This report explores how upcoming EU legislation will impact existing business models for data utilisation.
Proposed EU Regulations’ Impact on Data Utilisation – A Multi-Case Study within Public Transport

Håkan Burden and Susanne Stenberg,
RISE Research Institutes of Sweden
Måns Olsson, Lund University

RISE Research Institutes of Sweden AB
RISE Report: 2023:47
ISBN: 978-91-89757-97-4
Gothenburg, April 2023

Front picture generated by deepai.org with the prompt “users and public transport”
This work is licensed under CC BY 4.0  https://creativecommons.org/licenses/by/4.0/
Abstract

Proposed EU Regulations’ Impact on Data Utilisation – A Multi-Case Study within Public Transport

Motivation: In a broad sense data sharing onboard public transport vehicles is governed by two different business models – interoperable and free of charge access for some data versus data that is restricted to specific uses by commercial contracts and existing legislation. Under the Digital Decade the EU has proposed new legislation with the ambition to promote a single digital market. The question then arises – how will the upcoming regulations affect existing business models for data utilisation?

Method: We have investigated two different cases where existing technology meets upcoming EU legislation. The questions have been framed through dialogue with actors in the industry, to cover topics and questions that are both concrete and current. Using the policy lab methodology, we have investigated the possibility to re-use surveillance film from public transport vehicles for passenger counting. The analysis compares GDPR and the Swedish camera surveillance act with the proposed AI Act, to see what new possibilities or obstacles arise. We have also explored the changes that the Data Act may impose on different actors’ access to data derived from the batteries installed in an electric bus.

Results: The AI Act will not change the business models within the eco-system but facilitate access to more personal data (including personal data where GDPR otherwise would be a barrier), useful for training automated passenger counting. Those responsible for placing the system on the market will still need to ensure that they are compliant with GDPR in terms of processing personal data. In terms of the Data Act the outcome is more disruptive as the owner and user of a vehicle is entitled to all data representing their usage, free of charge, and this will impair existing business models for data access. It is also possible for multiple actors to be users, for instance if the vehicle is owned by a public transport authority and leased by an operator.

Discussion: Our analysis shows that while the impact of the Data Act can resonate with the ambitions behind the regulation in terms of making more data interoperable and available free of charge, it can also have the opposite effect. The latter is specifically the case where altruistic data sharing already is in place and the Data Act imposes standard contracts for and role-based restrictions towards utilisation. Both the AI Act and the Data Act are complex and often difficult to assess. In relation to the Data Act, the recitals were helpful for interpreting the application of articles and definitions. For understanding the relationship between the AI Act and GDPR we combined the legal analysis with prototyping the impacts and relied on sharing insights with other actors. This highlights the need for multiple ways of performing the data collection and analysis as well as the suitability of policy labs as a research method.

Key words: Digital Decade, Data Act, Artificial Intelligence Act, ITxPT, Policy, Policy lab, Regulation, Regulatory development
Content

Abstract .................................................................................................................. 2
Content .................................................................................................................. 4
Preface .................................................................................................................. 5
1 Data sharing in the Digital Decade .................................................................... 6
2 The policy lab methodology ............................................................................. 7
  2.1 Policy and policy labs................................................................................. 7
  2.2 The Bus-as-a-Service project .................................................................... 7
  2.3 Aim and scope of the policy lab ................................................................. 8
  2.4 Data collection and analysis ..................................................................... 9
  2.5 Validity measures .................................................................................... 9
3 Traffic safety through Artificial Intelligence .................................................. 11
  3.1 Using cameras for the safety of passengers ............................................. 11
  3.2 Protecting personal data ......................................................................... 13
  3.3 Counting passengers with data from surveillance cameras .................... 15
  3.4 The AI Act and future exempts from GDPR .......................................... 17
  3.5 Reusing personal data to enhance passenger safety ................................ 19
4 Sharing battery data ....................................................................................... 21
  4.1 Data and circular economy ...................................................................... 21
  4.2 The Data Act ............................................................................................ 21
  4.3 The implications for bus 7201 .................................................................. 24
  4.4 Battery data and the Data Act ................................................................. 26
5 Final words ...................................................................................................... 28
References .......................................................................................................... 29
Preface

This study was conducted as part of the Bus-as-a-Service project (Vinnova grant nr 2021-02552) to explore how upcoming EU legislation will impact existing business models for data utilisation.

The outcome is to be seen as a preliminary analysis. The acts under investigation are not finalised and may change in a way that impacts our findings. The endeavour was also scoped to explore two aspects of data utilisation in relation to two proposed regulations, it is therefore obvious that all aspects of the current situation or other upcoming changes to the legislation have to be taken into account for a comprehensive analysis. There is also an on-going initiative targeting vehicle data that might impact the scope of the investigated policies and subsequently our analysis. As more is known and the pieces are discussed in a broader perspective, new insights that contradict or change our analysis will surely arise.

Our ambition was, and still is, to start a discussion on the impact of new legislation, not perform a formal investigation. That said, we will have reasons to re-visit the topics to both broaden and detail the work as the proposed acts find their final versions and stakeholders start to adjust affected business models.

The report is structured so that the first section introduces the Digital Decade and the relevant, proposed legislation. Then follows a description of our policy lab, both in general terms and specifically for this study. The two following sections describe the analysis and outcome of each case – first the reuse of data from surveillance cameras for automatic passenger counting in relation to the proposed Artificial Intelligence Act; second, the access to battery data for electrified vehicles in relation to the upcoming Data Act. Section three and four include the conclusions from each case. Section five therefore gives a high-level conclusion regarding the methodology and the importance of a continuous dialogue on the impact of the digital decade in relation to other initiatives within digitalisation and existing regulation.

Finally, a few words on our responsibilities as authors. We are indebted to the people who have taken time to share their thoughts and questions with us, your input was invaluable for detailing the understanding and finding new interpretations. Thank you! The report still represents our analysis and our choice in how to frame and address the challenges and opportunities posed by the proposed legislation. We are therefore solely responsible for the content of the report and it does not necessarily reflect the opinions or perspectives of those we have interacted with.

Håkan, Susanne and Måns
Gothenburg, April 2023
1 Data sharing in the Digital Decade

In 2021 the European Commission released “the European way for the Digital decade” (Commission, 2021). Due to how the COVID-19 pandemic changed the reliance on digitalisation for working, education, socialising, accessing societal services, innovation and much more there was a need to address the vulnerabilities of the digital space to lessen the dependence on non-European products and services as well as the impact of disinformation on our democratic systems.

Four cardinal points were recognised as critical for enabling the transition on a European scale – the digital skills of citizens and professionals, secure and sustainable digital infrastructure, the digitalisation of public services and the digital transformation of businesses. In 2022 the European Parliament and the Council of the European Union detailed targets for each cardinal in the Digital Decade Policy Programme (EU, 2022). The aims are high. As examples the policy programme claims that by 2030 there will be an increase of trained ITC specialists from 8 million to 20 million, EU’s share of produced semiconductors is doubled on a global scale, all citizens have access to medical records online and 75% of all EU companies use AI, big data or cloud services.

In parallel, a number of legislative acts have been proposed to facilitate the transition. The acts range from responsibilities for platform providers (Digital Services Act and Digital Markets Act), technical requirements for cyber security (Cyber Resilience Act), obligations for making data available (Data Governance Act and Data Act), and responsible AI systems (Artificial Intelligence Act). However, there are already business-related initiatives for free of charge and interoperable data sharing and utilisation. IT for public transport, ITxPT, is such an initiative within public transport.

ITxPT is a non-profit organisation enabling data access and interoperable IT-solutions (ITxPT, 2023). The idea is that certain data should be shared across actors with a stake in public transport. A typical case is how the ITxPT-specification enables the sharing of positional data across the on-vehicle IT-network so that the supplier of internal screens can give passengers information about connections at the next stop, the operator knows where the vehicle is in relation to the timetable and the authorities charge for a ticket for the right zone. And with only one GPS on each vehicle. Aggregated across data sources and needs this reduces the number of data-generating products within the fleets and has a positive impact on maintenance, the usage of physical resources and facilitates innovation by data sharing.

While the ITxPT specifications do not cover all data available from a public transport vehicle they have already been used in procurement of IT-solutions for public transport (see e.g. Storhaug, 2017; Transport for London, 2021). The question then arises – how will the proposed legal acts within the Digital Decade affect existing initiatives for data utilisation driven from a business perspective? Or put in other words - to what extent will the upcoming regulations facilitate industry’s digital transition? That is something we set out to explore in the Bus-as-a-Service policy lab.
2 The policy lab methodology

This section starts by setting out the generalities of policy labs and then details them in relation to the context of the Bus-as-a-Service project. We then describe the aim and scope of the policy lab. The strategies for data collection and analysis are then given and followed by our chosen validity measures.

2.1 Policy and policy labs

New technologies and businesses models can pose new challenges if it is unclear how they relate to existing policies, the latter are often seen as slowing down or creating barriers for successful innovation (Schneier, 2019). As technological and business innovation evolve faster than laws, standards and guidelines it creates challenges for sustainable development as the rules for a level playing field become blurred, creating social tensions between entrepreneurs, politicians and members of society.

The policy lab methodology entails in our case conducting an investigative legal analysis, including mapping the circumstances to the responsibilities and definitions set not only by legislation and regulatory frameworks already in place but also to clarify and visualize options in relation to upcoming proposed legislation. This allows us to relate the technical developments to the uncertainties of business and policy development. Furthermore, we utilise continuous interaction with actors, this includes policy stakeholders as well as policymakers, to ensure that multiple perspectives and interests are covered. A visit to the actual site or a demonstration of the technical innovation gives deeper understanding of the challenges but also an opportunity to observe the actors in relation to both the phenomena and each other (Robson, 2002).

Policy as a concept therefore resonates with the concept of governance – the interactions and their rationale between private and public stakeholders that play a role as decisions are planned, executed and evaluated in a societal context (Stoker, 1998). There are several ways to facilitate policy development, such as test beds (Engels et al, 2019), regulatory sandboxes (Zetsche et al, 2017) and labs. For the case of this contribution the focus is on policy labs as an enabler for adequately safe introduction of new technology.

An EU report from 2016 defines the activities of policy labs as to “approach policy issues through a creative, design, or user-oriented perspective […] strive to organize experiments to test proposed policies […] work for or within a government entity or public administration and contribute to the shaping or implementation public policies“ (Fuller, 2016). From this perspective a policy lab can be an organization, a place (physical or virtual), methodology or a project that aims to shape or implement public policies, through co-design with relevant stakeholders (Hagy et al, 2017), in an agile fashion (iterative and incremental development) (Mergel, 2016) and drawing on multiple disciplines (Junginger, 2016).

2.2 The Bus-as-a-Service project

Bus-as-a-Service is a research project financed by the Swedish Innovation Agency Vinnova through the strategic innovation program Vehicle strategic research and innovation (BaaS, 2021). The project builds on the demonstration arena Electricity
where the regional public transport authority Västtrafik together with the Volvo Group, Ericsson and others develop and demonstrate new products and services that contribute to sustainable travelling (Electricity, 2023). BaaS was initiated in November 2021 and will run until March 2024.

In the BaaS project Västtrafik, is joined by Transdev who operates the traffic with the designated innovation bus 7201 which is delivered by Volvo. There are also three technology and service suppliers in terms of Luminator Technology Group, Consat and Pilotfish. Hogia and Triona are service providers. Academia is represented by RISE Research Institutes of Sweden and ReVeRe which is a resource for vehicle research co-hosted by the University of Gothenburg and Chalmers University of Technology. The project is coordinated by Lindholmen Science Park. ITxPT is the final member of the project.

At the core of the project stands bus 7201. It is a demonstration and experimentation vehicle that is used in regular traffic assignments on route 16. The IT-architecture onboard is built according to the ITxPT-specifications enabling data sharing of vehicle position, next stop and more. All actors in the project have access to the network and can share or produce data. Transdev also has a special agreement with Volvo enabling access to some of the data regarding the battery. These data points are beyond what is shared freely on a regular basis on other buses within their fleets and not published on the shared ITxPT-network. We refrain from being more explicit in respect to their trade agreement.

2.3 Aim and scope of the policy lab

The aim of this specific policy lab was to address perceived unclarities regarding data access and usage from an eco-system perspective and how these might be resolved through new legislation within the Digital Decade. The question then arises – how will the upcoming regulations affect existing business models for data utilisation?

To answer the question we scoped the problem and solution space by investigating two cases:

1. Traffic safety and the AI Act
2. Connected vehicles in relation to the Data Act

In both cases the analysis was built upon bus 7201 and the specific configuration of stakeholders within the BaaS project. We have also chosen to not include more draft legislation than the AI Act and Data Act into our analysis.

The ambition is not to give an extensive and complete analysis of the two acts impact on data utilisation. Rather, our ambition is to initiate a discussion on the possible impacts of new regulation on existing and proven business-to-business initiatives for data utilisation. In the long run it is important that the ongoing legislative regulation facilitates private initiatives striving for the same over-arching aims as of the Digital Decade instead of counter-acting them.
2.4 Data collection and analysis

The data was analysed by a set of different instruments which enabled triangulation by collecting different kinds of datasets and multiple formats and opportunities for validation of the emerging analysis (Golafshani, 2003). First, we started the work by inspecting bus 7201 in the depot to explore different components such as the cameras and the internal screens along with the different possibilities for adding new physical and digital systems onboard. At the same time, we had the opportunity to talk with representatives from Västtrafik, LTG and ITxPT regarding the perceived challenges and opportunities for data access and sharing.

Second, we analysed the relevant legislation, both those regulations that are in force and those being proposed. Two of the acts are still being negotiated and we have therefore made explicit which version of the act we have used in the reference list. For this work the definition of policy was thus scoped to include EU and national legislation, in force and proposed. The analysis was done individually by the three authors and then we shared insights and questions to reach a common understanding. The analysis was done in relation to our two specific cases. Each relevant policy was analysed multiple times as insights from analysing one policy often triggered a need to cross-reference to other policies. In this way the data collection and analysis was interwoven over time. Interweaving collection and analysis is suggested as a validation technique as it enables the researchers to try out hypotheses during the investigation and opens for collecting new data or analyse existing data in new ways (see e.g. Seaman). This approach is also referred to as member checking (e.g. Lincoln and Guba, 1986).

Third, we shared the emerging analysis with BaaS participants twice and once with the Swedish Authority for Privacy Protection through three workshops: first with the BaaS participants, then with the national competent authority and finally again with the BaaS participants. The sequence of workshops enabled insights from one workshop to be integrated with the analysis before the next workshop so that the analysis was incrementally validated and enriched.

Finally, we used personal communication to resolve unclarities regarding individual stakeholders’ access to data, interests in data access or responsibilities towards passengers, traffic safety and so on. This was either done through e-mails or informal meetings such as over lunch or coffee. Informal communication has the drawback that formal data collection techniques are less usable but gives the respondent a more relaxed and open format for sharing which can yield new insights (Davis, 1978).

2.5 Validity measures

Lincoln and Guba suggest that the trustworthiness of qualitative analyses derived from data collected from real-world research can be assessed in terms of four aspects (1985):

1. **Credibility**: How well the analysis reflects the phenomena under investigation. Prolonged engagement, persistent observations, triangulation, peer debriefing, negative cases and member-checking are techniques for managing credibility.
2. **Transferability**: To what extent the analysis is applicable in another context. This can be handled through cases in different contexts but also by supplying details about the context so that comparisons can be drawn in later research.
3. Dependability: The possibility to replicate the study. The recommended strategy is external audits by other researchers.

4. Confirmability: To what degree the findings are influenced by researcher bias. This can also be managed by triangulation, here in terms of number of researchers and perspectives. Recording design decisions is another strategy.

In the case of the work presented here the credibility measures relies on a prolonged engagement with the community and the ITxPT initiative (see e.g. Burden and Ohlin, 2019). In relation to the relevant policies the experience varies from being the first-time analysing a case in terms of data collection from camera surveillance to having actively analysed how the AI Act evolves through the on-going negotiations (Burden and Stenberg, 2021; Burden and Stenberg, 2022a; Burden and Stenberg, 2022c). Triangulation was utilised in terms of collecting data from multiple sources and peer debriefing through workshops. The iterative and incremental analysis enabled member-checking.

Transferability is managed by describing the context of our phenomena and how we have conducted the study. Dependability was not managed by the recommended strategy of a formal audit by external researchers. Instead, we have used external actors such as a national agency and members of the BaaS project for presenting emergent findings and assess the adequacy of the collected data which in turn has had an influence on the final analysis. The formal audits have been supplemented by informal discussions with other researchers at RISE.

The external audits have also enabled actors with different stakes and perspectives to comment on both the product in terms of analysis and process in terms of data collection and decisions regarding scope and application for the analysis. Pairing the external audits with the analysis being done both individually and as a team means we have a triangulation of viewpoints mitigating researcher bias in line with the recommendations for confirmability.

It is worth pointing out that the analysis still represents the interpretation of the authors and that the organisations and representatives we have interacted with can hold different views than those presented in the report.
3 Traffic safety through Artificial Intelligence

Our first case is reusing data from surveillance cameras for automatic passenger counting (APC). We begin by describing the case and the motivation for APC, then how the collected data refers to the General Data Protection Regulation (GDPR, EU 2016/679) and the proposed AI Act in the form of the general approach agreed upon by the Council (AI Act, 2022). We conclude the description of the case with our initial findings.

3.1 Using cameras for the safety of passengers

As a starting point people should be able to move freely in society in safety and with trust in each other. One result of this is that, as a general rule, permission is required from the authorities to set up cameras and film people in public places or if it is representatives of the state who want to use cameras overlooking persons. There may also be explicit rules for when cameras can be used. One such exception is cameras on board public transport, where the Camera Surveillance Act allows surveillance on public transport vehicles without permission (§ 9 p 6) if it is surveillance aimed at preventing or detecting criminal activity, investigating or prosecuting crimes, prevent or detect disturbances to public order and safety or accidents or limit the effects of such disturbances or accidents occurred.

But could the images also be used for counting the number of passengers? Today, the counting of passengers in buses is carried out using two methods. Firstly, data is collected from ticket sales. Secondly, IR sensors mounted by the doors of the buses count the amount of people passing through. The current IR sensors work by transmitting a signal across the door opening, which breaks as soon as someone passes it. It is restricted to one or few locations and cannot always distinguish the people entering a bus from those leaving it. On many routes within the Västtrafik area, entrance and exit through all doors of the bus is allowed which means faster onboarding and disembarking but also less accuracy in the passenger counting. The ticket machines offer complementary data, but naturally fail to count passengers riding without a ticket and passengers who ride with a period ticket who do not present their ticket to the machines.

Figure 1 shows two images. The upper image is taken from a demonstration of a passenger counting system (Singh, 2015). Here the passengers are employees at Viscando and Consat. The two companies trained an AI system to not only count the number of passengers but also place them in relation to the bus seat configuration and keep a track of the number of sitting and standing passengers. The rights for data collection and analysis was managed by the subjects explicit consent. The output of the system is shown in the lower image of Figure 1. The accuracy of the actual system has room for improvement due to scarce amounts of available training data. For validation purposes a star was overlaid on each counted passenger so it would be easier to assess which passengers had been counted (or not).
Figure 1: A demonstration of an AI system counting employees from Viscando and Consat on a public transport vehicle.

In comparison to using ticket machines and IR sensors for passenger counting, an AI system based on pattern recognition could not only be more accurate in the total numbers of passengers but also facilitate a nuance between standing and seated passengers as well as indicating if the place reserved for wheelchairs and pushchairs is taken or not. Such information can not only help the driver to assess if the bus is full and if the passengers are travelling in a safe way but also guide passengers in where to find seats or if they should wait for another bus.
According to the GDPR, personal data means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR art 4.1). For the purpose of this report, we have chosen to treat the camera pictures of people as personal data. The Camera Surveillance Act also states that it complements GDPR without giving more details in how.

The demonstration was made in 2015, before GDPR was in place and before the national exempt for camera surveillance within public transport vehicles. The relevant authority at that point of time then assessed the solution to violate the integrity of the passengers and the initiative was put on hold. Could upcoming EU regulations change that assessment? Before we explore the impact of the AI Act we need to highlight how GDPR views integrity and personal data.

3.2 Protecting personal data

Since personal data is connected to a living person there are rules guiding how to deal with the data in a responsible way, the most known regulation being GDPR. The regulatory framework is with our wording based on the principles of Know your purpose, Less is more and Necessity of use or consent by the person concerned. In the terminology of GDPR the person concerned is referred to as the data subject and the one processing personal data as the controller. This section will give a summary of articles 5 and 6 that set out the principles and legal prerequisites for processing personal data. The summary is scoped towards the case at hand and might black important details for other purposes.

3.2.1 Principles for processing personal data

The principles of GDPR are that personal data shall be (article 5):

(a) processed lawfully and fairly in a transparent manner;
(b) collected for a specific purpose and not processed in a way that is incompatible with the given purpose;
(c) limited to what is necessary in relation to the purpose;
(d) accurate and that inaccurate data is rectified or deleted without delay;
(e) saved for no longer than is necessary for the purposes, if it is possible to identify data subjects from the data;
(f) processed in a manner that ensures appropriate security of the personal data;

Point b is further elaborated in article 6.4, to which we will return in section 3.2.3. It is the controller who is responsible for, and who is obliged to demonstrate compliance with, the paragraphs detailing these principles.
3.2.2 Lawful processing of personal data

Lawful processing of personal data requires that at least one of six prerequisites are met (article 6.1):

a) the data subject has given consent for processing the personal data for the purpose;
b) the processing is necessary to fulfil contractual obligations towards the data subject;
c) the processing is necessary for compliance with legal obligations, as defined by EU or member state law;
d) the processing is necessary for protecting vital interests of the data subject;
e) the processing is necessary in relation to public interest, or an exercise carried out by an official authority, as defined by EU or member state law; and/or
f) the processing is necessary for the purpose in relation to a legitimate interest pursued by the controller (but the legitimate interest cannot override the fundamental rights of the data subject).

Public authorities shall not motivate their processing by claiming point f. Aside from the concept of public interest, a more general weighing of conflicting interests is possible according to 6.1 f. Here the interests of the individual not to have their personal data processed, is weighed against the interests of the controller. The rule is to be applied as a general clause, when none of the previous rules applies. The incentives to process the personal data is here balanced against the right to privacy and protection of personal data, both explicitly recognized in articles 7 and 8 of the EU charter (Sartor, 2020). A justified interest may, for instance, exist in a relationship where the data subject is a customer of the person processing his data (recital 47 of GDPR). The term also presumes some predictability. If the data subject cannot reasonably expect his or her data to be processed in a specific context, it is less likely that a balance can be achieved.

3.2.3 Processing of personal data in a new context

Personal data already collected may not be used in new contexts without restrictions (article 6). If there is not consent for processing the personal data for new purposes, or legal grounds by EU or member state law, the controller needs to show that the processing for another purpose is compatible with the purpose given for collecting the data. In the assessment the following five considerations shall be taken into account:

a) the connections between the purpose given at the point of collection and the new purpose;
b) the context and the relationship between data subject and controller;
c) the nature of the personal data;
d) the possible consequences for the data subject of the additional processing; and
e) the application of appropriate safeguards such as encryption and/or pseudonymization.

Personal data which is particularly sensitive in relation to individuals’ fundamental rights and freedoms merit specific protection (recital 51). However the recital then adds that “processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric
data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.”

When the new treatment of the data is seen as compatible with the current treatment, no further legal foundation is required than that which warranted the collection in the first place (recital 50).

3.3 Counting passengers with data from surveillance cameras

This section will now relate the principles and criteria for lawful processing of personal data with the further processing for automatic passenger counting. The reasoning will go through the criteria in the reverse order to explore the criteria for such re-use, as it is only worth looking at the relation of the additional processing to the principles in article 5 if the additional purpose is compatible with the purpose given for collecting the data.

3.3.1 The purposes for camera surveillance and automated passenger counting

First, we regard the link between the purpose motivating the collection of personal data and the secondary processing. The purpose for collecting the personal data goes back to the motivation for allowing camera surveillance on public transport vehicles - to prevent or detect criminal activity; investigating or prosecuting crimes; preventing or detecting disturbances to public order; preventing accidents; or limiting the effects of such disturbances or accidents.

Using the camera film also for automated passenger counting will allow for information about the level of on-board congestion at specific times and routes, to be distributed in order to give passengers an option to travel at times when there is more free space in the buses. Using cameras, it is also possible to show passengers the status of the relatively few spaces available for strollers and wheelchairs. All relating directly to the given purpose of preventing and minimizing effects of accidents on-board the bus in operation of public transport.

Furthermore, a purpose with real-time automated passenger counting is ensuring that the driver has the necessary information regarding when the maximum number of allowed passengers is reached. This is an important measure to increase traffic safety, and at the same time it requires a high level of precision in order to not leave more passengers than necessary waiting for the next departure, which would decrease both efficiency and customer satisfaction. According to the proposition of the Camera Surveillance Act the purpose to detect, prevent and limit effects of accidents entails not only accidents that effects life and health of people, but also property and environment (compare CSA 8 § 4 par, see prop. 2019/20:109 p. 50). In conclusion, the two purposes can be aligned as preventing and limiting effects of accidents.

Second, we consider the context and relationship between the data subject and the controller. When evaluating new processing of previously collected data, it is important to establish whether the typical data subject can reasonably expect his or her data to be used in this way (see e.g. recital 50, GDPR). The use of surveillance cameras is
highlighted by information in the bus, the interesting question to consider is if it is reasonable to assume that the passengers know that the cameras and subsequently the personal data are also used for the additional purpose of passenger counting.

Even if the real-time passenger count was displayed in various ways for the passengers, such as by a green-yellow-red sign in and on the vehicle or by similar information in the trip planner, it is not obvious for passengers that the information is derived from the surveillance cameras. Here it is probably advisable to make the re-use explicit for passengers, for instance by an information campaign.

Third, as the personal data is taken from photographic media and the outcome is not unique identification of a natural person the processed data has, for the reasoning of GDPR, no particular nature warranting special considerations.

Fourth, to use collected data for new purposes, one needs to make sure that the consequences of the new processing are either negligible or beneficial to the data subject. This means that an assessment is to be done, where one aspect is what kind of processing actually is taking place (Panel for the Future of Science and Technology, 2020). If the situation involves a whole new way of processing the already collected data, one that is carried out “by a different controller and in another context” and in a way that was not likely to have been considered when the data collection was originally started, it will in many cases impact the consequences of the processing. The degree of specificity of the consequences also impacts the assessment. If the consequences of the new processing are uncertain, they are less likely to qualify as compatible with the existing. This is also true for consequences that may be achieved with other methods.

Using APC with personal data from the surveillance cameras will give a higher degree of safety, since the accuracy of passenger counting will improve a lot compared to the counting of passengers through doors. The current way of counting passengers in Gothenburg, while useful for other purposes, might for instance not be accurate enough to use as a final reason not to let more people enter the bus. A relatively large margin of error is easier to accept when the point of the data collection is not to use isolated entries, but rather to draw conclusions from the data over time. If passenger counting can be done with virtually no margin of error, it becomes much easier to use the system not only to increase safety onboard through for instance traffic planning, but also to increase safety in individual cases, vehicle by vehicle. This opens up to reach the max amount of sitting and standing passengers, trolleys and wheelchairs without jeopardizing traffic safety.

Furthermore, the consequences on personal integrity on an individual level is small since the outcome of the processing fulfills the definition of anonymization as laid down in the Open Data Directive, “the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable” (EU, 2019, article 2) and the input is deleted as soon as it has been processed. E.g. for the purpose of passenger counting the input in terms of personal data is never saved but only used for rendering information where it is no longer possible to identify data subjects. Using a technique that enhances the safeguarding of personal integrity is also recognized in relation to camera surveillance (CSA 8 § 2nd par, prop 2017/18:231 p. 145). The anonymization addresses the fifth concern regarding the application of suitable safeguards.
Given that the following reasoning are detailed for the specific circumstances it would be possible to claim that the two purposes are aligned and that the processing for passenger counting is legal (following recital 50).

3.3.2 Complying with the principles for processing personal data

It is now time to explore how the principles for processing personal data relate to our case. First out is the question of lawful, fair and transparent processing. If the given purpose at the time of data collection is compatible with the purpose for re-using the data, no further legal foundation is required and the processing for passenger counting can be seen as lawful. The recommendation to inform the passengers about re-using the personal data for passenger counting would also be in line with fair and transparent processing.

Since the purposes can be aligned we consider the second bullet managed and focus on the adequacy and relevance of APC processing. This topic is also covered by previous reasoning but here it is also worth pointing out that re-using already collected personal data reduces the amount of collected personal data compared to having a separate system with its own cameras.

The principles relating to accuracy (d), data storage (e) and integrity (f) are handled together since they reflect different aspects of the system design. Our conclusion is that a software that deletes personal data just mere milliseconds after receiving them has a good chance of reaching a sufficient safety standard. The software is also designed to work in the individual vehicles, so that the information that leaves the bus carries no personal data. It will only be the information needed to generate the lower image in Figure 1 that leaves the bus while the upper image is deleted as soon as the analysis is completed.

A human could derive the lower image of Figure 1 given the upper image, but not place the corresponding individuals in the right place given the lower. We can therefore conclude that access to the lower image by itself does not pose an integrity issue.

All in all, there is a case in re-using collected personal data for APC from the perspective of GDPR. As stated earlier, the AI Act will allow for exempts from GDPR under specific circumstances, will that make it easier to deploy systems that re-use personal data for APC?

3.4 The AI Act and future exempts from GDPR

The proposed Artificial Intelligence Act (AI Act) was initially proposed in the spring of 2021 (Commission, 2021). Since then the act has undergone substantial changes and in December 2022 the Council of the European Union delivered its position (AI Act, 2022). It is the latter that is used for the purpose of our analysis.

3.4.1 Artificial Intelligence and the notion of risk

The AI Act defines technical requirements for those systems that are perceived as posing a high risk towards health, safety and fundamental rights, as well as General Purpose AI.
Since passenger counting fits with the definition of the latter in terms of pattern recognition it is worth remembering that a future APC will need to comply with the technical requirements posed in articles 8 to 15, which will be detailed in upcoming implementing acts. Here it is worth pointing out that article 10 states that datasets used for training, testing and validation need to be “relevant, representative, and to the best extent possible, free of errors and complete”.

We do not consider APC to be a case of the high-risk activity remote biometric identification since the output of the system is similar to the lower half of Figure 1 and not possible to link with a specific individual. This also excludes APC from any of the forbidden activities regarding remote identification of individuals. In short, our analysis shows that APC will not be considered illegal under the AI Act but will have to comply to upcoming technical requirements for AI systems and be CE-marked in accordance with the compliancy requirements.

3.4.2 Regulatory sandboxes

The AI Act also opens up for the usage of regulatory sandboxes for developing AI systems. The overall purpose of the regulatory sandboxes is to facilitate innovation, promote the development of an AI eco-system of actors as well as compliance with the regulation and subsequent requirements. The regulatory sandboxes are to be governed by a national competent authority and within them it will be possible to make exempts from GDPR. The exempt enables that personal data lawfully collected for other purposes is used for developing, testing and training innovative AI systems.

To be applicable for an exempt the system under development needs to fulfill certain criteria (our numbering):

1. The system shall be developed for safeguarding substantial public interests within public safety and health, the protection of the environment, the efficiency of public administration, the cybersecurity of critical infrastructure and/or mobility and transportation.
2. The personal data is needed to comply with the technical requirements set out in articles 8 to 15.
3. The rights and freedoms of the data subjects are monitored and relevant mitigation strategies are in place to counter possible risks.
4. The personal data is stored in an adequate and secure way, not transmitted to other parties (unless the disclosure is in line with EU regulations) and deleted after the participation in the regulatory sandbox has terminated.
5. The processing of personal data is logged and done according to national or Union law, and the rationale for the processing is stored together with the testing results.
6. The work is summarised in the annual report conducted by the national competent authority.

3.4.3 Exiting the regulatory sandbox

In relation to the criteria the case can be argued to contribute to mobility and transportation (criteria 1). Since training an APC requires large amounts of data the regulatory sandbox might be a feasible way of obtaining lawfully collected personal data
from surveillance cameras in order to comply with article 10 and data quality (criteria 2). Given that criteria 3 to 6 will have to be addressed by the setup of the regulatory sandbox and handled by the actors within, APC qualifies as a system to be included in a regulatory sandbox and thereby achieve exempt from GDPR.

The national competent authority is not obliged to introduce regulatory sandboxes in general or for APC specifically. If this option is to be made available actors within public transport need to make it clear why their case has priority and why the limited resources of the authority should be spent on APC instead of other, pressing matters.

However, for using the resulting system outside of the regulatory sandbox there is still a need to perform the analysis relating to articles 5 and 6 in GDPR. Hence, the AI Act will enable access to personal data needed for the development of reliable APC through exempts from GDPR but not the usage of the system. If the resulting system is to be used within public transport compliance with GDPR is still mandatory.

3.5 Reusing personal data to enhance passenger safety

Today passengers are filmed by surveillance cameras onboard public transport vehicles through an expressed exemption that allows camera surveillance within public transport in order to safeguard public safety and to prevent or minimize effects of accidents. The collection of personal data done by the cameras on the bus is thereby aligned with the purpose of the processing of the patterns of faces within the passenger counting system, namely in order to enhance traffic safety including to prevent or minimize effects of accidents inside as well as outside the bus.

A challenge in developing picture-based passenger counting systems is access to relevant and representative datasets for training and testing. The underlying AI-technology relies on large datasets to both capture less prominent cases as well as establishing confidence in the generated output. This is where the AI Act comes in. The proposed act includes articles allowing for exemptions from GDPR in using personal data for new purposes in a regulatory sandbox. However, you still have to make sure that you have the right to use personal data when the AI-system is deployed outside the sandbox. It is therefore only worth going through the AI Act if it provides access to more personal data to train the passenger counting system on.

Why go through the bother of GDPR when the Camera Surveillance Act allows for collecting the personal data? Because the Camera Surveillance Act primarily regulates the usage of cameras for surveillance and not the treatment of the collected data per se. So, while it allows for placing surveillance cameras in public transport it does not explicitly explain how the collected personal data should be treated, even if the first paragraph of the Camera Surveillance Act states that it complements GDPR. Our reasoning is therefore that we have a stronger legal justification for reusing the camera data for APC if that usage is explicitly compliant with GDPR – e.g. show how treating personal data complies with GDPR. Therefor the bother of relating the treatment of the personal data to the latter even if we already have justification for collecting the data.

To our knowledge there is one court ruling of how to interpret article 6.4 and the notion of processing personal data for a new purpose. In March 2023, the EU Court of Justice
made a ruling regarding to what extent a register of personal data held for the purpose of taxation can be used as evidence in court proceedings when the register includes data subjects not involved in the court case (EU Court of Justice, 2023). The EU Court found that article 6.4 is applicable in that case but that the outcome is dependent on the context, e.g. the analysis has to be conducted for each case. The court’s deliberation shows that article 6.4 and recital 50 can be used for conducting the case-based analysis but that the outcome from one case is not necessarily relevant for another case. In relation to our case the ruling shows that our method of reasoning is feasible but we cannot extrapolate the outcome from the court case to our case.

An interesting point for future analysis is how the original and new processing differ in character. In the current surveillance system, only a small fraction of the filmed material is actually seen, and only by police, when an accident or a crime has taken place. For the proposed use of the same data for passenger counting, on the other hand, an AI-system has to go through all the material but does so in less than a second. It also erases any personal data it receives right afterwards, so no personal data ever leaves the bus for the sake of the counting.

In conclusion, it seems that there is a need to further explore the treatment of collateral personal data, e.g. data that contains digital representations of persons but is interesting for other purposes. It is clear in the case of APC that we are treating personal data but also that the outcome and purpose are detached from the individuals that happen to be represented in the camera data. The need is further emphasized by the possibilities for local treatments (edge-computing) where data is collected, analyzed and discarded multiple times per second. Typical for treatment of collateral personal data is that the outcome of the analysis represents human behavior on a more abstract level and not actions or facts related to specific individuals.
4 Sharing battery data

This section details our analysis of how the proposed Data Act relates to the existing data utilisation for the batteries onboard bus 7201. The focus is on the roles defined by the act and how the rights associated to the roles affect the different stakeholders and their current business relations. For our work we have used the compromise text from December 2022 and then cross-checked the analysis with the new compromise proposals from January and March (Data Act, 2023).

4.1 Data and circular economy

Before we go into the details of the Data Act it is worth putting the initiative into a broader scope in terms of parallel regulatory initiatives. Since legislation regarding data access and sharing rules already is in place for the automotive (e.g. EU, 2013) and transport sector (e.g. EU, 2010), the proposed legislation under the Digital Decade complements existing regulations and might in turn be complemented itself depending on the outcome of an on-going initiative regarding vehicle data (Commission, 2022a).

In terms of upcoming regulation, the proposed directive on liability for defective goods states that products that can be updated or modified are central for achieving sustainability and waste-reduction (Commission, 2022b). The reasoning goes that for some products data is a vital part of enabling updates and modification since it is important to understand the previous usage and wear to better assess the optimal future of a product and/or its components.

Data regarding the current status of a battery and the impact of charging is important not only for the daily operations of an electrified vehicle, but the data also contributes to the life-long log of the battery and the different components within. Analysis of the log enables better estimates of when a battery needs to be replaced, what the replaced battery can be used for in the next lifecycle and if the battery can be reused as a whole or needs to be broken down into its different components to be reused individually.

Today vital services regarding the health of the battery in terms of prognoses for maintenance and replacement as well as possible second usage is something that the vehicle manufacturer can charge the vehicle owner for.

4.2 The Data Act

While the Data Act does not merely state which data should be shared between which actors, but also contains some details on how this should be done, we have decided to limit the scope of this paper to the first topic. Since data sharing between different stakeholders in public transit is already a reality, albeit under other conditions, we think that a large part of the technical aspects of data sharing are already being resolved by the industry.

4.2.1 Purpose and scope

It has been said in the proposal (COM/2022/68) that one purpose of the regulation is to enable data users to choose between different providers of third-party and repair
services. It further states the ambition to facilitate inter-operability so that data is made accessible in standardized formats and ways, enabling easy transition between services for the users as well as fair market rules for all actors. And finally, the ambition is to create more opportunities for digital innovation in general and specifically after-market solutions and maintenance of connected products.

Although the term is not present in the regulation itself, it is explained throughout the preparatory works and recitals that the Data Act is supposed to be applied on products on the Internet of things (IoT). An IoT product is distinguished from other, not connected products by its ability to collect data concerning its use and transmit this data via a publicly available electronic communications service. That brings us to the definition of product as defined by the Data Act.

4.2.2 Definitions with interpretations

Article 2 of the Data Act is the place where the legal definitions are stated. The definitions are supplemented by recitals to facilitate their guidance but also to motivate the definition and the guidance.

Article 2.1 defines data. Within the scope of the Data Act, data is seen as digital representations of activities, facts or information as well as compilations of the same. Recital 14a relates to article 2.1 as it clarifies that data “should be understood to cover data recorded intentionally or indirectly resulting from the user’s action”. That includes interaction with interfaces, relevant metadata, automatically generated data by sensors and diagnostics data as well as when the product is in active use, in stand-by mode and when it is shut off. Recital 14a also clarifies that data refers to both raw data and prepared data. The latter should be interpreted broadly and refers to data cleaned, sorted, classified and transformed as a preparatory step for further processing. Derived or inferred insights are however not covered by the definition of data as they do not originate from the use of a product but from additional investments in systematic processes that derive value from data. If prepared data exists or needs to exist in order for the data to be comprehensible, it also has to be shared with the user.

The concept of product is defined in article 2.2. A product collects, generates or receives data about its usage and environment. The product is directly or indirectly connected to a publicly available electronic network so that the data can be communicated. Recital 14 lists things that should be seen as products according to the Data Act – home equipment, consumer goods, medical equipment and wearables, agricultural and industrial machinery as well as vehicles. Recital 15 gives examples of things that are not to be seen as products in relation to the Data Act. The list includes things that play or record media such as smart screens, speakers and cameras, as well as things that processes and stores data i.e. smartphones and computers.

Related services are digital services that at the time the user buys, rents or leases the product, is interconnected with the product in such a way that the product will not be able to perform one of its functions without the service (article 2.3). The definition includes software and updates.

According to article 2.5, a user is then a natural or legal person who owns, rents or leases a product or receives a related service. A user can therefore be someone using a smartwatch to monitor their training or a company renting medical equipment. Their
relationship to the product and their generation of user data follows the same rules according to the Data Act. The Data Act allows for more than one user of a product. While typically only one entity will stand as owner or lessee of the product, there is no natural limitation to the number of users of a related service, i.e. recipients of the collected data. Recital 18 states that “each user may contribute in a different manner to the data generation and can have an interest in several forms of use, e.g. fleet management for a leasing company, or mobility solutions for individuals using a car sharing service”.

The natural or legal person who has the right or obligation to make certain data available is referred to as the data holder (article 2.6). A person who can enable access through technical design or access rights to non-personal data is also considered a data holder.

A third actor is denoted data recipient (article 2.7). Such an actor is neither a user nor a data holder but a natural or legal person to whom the data holder makes data available. This could be initiated by a request from the user or by legal obligations under Union or national law. The data recipient has the right to access the same data as a user, but not free of charge, not without the user’s approval and with a restricted right of usage. The distinction is needed in order to enable third party access to user data while still maintaining the data holder’s incentive to collect data, by letting them demand reimbursement for the costs of doing so.

4.2.3 The right to access data

Access to data is regulated in articles 3 and 4. Article 3 is the default way of access and states that the data should be provided to the user in a standardized, machine-readable format by default and free of charge. Products and related services should be designed in such a manner that data can be shared securely and easily.

If data, prepared or not, “cannot be directly accessed by the user from the product or related service, the data holder shall make available to the user the data generated by the use of a product or related service ... on the basis of a simple request through electronic means where technically feasible” (article 4). The same requirements are applicable as in article 3 on standardized and machine-readable formats, free of charge, securely etc. with the addition that the sharing should be carried out without undue delay.

A difference between the access described in articles 3 and 4 is how the latter mentions the need to respect trade secrets. It is the responsibility of the data holder to identify which data is to be seen as trade secrets. Necessary technical and organisational measures shall be in place to ensure the integrity of the trade secrets and if they are not deemed fit additional measures shall be agreed upon between user and holder.

Article 5 gives the user the right to request that the user data (which can be both raw and/or prepared) is shared with a third party, a data recipient. Recipients cannot use the data for developing services but if they already have a service for which the data fits that service can be used for processing the data. The holder should then be reimbursed if both holder and recipient are businesses. The compensation shall be reasonable, not exceed the costs directly related to making the data available which covers data reproduction, dissemination and storage but not collection or production (article 9). The holder shall provide enough information for the recipient to assess if the compensation is fair in relation to the costs of making the data accessible.
4.2.4 Interoperability

The Data Act strives to make data more accessible and easy to use among actors. It is for instance shown in the definitions of data and access through the emphasis on prepared data and standardized formats. The term interoperability is defined in article 2 as the ability of two or more products, systems, components etc. “to exchange and use data in order to perform their functions”.

This also opens up for the user to choose who should process the data for which purpose (and get reimbursed for their efforts). Providers of processing services shall ensure that users of their services can switch to another service provider if wanted (article 23). There are details on contractual terms and who pays whom for what, but we leave those for future analysis as the focus in our case is how the Data Act changes the existing business relations, not specifics in the subsequent contractual changes.

4.3 The implications for bus 7201

We will now map the definitions of the Data Act to our case in order to define roles and responsibilities within the eco-system. Before we dig into the analysis it is important to clarify that battery data is currently not part of the ITxPT-specifications. There are existing business models for battery data that are not aligned with the ITxPT business model, such as subscription services based on economic demand, and the idea we want to explore is how the Data Act could potentially make the battery data available for specific actors and how this resonates with the ITxPT vision.

4.3.1 Battery and bus

Today, sharing of battery data on bus 7201 is only carried out on a limited scale, for the purpose of research and development. Within the boundaries of the project Bus-as-a-Service, the partaking vehicle manufacturer, Volvo, has agreed to share such data with the traffic operator Transdev. To us, this serves as indicative proof that instruments for data collection already exist and are in use. We therefore conclude that the vehicle manufacturer takes interest in the information and has techniques in place for collecting the relevant data.

In the case at hand, we have found that the battery is in itself not a product according to the Data Act, but rather a component of the product bus. This also fits with recital 14 which explicitly mentions vehicles as products. A modern bus is connected to the internet, in order to share various types of data to multiple actors. The local network of the bus may also be seen as public, since it is utilized not only by the bus manufacturer, but also the operator and transit authority, for example to communicate with ticket machines and keep track of the whereabouts of the vehicle. That means it is not relevant if the batteries of electric buses have an independent way of communicating their data together with related services. The batteries are still one of many components of the bus that generate data based on how and where the bus is used. The subsequent data from batteries, the GPS and the thermometers should therefore be shared with the user.

Here it is worth mentioning that recital 14 clearly mentions vehicles as a type of product within the scope of the Data Act as late as March 2023 even if there have been on-going
initiatives for a specific regulation for vehicle data for twelve months (Commission, 2022a).

In the case at hand, the raw battery data affected by usage may include at least the temperature, voltage and amperage of the battery together with the timestamp. The mere sensors are not related services themselves but have to be aided by digital software to make the readings accessible to humans and other devices.

4.3.2 Data user, holder and recipient

In the case of bus 7201 we have assigned Transdev the role of the user. The relationship is straightforward as they own the bus and also receive a limited set of data from the batteries regarding the usage.

For the role of data holder, we have opted for the bus manufacturer as the bus manufacturer is the immediate data holder and distributor of the vehicle. This also fits with the definition of holder as someone who can enable access to the data. Seeing as the formulation of the Data Act consistently avoids data ownership as a concept, to focus instead on the access to data, there is no apparent reason as to why the manufacturer of an appliance should be seen as the “natural” data holder. It might be wise to note that this kind of relationship between a battery manufacturer and a vehicle manufacturer is not completely universal. In other sectors utilizing electric vehicles, battery manufacturers play a much bigger role in the vehicle maintenance and therefore receive the data they need to maintain the product that they have delivered. In terms of the Data Act, the product is then designed in a way so that the overall product provider does not have the means to enable access to the user’s battery data.

In terms of recipients, actors on the ITxPT network could be seen as possible candidates. But the current business model does not cover reimbursement for data not for exclusive access within the network. That means that if you have a product or service on the ITxPT-network you share data free of charge with everyone else on the network. If you’re in, you’re all in. We have therefore concluded that there are no immediate candidates for the role of recipient in our case.

4.3.3 Alternative configurations

By investigating the possibility of multiple users, we seek to see whether the Data Act creates incentives to change the contractual relationships between the different actors. For instance, Västtrafik could take over the role as owner or lessee of the vehicles from the traffic operator and only contract the operator for staff or sublet the vehicles. It seems possible that such an arrangement would make it easier to argue that both Västtrafik and a traffic operator are users of the same product. Västtrafik by ownership, Transdev as lessee. This scenario is different from the current, where only one of the two parties has a contract defining their access to the product itself.

It could be that the definition of user based on access to a related service is interesting in the case where Västtrafik through procurement requirements have the right to access certain information regarding the vehicles that are instrumental in delivering public transport. This is a case we would like to come back to and explore in more detail.
We mentioned Transdev and Västrafik as potential users. A third potential user is the driver of the bus. While drivers in our scenario do not own the buses they drive, there might be a possibility that they are still recipients of related services concerning the performance of the battery. A related service is defined by its necessity, that the product itself becomes less operable without it. A bus driver will be less able to operate the bus without receiving information about the status of the battery.

One of the purpose of legal persons is to let multiple people act as one in their common relationships with third parties, here data holders. We have not found anything that points towards the Data Act interfering in this structure by giving special status to some representatives, in this case the drivers. As the Data Act makes no attempt to change existing policies on the relationship between businesses and their employees, the driver is a representative of the business and the business is the user.

4.4 Battery data and the Data Act

The Data Act will change the existing business models between some of the actors within the ITxPT eco-system, even if the battery data is not part of the ITxPT-specification. It will no longer be possible to have subscription services with a regular fee for battery data between data holder and user. Other existing offers, such as subscriptions for information derived from the data is still a valid business opportunity as derived or inferred knowledge from the data is not covered by articles 3 and 4.

The Data Act also opens up for agnostic services as the user is now free to choose a third party to be the recipient of their data. The recipient could then in turn offer services based on user data, given that the recipient does not use the user’s data for training and evaluating their own service. But it also enables the data holder to offer agnostic services to actors who have chosen to buy, rent or lease their connected products from other manufacturers. As such the Data Act brings a disruptive element to the market as existing business models will soon be obsolete (Burden and Stenberg, 2022b).

In the latter case the ITxPT-specifications have become a de facto standard for data sharing within public transport. The ITxPT initiative thus resonates well with the intentions behind the Data Act – to facilitate data exchange between actors in an ecosystem using standardized data formats and networks for communication.

There are still open questions worth further examination. The first is the statement in article 1.2.4 which says that the Data Act does not apply to voluntary agreements between private and public entities. Can ITxPT be seen as a voluntary agreement even if some of the sharing is between private enterprises? Or does article 1.2.4 assume a bilateral agreement which excludes consortiums of both private and public actors?

For our initial analysis we have opted to view the bus as a product in itself. If the Data Act is also applicable to products and data in an ITxPT-network, how will it be applied? Some of the items on the network are explicitly not products (according to the definition of the Data Act), such as smart screens showing possible connections at the next bus stop. Some actors might be both data holders and users, such as a public transport authority with a product broadcasting a time-table on the network on a bus that it owns and leases to a public transport operator.
Since ITxPT is a standard for data exchange within public transport, and as such fits well within the initiatives towards a mobility dataspace (EU, 2023) it would be ironic if the initiative is not covered by the Data Act and the subsequent articles on dataspaces and operability. On the other hand, if the Data Act is applicable there is work to be done in understanding the implications and how the act will affect the current roles and agreements in detail.
5 Final words

First a word on our methodology. Both the AI Act and the Data Act are complex and often difficult to assess. In relation to the Data Act, the recitals were helpful for interpreting the application of articles and definitions. For understanding the relationship between the AI Act and GDPR we instead relied on sharing insights with other actors. In both cases it was instrumental to interact with the actors within the local ITxPT cluster to get insights in current business and technology development. This highlights the need for multiple ways of performing the data collection and analysis as well as a research method that allows for an iterative and incremental process.

The Data Act emphasises the need for interoperability so that data is shared in a format that is (re-)usable across actors. ITxPT’s standardisation of formats for public transport data could become the standard to be used within the EU. In terms of passenger counting this is probably uncontroversial since the major public transport stakeholders, and thereby default standard setters, on the harmonised market are members of ITxPT. For battery data we expect that the major trendsetters within electrification will define the standards and that ITxPT will reuse them for the purpose of public transport.

The analysis of each case can be influenced by further developments of the AI and Data Acts and/or new interpretations of GDPR in relation to edge computing. The analysis will almost certainly evolve as more aspects of the acts and the context are taken into account. And in this context “evolve” refers to anything between gradual increments to becoming obsolete. This is also in line with our intentions as we aim to initiate a discussion on the implications of the digital decade on public and private actors as new legislation will form tomorrow’s markets and innovation, not foresee the future with absolute accuracy.
References


This report explores how upcoming EU legislation will impact existing business models for data utilisation.

The ambition is, to start a discussion on the impact of new legislation, not perform a formal investigation.