Electronic Markets
The International Journal on Networked Business

Appendix 1 – Overview of interview participants

ID	Role	Core relevant experience	Overall work experience (in years)
I-01	Director of innovation	Involved in multiple data exchange projects (e.g., meta-platforms, data marketplaces) and relevant underlying technologies (e.g., privacy-preserving techniques).	28
I-02	Security solution manager	Working on data loss prevention technologies for data exchanges.	18
I-03	Product owner	Leading the commercialization of a data exchange platform.	14
I-04	Head of standard business reporting	Leading the implementation of data exchange technologies.	23
I-05	Project manager	Leading multiple projects on the topic of interoperable digital platforms.	10
I-06	Commercial director	Building digital platforms for clients focusing on digital goods.	24
I-07	Chief data officer	Responsible for shaping data policies, including business data exchange with external parties.	12
I-08	Technical innovation manager	Managing a technical lab to explore the newest data exchange technology, such as quantum computing or multi-party computation.	28
I-09	Data protection specialist	Analyzing legal aspects of data exchange.	3
I-10	Head of architecture, innovation, and technology	Exploring the newest technological advancement for data exchange (e.g., blockchain).	16
I-11	Senior strategy manager	Managing the Business-to-Business (B2B) stream of a large company, which includes data exchange activities.	32
I-12	Product owner	Leading the commercialization of data analytic platforms.	11
I-13	Risk manager	Conducting risk assessments for data-related exchange.	5
I-14	Senior consultant	Providing consultancy services in interoperability-related aspects, such as ensuring data portability in digital platforms.	22
I-15	Associate director	Providing consultancy services on information technology outsourcing where business data exchange plays a pivotal role.	24
I-16	Technical researcher	Researching technical aspects of business data exchange, for example, semantic web technologies, metadata management, or vocabulary management.	9
I-17	Deputy studio director	Leading an initiative to explore the interoperability of data marketplaces	13
I-18	Data science director	Managing a portfolio of data science projects, including business data exchange	12
I-19	Project manager	Involved in multiple data exchange projects (e.g., meta-platforms, data marketplaces).	19
I-20	Project manager	Developing use cases for business data exchange.	9
I-21	Consultant	Data sharing and digital identity consultant.	6
I-22	Project manager	Date e-commerce project manager, experienced professional in the telecommunications and financial industry.	20
I-23	Information technology architect	IT Architect/software developer, data sharing expert.	5

ID	Role	Core relevant experience	Overall work experience (in years)
I-24	Project manager	Experienced IT and project professional.	6
I-25	Consultant	Experienced professional in financial services and management consulting.	25
I-26	Senior researcher	Senior research specialized in trusted data sharing and business ecosystem architecture.	13
I-27	Director	Director of a pan-European trust and data sovereignty Framework.	15
I-28	Consultant	Board member of a regional collaborative organization specialized in future affairs, including digital and data-related topics.	15
I-29	Data management expert	Data management expert at a global professional services firm.	5
I-30	Researcher	Data expert and research engineer.	5
I-31	Developer	Developer and semantic web expert, data sharing initiatives expert.	6

Appendix 2 – Codebook

Higher-level facet	Facet	Second-order code	First-order Code
Protection	Data ownership	Data ownership fundamental	Data ownership as sovereignty facet
			Protection of data ownership
		Data possession	Data provider as owner
			Ownership clarification
			Ownership transfer
			Retention of intellectual property right
		Meta-data	Meta-data as data description
			Importance of meta-data
		Term of use	Data storage location
			Data usage condition
	Privacy	Consent	Benefit for data subjects
			Explicit consent from data subject
		Privacy fundamental	Privacy as sovereignty facet
			Protection of privacy
Provision	Data control	Data control fundamental	Data control as sovereignty facet
			Provision of data control mechanism
		Data provenance	Data flow tracking
			Data origin information
			Data tagging
			Data usage insight
			Data storage insight
			Knowledge about data consumer
		Data withdrawal	Data access revocation
			Dataset retraction
		Policy enforcement	Access condition check
			Legal enforcement
			Policy attachment
			Technical enforcement
	Security	Cutting-edge security mechanism specific for data exchange	Anonymization
			Confidential computing
			Distributed ledger architecture
			Encryption
			Federated learning
			Privacy-preserving data analysis
			Watermark
		Security CIAN principles	Availability
			Confidentiality
			Integrity
			Non-repudiation
		Security fundamental	Security as sovereignty facet
			Provision of security mechanism
		Verifiable credential	Authorization capability
			Credential verification
			Trusted identity
	Compliance	Compliance fundamental	Compliance as sovereignty facet
			Provision of compliance mechanism
		External compliance	Industry standard
			Regulatory compliance
		Horizontal compliance	Data usage audit
			Data exchange contract
			Dispute resolution
		Vertical compliance	Agreement with operator
			Technical compliance

Higher-level facet	Facet	Second-order code	First-order Code
Participation	Responsibility division	Accountable oversight	Liability chain
			Penalty
			Provision mechanism
		Interpretation of participation	Active oversight
			Membership enrollment
			Product installation
			Responsible use of platform and data
		Responsibility fundamental	Responsibility as sovereignty facet
			Responsibility division to ensure participation
Contextual condition	Data type (personal, sensitive data)	"Unlocking" privacy facet	Negative perception of data subject
			Surveillance capitalism
		Influence on compliance	GDPR compliance
			Privacy rule
		Influence on data control	Control mechanism for data subject
			Data usage knowledge for data subject
		Influence on data ownership	Decision about shareable data
			Difficulty in exercising right of data subject
			Ownership tension
	Data type (format variations)	Influence on data control	Complexity in data storage
			Data format
			Large data size
			Processed data withdrawal
			Real-time data
	Data type (industry-specific data)	Influence on compliance	Compliance practice maturity
			High governance standard
			Over-regulation
		Influence on ownership	Lack of capacity for data exchange
	Business data exchange setting	Influence on compliance	Cultural knowledge gap
			Different liability
			Different national law
		Influence on data control	Alignment of data marketplace architecture
			Data provenance difficulty
		Influence on ownership	Data marketplace selection
		Influence on responsibility	Data marketplace evaluation
			Domination of meta-platform
			Responsibility division
	Organizational size	Influence on compliance	Liability for large organization
			Understanding legal requirement for smaller company
		Influence on data control	Lack of capability for smaller company

Online appendix

1. Higher-level facet: Participation

1.1 Facet: Data ownership

Second-order code	First-order code	Illustrative excerpt
Data ownership fundamental	Data ownership as a sovereignty facet	"I think data sovereignty indeed means control over data ownership. Data ownership does not mean that you are always the owner of that data […] In practice, you see a lot of parties in certain sectors that will never arrange their own data ownership. In the construction industry, a small contractor is just going to use a platform with all the functionalities. That is totally fine. He should also not want to arrange everything himself. [In contrast], larger parties may want to arrange everything themselves […]" (I-21) "[…] Let's keep the example of IoT data, and you want to offer it. [Regarding sovereignty], you could define that this data can only be used by research parties, universities, or whatever. You can also write down this data only to build up on energy services or whatever you like. So, if you want to have a specific purpose for your data, you should be able to define this in the usage policies. And by agreeing on this, you can have the law enforcement and so on." (I-24)
	Protection of data ownership	"Data is easily stolen. Data can be difficult to watermark or safeguard in a very prominent manner […] And this becomes more difficult when data are constantly updated, for instance, every day, every week, every month. So, you need to have strong protection mechanisms for the ownership of the data […] Otherwise, without this protection, if you put the dataset in the market, then you will lose it the very next day, and somebody else will benefit." (I-01)
Data possession	Data provider as owner	"[…] data ownership should always remain with the provider, and that should be clear through whatever kind of licensing they do. And that licensing can certainly be handled by a marketplace; there should be no issue there." (I-25) "That is basically what the specific data exchange is all about. It is not so much about us [data providers] transporting the data because the data simply remains local with the owners. What matters to us is that we can record and clarify the rules that we mutually make with each other in order to ultimately share data on a large scale in the future. This way, we know where we stand and also have a place to go if parties do not adhere to the rules for resolving disputes." (I-28)
	Ownership clarification	"[We need to have] insights on how the data are being used. So, if you act like aggregators, there is a policy about how long it is stored. But that depends a bit on what happens to the data ownership. Is the ownership transferred to the platform, or is it still owned by the data provider?" (I-10) "Data sovereignty is self-determination over data. That means you know which data belongs to you and is labeled to you. You always need that classification for that: this organization has this and that dataset. Knowing that, it is indeed about access control: who can query my data at the source? And if someone has asked that question, what can he do with it? It is about usage control through licenses." (I-27)

Second-order code	First-order code	Illustrative excerpt
	Ownership transfer	"Data ownership does not mean that you are always the owner of that data […] In practice, you see a lot of parties in certain sectors that will never arrange their own data ownership. In the construction industry, a small contractor is just going to use a platform with all the functionalities. That is totally fine. He should also not want to arrange everything himself. [In contrast], larger parties may want to arrange everything themselves […]" (I-21)
	Retention of intellectual property right	"Suppose I am the provider of the data in this [meta-platform] scenario. The only thing interesting is Intellectual Property Rights (IPR). If I am a provider, this means that I have a [data] product that I put on the market, and I want to define the terms or conditions of using the product […] the product should be sold a lot at the highest price possible. So, I am only putting the minimum terms and conditions to safeguard my product and my ownership of the product in terms of IPR, nothing more." (I-01)
Meta-data	Meta-data as data description	"Because when exchanging data, you have to know the quality of the data with respect to your needs. You have to know how frequently the data is updated, how long the data set is, which standard it complies with, and other relevant areas. You have to express it with a lot of meta-data." (I-01) "There are different types of meta-data. There are some meta-data that can be used to describe what is in the data. Sorry, all of the meta-data describes what is in the data, but some describe what is in the data only with respect to the data itself. Then, there are some other meta-data, which, for instance, describe how this dataset corresponds to other datasets. For instance, how it is classified. So, you can have an external classification; this dataset is about health, that dataset is about climate science, and so on." (I-18)
	Importance of meta-data	"I think the key [to control data] is having good meta-data, both technical meta-data and quality assurance. For example, I have a data quality department under me, so we are handling data quality. Technical data quality is one thing, but business data quality should also be considered." (I-07) "I think you might also have to look at meta-data a bit [when considering data sovereignty]. In principle, meta-data can already reveal a lot about a company and what they do; there is quite a lot of information behind it. And that is something that will become important in such a marketplace because you do not yet know exactly who will request that data. That meta-data is actually another piece of data that you want to maintain control over in the same way." (I-23)
Term of use	Data storage location	"Data access, for me, needs to be controlled. Going back to my example of Snowflakes and Amazon earlier, that should be under the control of the owner. You are the one who knows where you want to store the data and in what format you want to sell it or distribute it." (I-22) "The storage is always under your ownership, in your sovereignty, in, let's say, a geographical or location context. So, to me, there is no use case where you should even give up this sovereignty regarding storage because you are always giving just access to a specific file, request, or whatever." (I-24)
	Data usage condition	"[Data ownership means]: I can define my policies and be sure that no one accesses my data without my consent, I can define how long the access is granted, I can define who is getting access. I have a data contract to define how to use this data for which purposes. So, as long as I define all the conditions, no one other, and not the platform, I am fine. What also is very relevant is to declare how this [a data product] is charged." (I-24)

Second-order code	First-order code	Illustrative excerpt
		"Well, first of all, it [data sovereignty] includes that I am able to define usage policies. I can say how to use the data and for what purpose. If someone uses my data, it means controlling the usage policy so I can control what the data consumer does with my data." (I-30)
	Monetary incentive	"There is always a business case behind it [data exchange]. So, you always need to identify how this data improves your decision-making and how much money you can make from it. Take security as an example; we have clients who set up IT systems for others. No company of a reasonable size has all their IT systems with one provider. And you are only as secure as your weakest system, as they are all linked together. If one system is not well-protected, you have an issue. We have identified that you would want all the logs that tell you about the system's safety to be shared with a centralized security operating center. So, everyone needs to share their data to that specific point because everyone wants to be secure. A security incident can harm your reputation and cost you money. It is an easy use case where you say we all need to share data on how our IT systems are operating. The easier you make it to share that data, and the more neutral the party that collects the data, the higher the chance that people will do it." (I-03)
		"I think the monetary incentive is secondary to security. Monetary incentives can come in two forms: real cash value and also brand value. So, when it comes to pushing our services into newer industries like fintech, healthcare, or insurance, it might not always be a direct monetary incentive that we receive. It could be a brand incentive. Even partnering with governments in terms of open data can bring goodwill. So, I believe security is key, as well as monetary incentives." (I-05)
	Period validity	"The allocation to certain [data exchange] services may vary. Some services get one month of storage, some get three months, and others might be available only for a week. It really depends on the service, and it also depends on the client's needs. Sometimes the data might no longer reside in our environment but has to be pushed for longer keeping with the clients." (I-05)
		"So, what happens if the connectors agree that this data on the sink is to be deleted in 90 days? Technically, we could build this because we control both the source and the sink, and we have a legal agreement that allows this connector to delete the data in the sink after 90 days […] So, yeah, having control could be further elaborated. There could be things like deleting the sink after X days." (I-24)

1.2 Facet: Privacy

Second-order code	First-order code	Illustrative excerpt
Consent	Benefit for data subjects	"It is indeed interesting what, for instance, [the name of a telco company] can do with location data. [As a bank], we can do the same with spending data. So, we know what people buy, how much they buy, and at which location. This information is really interesting. If you anonymize it, it has some commercial value. It is difficult, yes. And there has to be some kind of link or proof explaining why you are sharing this data. So, using [the name of a telco company]'s location data to provide better route information has clear value for the customer. In this case, it is using customer data to benefit the customer.

Second-order code	First-order code	Illustrative excerpt
		However, data on spending is not directly interesting for the customer. It is more interesting for companies who want to advertise." (I-08) "So, yes, you could have a platform with multiple parties, including a bank. But the bank will never provide data to the platform unless the customers say so. And that is where my philosophical thoughts come in. Customers need to see benefits to share their data." (I-13)
	Explicit consent from data subject	"[…] Consent of the individuals is necessary. So those parties [data providers] cannot access that data without the individual providing the consent right for extracting the data." (I-13) "Another issue that will always be out there is Personally Identifiable Information (PII) contents and how you protect that so that data does not get sold without explicit consent. But I think that is at the data provider level; I do not know if it is the job of the meta-platform or any marketplace." (I-25)
Privacy fundamental	Privacy as sovereignty facet	"For their customers, for their reputation, for everything, a company needs to have control over their data. Therefore, interoperability is an attractive option for them that offers users greater privacy and better control. So, controlled data is data sovereignty over their personal data in general […] So, if you exchange this other information via an interoperable marketplace, they surely need this feature." (I-20) "[If a data marketplace wants to join a meta-platform], I think you should look at the minimum standardization you need because then you are interoperable and portable. I think those two things are important. Looking at data sovereignty, security is also important because you do not want everything to be put out in the open. There is also a part of privacy that parties need. That is a bit of the triangle within which you have to operate." (I-26)
	Protection of privacy	"Privacy has to be assured in the data marketplace. You know that whatever they share with the platform is going through a secure tunnel. So, security in terms of data transportation and the exchange of data from one micro-PC to another, up to the buyer, is really important." (I-05)

2. Higher-level facet: Provision

2.1 Facet: Data control

Second-order code	First-order code	Illustrative excerpt
Data control fundamental	Data control as sovereignty facet	"And this data sovereignty means that organizations that create or generate data stay in control over these data, even after sharing it with other organizations over a meta platform or even a single data marketplace." (I-22) "So, to me, data sovereignty is being in control of your data as much as it is over your metadata. And that you just have non-repudiation, traceability, that sort of thing. So, what I am actually saying with that is traceability, in order to be able to control it [(meta)-data] at all, you first have to know where it is. You have to have insight into that to be able to enforce anything at all." (I-26)

	Provision of data control mechanism	"Okay, then come the more complicated business models, like, 'Okay, this person can only have access up to three times to the data set, and this is already the fourth time, so I should deny the access,' and so on. These kinds of access control mechanisms on the data provider side are necessary, but they definitely require some sort of commonly agreed-upon identity mechanism—something equivalent to the TLS certificates that are used in standard HTTP. So, when you receive a request, you have to be sure who is making this request, not only by their credentials but also by some other piece of information that a trusted third party can certify." (I-16) "Specifically, for data sovereignty, keeping control over your own data, I think it is about two things: access control, someone needs access, or usage control because a party needs it for a certain thing […] You can do access control and usage control via legal enforceability via contracts or via technical enforceability, which you can use to technically enforce that someone cannot do something." (I-26)
Data provenance	Data flow tracking	"For example, we have data lineage implemented. I can check its availability, but we are tracking how data flows through our organization and have included all relevant business stakeholders. For example, when we talk about artificial intelligence, as proposed by the European Commission, employees should be able to explain to customers how their data is treated and what models are used. So having a complete data flow, from a logical standpoint, would be valuable, if not always used, but certainly viable from a strategic point of view" (I-07).
	Data origin information	"If you put too much emphasis on buying data, it can create confusion about where the data is actually coming from. If I look, for example, from a [the name of the company] perspective, I always doubt that we have any data at all. Because we are more or less maintaining the data of our customers, we have data about their activities, and you can ask for consent, but that is always a grey area. So, if you collect, the data always comes from somebody else unless you have machines standing in somebody else's environment." (I-03)
	Data tagging	"There is a lot of discussion around tagging data contents [to enhance data sovereignty] so you know who the ultimate owner is. And I think that is the answer. So that at the end of the day, you can review where the content comes from. You can say this comes from Data Provider A." (I-25)
	Data usage insight	"But for me, as [the name of the company], I have no clue what the other side will do with the data. They have just bought it; it is theirs now. I think you should always be able to show people, 'These are the data that I, as a data provider, am offering to the market. These are its uses, and this is what the users [data consumers] are doing with my data.' Otherwise, we always end up in this gray area where this data goes, and nobody knows where the data set originated from. Data should become more transparent, rather than less transparent." (I-03)
	Data storage insight	"Control, I think, is the management of your data. As a provider, you should at least have an idea of where your data is residing. You should also know if there is any demand for your data on different platforms and have insights into its usage or potential use." (I-10)
	Knowledge about data consumer	"The most important thing is to have trust. What will happen to my data? Do I have control over it? Do I know who is on the other end? Can I say who can and cannot access the data? I think that is a concern we often hear about." (I-28)
Data withdrawal	Data access revocation	"I think that [providing technical enforcements for data control] is the main part where the industry has been struggling in the ideal world: You can share

		data. You have some control over what is done with the data. You can revoke the rights to use the data at any time." (I-02)
	Dataset retraction	"Additionally, you can also remove any data that could potentially leak information about the data subject [to protect privacy]." (I-31)
Policy enforcement	Access condition check	"[…] everything should remain on your premises all the time unless there is a contract for this. And this requires that data providers have some way to validate that the access being requested to their assets is according to the contract [or agreed terms of uses]." (I-16)
	Legal enforcement	"How can you keep control over your own data if it is processed by another party? That is partly difficult, remains difficult, and always will be difficult. But, you do have a bit of technical enforcement on the one hand and a bit of legal enforcement on the other. You can force it [the data] to be used in a certain way. In any case, indicating what is allowed with data, I think that is already Step 1. That both parties know what is allowed. And then the next question is, how can you actually make that sliding scale from technical and legal as far as possible towards technically enforceable? You can think of confidential computing and things like that, remote at station so that you know for sure which piece of software is running, and I know that there is a stamp on it from someone who is allowed to issue a certificate. Then I have enough confidence that it will be processed properly." (I-23)
	Policy attachment	"As a provider, I would like to know who can access my data. Yes, [I would like to] see my meta-data. So, I would not choose a platform where I would upload data. I would choose a platform where I only show meta-data to others and see meta-data from others. I really want to attach policies, which have to be accepted before someone can access my actual data. For me, data sovereignty means acting with choice" (I-24)
	Technical enforcement	"In the connector world, they [researchers and practitioners] often talk about fully enforced policies. In your data source, you have a connector. You have another connector in your data sink. And you have your offer, you agree on the contract, and then you have all the terms, conditions, and policies. After that, the data gets transferred from the data source to the sink. Technically, we could build this." (I-24)

2.2 Facet: Security

Second-order code	First-order code	Illustrative excerpt
Cutting-edge security mechanism specific for data exchange	Anonymization	"We have used it [anonymization] for certain projects, some kind of the way that we control the privacy and also the quality of the data. So, we add some kind of noise to the data. Let's say I would like to share my data with another company, but I will not share everything related to the personal information. So, I can hide all of this information, or I can do some kind of anonymization on all of this data." (I-31)
	Confidential computing	"I am not entirely sure [that fully controlling data to enhance data sovereignty is technically feasible], but you could look into confidential computing, that is heading in that direction. This is mainly related to usage control. Because what you see practice is a trusted third party, and people think everything will be fine. And with legal enforceability, that is very handy because there is one company responsible if it leaks. The problem is still there, but it has been bought off. That is the practice now, but you would actually like to go further in the future." (I-26)

Second-order code	First-order code	Illustrative excerpt
	Distributed ledger architecture	"If it [data exchange] will be more regulated or governed by a platform owner, then you already have that kind of dependency, which could be a barrier to tapping into such a platform. Because you might say, 'Hey, I am not in control anymore […]' I think it also depends on the opportunities that technology may provide. So, if you look at, let's say, the technology that is also used in blockchain networks, you still can create, to some degree, a kind of control for an end-user based on business rules." (I-15)
	Encryption	"So here is where an extra layer, let's say kind of an extra layer of security has usage control has to be built around assets, so that they be, for example, transmitted in some encrypted form. This encryption requires both a key that the consumer has and a rotating key that the producer issues for every access, and that way, the producer knows exactly how many times it was accessed. So, this kind of encrypted data container exists." (I-16)
	Federated learning	"[To enhance sovereignty], we could have contractual constraints, of course. That is one thing, and then it would just be illegal to do otherwise. Another thing, from a technological perspective, is that if you want to train a machine learning model, you could maybe consider things like federated learning. That could be an option because then you do not have to share your actual datasets, only a trained machine learning model, basically." (I-17)
	Privacy-preserving data analysis	"Maybe technologies that they have worked for [in a project] can help. Here, I am not an expert, but the privacy-preserving data analysis and deep learning in distributed frameworks, things like that probably can help [to ensure data sovereignty]." (I-17)
	Watermark	"Your question was more like, 'Can we enforce this?' Let's say we agree people will never give up data sovereignty; what soft means do we have to enforce it? So, yes, there are these kinds of contractual means, like, as I mentioned, watermarking data, so that you can see where it was compromised and so on." (I-16)
Security CIAN principles	Availability	"We actually categorize this into three layers in the triple-A model: availability, accessibility, and application. In the world of data sharing, you need all three of these things. So, you need the availability of data, you need accessibility, and then you can use it in a certain application. That is where the added value lies. I think when you talk about data ownership and data quality, it is all in that availability layer. Such a meta platform is in the accessibility layer. What it does is try to organize some of that access to that data. Ultimately, you have all kinds of parties that will do great things in that access layer. When you talk about data sovereignty, I think you are talking about keeping control over this whole process. And then for the accessibility layer, a platform is a good way to arrange it." (I-21)
	Confidentiality	"And then, of course, the limit of confidential data [that prevent sovereign data exchange] […] There is still a risk of re-identification. Especially with the research party, they have access to other party data, right? Even though we talked a lot about the payments network, we talked a lot about aggregation; we could not get our senior management comfortable about sharing that data. And that is why banks are a bit of an odd one out. You know, we have this senior management body that needs to sign off, and we have this implied duty of confidentiality. We have a contractual duty of confidentiality to our customers because of our function as a bank, and it has been historically this way. And I think the only way that is going to move is if a Bankers Association like [an association], you know, along

Second-order code	First-order code	Illustrative excerpt
		with maybe regulators, agrees that we can move on this point. I do not think any bank individually will move here." (I-13)
	Integrity	"[…] The second thing is the overall platform security that you provide. So, are only people who are paying your subscription, for example, able to access it? Or, for example, can people see both sensitive and some of the non-sensitive data? Even if they are both buying, can someone with only access to non-sensitive data see that and have the rest masked or something? And the other thing is the platform itself. How safe is the platform? Because it also addresses things like the confidentiality, integrity, and availability of the platform." (I-12)
	Non-repudiation	"I would say generally there are like five principles in cybersecurity for which data has to adhere. I have forgotten most of the terms, but I do know that in terms of non-repudiation, being unable to deny the source of that data, and also authentication, verifying that you are who you say you are, those are important. So, in terms of making sure that we know who the buyers are, we know that the platform is the platform; those five principles in cybersecurity for access to data are important and guide most of it. I think the use of the data after it has been bought has to be really verified as well. Because, I mean, and that is why I said the quality of buyers is really important." (I-05)
Security fundamental	Security as sovereignty facet	"In terms of [sovereign] data sharing, given that this involves very confidential information, first of all, security is key. We have to make sure that our systems are definitely secure. I mean, as a very big telco, security is key. It is a key feature in everything that we do." (I-05)
		"[If a data marketplace wants to join a meta-platform], I think you should look at the minimum standardization you need because then you are interoperable and portable. I think those two things are important. Looking at data sovereignty, security is also important because you do not want everything to be put out in the open. There is also a part of privacy that parties need. That is a bit of the triangle within which you have to operate." (I-26)
	Provision of security mechanism	"So, if security certification and control of our data are established, I do not see any issues from a business perspective with the [meta-platform] model you proposed […] For example, when we talk about data ethics, in the banking sector—regardless of regulations—we have guidelines on whom we provide loans to. We are not allowed to finance, let's say, the military industry. So, for me, having the option to decide to whom I want to share my data within the meta-platform would be great. It would also be beneficial to have certified buyers for this data. For example, I am not willing to share my customer data with a military organization or an organization I consider unethical […] If I am uploading data, I could have the option to say that I am willing to sell this data only to certified partners that have undergone due diligence. This would make me more willing to trust the platform." (I-07)
Verifiable credential	Authorization capability	"In this case, you have a broader network of parties with whom you work dynamically. And how that game works, we are, of course, still discovering that together. But you are now seeing the first practical applications, such as with large public administration bodies [exact names removed]. They will also use our framework for their data infrastructure. You see cases of this kind everywhere now, which has led to an initial understanding. And I, as an organization, have a method that is actually being used when a party requests access to the data I have. Then I can authorize. This is really

Second-order code	First-order code	Illustrative excerpt
		something that needs to find traction. And because we are going to do this with a large public organization [exact name removed], this can be rolled out to 1.5 million companies." (I-27)
	Credential verification	"We have to trust and verify the credentials, but then also identify all the entities who are there. So, what is the mechanism, or how can it prove that the person, the entity, or the company is who they say they are? I think if the functionality and all these criteria are the same, I do not see any difference between publishing on a metadata platform and on a marketplace." (I-24)
	Trusted identity	"I would need a public organization, someone in the middle, who could assign a credential saying, 'Yeah, people interacting here are good guys.' Like certification. If you have certification, you are allowed—I do not know—by the data protection authorities. For example, you have passed this exam to be able to operate in a data market because you have demonstrated in advance that you have the security and privacy obligations in place. You are secure, you are performing well, and you are trustworthy." (I-19)

2.3 Facet: Compliance

Second-order code	First-order code	Illustrative excerpt
Compliance fundamental	Compliance as sovereignty facet	"From a legal perspective, we are always very cautious before we actually join this kind of thing [a meta-platform for sovereign data exchange]. For example, when we have vendors in the security domain from certain countries, it can take months to get the contract signed because of all the GDPR clauses and other liability differences between countries. Especially when it comes to potentially privacy-sensitive data, it is something that will be looked into very thoroughly. But it is not impossible; we have signed a contract with a particular company. It just takes more time. That should be a good data governance policy to consider GDPR and DPO stuff." (I-02)
	Provision of compliance mechanism	"Now, the interesting thing is, of course, that when you are going to set up a relationship with a data marketplace, you have, let's say, specific requirements for that data marketplace. So, for example, if some customers are connected to Marketplace A and others to Data Marketplace B, but you want to expose it to as many as possible. But you also have to comply with the different technical requirements or certification requirements for different marketplaces. Of course, it makes it easier for somebody who wants to share or sell the data to have one certification or one set of technical standards. It makes it much easier to share." (I-12)
External compliance	Industry standard	"Yeah, I think, for example, for [the name of the company], we do have a cybersecurity defense team that is a standalone business, and then we also have security for each of the services that we use. So, there are several principles for which those things that we are sharing have to meet—those generic, fundamental cybersecurity principles and then internal principles as well. So, there is always a framework for security, to be sure, and there are several certifications as well in the industry. So, if we are going to respect those certifications and industry standards, there are loads of criteria that I think a metadata platform has to be abreast with so that they can align." (I-05)

Second-order code	First-order code	Illustrative excerpt
	Regulatory compliance	"The core principle is that there is always control by the entitled party. So, the entitled party controls what happens to his data and where it is published. The entitled party has data classifications [shareable vs. non-shareable data]. But for [privacy] protection, there must always be explicit consent [from data subjects that] in line with the Data Governance Act." (I-27)
Horizontal compliance	Data usage audit	"[I need] prove that it [the data product] is only being used as we defined in the contract. There should be some kind of audit or auditability. I want to know that the data is ending up with the buyer, but not somewhere else, like on a new marketplace. Essentially, I want to ensure that it is only being used for the intended purpose." (I-08)
	Data exchange contract	"[…] data marketplace is something where you can put data and where someone can get their data, and you both have a clear contract on how is going to use the data. So, it is not an open market. It is more like a data broker system where a lot of trust and security measures are needed. The consequences of how the data is used are significant. In my view, data marketplaces are invaluable. If we do not have a data marketplace in the future, we will lose." (I-08)
	Dispute resolution	"That is basically what the specific data exchange is all about. It is not so much about us [data providers] transporting the data because the data simply remains local with the owners. What matters to us is that we can record and clarify the rules that we mutually make with each other in order to ultimately share data on a large scale in the future. This way, we know where we stand and also have a place to go if parties do not adhere to the rules for resolving disputes." (I-28)
Vertical compliance	Agreement with operator	"You are introducing, again, an entity that needs to be taken into account when you set up agreements. So, if I need to set up a one-on-one, I now have a data provider who has an agreement with the data market. The market has an agreement with the meta-data market, and the meta-data market needs to have an agreement with the information provider. The more parties you include, the more difficult it can get." (I-03)
	Technical compliance	"I believe compliance also has a technical facet, given that your data should be standardized or normalized. This ensures that the formats are the same and also means the same thing. For example, if you share temperature data in a certain location, you have to specify whether the location is indoors or outdoors. All these kinds of things have to be specified because if you use or interpret the data the wrong way, it has no value. Wrong decisions may be made based on that incorrect interpretation." (I-11)

3. Higher-level facet: Participation

3.1 Facet: Responsibility

Second-order code	First-order code	Illustrative excerpt
Accountable oversight	Liability chain	"If there is a data transfer made between two platforms […] Who is responsible if something goes wrong there? Is it both parties, or just the providing party, or is it the receiving party? […] Sometimes, you stay responsible for it [liability] even if you share it because you gain something

Second-order code	First-order code	Illustrative excerpt
		from sharing the data. You should also be the one liable if something goes wrong, which hurts the consumer." (I-13)
	Penalty	"[…] you are responsible for when you do bad things with your data. So, when you track someone with the data, and it is not allowed because they are just a free civilian in [country], you should get a penalty." (I-06)
	Provision mechanism	"And of course, data marketplaces also need complementors, third parties, that help with the development of, for example, these applications that can be used for the data-based services or to provide additional security services." (I-30)
Interpretation of participation	Active oversight	"If you look at what we are doing now if a data space is going to use our framework, they are using the nodes in our network of all participants and monitor whether participants signed everything. This means that they already have a basic governance of all parties involved in such a data space. And they actually already arranged a lot of components for the baseline. What you need, actually, is a player who does that. What you see now are data spaces such as Catena-X, which are setting up a new association or foundation that will monitor this in a non-profit model above or between the parties. So that everyone can say, okay, we want to add this service as well" (I-27)
	Membership enrollment	"Yes, so I would say, 'OK, I want to become a member of [a data market].' And then maybe you, [a name], and [another name] check if I am trustworthy enough. If I am, then I can participate in [a data market]. This could become interesting; we could have different layers of security. Some people might say, 'OK, I only exchange data with the most trustworthy people, those that have been manually selected.' Like, [a name] has been approved by [another name] and [yet another name], so he is super trustworthy. We believe that if we exchange data with him, he is not going to put it on the dark web." (I-17)
	Product installation	"Not every party is going to write its own software to participate in such a marketplace. But they just use a product that is available, and they install it." (I-23)
	Responsible use of platform and data	"To me, there is no technology solution for that [being control over data in meta-platforms]. In my opinion, being in control means you have trust in a system that its participants and constituents will be using meta-platforms and the data in only acceptable ways, like pre-approved ways or pre-agreed upon ways. I do not think there will be any ability to technically limit that [data usage]. Data, in its nature, is digital. Digital means like there can be a thousand copies without any overhead, without any cost." (I-29)
	Willingness to share data	"Well, the fields where this [meta-platform participation] is very useful, where I think banks are willing to share information, is, for instance, on corruption. So, I think we are very much interested in sharing information about clients who made a bad deal or did a malicious transaction within one bank. We would like to share that information with each other, even on a European level, so that they do not go to other countries so that you are able to distinguish between them. [This is also the same with] bad intermediaries. So, if you got an intermediary who frauded or an accountant who is problematic, then you do not want them to be able to just start a new company and go to another bank and start the practice again. So, I can understand that we say, OK, we want to share information about companies." (I-04)

Second-order code	First-order code	Illustrative excerpt
Responsibility fundamental	Responsibility as sovereignty facet	"So, for example, if you are a meta-platform and a data marketplace gets data products from you and then sells it to data consumers, and then that data marketplace has security issues or goes down, or the data is corrupted, and then the question is that who is responsible for that? Is it the data marketplace itself? Is it the meta-platform?" (I-12)
	Responsibility division to ensure participation	"Who should provide the infrastructure [for sovereignty]? It could be a meta platform, but it could also be a marketplace. But the governance, from my perspective, has to be some cooperative model—an association or a foundation or any other form. If you want to maintain trust, because that is ultimately what this is about, because you will only participate in it if you know that this is reliable, then it must also be reflected in the way in which you organize it together." (I-28)

4. Contextual conditions

4.1 Data type (personal, sensitive data)

Second-order code	First-order code	Illustrative excerpt
"Unlocking" privacy facet	Negative perception of data subject	"Yeah, the thing that is always very critical, of course, is privacy. So, first of all, at least at the moment, we only share metadata. So, it is not linked to individuals. The things that, even if it is metadata, there is the feeling of customers that that it is still not meta-data, but actual data. We have seen this discussion before again when it became public. That indeed [company] shares the location information for the scope it monitors. The first thing that was on the radio, of course, was people discussing. The privacy and whether it was actually personal data or not, or whether you would be tracked now or this kind of thing. And I think a similar discussion has been seen for the COVID safety app, where you can see if you have been close to other people who were infected. That is also only based on metadata, so there is no personal data in there, but still, it always starts from a perspective that people are a bit afraid and a bit suspicious. So that is the thing that is important that if it is shared that it is not there, there we still have some control over who will get this information." (I-02)
	Surveillance capitalism	"I will make a bold statement. When your future business model is based on data of customers, you will not make it. You are tracking them; it means surveillance capitalism. And it nowadays a big issue in Europe." (I-06)
Influence on compliance	GDPR compliance	"So, I think one issue is GDPR and data privacy because you have to be careful. You have to ensure that the data you exchange is compliant with regulations and it is also what our customers expect. The worst thing you can do to someone is to share their data without permission. Imagine if you shared someone's data with another company without being transparent. You are causing damage." (I-10)
	Privacy rule	"You know, the data privacy rules in the EU are quite strict. If they have data that has to do with their customers, for instance, they have to be very careful in sharing this data. They need the right approvals from the customer and so on before they share. So, companies are already a bit reluctant because if they [unclear], then they get fined by the authorization, and that may hurt their reputation. Especially smaller companies also find

Second-order code	First-order code	Illustrative excerpt
		it complex to understand what they can and cannot do. They may have a data privacy officer, but understanding all these is [still] complex." (I-11)
Influence on data control	Control mechanism for data subject	"Someone needs to be in control, and that could be the user. It could be a platform owner. So, based on the more open type of network, I would say that the customer, the end user, should be in control." (I-15)
	Data usage knowledge for data subject	"So, I would like to know, who is checking my content? What is [name of a company] doing? It must be monitored. European laws are working on more transparency in all the algorithms, but I want to know what the big tech is doing with my data. I do not know what my telecom provider is doing with my data. Yeah, it is safe, it is secure, but how are you looking at it? When you go to the hospital and your data is in the doctor's electronic system, and someone is checking your file, they know. When a doctor who is not your doctor checks your file, there is a notification: 'Hey doctor, why are you checking that guy's file?'" (I-06)
Influence on data ownership	Decision about shareable data	"[When involving data of our end-customers], I think we are currently in this situation where we really do not know what data we want to share or do not want to share. There is no clear definition: shareable data or non-shareable data. So, the easiest thing for a bank to do is OK; if we have forced, we will share it. If you have a clear business case and we have that whole bunch of lawyers saying, OK, you can do this, then we are doing it. Yeah, but then it is not something they will play with, or they will say, well, let's put some data in a marketplace. Let me trust and see what happens and is not going to happen." (I-08)
	Difficulty in exercising right of data subject	"The real challenge is how will the data subject—so you and me—exercise our data rights. It is easy to erase data, for example, in the bank, but if those data are sent to a mining company in the EU, [a country], it is necessary to contact this company. 'Please erase my data.' I must have a clue which company it is. So, I have to be informed if you want to pass this thing to sell personal data on the data market platform. Because you do not have just a mining company. You have hospitals. You have telco companies from all over the EU. We are talking about maybe 100,000 controllers, for example. The data subject will not have control over his or her data, and nor the data controller which is selling those data." (I-09)
	Ownership tension	"I always doubt that we have any data at all because we are maintaining the data of our customers. We have data about their activities. You can ask for consent, but that is always a grey area. So, if you collect the data, it always comes from somebody else." (I-03)

4.2 Data type (format variations)

Second-order code	First-order code	Illustrative excerpt
Influence on data control	Complexity in data storage	"The difficult thing about that [controlling data via meta-platforms] is often this: How do you keep that data up to date if it is stored somewhere else? Because often, when you copy it to a database, the data is already outdated. So, how do you ensure that it [a data product] stays up to date and thus retains its value?" (I-21)
	Data format	"Then you have different classifications of data [that need to be controlled]. And you have various kinds of datasets: transaction data, streaming data, and you have static datasets. Within those, you also have a few subvariants.

Second-order code	First-order code	Illustrative excerpt
		You can fill in different colors in your matrices so that you can issue different authorizations for different types of datasets." (I-27)
	Large data size	"So there [in a controlled data exchange use case within the aircraft domain], they look at a test set-up, where you could do a few things with test data. And in this case, they are also looking a bit further because if you want to do that globally, it involves enormous amounts of data. We are talking about terabytes of data; you do not just send that from one place to another. So, how are you going to do that if you want to spread it all over the world? How can you make that data quickly accessible, run analysis on it, and get it back?" (I-28)
	Processed data withdrawal	"Actually, they may not even want to remove everything. They might just want to remove parts of it, and they could have good reasons for that. For instance, maybe GDPR is a factor, but let's not think about personal and sensitive data. Let's just think about normal data. They might not want the data to be available anymore for a certain reason. What does that mean for the entity that has already used that data and has invested in it? Are they required to retrain their models or not? I do not have a solution to this; I just feel this is an area that needs a lot more discussion and understanding. Because I think it will lead to clashes, basically." (I-18)
	Real-time data	"So, we provide a data lake and data hubs, that type of [controlled] services where we gather historical data but also near real-time data for analytics […] Talking about sharing or providing data to others, this goes through standardized reports. So, client reports and regulatory reports, which can be in any format—shared so that the format can be anything from PDFs, JSON, XML, or CSV—really depends on the requirements. And let's say the medium is often a straight point-to-point connection, so it can be through file shares." (I-28)

4.3 Data type (industry-specific data)

Second-order code	First-order code	Illustrative excerpt
Influence on compliance	Compliance practice maturity	The capital markets as a data provider area are fairly mature [...] And what is also interesting is that the financial and capital markets industry is highly regulated. So, they are mature in compliance practices." (I-25)
	High governance standards	"Well, if that is the case [the ownership of data will be kept in for data providers], I think your platform should adhere to the policy of the company. Then, the data provider will enforce or check that the data platform's policies, governance mechanisms, and legal requirements comply with the organization's own. I think you need to set the policy [of data platforms] as stringent as the most stringent customer you want to onboard. If you want to have a bank, you should raise the governance standards to that of the banking industry. If you just say, 'OK, let's go to the telco [standards],' then you have to go to the level of the telco." (I-10)
	Over-regulation	"The second factor [for not adopting meta-platforms] is the over-regulation of the banking industry. There are a lot of regulations on the table. [For example], as a bank, we are still mostly on on-premise architecture. Actually, just yesterday, we had a Board of Directors meeting where we presented the cloud strategy, so it is time to start thinking about moving to the cloud. We are still behind the wall, thinking about our infrastructure.

Second-order code	First-order code	Illustrative excerpt
		Regulations like GDPR and a lot of security regulations make it bureaucratically very hard to start such a project." (I-07)
Influence on data ownership	Lack of capacity for data exchange	"We are a legacy company; we are on the market for 30 years. The technology debt or the legacy issues of improving our IT services do not allow us to think about innovations in so much scope. So, let's speak hypothetically. We see the business value of sharing the data, definitely. I see the value of sharing the data, not our customers' data. But maybe we get data which are more on the macroeconomic scale, and so on. But if we want to sustain innovations and improve our applications, we get limited business and IT resources, and often, we are not even able to tackle the hygienic innovations that we want to do in a timely manner. So, when you are going to do more abstract topics like sharing the data, it will not have so much priority. So, in terms of realization, this is one factor [that hindrance adoption of meta-platforms]." (I-07)

4.4 Business data exchange setting

Second-order code	First-order code	Illustrative excerpt
Influence on compliance	Cultural knowledge gap	"We have a different culture when it comes to data, so it looks like the EU inhabitants are very keen to keep their data for themselves. In the US, it is already less, they said. It is proposed that in Asia, you do not even have a choice. How do you manage these cultures and all these perspectives? If everything is for sale [in a meta-platform that aims for cross-border data exchange]?" (I-03)
	Different liability	"From a legal perspective, we are always very cautious before we actually join this kind of thing [a meta-platform for sovereign data exchange]. For example, when we have vendors in the security domain from certain countries, it can take months to get the contract signed because of all the GDPR clauses and other liability differences between countries. Especially when it comes to potentially privacy-sensitive data, it is something that will be looked into very thoroughly. But it is not impossible; we have signed a contract with a particular company. It just takes more time. That should be a good data governance policy to consider GDPR and DPO stuff." (I-02)
	Different national law	"I think sharing data within the European Union will be as free as possible. However, sharing data outside of the European Union will be very complicated. Sharing data with countries outside the European Union is very strict, but sharing data within the European Union? If you want to, just share it; there is no problem. You have this legal ground." (I-09)
Influence on data control	Alignment of data marketplace architecture	"[So, you see a potential risk there? Even though the platform promises you full control, it might be, due to even technical differences between the underlying data marketplaces, difficult to actually achieve. Do I understand you correctly?] Technically and legally, yes. You have your conditions for how a user can use your platform, but Marketplace A has different conditions than Marketplace B. How do you reconcile all their terms and conditions? With just one click?" (I-24)
	Data provenance difficulty	"I think this value-oriented approach to data will be a significant strategy in the future. To be transparent towards our customers, I want to show the full pipeline. For example, I want to show the full pipeline about how their data is used. But, if I have a blind spot when I share data with some metadata platform, it will not be very transparent." (I-07)

Second-order code	First-order code	Illustrative excerpt
Influence on data ownership	Data marketplace selection	"You will investigate which channel [data marketplace] is loyal and has good processes. If a channel, for instance, is ruled by mafias, you will try to avoid it because you will be robbed or you will lose your credibility. At this stage, this is an extreme paradigm. But as long as you can evaluate all these different data marketplaces, which are channels to reach the market, and you can find bilateral agreements with them— even if the agreement with each one may differ, it does not matter. You can have this contractual relationship with many of them, or all of them, that can benefit your business in one way or another. And yeah, your product is in as many channels as possible." (I-01)
Influence on responsibility	Data marketplace evaluation	"And then you have to evaluate what a meta-platform is because I think that the meta-platform will not only have to create different APIs for each data marketplace, but it also has to understand the different rules of operation. How are data available? How are data evaluated? Who has liability if the transaction or the data at the end of the day is not of adequate quality? What are you going to do, return the data?" (I-01)
	Domination of meta-platform	"[…] what makes me doubtful is such a meta-platform will always be coupled to commercial aspects and capitalistic systems which are inherently non-democratic." (I-29)
	Responsibility division	"It is definitely tough. It comes down to who is responsible for providing certainty about the data, right? So, who is responsible for setting the data limits? Who is responsible for proving that the data is secure, that the data is of quality, that the ownership is correct? That the descriptions are correct? That the meta-data is correct? So, the question is, where do you place those responsibilities? For example, if you are going to create an aggregation of different data marketplaces, who is responsible for providing the lineage from supplier to buyer? If you have two stops, which are two separate entities, who is going to be responsible for showing the data flow from customer to supplier? We have two parts in the chain. Yeah, I do not know; It is an interesting thing to think about. And I think that is one of the hardest parts, also for us internally. But I think externally, it will be even more complex: How do you prove it, and how do you secure it, and where does the responsibility lie? That is the most important thing. Who is responsible for making sure that it is doing OK?" (I-12)

4.5 Organizational size

Second-order code	First-order code	Illustrative excerpt
Influence on compliance	Liability for large organization	"So, of course, my biggest fear is just consumers not trusting us anymore, right? Because if something goes wrong. That is bad if we are making a mistake, but if a mistake is made because we chose to share data with a third party, that is even worse. Maybe we should not have shared the data in the first place. That is bad press. And we should never forget who generates the data. It is you or me making a payment online, right? […] If I find out my bank has shared my data. I am going to look at my bank from a reputational point of view, not a third party. Because the third party probably does not have the resources to pay damages. It is the bigger player in the market that is always going to bear the brunt of it." (I-13)
	Understanding legal requirement	"You know, the data privacy rules in the EU are quite strict. If they have data that has to do with their customers, for instance, they have to be very careful in sharing this data. They need the right approvals from the

Second-order code	First-order code	Illustrative excerpt
	for smaller company	customer and so on before they share. So, companies are already a bit reluctant because if they [unclear], then they get fined by the authorization, and that may hurt their reputation. Especially smaller companies also find it complex to understand what they can and cannot do. They may have a data privacy officer, but understanding all these is [still] complex." (I-11)
Influence on data control	Lack of capability for smaller company	"Larger organizations have those [data exchange] capabilities. The smaller ones can rely on external parties, for instance, for data storage." (I-21) "But that is why we are starting [data exchange] with large players who want large datasets and can deliver large datasets. Because of that, you also have the liability taken seriously. The chances of violation are smaller than with many small players. [With smaller players], there is less control." (I-27)