameras).

- **Social acceptance:** Even when person-related data is minimised or not collected at all, the question remains as to social acceptance of extensive camera systems in public spaces. Continuous and broad discussions about the topic are a must-have, in order to strike a balance between added value and potential disadvantages.

Glossar

Car park an area or a site that is specifically designed for parking vehicles. Within the scope of the AI Innovation smart parking project, it refers to the entire area available for parking and recorded by Parquery's AI technology.

Parking space a specifically designated space within a car park for parking a vehicle on. In the context of the project at hand, this can also be a specific area identified through image recognition.

Privacy by design an approach of technology development that integrates data protection and data security into the design and architecture of a system from the outset. In the smart parking project at hand, this is implemented by way of measures such as use of low-resolution images to prevent any persons or vehicles from being identifiable.

Privacy by default a principle by which the default standards of a system should be designed in such a way that they offer maximum data protection without users having to carry out any additional settings. This means that data protection settings were chosen in the project from the start that protect privacy.

Privacy masks techniques or software tools that serve to mask sensitive areas or render them unrecognisable. In the context of smart parking projects, such masks could be used to render pedestrian zones or building entrances unrecognisable.

Individuals and organisations involved in this report

Expert interviews

Georg Spycher, Parking Zürich AG

Angie Garz, Parquery AG

Peter Koch, Office for Communications and Business Development, City of Frauenfeld

Authors



Dr. iur. Stephanie Volz,

Regulatory Expert Innovation Sandbox for AI, ITSL University of Zurich



Raphael von Thiessen,

Head of Innovation Sandbox for AI, Division of Business and Economic Development, Canton of Zurich

Case study provided by the Innovation Sandbox for AI

The company Parquery AG served as a case study within the Innovation Sandbox for AI. The organisation submitted a project proposal to the Sandbox in the spring of 2022. Parquery develops smart parking solutions based on image recognition. Thanks to the city of Frauenfeld as a project partner, the use case was implemented between August 2022 and November 2023. The contents of this report were developed based on this specific case study.

Imprint

Publisher

Division of Business and Economic Development,
Canton of Zurich
Metropolitan Area Zurich Association
Innovation Zurich

Project conception and coordination

Raphael von Thiessen
Location Promotion Canton of Zurich
8090 Zurich
raphael.vonthiessen@vd.zh.ch

Concept in collaboration with:

Stephanie Volz
Isabell Metzler
Patrick Arnecke

Authors

Dr. iur. Stephanie Volz
Raphael von Thiessen

Design

Sibylle Brodbeck, sibyllebrodbeck.ch

Publication

This report is published exclusively in digital format
and in the languages German and English

Translation

Mila Myrsep, Word for Word Ltd. Liab. Co.

Copyright

All contents of this publication, especially texts and
graphics, are copyright protected. The copyright is
held by the Location Promotion Canton of Zurich.
The publication can be passed on to third parties
with the copyright information, and it may be
quoted from with complete source references.

© 2023 | Canton of Zurich

Project Steering

Division of Business and Economic Development,
Canton of Zurich
Statistical Office, Canton of Zurich
Division of Digital Government, Chancellery,
Canton of Zurich
Office for Economy, Canton of Schwyz
Metropolitan Area Zurich Association
ETH AI Center
Center for Information Technology, Society, and Law
(ITSL) University of Zurich