REPORT

The New Hanse: Data sharing between public and private actors in the public interest

A first legal assessment toward a legal blueprint

RA Prof. Dr. Max von Grafenstein LL.M.

October 2023

THE NEW INSTITUTE

Introduction by Francesca Bria,
President Italian Innovation Fund and Programme Director The New Hanse

In today's rapidly transforming economy and society, data has become the meta-utility with the potential to revolutionize how we work, live, and travel. Nowhere is this more evident than in cities, where a multitude of digital devices and sensors generate an abundance of data, encompassing almost every aspect of urban life. Despite this data treasure trove, its potential for public good has remained largely untapped, primarily due to data residing in private silos and scarce fair private-public sharing arrangements. This is problematic since data is a key element to creating more democratic and sustainable futures. Therefore, there needs to be a better understanding and, more importantly, a better framework for governing and sharing data in the public interest – and blueprints for how private-public data sharing can work.

Addressing this issue, The New Hanse investigates and tests next-generation data sharing agreements and governance models that facilitate Business-to-Government-to-Society (B2G2S) data sharing, which means the sharing of data between the private, public and third sectors at the city level. At the core of this initiative is the Urban Data Challenge Hamburg, facilitating the exchange of private and public micromobility data to drive green and sustainable innovation and enhance urban planning for the benefit of citizens. This experiment allows us to draw conclusions from hands-on testing to achieve the desired objective of data sharing for the public interest.

The challenge also serves as a practical experiment to explore and resolve the major policy, legal and technical building blocks needed for safe, secure, and responsible urban data sharing that can be adapted, replicated, and shared amongst other European cities, such as:

- What role should the city play in fostering private-public data sharing arrangements? Should the city be in the driving seat, by legally mandating data sharing for the public interest? Should the city act as facilitator, neutral data intermediary or provider of digital public infrastructures and financial investment?
- How can we navigate the intricate landscape of local, federal, and EU laws and regulations to strike a balance between protecting individual rights and promoting data sharing for collective urban development? How do the piloted approaches relate to the data regulation underway at the EU level, especially in the area of B2G (Business-to-Government)?
- In pursuing data sharing in the public interest, what regulations, legal and technical tools, and incentives can be harnessed to

encourage private entities to participate actively and contribute their data for the public interest?

We have asked legal scholar Max von Grafenstein of the Einstein Center Digital Future and the Alexander von Humboldt Institute for Internet and Society to delve into these questions with a specific view on implications for the City of Hamburg, and other European cities. We have commissioned a preliminary legal assessment by taking an interdisciplinary data governance perspective. This report "The New Hanse: Data Sharing between public and private actors in the public interest", that was finalized end of 2022, outlines the intricate and ever-evolving landscape of privacy and business protection laws, local laws (such as the Hamburg Transparency Act or the Berlin Mobility Act), Member States laws (such as the German Federal Passengers Transportation Act), and EU laws (such as such as the EU Data Act).

At the heart of the argument presented, lies the need for the city to strategically design its data governance model making use of various data sharing rights and mechanisms (both voluntary and mandatory) to amplify the public value of data sharing. Furthermore, the report suggests the establishment of an independent data sharing intermediary to facilitate and monitor data sharing at the technical, organizational, and regulatory levels. Such an intermediary mitigates compliance risks, negotiates conflicts of interest, and trust issues, providing the essential structures for successful data sharing in the public interest. Setting up an **independent data intermediary for the public interest** will give citizens and cities more democratic control over their data, through the right to decide what uses of the information collected are legitimate, or under what circumstances it is produced and for what purposes. This way, data sharing can facilitate further innovation, better urban services, while guaranteeing the protection of data rights of citizens and a more dynamic and competitive digital ecosystem.

“An intermediary that is independent of the City of Hamburg might be a more suitable choice [than the City in the role of an intermediary itself], not only because it is trustworthy from the point of view of all parties involved due to its independence, but above all because it seems to have the better organizational capabilities to install and operate the necessary structures and procedures in a scalable and, therefore, cost-effective manner,” argues Max von Grafenstein.

This idea of an independent data intermediary has found resonance in the ongoing work of the Data Commons Working Group, composed of renowned international data and digital experts. It is set to become a cornerstone of the forthcoming blueprints for data sharing for the public interest, that is the main output of the New Hanse project.

In the meantime, this report provides you with valuable insights into the role of an independent data intermediary, its relationship with local, federal, and EU laws, and the ways in which it can effectively surmount key obstacles to data sharing for the public interest in Hamburg and beyond.

Data, when democratically controlled, can enable cities and Europe to transform its economy and society for the better. In the context of the twin digital and ecological transition, a form of democratic data governance that enables cities to put data and digital infrastructure at the service of citizens to tackle the great challenges of our time, is more urgent than ever.

1. Starting point: How to make data governance work?

Debates around data governance and data sharing for the public interest are largely focused on data sharing frameworks, models and structures, but practical applications, let alone institutionalized sharing arrangements, are rare. While various papers on different models exist, none provides a tested, proven and easy-to-use approach for the sharing of data between the private, public and third sectors at the city level. The New Hanse, an initiative of Hamburg-based The New Institute, was launched in 2021 to fill this gap by aiming to generate and test an urban data sharing blueprint that outline the major 1) legal, 2) policy and 3) technological building blocks needed for safe, secure and responsible urban data sharing that can be adapted, replicated and shared amongst other European cities.[1]

1.1 The Urban Data Challenge: Exchange of micromobility data between private and public bodies to improve urban planning

To this aim, the New Institute has partnered with the City of Hamburg represented in the overall cooperation and program by the head of the Senate Chancellery (SK), State Secretary Jan Pörksen, and Hamburg's Chief Digital Officer, Christian Pfromm. Further involved FHH institutions are the Department for IT and Digitalization (ITD), the Ministry of Transport and Mobility Transition (BVM) and the Agency for Geoinformation and Surveying (LGV). with its Urban Data Platform (UDP). With this cooperation, the New Institute aims at developing, testing and refining a data sharing arrangement that facilitates access to micro-mobility data held by private companies, while setting up a shared governance framework. This will be achieved by opening up challenges of the administration to the public in the form of a data innovation challenge in a sandboxed experiment ("Urban Data Challenge Hamburg"), allowing one to draw conclusions from experimentation to achieve the desired objective of data sharing for the public interest.[2] The goal of the Urban Data Challenge is to solve a concrete mobility challenge for the city, involving private companies in the solution process, by using floating bike data (from the city and companies) and other micro-mobility data sources to improve urban planning and subsequently micromobility (management, policy and regulation) in the city of Hamburg.[3]
A concrete starting point for this is data from E-Scooter providers that are collected when end customers use their services. According to the model contract that the city of Hamburg (Freie und Hansestadt Hamburg, i.e. FHH) drafted for the

[1] See the following considerations as well as the description of the pilot case in the CONCEPT BRIEFING SEP 2022 – DATA COMMONS WORKING GROUP as well as in further TNI documents being cited in the following text.
[2] Ibid.
[3] Urban Data Challenge Hamburg – Bike and Micro Mobility, p. 1.

cooperation with Hamburg-based E-Scooter providers, the "FHH intends to use the provider data to be provided for the following internal evaluations, among others: Number of vehicles offered (per day, average per day, total vehicles used), total number of all trips, (...), locations with the most or fewest rental transactions, locations where the rental process was terminated most frequently, start and destination coordinates of all rental operations, (...). In order to enable an evaluation of the data in almost real time, changes in the status of the vehicles and new events (e.g. journeys) are to be made available via the API within one minute. The provider agrees to transmit anonymized usage data to FHH for the purpose of monitoring and statistical analysis, as well as to cooperate in surveys of its own customers on mobility behaviour by FHH."[4] In detail, however, it is still unclear which data will be processed, how and by whom (e.g., aggregated, normalized, pseudonymised, anonymized) and returned to the city and ultimately to citizens (while balancing conflicting interests, such as data protection and business freedom).[5]

1.2 Elaborating on a working data governance-model

In particular, it is unclear which role the FHH should optimally assume within the framework of the data governance model to be defined: as data contributor, data recipient, data intermediary, or all three roles simultaneously?

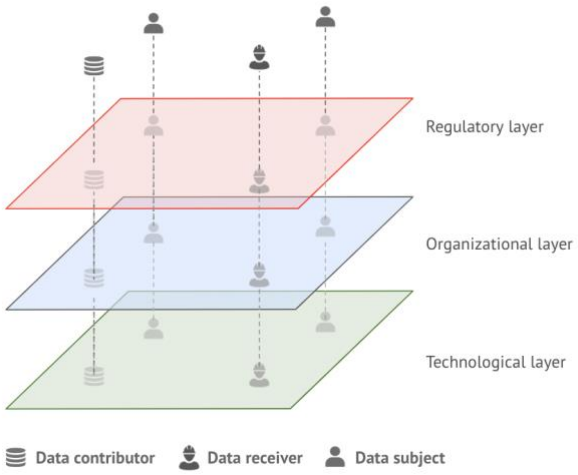
1.2.1 Terminology: Data governance layers and roles

To better understand this question, it is necessary to briefly clarify three analytical layers of data governance on which the actors in their different roles may act as well as the terminology used for this (see also the illustration below and in more detail in the conclusion as well as the referenced HIIG Discussion Paper – also keep in mind that the various laws addressed here typically each use their own, though similar, terminology):[6]

At the regulatory level, it is determined which actors have access to which data for which purposes and under which (technical and organizational) conditions. In the EU, this is increasingly being done by the legislator and, accordingly, by the regulation addressees who have to interpret and apply these laws. In addition to these legal regulations, however, these decisions can also be made on the basis of

[4] Agreement between E-Tretroller Provider and FHH, p. 5.
[5] Cf. the proposed questions to be addressed through the Urban Data Challenge, Urban Data Challenge Hamburg – Bike and Micro Mobility, p. 4.
[6] Cf. the definitions in the Executive summary: Hamburg B2G Data Sharing for the Public Interest, pp. 4 and 5, which are slightly adopted according to the data governance framework (including the pictures) proposed by v. Grafenstein to highlight further differences in the data governance solutions, see M. v. Grafenstein (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735.

purely economic or cultural considerations. To understand the effects of these regulations, it is important not to look at the law as an isolated phenomenon, but to consider its interaction with the other decision-making mechanisms. In contrast, the organisational layer consists of the structures, processes and practices that implement the regulatory decisions. Finally, the technological layer is determined by its architectural design consisting of the software and hardware infrastructure for processing the data. Since the legal, organisational and technological aspects are interdependent, these must also not be considered in isolation from each other, but rather their interaction must be respected. Thus, even though this assessment focuses on the legal issues, it will always consider the interplay with the other data governance levels as well.



Stakeholders interested in data act with different focuses on the aforementioned data governance layers. For the following analysis, this assessment distinguishes between the following roles: “Data contributor” describes an entity that provides data under its de facto control and has the right to do so, so the data can be used by others following pre-agreed rules. In general, a data contributor can also determine which quality of data it discloses to third parties (e.g., speed, volume, aggregation, obfuscation, pseudonymisation, and so on). A sub-category of a data contributor is a “data holder”, which is an entity having de facto control over its data while not granting access to it. A “data recipient” means an entity that receives data that does not belong to it, and that is able to use the data under well-defined conditions agreed with the data contributor. Further, a data processor means an entity that technically processes data on behalf of the data contributor and/or the data recipient (but not for their own purposes). Altogether, these entities are sometimes also called “data users”. Last but not least, a data intermediary is an entity that focuses on facilitating the sharing of data between data contributors and recipients on the technological, organisational and/or regulatory data governance layer. A data intermediary may exclusively act on behalf of the data contributors and data recipients (cf. the data intermediation services under Art. 10 et seq. Data Governance Act),[7] and can include the technological layer

[7] In the present context, the term "data intermediary" is used as a generic term, which in principle includes both the use of data exclusively for third-party purposes and for the data intermediary’s own purposes; see, in contrast, L. Specht-Riemenschneider and W. Kerber, who distinguish between a "data fiduciary" (Datentreuhänder) who acts only for third-party purposes and a data intermediary who acts for its own purposes, L. Specht-Riemenschneider and W. Kerber, Designing Data Trustees – A Purpose-Based Approach, p. 8; see in detail the discussion on the functions of data intermediaries going back to the 70s, Jörg Pohle (2022). Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. Vortrag 5 der Reihe „Zu treuen Händen“ | Februar 2022. Eine

(acting as a processor), but may also focus its support on the organisational-legal layer deciding on who gets access to which data under which conditions, and controlling that all parties involved adhere to these terms (cf. the monitoring and certification bodies under Art. 40 et seq. GDPR). Last but not least, a "data subject" is a person whose data is processed without being a data holder (which might instead be the provider of an Internet of Things-device that the data subject is using) and/or whom the use of the data is affecting in one or another way.

2.1.2 Challenges arising from voluntary and mandatory sharing

Against this background, one particular challenge that public authorities are increasingly facing in practice is that they have to organize access to and use of data in a complex structure of often conflicting legal requirements. Where no statutory data access rights exist yet, the public sector basically has to decide whether to organize access to data on a voluntary basis via incentives or whether it is better to organize data access via the establishment of new mandatory laws. Here, a first challenge arises from the interplay of voluntary and obligatory sharing approaches. This is because whenever an actor is required to share certain data by law, it loses the ability vis-à-vis another actor to exchange that data for other data held by the other actor that does not fall within the scope of this law. To anticipate all conflicts resulting from such gaps and resolve them in laws, legislators would therefore need the necessary detailed knowledge of the respective context. However, because of their central and overarching position in society, legislators often do not have sufficiently detailed knowledge of every social and economic context. Despite extensive consultation with stakeholders, laws might therefore risk failing to have the desired effect because they do not sufficiently take into account the context-specific conditions and logics of the actors involved in such a context.[8] For example, requiring data holders to share certain data for no additional compensation generally deprives data holders of the ability to negotiate such compensation themselves.

Thus, if a data holder is not interested in the same type of data as the data that it has to publish itself, but in completely different data, this data holder can no longer negotiate this other data as compensation for disclosing its own data. An example

---

Online-Vortragsreihe der Verbraucherzentrale NRW e. V. mit Unterstützung durch das Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg.

[8] See M. Eifert, Regulierungsstrategien, in: Wolfgang Hoffmann-Riem / Eberhard Schmidt-
Aßmann / Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", 2nd edition, München: C.H. Beck, 2022, § 19, cip. 1 and 2, especially, cip. 59; cf. also W. Hoffmann-Riem, Innovationsoffenheit und Innovationsverantwortung durch Recht – Aufgaben rechtswissenschaftlicher Innovationsforschung, in: Archiv des öffentlichen Rechts 131 (2) (2006), pp. 255–277.

for this regulatory challenge are current Open Data laws: In principle, public bodies could make the sharing of their data with private companies dependent on the fact that private companies in turn release their data. However, this is only possible to a limited extent due to current Open Data laws. Open Data laws usually oblige public authorities as well as private companies that offer a public service and are under the control of a public authority to make their data freely available without conditions. This boundary should not be underestimated: One example where this becomes relevant is Mobility as a service-platforms (MaaS-platforms), which typically bundle the offering of different types of public and private transport services in one mobile app. Such platforms enable the collection and aggregation of valuable data for, among other things, the transformation towards a climate-neutral transportation system in a city or certain region. The main incentive for private mobility providers to join these platforms and share their data is the participation of other key operators who provide data about essential means via the platform (which is typically public transportation).[9] This mechanism of reciprocal data sharing does not work as an incentive for private providers if the other providers, such as public transportation providers, are required to publish or share their data anyway due to Open Data laws.

An important question, therefore, is whether a data governance model could be designed in such a way that a public body, such as the FHH, seeking to install, and eventually operate, a platform for data sharing, does not lose this incentive mechanism vis-à-vis private companies. This would require a mechanism to ensure that the public bodies still organise access to as much data as possible, avoiding closed data clubs that limit "democratic access" to this data.[10]

1.2.3 Challenges arising from conflicting protection laws

Another challenge arises from the fact that in both cases, in voluntary and obligatory sharing cases, various conflicting protection laws must be respected, first and foremost data protection and trade secrets. Compliance with these protection laws usually involves so much legal uncertainty and expense that voluntary sharing hardly seems worthwhile and even statutory claims threaten to run dry. If, for example, a government actor wants to tangibly facilitate data sharing in practice, it must establish, or at least support the establishment of, mechanisms that enable or facilitate compliance with those conflicting protection laws. The present assessment will address this challenge with a focus on the current legal situation, but also on draft legislation under discussion.

[9] B. Carballa Smichowski (2018). Determinants of coopetition through data sharing in MaaS. Management et Datascience, 2 (3). https://doi.org/10.36863/mds.a.4160.
[10] Cf. Executive summary: Hamburg B2G Data Sharing for the Public Interest, p. 4.

1.3 Questions to be addressed in the present legal assessment

Against this backdrop, the TNI asked for a legal assessment of the following questions:

- To what extent are the provisions of the Hamburg Transparency Act compatible with the role of the City of Hamburg itself as a data contributor, recipient and/or intermediary, if the governance rules would provide for "preferential access" regulations between the parties organized in the pool, e.g. within a "data pool", or are only general Open Data solutions legally compliant? What other approaches could be proposed?
- How do the piloted approaches relate to the data regulation underway at the EU level, especially in the area of B2G? Could the project help to define data governance in the public interest – especially with regard to the different data roles and data usage perspectives involved? Similar questions arise in the area of national data laws: What insights can be expected? What developments need to be taken into account (e.g. Mobilithek etc.)?
- What instruments are available to the city of Hamburg in the future (legal, organizational and/or technical) to create incentives for data sharing? How can the measures necessary for fair data sharing be refinanced (as an exemplary list of pro and con arguments)?

To answer these questions, the present document provides **a preliminary legal assessment by taking an interdisciplinary data governance perspective**, which means not simply looking at law as an isolated phenomenon but to take its interplay, in particular, with the other data governance layers into account: The regulatory, organisational and technological layer. On this preliminary basis, it should be possible to draw initial fundamental conclusions for the design of the data governance model. The outline thus aims to serve as an initial basis for the following negotiation, evaluation and specification processes of the project. In the course of this process, it will be necessary to determine, among other things, which data should or can be *specifically* exchanged by which actors under considerations of which protection measures. At the same time, the model should be flexible enough to cover a wide range of data sharing situations. Due to the complexity of the problems and possible approaches to solving them, it is likely that further unidentified challenges will emerge in the implementation process.

2. Open data, data protection, business secrets: Managing compliance risks, legal liability and costs

Keeping the above mentioned restrictions in mind, this assessment comes to the preliminary conclusion that the FHH must not publish or share, according to the Hamburg Transparency Act, data that the city processes or manages solely on behalf of private parties. However, the city should not itself take on the role of an intermediary, enabling and monitoring, on a legal and organizational data governance layer, the exchange of data between data providers and data recipients. This function should rather be taken by an independent intermediary, which is able to manage (and, in the best case, take over) the compliance risks in a scalable way. Though, FHH may participate in the data exchange as data contributor and data recipient. The FHH may also support the data sharing under certain conditions as a purely technical service provider with its Urban Data Platform. For this, the systems on which the FHH relies in its roles as technical service provider on the one hand and as data contributor or data recipient on the other hand would have to be sufficiently logically separated.

2.1 Managing data of the city: Hamburg Transparency Act (G2All – Hamburger Transparenzgesetz)

Whether the FHH is subject to an obligation to publish or share information received in the context of the Urban Data Challenge under the provisions of the Hamburg Transparency Act essentially depends on three questions: First, whether FHH is a "public body" in the meaning of the Hamburg Transparency Act; second, whether the data in question is "official information available" at this body; and third, what type of data are present, which especially means whether the data are subject to certain protection laws such as for data protection or business secret protection.

2.1.1 (Un)Available “official” information at FHH or other public bodies

An obligation to publish or share information exists only to the extent that the information is available at public bodies (§ 1 sect. 1). In principle, all authorities of the FHH as well as legal persons under public law subordinate to FHH are obliged to publish or share their information (§ 2 sect. 3 sent. 1 in conjunction with § 1 HmbVwVfG). In addition, natural persons and legal entities under private law are also obliged to publish or share their information if they perform public tasks or public services and are subject to the control of the FHH (§ 2 sect. 3 sent. 2 in conjunction with sect. 4). Such control exists if they

- are subject to special obligations vis-à-vis third parties in the performance of the public task or service; or have special rights, in particular a

contracting obligation or a connection and use obligation exists (sect. 4 no. 1)
- or hold a majority of the subscribed capital or voting rights of the enterprise (subsection 4 No. 2 lit. a and b)
- or can appoint more than half of the members of the administrative, management or supervisory body of the enterprise (sect. 4 no. 2 lit. c).

Furthermore, the information must be "official" and "available" at such a body in order to trigger the duty to publish or share that information. For this, it will be necessary to assume that the body may use the data for its own purposes (which may also be defined by law). To the contrary, it is not sufficient if the body only has technical access to the data and only uses the data on behalf of a third party (i.e., the actual data holder). This results from § 1 sect. 2 Hamburg Transparency Act, according to which the publishing and sharing duties only relate to "official information available" at the body. To consider information as "official", the body must collect, store or process data for the fulfilment of an own governmental task.[11] In contrast, if an authority processes data exclusively on behalf of another entity, this does not occur for a governmental task of the processing authority. Rather, one has to look at the legal situation of the commissioning entity. If one is of the opposite opinion, this would actually conflict with further legal concepts, too. For example, it would conflict with the principle "pacta sunt servanda" (i.e. that contractual agreements must be complied with).
This principle applies at least as long as such a contractual agreement does not constitute an act of circumventing a legal obligation. However, as long as there is no legal basis for the original collection and processing of data, it cannot be circumvented by contractual agreements. The Transparency Act does not provide such a legal basis, because it itself presupposes such a basis (by referring to "official" information). Last but not least, the opposite opinion would also conflict with the legal concept of the "processor" in data protection law (Art. 4 No. 8 GDPR), which also presupposes the possibility that an entity processes data exclusively for the purposes of another person (and therefore has a significantly weakened legal responsibility, Art. 28 GDPR).

In conclusion, the FHH is obliged to publish or share information as soon as it receives the information and is not bound by a contractual relationship to the purposes of the actual data holders, i.e. may use the information for its own public tasks. If, in contrast, the FHH or one of its authorities (for example, the LGV as operator of the Urban Data Platform) acts only as a technical service provider and, as such, processes the data exclusively for the specified purposes of the actual data holder, **the present assessment comes to the conclusion that there is no obligation to publish or share the information of the FHH (LGV) according to the Hamburg Transparency Act.** Since, according to current planning, the city in its potential

[11] C. Schnabel in A. Maatsch and C. Schnabel (2021). Das Hamburgische Transparenzgesetz. § 2 cip. 8.

function as processor may use the data exclusively for the purposes of the data contributors and recipients (and may not anonymize the data to use it for its own purposes), no publication or sharing duty arises in this respect.

Edge cases may arise if the FHH takes on the role of a data intermediary or brings in an "independent" data intermediary. As shown before, also a person under private law, which takes on the role of an intermediary, becomes subject to the duty to publish or share information if its intermediation services are seen as a public task and the private body is subject to the control of FHH. This is the case, if FHH holds the majority of the capital or voting rights or can provide more than half of the members of the administrative, management or supervisory body (sect. 4 no. 2 lit. a and b). Such a control may also exist if the private intermediary is subject to a contracting obligation (sect. 4 no. 2 lit. c). Such a contracting obligation could, for example, be seen in an obligation of the intermediary to connect all interested data contributors and data recipients to its system, provided that they comply with certain conditions (e.g. on data or business secret protection). Here, it will be necessary to investigate further to what extent this is a purely self-imposed obligation on the part of the intermediary or whether such an obligation is not at least indirectly enforced by the FHH, for example, if the city provides financial support to the intermediary dependent on such a contracting obligation. In the present case, such financial support is obvious, since according to current planning, at least the data contributors are not to pay a fee to the intermediary. If this also applies to data recipients, there is no alternative but for the city to take on the financing. In conclusion, the question is to what extent such an intermediary is actually "independent" (which means here not only legally but also financially independent from the FHH).

A second edge case may arise with the question of when an intermediary exceeds the leeway given to it in the management and control of the data, so that it makes decisions according to its own (i.e. self-set) purposes. Only if the intermediary exceeds the margin that the data contributors and recipients have given with their purposes, the data can be seen as "available official information" to the intermediary, so that a duty to publish or share the information may arise for the intermediary. (Thus, even if a private intermediary were not "independent" but under the control of FHH, for example due to a contracting obligation – see previous paragraph – a publishing or sharing obligation would only exist if the intermediary also processes or manages the data for its own purposes). However, a problem arises due to the limited knowledge available to the data contributors and data recipients when they give their instructions to the intermediary. This is because such instructions only extend to the processing purposes that are known and specified at the time of the instruction. The more unknown purposes these instructions cover or the more generally these instructive purposes are formulated, the more likely it is that the question arises as to whether the intermediary exceeds the legally permissible leeway in the subsequent actual control and thus also pursues its own purposes after all and thus the Hamburg Transparency Act comes into play. (Insofar as it is primarily a matter of avoiding the application of the

Hamburg Transparency Act, this situation also speaks in favour of an intermediary independent of the FHH taking on this control.) In addition to the question of the impact of such discretion on the applicability of the Hamburg Transparency Act, there is of course the additional question of when processing purposes are formulated too vaguely so that they are no longer compatible with data protection law.[12] This question will also have to be clarified further in the course of the implementation process.

2.1.2 Data that (is protected and) must (not) be shared by a public body

Only if the FHH is seen as a „body" in the meaning of the Transparency Act and the data in question is "official information available" at this body, it is necessary to examine which specific types of data are concretely at hand. Doing so, the Hamburg Transparency Act differentiates between an obligation to publish and an obligation to share the information. The publication duty means that certain information must be "actively (...) entered into a central, electronic and publicly available information register" (§ 3 sect. 4 n. 8, § 2 sect. 6). In contrast, the duty to share information means that "information must be made available upon request" of another party (§ 3 sect. 4 n. 7). Types of data that are subject to the active publication duty are enumerated exhaustively in the Transparency Act. All other information is at least subject to the duty to share (§ 3 sect. 3). Fees or reimbursement of costs for sharing data are charged to the requesting applicant according to special provisions (§ 13 sect. 6). This could open up the possibility for the city to set special fees for particularly extensive data uses, for example.

The types of data listed in the Transparency Act for which there is an active publication duty could include, in particular, geodata (§ 3 No. 9). However, personal geodata are excluded from this, as a special provision exists for this type of data (§ 4 sect. 1 no. 3). According to this special provision, **personal geodata (i.e. information about the location of natural persons) must only be actively entered into the information register if this is permitted under applicable data protection law**. **After a cursory examination of data protection law, no such provision is**

[12] See for example the discussion whether bringing in intermediaries is incompatible with data protection law due to a too vague purpose specification at O. Stiemerling, S. Weiß, C. Wendehorst. Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG – Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, pp. 42 et seq.; in fact, however, this is a question that depends on the concrete data protection law requirements for the purpose specification and can be solved both conceptually and in practice, cf. M. v. Grafenstein. Grafenstein, M. v. (2020). Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I. European Data Protection Law Review, 6(4), 509-521. DOI: 10.21552/edpl/2020/4/7; ibid. Part II. European Data Protection Law Review, 7(2), 190-205. DOI: 10.21552/edpl/2021/2/8; ibid. part III. European Data Protection Law Review, 7(3), 373-387. DOI: 10.21552/edpl/2021/3/6 (all available as open access).

apparently applicable to micromobility data in the present case; in particular, the provision in Article 6 (1) (f) of the GDPR ("legitimate interests") is not likely to be relevant because the data protection risks of publishing personal geodata regularly outweigh the general information interest of the public in that kind of data.[13] The possibility of minimizing the relation of the data to the data subjects, which does not yet reach the level of complete anonymization, is not considered to this extent (see point 2.1.3 below). Besides, completely anonymized geodata are not subject to data protection law and could therefore be published (for the difficulty of anonymizing personal geodata, see section 2.2.1 below). Personal geodata thus only have to be published – just like all other personal data – if the data subjects have consented to the publication of their personal data (§ 4 sect. 1 no. 6).

In addition to the active publishing duty, there may also be a sharing duty. Here, too, this is generally the case if the data subject has consented (§ 4 sect. 1 no. 3). If such consent is not available, the public body required to share the information must attempt to obtain the consent from the data subject at the request of the applicant (§ 12 sect. 7). Irrespective of the consent, the information must also be provided if it is "necessary to avert considerable disadvantages for the general welfare or dangers to life, health, personal freedom or other serious impairments of the rights of individuals" (§ 4 sect. 3 no. 2). In the present case, this is not readily apparent. A right to share the information is more likely in the event that "there is a legitimate interest in the information and there are no overriding interests worthy of protection that conflict with sharing the information" (§ 4 sect. 3 no. 4). In any case, the data subject must be informed about the sharing request regarding her personal data and given the opportunity to comment; upon request by the data subject, the name of the applicant must also be disclosed (§ 4 sect. 5).

In addition to personal data, the use of data containing trade and business secrets is also likely in the pilot case. According to the Hamburg Transparency Act, trade and business secrets are all facts, circumstances and processes relating to a company which are not in the public domain but are only accessible to a limited group of people and the legal entity has a legitimate interest in the non-disclosure (§ 7 sect. 1 sent. 1). The law assumes that there is a legitimate interest in the non-disclosure if the disclosure of a fact is likely to either a) promote the competitive position of a competitor or b) diminish the competitive position of the company's own business or c) if it is likely to cause economic damage to the holder of the trade secret. With criteria a) and b) in particular, the law appears to also protect the so-called "negative interest" of the company concerned, according to which a trade secret does not need to have a specific asset value, but it is sufficient that it "may have an adverse effect on the company if third parties, in particular competitors, gain

[13] See, for instance, European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, pp. 5 and 6, moreover, only private entities can invoke Art. 6 sect. 1 lit. f GDPR, whereas public entities cannot invoke this legal basis.

knowledge of the data."[14] However, trade and business secrets are only subject to the duty to publish or share the data if the interest of the general public in the publication or of an applicant for sharing the information) outweighs the interest in keeping the trade secret. As a general rule, since the publication of trade secrets generally interferes more deeply with the interests of the owner of the secret than does data sharing (especially if the data is not shared with competitors but other less problematic entities), data sharing will be possible more often than its publication. In any case, the company concerned must be given the opportunity to state their views before publication or before sharing the data; if the data shall be shared, the name of the applicant must be disclosed to the company concerned upon its request (§ 7 sect. 4).

In addition to the exceptions for personal data and trade and business secrets, there may be further exceptions to the duty to inform. In the present case, such an obligation could, for example, be exempted for research data in the case of basic research or application-related research (§ 5 no. 7).

2.1.3 Voluntary publication of protected data (Data Governance Act)?

If the FHH processes its own data (i.e. for its own – i.e. legally defined – purposes or at least public tasks), in principle, this data is subject to an obligation to publish or share it under the Hamburg Transparency Act. In this case, the disclosure cannot be made dependent on a return service, such as the disclosure of the interested data recipient's own data.

An exception to this could be in the case of protected data, such as personal data and trade secrets. This can be the case if an Open Data law categorically excludes such protected data from its scope, and an entity that is basically covered by the Open Data law would, however, find a way to share the data in a manner that complies with data protection law or trade secrets law. An example would be that an entity does not fully anonymize the data (because then data protection law would not apply, which in turn would lead to the application of the Open Data Act), but implements complementary protection measures so that the data could be shared in a manner that complies with data protection law. Since in such cases there would be no obligation to publish or share the data under the Open Data Act, one could make the disclosure of such data conditional on the counter-disclosure of the interested data recipient's own data.

According to this preliminary assessment, however, it is unclear whether such a solution would work under the Hamburg Transparency Act. The reason for this is that **the Hamburg Transparency Act does not categorically exclude personal data and trade secrets from its scope of application, but rather makes a claim to share**

[14] Goldhammer, Geschäftsgeheimnis-Richtlinie und Informationsfreiheit, NVwZ 2017, 1809, 1812, referring to BGH GRUR 2006, 1044.

such data dependent to the condition that the interests of a data receiver in accessing the data are higher than the interests of the data subject in not sharing the data. This balancing rule is, actually, identical to the processing permission from Art. 6 sect. 1 lit f GDPR ("legitimate interests"). This comparison is interesting for the scope of the data sharing obligations of the Hamburg Transparency Act because **the data controller is allowed under Art. 6 sect. 1 lit. f GDPR to have the balance turn out in its favour by reducing the processing risks for the data subjects (meaning the data subjects' interests in not processing the data) through appropriate protection measures**.[15]
The question is hence whether the Hamburg Transparency Act operates according to the same mechanism: Does an interested data recipient obtain a data sharing right in the moment an authority implements protection measures up to a point where the risks for the data subject no longer outweigh the interests of the data receiver in accessing the data? Just to clarify: The interested data recipient is certainly not entitled to demand that the authority implement these measures to weigh the pros and cons in its favour. But if the authority implements these measures voluntarily, does the sharing right automatically apply? What speaks in favour of this is that the Hamburg Transparency Act simply focuses on the result of the weighing. How the result comes about is not relevant according to this law.

However, there are also alternative regulatory approaches. For example, Chapter 2 of the Data Governance Act-draft (DGA-draft) provides harmonized rules for the publication of protected data (especially personal data and trade secrets). According to the legislator, Chapter 2 DGA-draft complements the Public Sector Information Directive II (PSI II), which obliges the EU Member States to ensure the re-use of public sector information for commercial and non-commercial purposes, except this data is protected (e.g. by data protection or trade secret protection, Art. 1 sect. 1 to 3 and Art. 3 sect. 1). Particularly relevant to the present pilot is that the regulations in Chapter 2 DGA-draft do not establish a right to share or even publish such data. Rather, **the regulations of the DGA-Draft only provide a harmonized framework under which public entities may publish protected data if they choose (only *if* they do, they must apply these standards). The DGA-draft thus leaves open the possibility for public authorities to impose conditions on the use of the protected data provided. Indeed, these conditions must be non-discriminatory, proportionate and objectively justified with regard to the categories of data and purposes of re-use and the nature of the data for which re-use is allowed; in particular they must not grant exclusive rights or otherwise serve to impede competition (Art. 4 and 5 sect. 2 DGA-draft). However, reciprocity agreements, whereby a party requesting access to another party's data is obliged to make its own data available in return, may often be the very thing that establishes a level playing field for fair competition.** According to the view expressed here, this may apply at least to private actors, such as public transport companies, which provide services of

[15] EDPB, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (844/14/EN WP 217), pp. 42 et seq.

general interest and are subject to the control of the public municipality (see above under point 2.1.1). If such providers are forced by Open Data laws to make their data publicly available without getting access to the same data of their private competitors in return, this may be the real obstacle to fair competition. The legislator of the Hamburg Transparency Act might therefore consider following the option taken by the EU legislator to (more clearly) exclude protected data from the scope of application in such a way that their release can be made subject to conditions (supposed that this leads, in the end, to more data shared – see for such mechanisms below under point 3.3.3). Of course, such ideas are only obvious if the respective entities or data are subject to the data sharing obligation at all (see above under point 2.1.1 and 2.1.2).

In any case, such conditions for data access are important not only with regard to the aforementioned reciprocity agreements. It is also important to clarify that**, according to the DGA-draft, when accessing protected data, not only can the data be pre-processed to different degrees (for example, anonymised or pseudonymised), but also different conditions can be imposed on the context of access (Art. 5 sect. 3 and 4): from remote access (to "normal" protected data) in the context of a secure processing environment to on-site access (to particularly sensitive protected data) within the physical premises of the entity where the data exists. This in itself should actually be self-evident, but it makes the approach prominent that these technical, organizational and legal safeguards must be applied in combination and, above all, depending on the nature of the data and the purposes for which it is used.**[16] This is important in the present case because many Open Data laws, including to some extent the Hamburg Transparency Act, assume a simplistic approach according to which protected data can be published. For example, the Hamburg Transparency Act seems to assume that personal data could simply be "obscured" (in practice, "blacked out") for publication (§ 4 sect. 1 sent. 1 and § 7 sect. 3 sent. 3). This procedure does not fully do justice to the complexity of data protection, but also of trade secret protection. In practice, this process often leads to much information not being published because its relation to natural persons or the trade secret only arises from the relationship between different pieces of information and/or its specific context. In such constellations, the relation to natural persons or trade secrets cannot simply be "blacked out". Rather, this requires a combination of the technical, organizational and legal methods mentioned in the DGA-draft if the data is not to be withdrawn from further use as a whole. This challenge will be briefly illustrated in a bit more detail in the following chapter.

[16] M. v. Grafenstein (2020), How to build data-driven innovation projects at large with data protection by design. HIIG Discussion Paper Series, 2020(3), 93, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606140, referring to M. Elliot, E. Mackey, K. O'Hara, C. Tudor (2016). The Anonymisation Decision-Making Framework. UK Anonymisation Network (meanwhile, there is the 2nd edition available under: M. Elliot, E. Mackey & K. O'Hara (2020). The Anonymisation Decision-Making Framework 2nd Edition: European Practitioners' Guide.)

2.2 Managing data of private contributors: Data protection and business secrets in light of data commons

Even if the Transparency Act does not come into play and there is no basic obligation to provide information, actors who wish to share such data inevitably face the question of how this is to be done in compliance with data protection and business secrecy protection.

2.2.1 The complexity of “personal data” and anonymisation in data protection law

The challenge with data protection law is that the scope of application is extremely broad and vague. The GDPR (Art. 2 sect. 1 in conjunction with Art. 4 No. 1) defines personal data as “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”. Recital 26 of the GDPR further explains how one can assess whether a person is identifiable or – in a reverse manner – not, which means how personal data might be anonymized: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." The mere possibility that individuals could be identified, at least by third parties (taking into account their possible additional knowledge), and the reference to "reasonably likely" means used, extends the scope of application extremely far. Because of the extremely broad scope, especially movement data can only be anonymized with great difficulty due to their multidimensional relations to natural persons. Entire branches of research have been dealing with the question of how to successfully anonymise movement data for years.[17]

However, it is important to note that **even if data *per se* do not relate to a person or if originally personal data have been successfully anonymized, a relation to a person may subsequently arise (again) solely on the basis for which purpose it is used or how it is used.** According to the European Data Protection Board, which has since been confirmed by the European Court of Justice, information also relates to

[17] EDPB, Guidelines 04 / 2020 on the use of location datatracing tools in the context of the COVID and contact 19 outbreak Adopted on 21 April 2020, pp. 5 and 6 with further references.

an individual when it is used to evaluate or treat her in a certain way ("purpose element").[18] For instance, certain weather conditions could be used to evaluate whether a person was driving at an appropriate speed on the road. Of course, weather conditions *per se* do not relate to an individual. However, this data used to evaluate an individual's behaviour makes them "personal data", so that the person concerned could assert her right to information and correction in the event of legal proceedings being brought against her. Such rights might indeed be important, especially, if this data (i.e. attributions to the data subject) should prove to be incorrect. Here, **technical anonymization procedures can hardly do anything. In such cases, it is much more a matter of organizational and legal controls to ensure that the data is used in a transparent and fair manner and that the individuals concerned, i.e. data subjects, have the opportunity to intervene if they have objections.** This applies all the more if personal data are used for purposes other than those originally intended (see Art. 5 sect. 1 lit.b) and Art. 6 sect. 4 GDPR). If the data cannot be completely anonymized because this would frustrate the intended use, not only technical procedures are required to minimize the personal reference as far as possible, but also organizational and legal procedures to ensure that the data are not misused. The difficulty in each case is to understand what constitutes "misuse" or "fairness" in a specific case by integrating legal, technical and organizational aspects, in order to avoid such misuse in the future, especially in the case of new purposes. The difficulties and, correspondingly, effort required for resolving these issues very often result in data not being shared in practice. This practical result is unfortunate, given that the sharing of data would actually be allowed.

2.2.2 Preventing breaches *and* proving proper use of business secrets

Trade secret protection is similarly complex. Here, at first, one has to distinguish between two different definitions: on the one hand, between trade secrets in the relationship between private parties and the public sector within the meaning of the Hamburg Transparency Act (see above under point 1.1.2) and trade secrets between private parties within the meaning of the EU Know How Directive.[19]

Insofar as the Hamburg Transparency Act does not apply because the data is only shared – potentially with the help of an independent intermediary – between private actors, the narrower protection of trade secrets comes into play. Between private actors, the Know How Directive presupposes for a trade secret that the information is a) secret, i.e. not known to anyone typically familiar with the nature of such information, and is b) for that very reason of commercial value to the

[18] See also the "result"-element at Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN, WP 136, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, pp. 10 and sequ.
[19] Directive 2016/943/EU, implemented in German law through the Geschäftsgeheimnisgesetz.

company concerned, as well as is c) subject to secrecy measures (Art. 2 No. 1 of Directive 2016/943/EU). This definition seems to exclude the **negative interest of the company, according to which any adverse effect on the company would be covered (see above under point 1.1.2), but only to cover its direct commercial interest, hence, its know-how, innovation, entrepreneurial performance and protection against economic free riders**.[20] This narrower definition of a trade secret appears to reduce the potential of legal conflicts compared to the broader definition (which includes any negative interest of the affected company), thereby reducing the need for the corresponding conflict resolution mechanisms.

However, this finding is put into perspective in practice if the data is to be shared voluntarily. This is because the likelihood that a data contributor will voluntarily share its data with private data recipients is higher, if it can ensure, in addition to the direct protection of its commercial interest to which it is entitled by law, the protection of its negative interest.

Interestingly, this interest is also taken into account (at least partially) by the Data Act-draft. Among other things, **the Data Act-draft provides for a sharing obligation between private parties for so-called usage data, i.e., data generated during the use of products or services (Art. 1 sect. 1 Data Act draft). The obligation is imposed on the provider of such a product or service as the so-called data holder. A data holder must share the data with its users and also with third parties if users request it or the third parties do so on their behalf (Art. 5 sect. 1 Data Act-draft).[21] Here, too, data protection law (Art. 1 sect. 3, Art. 4 sect. 5, and Art. 5 sect. 6 and 7) and business secrets must be respected**. As far as trade secrets are concerned, they must be shared only under the following conditions: First, if it is strictly necessary for the purpose of the agreement concluded between the user and the third party; second, if the third party has taken all the protection measures necessary for the protection of the trade secret, which the third party has agreed upon with the data holder (Art. 5 sect. 8); and third, neither the user nor the third party may use the data to develop a product that competes with the data holder's product (Art. 4 sect. 4 and Art. 6 sect. 2 lit. e).

So far, it is unclear how a data holder may prove that the data recipient has used or is still using the data for a competing product despite the ban. It stands to reason that this problem will be solved procedurally via a shift of the burden of proof: If the data holder finds out that the data recipient offers such a competing product on the market, proof of this fact will presumably suffice to substantiate evidence that the data has been or is going to be misused. Now the data recipient, for its part, must disprove the allegation to have misused or is misusing the data for this

[20] See M. Goldhammer, ibid.

[21] See also other existing sharing duties, such as under § 20 sect. 1 a GWB (German Act against Restraints of Competition), which grants a sharing right amongst competitors in the case one company has a need for the data that is controlled by a competitor and the competitor denies access even for a financial return.

product. If the data recipient fails to do so, the data holder can stop sharing the data and the receiver must delete the data it has already received and (!) destroy the competing product, Art. 11 sect. 2).

Thus, what applies to a legal data sharing obligation such as under the Data Act-draft applies at least as much to voluntary data sharing: **If data sharing is to work in practice, both the data holder (i.e., data contributor) and the data recipient need suitable and cost efficient procedures that prevent possible misuse and enable or facilitate proof of proper use.**

2.2.3 How to most effectively and efficiently cope with the risks and liability?

In conclusion, the challenge is to make as much data accessible and as comprehensively as possible, not in spite of data protection and business secret protection, but with it. This challenge is demanding because this requires integrating the different perspectives of the data contributor and data recipient regarding the benefits and risks of the data (or its use), legally, technically and organizationally. Moreover, since the benefits and risks may change with each new use case of the data, this must be done on an ongoing basis. To reach this aim, there is a need for appropriate technical, legal and organisational structures and procedures to be created and deployed.

On a technical level, the Urban Data Platform of the FHH can provide an important building block in this respect. On a legal level, the FHH obviously wants to provide a strong incentive for the providers to participate by taking over liability in its model agreement with the E-Scooter providers participating in the present pilot project (point 2 under "data & statistics" in the last rule): "*FHH is responsible for compliance with data protection regulations and ensures that the provider's data is not passed on to market participants. Furthermore, FHH will not publish any data that allows conclusions to be drawn about the business figures of individual providers.*" For sure, this incentive may work, as FHH intends to relieve the E-Scooter providers of the high level of legal uncertainty regarding the legally compliant processing of data. However, it is questionable whether such a liability transfer from the providers to the city is legally permissible at all (see, for example, Art. 42 sect. 4 GDPR). More important however is the question of whether the FHH can sufficiently control the liability risk so that this justifies the liability transfer.

Thus, within the framework of the applicable laws, **liability should lie where the appropriate structures and procedures are in place to best identify and resolve conflicts of interest in the data in question**. In the view expressed here, an intermediary that is independent of the FHH might be a more suitable choice, not only because it is trustworthy from the point of view of all parties involved due to its independence, but above all because it seems to have the better organizational capabilities to install and operate the necessary structures and procedures in a

scalable and therefore cost-effective manner. This is explored in more detail in the following chapter.

2.3 Conclusion on the role and functions of the FHH and an independent data intermediary

2.3.1 Urban Data Platform (LGV) as technical service (data processor)

In order to reduce the costs incurred by the parties involved in the technical instalment and operation of the conflict-resolving structures and procedures, it appears possible for the FHH to provide the technical structures via the LGV. This presupposes that the LGV processes the data exclusively as a technical service provider, i.e. for the purposes of the data contributor and data recipients. An obligation to provide information according to the Hamburg Transparency Act would not arise to this extent. It should be emphasized once again that this assessment is based only on a preliminary examination. One issue would be to clarify how centralized or decentralized the technical infrastructure is. The more centrally the data is stored, the higher the risk of misuse by the technical service provider or by third parties (who can access one big data set, while the original data holders lose their factual control).[22] Another related problem is that the city itself also feeds data into the system as a data contributor and uses data as a data recipient. To avoid possible conflicts of interest through the appropriate technical and organizational design, one would have to sufficiently logically separate the system of the LGV, through which the FHH processes the data exclusively as a service provider, from the system through which the FHH also processes the data for its own purposes. Whether the competent data protection agency (i.e. Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) shares this opinion and to what extent the proposed logical separation of the systems may be sufficient must be investigated and clarified with the data protection agency in the following steps of the project.

2.3.2 An independent data intermediary as legal person of private law

Furthermore, **it is conceivable that the FHH also provides the organizational structures and procedures that are necessary for the legal control of access to the**

[22] A. Blankertz and L. Specht (2021). What regulation for data trusts should look like. Stiftung Neue Verantwortung, p. 14; M. v. Grafenstein (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735, pp. 21 et seq., however, see also the opposite view on weaker IT security of de-dentralized structures at Günther et al (2017). Debating big data: A literature review on realizing value from big data. The Journal of Strategic Information Systems 26(3), 191–209 doi: 10.1016/j.jsis.2017.07.003, p. 197, with further references.

data and its use by the data recipients. According to this preliminary assessment, this would not give grounds for an information duty under the Hamburg Transparency Act, as long as this control is carried out solely within the instructive limits given by the data contributors and receivers (see, indeed, the problem resulting from the uncertain limits for the margin of discretion of the intermediary above under point 2.1.1). **In the end, however, two other aspects are decisive for the involvement of an independent data intermediary instead of the city itself.**

First, **there is a serious control or trust issue since the city would not only have to control itself as a data contributor and recipient. Rather, with the city as a state entity, one would make someone a controlling authority whose power over the private sector has actually been tried to be restricted during the last centuries.** This is particularly evident in data protection law, which was created primarily to limit the state's informational power and the resulting risk of abuse (and was then also extended to private companies by way of ordinary law). Thus, if the state itself were to take on such a control function, this would turn the situation upside down, at least with regard to compliance with data protection law. **This problem already arises when the city takes on the function of a technical service provider (see previous point). But the problem would increase significantly if the city were to control data access and use as well.** Here, too, of course, it should be made clear that these concerns do not entirely preclude a role for the city as an intermediary. Rather, this question ultimately depends on the actual risk and thus on the specific technical and organizational measures implemented. **However, the technical and organizational design that would best contain the risk here would be if a data intermediary independent of the city were to perform these control functions**, not the city itself. Of course, the city can and should do everything in its power to support the independent entity with all the necessary resources (while preserving its independence, see above at point 2.1.1).

Second, **another problem results from the complexity of the conflicts of interests to be solved. Controlling access to data and its use in order to comply with data protection or trade secret protection and at the same time to increase the data commons requires the appropriate structures and procedures to generate and apply the necessary knowledge**. If these are not in place, the data will not be shared for practical reasons alone, even if they could be shared in principle. The Hamburg Transparency Act can serve as an example: As shown, protected data may be shared if the interest in access is higher than the risk for the natural or legal persons concerned (i.e. their interest in not sharing the data). This is because the personal relation of information or a trade secret often only results from the combination of different data (sets). Thus, the (often iterative) sharing of such data (sets) while maintaining data protection or trade secrets requires the application of fairly complex technical-organizational measures. From the city's point of view, publishing or sharing protected data is not only costly, but also fairly risky from a legal point of view. In practice, this leads to negative decisions in cases of doubt, i.e., not making protected data available even if it is allowed in principle. Whether

the Data Governance Act (Chapter II) will change this remains to be seen for the time being (see section 1.1.3 above).

In any case, due to their central and specialized role within a certain data processing sector, it seems more likely that an independent data intermediary will generate and provide the needed knowledge, structures, and procedures in a scalable and thus more cost-effective manner than the public agency itself.[23] Last but not least, liability for these legal issues can also be distributed in a manner that corresponds better to these real capabilities.

There is therefore a case for leaving the organizational-legal control to an independent data intermediary. With the objective of making as much data as possible accessible (i.e., also from private companies not subject to the Hamburg Transparency Act), this intermediary can set up the necessary structures and procedures. As long as it is a private law entity that is not under the control of the FHH, the Hamburg Transparency Act does not come into play (see above under point 2.1.1). Should this be an explicit goal, special attention will have to be paid to ensure that, for example, financial or other support of the intermediary by the FHH does not undermine the independence of the intermediary. It is important to emphasize once again that the aim of this concept is ultimately to increase the volume of the data to be made available, precisely because private companies are also to be won over as data contributors, which would not themselves be obliged to provide information under the Hamburg Transparency Act (see the following chapters).

2.3.3 Stakeholder participation to identify conflicts and solutions

There are numerous detailed questions to be clarified for the concrete design of such a data intermediary.[24] In the following, only a few aspects will be mentioned. For example, Chapter 3 of the DGA provides for a number of legal requirements for so-called data intermediation services. The most important of these provisions is the obligation of such services to register (Art. 11) and the requirement to use the data exchanged exclusively for the purposes of the intermediation and even the metadata only for the development of the service and for IT security and fraud prevention (Art. 12 lit. a and c). For data altruism organizations there shall also be further registration possibilities (Art. 17 et seq.). However, since these regulations do not address the problem – which is considered to be essential here – of how such data intermediaton services should actually resolve the conflicts as described above by **increasing legal certainty in a scalable way**, they will not be discussed

[23] M. v. Grafenstein (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735, pp. 6 and 24.
[24] See, for example, D. Piétron et al. (2021). Öffentliche Mobilitätsplattformen – Digitalpolitische Strategien für eine sozial-ökologische Mobilitätswende, esp. pp. 57 et seq.

further here. Instead, more general organizational and procedural aspects that are considered to be important for the conflict resolution will be highlighted:

To identify and resolve conflicts of interest in the best possible way, the intermediary should in any case involve all relevant affected parties (or groups of affected parties) via suitable structures and procedures. To ensure that participating natural persons cannot themselves be held legally liable for the decisions, the intermediary should be an independent *legal* entity. The affected parties had then to be involved in the decision-making process mostly through committees and forums or similar structures and procedures.

Thus, beside an operational management body, the following structures and procedures may include: An expert committee with the CDO, ITD and BVM, the responsible freedom of information and data protection authority, other experts. Further, the participation of the data contributors and recipients, which is crucial for the successful identification and resolution of the conflicts of interest, in particular the FHH, the E-Scooter providers, as well as the E-Scooter users and other affected citizens (especially data subjects). These participants may be involved in one or another way in defining the data access and usage rules, in particular on the questions of a) which data recipients b) may access which data c) in which quality (e.g. aggregation) d) from which data contributor e) for which purposes f) under which technical/organizational conditions. The specific methods and the degree of participation, has to be specified in the following steps of the project in accordance with the specific question to be negotiated.

3. Data laws granting public bodies (and third parties) access to data held by private companies

A preliminary assessment of the present project in the light of the Transparency Act (G2All) has already taken place (see above point 2.1). **In the following, the focus will be on European, but also German laws or draft laws, which in turn could now oblige the participants of the present project to disclose data to the FHH (B2G) and, simultaneously, to each other (B2B and B2C). The regulations presented in the following are important because they represent different models of how to avoid the problem of Open Data laws described at the beginning, according to which only the public sector is obliged to share its data.**

3.1 Data Act (chapter V – B2G): Incentivising private parties to negotiate access to their data (with public bodies)

In addition to a data sharing obligation between private (B2C and B2B) parties (see above under point 2.2.2), the Data Act-draft also provides in Chapter V for a cross-sectoral obligation to share data with public bodies. Doing so, Chapter V of the Data

Act-draft provides a now mirrored right for the public sector to access third-party data. The scope and practical implications of these provisions are currently vividly debated and, consequently, are also central for the current project (including the UDC).

The debate is based on a tension inherent in the law itself, or at least one that is not yet clearly resolved: On the one hand, **the EU Data Act expressly provides for such a data sharing obligation only for "exceptional need" (Art. 14). On the other hand, the data sharing obligation is designed in such a way that it ultimately takes on the function of a backup regulation, should the national or local legislator not get off the ground quickly enough and create its own data access regulations.** According to Art. 14 Data Act-draft, a private data holder must grant a public body access to its data in one of the following three alternative cases: first, if the data requested is "necessary to *respond* to a public emergency"; second, if the data is necessary to "*prevent* a public emergency or to *assist* the recovery from a public emergency" (lit. a and b – italics added by the author). Finally**, the obligation also exists in case the public body needs the data to "fulfill a specific task in the public interest that has been explicitly provided by law" and the public body "has been unable to obtain such data by alternative means, including by purchasing the data" or (!) "by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data"** (lit. c).[25]

This last alternative means in brief, as long as the national legislator does not get its act together to create a data sharing obligation in time, the authority can invoke the Data Act provisions.[26] The discussion is now sparked by the question of whether the term "specific task in the public interest" is too broad, with the result that the public sector has almost unlimited access to data from the private sector.[27] Or whether the term is too narrow or, at least, too vague with the consequence that the authorities do not assert the access claim in practice because of the legal uncertainty associated with it.[28] Finally, a third criticism is voiced from the perspective of data protection law, according to which the term is too broad and too vague to serve as a sufficiently specific legal basis for accessing and using personal

[25] See regarding the reasoning of the legislator, EU Commission. Impact Assessment report. COM(2022) 68.
[26] M. v. Grafenstein, Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735, p. 27; cf. MPI (2022). Position Statement on the EU Data Act, p. 51.
[27] See, for example, BITKOM (2022). Bitkom Position Paper EU Data Act Proposal; V. Demary (2022). Der Data Act-Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen.
[28] See, for example, D. Gill (2022). The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, referring to an opposite opinion form the automotive sector; I. Dachwitz (2022). Data-Act-Verordnung, referring to further authors.

data in the case of access (compare, for example, the stricter requirements under Art. 6 sect. 1 lit. e and sect. 3 GDPR).[29]

It is not possible to go into the discussion further here, but only to point out two aspects: On the one hand, undetermined legal bases whose applicability is disputed in a specific case can and are used in practice, at least, as a bargaining chip in the context of negotiation processes. The exchange then follows more or less the logic: "If you don't give me your data voluntarily, I'll force you to do it by law." – or similarly – "Let's find a solution together now, rather than letting the legislator set the conditions because this way you have the opportunity, or more leeway, to set the conditions as well." Such **undetermined legal bases for claims are therefore suitable for at least starting the negotiation process by driving the parties involved into an exchange.** The negotiation process initiated in this way can then produce results which, in turn, can be used to further concretize the legal foundations. The importance of such a pace-maker effect in practice of vague laws should not be underestimated (indeed, the whole GDPR is peppered with vague regulations having such an effect in practice, whether it is intended or not).

In order to increase legal certainty for all parties involved, the results obtained in this way could then finally be published by the competent authorities in public statements or even by the EU Commission in a Delegated Act. These results should not only clarify which cases are covered by a "public interest" (and which are not), but also under which technical and organizational conditions this can and must be done in order to comply with the conflicting protection laws. To this end, the current Data Act draft should be supplemented by corresponding tasks and competencies.

3.2 Federal Passenger Transportation Act (B2All – Germany): Obligation of all parties to share their data in a specific context

In fact, at least **in Germany, the legislature is beginning to create increasingly concrete sectoral legal bases for the publication or sharing of specifically defined data**. Relevant in this case is, for example, the Federal Passenger Transportation Act (§ 3 a Personenbeförderungsgesetz) which requires providers and intermediaries of mobility services to make available both static and dynamic data related to the carriage of passengers through a national access point (Mobilithek). These data include: Provider name and contact information, schedules, routes, service area and times, locations and stations, fares, estimated time of departure and arrival, and actual or projected availability and capacity utilization of the mode of transportation. Apart from its sectoral approach, this regulation also differs from the regulatory approach of Chapter V of the Data Act-draft insofar as it does not create

[29] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), pp. 3 and 40 et seq.

data access rights for the administration for individual cases, but rather generally obliges all holders of data related to the carriage of passengers to make this data public. Thus, by simply obliging all data holders in the sector to publish their data, there is no imbalance in data access (of course, there may be imbalances in processing the data due to higher skills or technological resources).

3.3 Berlin Mobility Act (Berliner Mobilitätsgesetz): Differentiating between data access for non-commercial and commercial use

Finally, **it is interesting to note another local regulation that the city of Berlin has enacted regarding availability data of all publicly accessible means of transport. In this legal context, means of transport are publicly accessible if they can be used by the general public by carrying pre-purchased authorization cards or by paying directly for the ride** (§ 2 sect. 10). Thus, this also includes private cabs, ride-sharing services, and so on. According to § 5 sect. 6, availability data should be available free of charge in real time for non-commercial use and be usable for Internet-based, non-commercial applications. In contrast, commercial use requires that the data receiver must in turn make its own data available in real time free of charge for all and in a machine-readable form.

3.3.1 A market-friendly approach or just a lack of legal competencies

The actors are thus free to choose whether or not to access the data, as well as for what purpose, and whether or not to enter into an associated data sharing obligation. The regulation therefore gives the actors their own scope for decision-making, in contrast to § 3a Passenger Transportation Act. In doing so, the regulation seems to represent a kind of compromise between the goal of making as much data as possible available to the general public and, on the other hand, not simply forcing all data holders to do so and thus depriving them of their ability to pursue their individual situation-specific rationales and strategies to share data or not.

Of course, it is also possible that the city of Berlin simply did not see any legal competence to impose an all-encompassing data sharing obligation – and therefore only could establish a rule *how* data holders can get access to a data pool that is more or less under the control of the city. This thought gets clearer with a view to § 68, which is only available as a draft, so far. Pursuant to the draft of § 68, the competent body of the city of Berlin is obliged to create a public platform for the exchange of traffic-relevant data. To this aim, the draft provides certain conditions for this platform. For instance, the city may apparently resort to third party providers for the construction and ongoing operation of the platform; however, the city must not become dependent on these providers avoiding so-called lock-in effects (§ 68 sect. 2 no. 1). Further, the law makes a distinction, comparable to Art. 5 sect. 4 Data Governance Act-draft, between public and non-public access areas, the

latter being intended for protected data and to be provided with a graded access authorization system (§ 68 sect. 5). Thus, against this backdrop, § 5 sect. 6 can also be seen simply as a further principle, according to which conditions the data can be used, should they be shared.

3.3.2 Reciprocal sharing duty in case of commercial use, open data in case of non-commercial use

In any case, the structure and potential effects of § 5 sect. 6 Berlin Mobility Act on data sharing is interesting for the present pilot project: On the one hand, it creates an incentive for data providers to make their data available voluntarily. If they wish to access data from the platform for commercial purposes, they must also make their own data available. Thus, in principle, the data pool is constantly enriched with new data sets. On the other hand, the data is made available unconditionally for non-commercial purposes. In this case, no reciprocal data sharing obligation applies; and even access is free of charge. This means that, at least in terms of its design, the regulation comes pretty close to the goal of ultimately making as much data as possible available to both the general public as well as commercially-driven entities. Of course, one had to examine in more detail for which data this regulation can still apply or to what extent it is superseded by other preceding laws, such as the Passenger Transportation Act

3.3.3 Applying the idea to the pilot case: Assessing non-/commercial use, the suitable data for the return match or a suitable cost takeover

The basic principle could also be applied to the present project: **To the extent that there is room for manoeuvre because data does not already have to be published due to the Hamburg Transparency Act (see above under item 2.1) or due to the Federal Passenger Transportation Act (see above under item 3.2), a similar regulation could also be used for the present project.**

In such case, it would be important to note that § 5 sect. 6 Berlin Mobility Law refers solely to "availability data." In turn, a data receiver can also only offer such data in order to gain access to the data pool. However, the present pilot project is likely to involve more data categories, at least in the long term. In this respect, **it would therefore be necessary to examine the extent to which parties interested in the data in the pool not only share their data from the category for which they are requesting access as a *quid pro quo*, but also at least from the other categories that are already available in the data pool**. However, consideration should also be given to the possibility for requesting parties to offer data from entirely new categories as counter service to enrich the data pool with new types of data. Ultimately, if a data recipient cannot or does not want to offer its own data in return for access to data from the data pool (which such a data recipient wants to use for commercial purposes), one has finally to consider whether it could also provide its return

service by taking over some of the costs for the technical, organizational and legal infrastructure. This last option would at least help refinance the infrastructure costs.

In any case, to answer such questions, **there is need for a structure within an independent data intermediary to assess: a) whether the party interested in accessing data in the pool has commercial purposes and, if so, b) whether comparable data can be accepted as counter service or c) whether costs can be assumed instead and, if so, in what amount**.

4. Incentivising voluntary data sharing, refinancing infrastructure costs

The previous comments show that in practice – as in the present pilot case – it comes down to an interplay between voluntary data sharing and legal data sharing rights and duties, which also partly overlap. **For some data categories that a municipality needs for certain purposes, it may be able to legally compel third parties to disclose the data; for other data categories, it will have to rely on the data being given to it voluntarily.** For this reason, it is also important for this pilot case to briefly summarize the interplay between these two mechanisms.

4.1 Voluntary data sharing as an indispensable complement to data sharing obligations

If data holders are to share their data voluntarily in the absence of a legal obligation, the value of data sharing must decisively exceed the associated risks and costs from their perspective to overcome the so-called value for risk-dilemma. If a municipality like FHH (or the federal government or EU legislature) wants to encourage data holders to share their data voluntarily, it must therefore help increase the added value from the data holders' point of view and help reduce the (compliance) risks and costs to the point that the data holders see sharing their data as worthwhile. This is also what a successful data governance model must achieve – and a data intermediary can play a crucial role to reach this goal.[30]

However, even if the data holder is legally required to share its data, the appropriate data governance model is important. This is because, as shown, **even legal claims for many data categories depend on the need to comply with conflicting, often legally protected interests, first and foremost data protection and business secret protection**. **Due to the complex intertwining of legal, technical and organizational aspects, this needs the appropriate procedures and structures to generate the necessary knowledge in a scalable manner and to apply it according to the continuously changing purposes of data use**. Here, too, data intermediaries can

[30] M. v. Grafenstein, Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735, pp. 6 and 24.

play a role ranging from relieving the burden on all parties involved to actually enabling data sharing.[31]

4.2 Increasing the value of data sharing: qualitative rewards

As far as increasing the added value of data sharing is concerned, it seems more promising to focus on a return that can be measured qualitatively (from the point of view of the data contributor), such as access to the interested data receiver's own data, than on quantitative measures. (However, beside a "data for data"-deal, other qualitatively measurable returns, such as services that can be used free of charge, or an analysis result obtained by disclosing one's own data is promising). In contrast, functioning quantitative approaches such as the payment of an objective market price for the disclosure of data, on the other hand, have hardly been established to date. The reason for this is that the emergence of an objective market price requires stable market relations, i.e., that certain types of data for certain purposes are exchanged between a sufficient number of market participants for a monetary payment so often that an objective market price emerges.[32] But current data markets – with the exception of the legal grey area of the advertising market – are still a long way from reaching this point. Until then, it is therefore more promising to concentrate on qualitative services in return, such as the data recipient's own data. In any case, the quality that a data holder attaches to such a *quid pro quo*, so that the data receiver reveals its own data in return, can and should be negotiated within the framework of stakeholder participation, as mentioned before (see under point 2.3.3).

4.3 Reduction of (compliance) risks and costs

Regarding the reduction of risks, one has firstly to distinguish between the actual risks for the data subjects – for example, in data protection law, the data subject, or concerning the protection of trade secrets, the holder of the secret – and the compliance risks for the data contributors and recipients, who must not violate these laws to maintain the trust of data holders and, also, avoid legal sanctions. To reduce data protection and trade secret risks for the data subjects and trade secret holders, laws provide, on the one hand, an objective standard for their assessment and, on the other hand, requirements for their reduction.[33] In addition, in some areas, these laws also provide procedures by which data users can reduce their compliance risks.

---

[31] Ibid.

[32] M. v. Grafenstein, Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework. HIIG Discussion Paper Series, 2022(2). DOI: 10.5281/zenodo.6457735, p. 21, referring to A. Krotova and M. Spiekermann (2020). Data Valuation Model: Handbuch für Bewertung von Daten in Unternehmen – Demand Project - Data Economics and Management of Data Driven Business, p. 30.

[33] Ibid., pp. 13 et seq.

Such procedures are particularly useful when the application of the law is characterized by significant legal uncertainty, such as in data protection law.[34] In these cases, interestingly, these procedures may even generate innovation-promoting effects or competitive advantages. One reason for this is that the standardization of legal requirements, which results from these procedures, reduces the effort required of data users for the otherwise necessary legal case-by-case assessment. Another reason is that data users may increase the confidence of end users and business customers in the usage of the data and thus set themselves apart from their competitors on the market.[35] In data protection law, in particular, Articles 40 et seq. GDPR provide for such procedures.

For the present pilot project, especially the codes of conduct provided for in Art. 40 and 41 GDPR might become relevant. According to these provisions, the data contributors and data recipients can specify the legal requirements of the GDPR in a code of conduct for the processing operations they carry out and have their compliance monitored by a so-called monitoring body. Since such a code of conduct must be approved by the competent data protection authority, data contributors and receivers can use adherence to such a code of conduct as a kind of evidence of GDPR-compliance (see Art. 24 sect. 3, Art. 25 sect. 3 and Art. 83 sect. 2 lit. j GDPR). This implies, by the way, that the intermediary does not take on the technical service. Rather, with its set of rules and procedures, the intermediary (aka "monitoring body") controls the data contributors and recipients as well as the technical service providers they use for their purposes. It stands to reason that the data intermediary recommended here, which alone takes on the organizational-legal control of access to and use of the shared data, could take on this function.

After cursory examination, it seems also reasonable that the same entity might control compliance with the other requirements arising from the protection of trade secrets as well as the further control issues raised earlier. Even if there is no legally explicitly recognized proof of compliance for these further requirements (unlike in the GDPR), the participation processes recommended here nevertheless reduce the *de facto* "compliance"-risk that sharing and subsequent use of the data will conflict with any of these interests. It is worth highlighting that these interests may include, of course, the overarching interest in making as much data as possibly accessible (see above under point 2.2.3 and 3.3.3).

---

[34] Cf. regarding certification mechanisms, for example, A. Blankertz and L. Specht (2021). What regulation for data trusts should look like. Stiftung Neue Verantwortung, pp. 4/5, 10, 25, and 38.

[35] M. v. Grafenstein (2022). Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design. In González-Fuster, G., van Brakel, R., & P. De Hert, Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed.. Cheltenham: Edward Elgar Publishing.

Last but not least, the recommended data intermediary can lead not only to a reduction in risks, but also in organizational costs. This is not only due to the standardized structures and procedures and the associated scaling effects. The data intermediary is also able to distribute these costs among the various participants in the system according to its objectives, thus providing a further incentive to participate. For instance, as mentioned earlier, the intermediary may impose costs on those data recipients who use the data for commercial purposes and in return do not (or cannot) feed comparable data into the system.

5. Concluding summary

This preliminary assessment primarily takes on the perspective of a city (in this case, FHH) that intends to share as much data as possible between itself and other parties for use in the public interest, by relying on an appropriate data governance model. The assessment has shown that in the present pilot, as well as in future similar projects, many different laws come into play (at the EU, Member State, and local levels) and partly overlap, as many different parties exchange different categories of data for different purposes. Finding a data governance model that works is therefore done by continuously matching the actual circumstances, i.e., the actors and their data and processing purposes, with the applicable laws. Based on pilot projects like the present one, it is possible to typify such data governance solutions for the corresponding processing sector.

In the present pilot case, for instance, according to the Hamburg Transparency Act, FHH is obliged to share its own data, i.e. the "official information" it holds. In contrast, if the city processes data exclusively on behalf of others, for example as a technical service provider, the Transparency Act does not come into play. Even if the Transparency Act applies, the city would only have to share data under limited conditions, especially if it is personal data or data containing trade secrets. However, beside the Hamburg Transparency Act, there are numerous further laws regulating access and use of the data in question, such as the German Passenger Transportation Act, but also draft laws currently discussed such as the EU Data Act.

This **diversity of applicable laws has far-reaching consequences for the needed performance and thus the design of the data governance model. An important observation is that most actors may have to make use of both voluntary data sharing *and* various data sharing rights to reach their respective overarching goal. To resolve the conflicts of interest that arise in such situations, the city should have recourse to a data intermediary that is independent of the city** and that organizationally helps define the conditions for access to and use of the data as well as monitors compliance with them, according to the following reasons and conditions:

Insofar as the stakeholders involved are dependent on the voluntary sharing of data by the others, an independent data intermediary is the best way to introduce a ***quid pro quo*-rule. Such a reciprocal data sharing clause creates a concrete incentive for private companies to disclose their own data, too.** The mechanism concretizes the often vague added value of sharing own data and thus helps to overcome the first hurdle of the so-called value for risk-dilemma in voluntary data sharing. In addition, the intermediary also helps to overcome the second hurdle of the dilemma: namely, to reduce the risks, in particular the compliance risks with data protection and trade secret protection when sharing data, as well as the costs.

With these two levers, i.e. increasing added value and reducing risks and costs, an intermediary can make data sharing worthwhile for data contributors and can support data contributors and recipients to find the right tipping point where the perceived value really exceeds the risks and costs. Where this tipping point exactly is has to be defined in a negotiation process between data contributors and receivers (with the support of the intermediary).

To avoid closed data clubs in voluntary data sharing constellation by means of a reciprocal data sharing clause, the following aspects should have to be taken into account: Firstly, it would have to be considered that this only applies to commercial uses; non-commercial uses, on the other hand, would be free of charge (either in the form of data or financial compensation). Second, other types of data could be allowed in return for the types of data received, in order to enrich the data pool with further data types. Third, data receivers could also be given the option of providing a monetary value in return for the data they receive instead of their own data. This could at least partially refinance the costs of implementing and operating the infrastructure. Last but not least, all these and the following conditions must apply equally to all parties interested in the data. In this respect, data access does not mean unconditional access, but it does mean non-discriminatory access.

In the case of legal data sharing obligations or rights, there is no value for risk-dilemma (as in voluntary data sharing), since data contributors are obliged to share their data anyway. However, here too, an intermediary helps to comply with protection laws and to reduce the corresponding costs. And here, too, the affected parties must be involved to reliably identify the conflicts of interest and (!) solutions. As far as the access of the state to data of private companies is concerned (Art. 14 et seq. Data Act-Draft et seq.), **the Data Act-Draft should add tasks and competences for the competent authorities as well as the EU Commission, according to which they could continuously add use cases in public statements or a Delegated Act, where a public interest exists and under which technical-organizational conditions the access to the data can and must take place to comply with the conflicting protection laws**. In this way, legal certainty could be increased for all parties involved.

Regarding voluntary (!) and obligatory data sharing, data intermediaries are well suited, given their central and specialised function in a certain processing sector, to

provide the structures and procedures that are necessary to identify and solve the conflicts of interests in a scalable way. In doing so, they should be able to clarify, for example, the following questions:

For voluntary data sharing,

a) are there commercial or non-commercial data processing purposes;
b) can a data recipient offer comparable (or other) data as compensation;
c) if not, the financial amount of its compensation for receiving certain data (i.e. refinancing the infrastructure);

for both voluntary and obligatory data sharing,

d) whether personal data are present and/or the data contain trade secrets (or whether these result from an interplay of iterative data accesses);
e) and if so, under which technical and organizational conditions which data receiver may use which data in which quality for which purposes, so that data protection or trade secret protection is met and the recipient can achieve its goals.

In this context, **it is recommended that the data, the processing purposes and the technical-organisational conditions are defined by the data contributors and recipients to such an extent that the intermediary does not have to leave the legally permissible room for manoeuvre when controlling access to and use of the data. This is to ensure, in essence, that the intermediary performs its control function only on behalf of the data contributors and data receivers.** To successfully identify and resolve the conflicts of interest, the intermediary will also need to involve all other parties affected by the data processing or groups of them (at least through representatives), as well as various experts, in the decision-making processes through appropriate structures and procedures.

To relieve the actors involved in these decision making processes as far as possible of the (legal) liability associated with the aforementioned questions, they should mostly be involved in the decision-making process via internal structures (e.g. committees and forums). **Liability should thus be borne primarily by the data intermediary.** The participation processes are thus ultimately procedures for reducing not only the conflicts of interests *per se* but also the associated legal liability. In data protection law, there are further formalized procedures available for reducing legal uncertainty and, thus, partly liability. In particular, a code of conduct (Art. 40 f. GDPR), in which all participants clarify the data protection conditions of their processing operations (in the respective processing sector) and have them controlled by the intermediary as a so-called monitoring body, is worth considering here. Since such a code of conduct is approved by the competent data protection authority prior to its application, not only the data controllers and processors involved but also the monitoring body can use it to reduce their compliance risk when applying the code of conduct (which means the GDPR).

After a cursory examination, supposed certain additional structures are put in place, it might be possible that the intermediary not only acts as a "monitoring body" for

the application of the GDPR, but also checks other criteria to comply with further goals and laws (see preceding paragraph). However, **as a "monitoring body", the data intermediary is only allowed to fulfil the monitoring function and must not process the data itself, not even if this occurs only on behalf of the data contributors and recipients (since this would undermine its monitoring function). Thus, the data processing must be done either by the data contributors and receivers on their own or by a third party (or sub-entity of them) on their behalf (e.g. the LGV of the FHH, see in more detail below).**

In conclusion, the FHH should not act as a data intermediary itself. Under certain technical and organizational conditions, however, the city could at least support data sharing as a purely technical service provider on behalf of the data contributors and data recipients (the following picture may illustrate this architectural design). In addition to this purely technical support, the city may also support the data intermediary financially. This would be particularly important for financing the initial implementation of the infrastructures and procedures, especially if the data intermediary were to be newly created as a non-profit entity under private law (ongoing operations, on the other hand, are more likely to be financed by the actors through fees or the like – see already above on this topic). Here, however, it would be important to ensure that the data intermediary retains its independence despite the financial support. This and the aforementioned technical and organizational conditions would have to be clarified at an early stage, especially, with the competent freedom of information and data protection agency in the following implementation process, as would several of the other questions raised before.