INNOPAY SITRA

Data sovereignty and soft infra-structure: key enablers of the European data economy

1 oktober 2020

innopay.com

White paper
Data sovereignty and soft infrastructures: key enablers for the next phase of the European data economy

As underlined by the new European data strategy, the European Commission wants to make Europe fit for the digital age and unleash the full benefits of better data usage for everyone. We wholeheartedly support this ambition. However, in order to achieve it in practice, we believe that it is necessary to make data sovereignty a design principle, develop a soft infrastructure for data sharing and focus on adoption of this infrastructure and the services built upon it. In this paper, we outline how this will accelerate the execution of the data strategy, the creation of common European data spaces and build a solid and sustainable foundation for the next phase of the data economy.

The European Commission (EC) has clearly expressed its aim to unleash the benefits of better data usage for everyone. These benefits not only include greater productivity and more competitive markets, but also improvements in health and well-being, the environment, transparent governance and convenient public services.

In a society where individuals are generating ever-increasing amounts of data, much of which is held by a handful of Big Tech firms, the EC has introduced the European data strategy. It outlines its vision for placing the interests of the individual first in accordance with European values, fundamental rights and rules about the way in which data is collected and used. These common rules and efficient enforcement mechanisms should ensure that:

- Data can flow within the European Union (EU) and across sectors under control of people, businesses and public organisations
- In particular personal data protection, consumer protection legislation and competition law are fully respected
- The rules for access to, and use of, data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place.

The new data strategy aims to make Europe a leader in a data-driven society. It seeks to create a single market for data that will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations.

At Sitra and INNOPAY, we fully support this ambition. However, we believe that it can only be successfully achieved if data sovereignty and a soft infrastructure for data form the basis for implementing the data strategy.

Data sovereignty as a design principle

Under the new strategy, people and organisations will have not only legal but also functional control of their data and will easily be able to re-use their data elsewhere. This concept is also referred to as 'data sovereignty'.

Data sovereignty expresses an organisation's or individual's self-determination with regard to their data; people, businesses and governments are able to control who has access to their personal or professional data and under what conditions. It enables the empowerment of individuals and organisations alike. And there is no discrimination between personal and non-personal data. After all, organisations' data-driven services are ultimately mostly consumed by individuals, and the usage of personal data improves the quality of those services. It could involve two businesses sharing data according to a mutual agreement, or it could relate to a public organisation's regulated access to certain information, for example.

Today's common approach to data life cycle management and design tends to be from the perspective of "data might also be shared". However, the complex issue of data control and consent cannot be integrated into applications and interfaces as an afterthought. That is why, at Sitra and INNOPAY, we strongly recommend that data sovereignty should be made an underlying key design principle. This means shifting the focus during the development stage to "how the data will be shared", including the basic dimensions of what, when, who and why as well as how.

The reasons why

There are several reasons why data sovereignty should be made a key design principle.

Firstly, data sovereignty works on all the different levels and for all the different roles in the data-sharing ecosystem. It works both with respect to the source holding the data on behalf of people and businesses (e.g. telecoms, utilities, banks, trading partners, etc.), by enabling consent to be given (and subsequently to be withdrawn) for the use of data for a specific purpose, but also for the sharing of data with other authorised parties, and with respect to all other parties with which a person or organisation decides to share their data (when the data comes from the initial holding source). Therefore, data sovereignty holds the key to a free flow of data for all involved.

Secondly, it serves as an easy-to-follow and actionable guideline. It is easy to grasp, yet encompasses many relevant aspects: legal, interoperable, functional, technical, governance, privacy, security, business models, etc.

Thirdly, a commitment to data sovereignty will allow European values – in particular with respect to democratic principles, personal data protection and privacy, consumer protection and fair competition – to take centre stage. Furthermore, it will set the EU's data model apart from the other two dominant geopolitical views: 1) that individuals are market actors who are solely responsible for sharing their data (e.g. by clicking on "I agree" as the only viable option), which creates a 'winner takes all' platform-based market, and 2) that the decision on what data is shared is state-led. In fact, it is the only robust answer if the aim is to create a human-centric data economy and steer away from the ever-increasing dangers of 'microtargeting', which is having a paralysing effect on society and the democratic debate.

Lastly, the right foundations are in place, since data sovereignty is already embodied in EU legislation; the General Data Protection Regulation (GDPR) has given people the 'right' to data sovereignty. The next and vital step is to now also give them the practical and functional means to exercise that right, including tools to manage, share and exploit their data and also ways to monetise/compensate for data benefits.

The benefits of data sovereignty

By making data sovereignty a central design principle of the data economy, we can realise significant benefits, including:

- People can easily switch providers, and enable their data to be commercialised by businesses (and also receive a fair share of the benefits)
- Businesses can trade more easily, securely and cost-effectively with other businesses (even those outside their regular physical supply chains)
- All parties holding data can offer consistent functionalities and ways of working to their customers, suppliers and employees
- The free flow of data will increase, thereby stimulating more and faster commercial innovation to create new kinds of data-enabled business models that generate new services
- The dominance of the Big Tech giants will be reduced since customer data will no longer be 'locked in'. This will level the digital competitive playing field, making it easier for other organisations to enter the market with innovative products and solutions, and creating a healthier growth climate for start-ups and scale-ups

Two examples of the benefits of data sovereignty in practice

On the road:
Imagine you and your family are taking a summer trip to Grandma's holiday cottage. Your rental car has an integrated satnav system that communicates with your mobile devices, so you can receive route suggestions, updates about the remaining travel distance, estimated time of arrival and any congestion ahead. This is all fairly convenient, but the data remains with one service provider and its use is therefore limited. In contrast, in a truly 'data-sovereign' economy, you have full control over what your data may be used for and the benefits you receive in return. For example, if you're willing to give your consent for your data to be shared between data ecosystem players, you will not only be directed to a local restaurant when you're ready to take a break, but may also receive personalised offers or discounts on your meal. If you wish to do your bit for the environment, you may choose to give consent for your trip data to be anonymised and used for research purposes to study emission levels and contribute to reductions. And depending on whether you want to surprise Grandma or not, you may decide to give consent for your trip data to be shared with your contacts so that they can track your progress with a little help from Alexa or suchlike. Data integration issues have already been solved using productised data sources built on top of existing interfaces, paving the way for the development of new business models that add real value.

Social networks:
Currently, it can be difficult to switch to a new social network because it means leaving all your existing contacts 'behind'. This is restricting healthy competition from new social network solutions, since it makes it extremely difficult for them to attract enough members to gain critical mass. Data sovereignty would enable you to 'take' your contacts with you whenever you decided to move to another platform, leaving you free to take advantage of innovative or improved features and services from new entrants.

Soft infrastructure for data sharing

Data is essential for the creation of new business models for data-driven innovations and services. However, there are two things standing in the way of access to sufficient data.

One is a growing unwillingness to share data due to privacy and security concerns. The realisation is slowly dawning that so much data is in the hands of so few. Big Tech giants such as Facebook, Google and Amazon are using people's data for their own benefit, yet giving nothing (or very little) in return. Besides that, this leaves large groups of people open to undesired and often imperceptible influencing and numerous privacy issues. So, people are slowly beginning to question the situation: 'Is this the way I want my data to be dealt with? Isn't it my data? And shouldn't I benefit from it?' But as things stand right now, the only choice they have is to take negative action, such as deciding to leave Facebook or refusing to share their data... and no longer being able to make use of certain services as a result.

This leads on to the second obstacle: the inability to share data due to a lack of interoperability – the ability of different systems to work in conjunction with each other and for devices, applications or products to connect and communicate in a coordinated way, without extra effort from the user.

One of the major consequences thereof is the increasing lack of data; organisations often have only partial views of their customers, leaving them prone to making ill-informed decisions. Moreover, access to data is required in order to use – and benefit from – artificial intelligence in a truly responsible way.

We believe that both of these obstacles can be overcome by a common, decentralised way of doing things related to the data of people, businesses and governments.
A standardised approach based on functional, legal, technical and operational agreements will clearly define how individuals and organisations can give and withdraw their consent for their data to be accessed, used and shared with authorised third parties, and how they can manage all their data irrespective of where it is kept.

The resulting framework of standardised agreements can be called a digital 'soft' infrastructure – 'soft' because it is not visible or tangible, and 'infrastructure' because it is very robust, powerful and built on convention and adherence. In fact, it is not so different from what we already have for roads, railways and pipelines (which are examples of 'hard infrastructures') and

for payments and telecommunications (which are examples of 'soft infrastructures').

Supporting cross-sectoral data sharing

If the aim is indeed to create a 'digital single market', it is essential to focus on precisely – and only – what is needed so that the soft infrastructure for data can be used by all sectors and applications. In other words, the basic set of agreements should be designed around the smallest possible 'common denominator' needed by all sectors in order to deal with data in this new era. Sector-specific agreements can then be implemented on top as necessary. Only then can cross-sector interoperability be ensured, based on the same underlying data-sharing mechanisms. After all, we don't have separate roads for sector-specific use by the agricultural, retail and chemical industries, for instance!

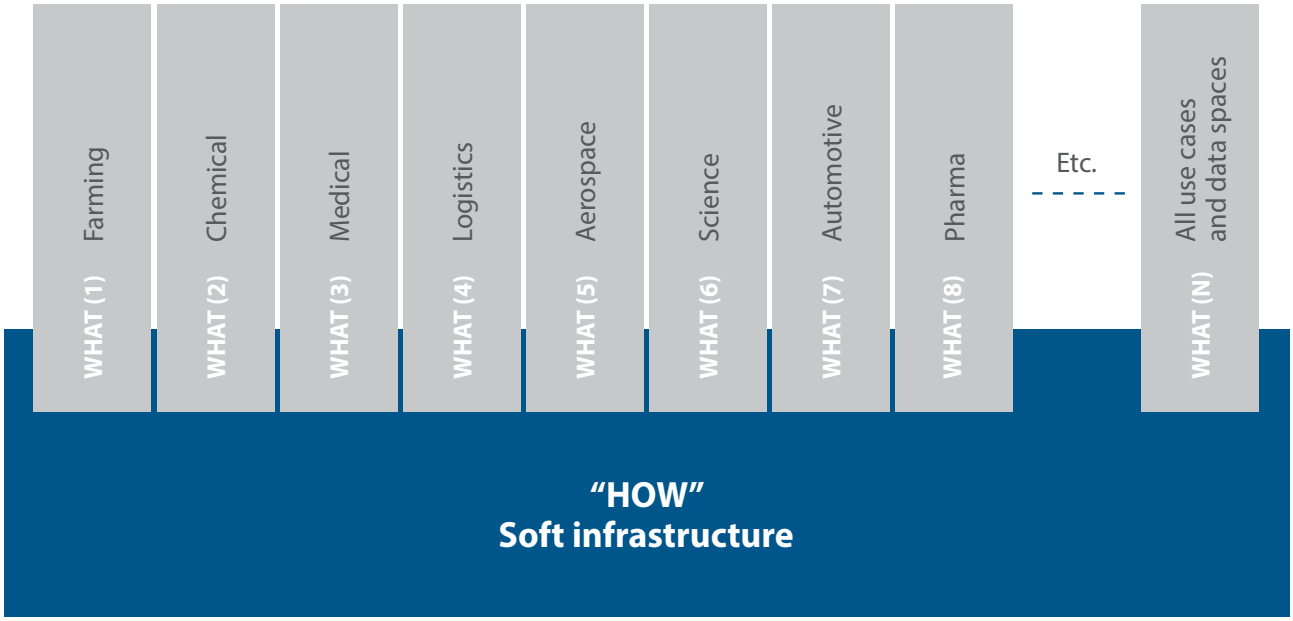

Figure 1: Generic agreements (the soft infrastructure) plus sector-specific agreements

There are currently several ongoing European initiatives or projects that have defined or are defining soft infrastructures. For example, a soft infrastructure or *afsprakenstelsel* (the Dutch concept of a scheme or trust framework) can already be found in payments, securities, GSM and logistics (e.g. iSHARE), where they form the basis for globally interoperable and trusted services. The Data Sharing Coalition is currently aiming to develop a generic common soft infrastructure or afsprakenstelsel for all industries. The architectural models of International Data Spaces Association, iSHARE and IHAN have lots in common and could easily augment each other.

In the European data strategy, data spaces (sectoral data initiatives) and the interoperability thereof play a central role. Extensive research into data sharing was conducted in the Netherlands in 2018 which led to the '9 block' analytical framework as well as the Dutch Vision on Data Sharing between businesses.

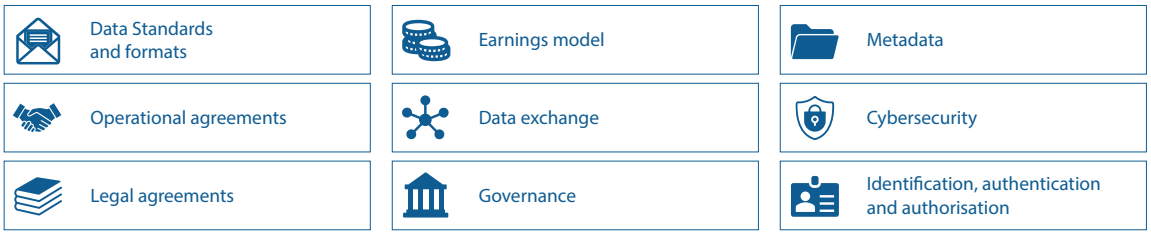

Figure 2: 9-block framework for data sharing

The vision revolves around harmonising (over time) the nine dimensions of data sharing across existing and new data-sharing initiatives, thereby achieving de facto interoperability and data sovereignty across sectors (spaces).

Focus on adoption first

Although the EU is at an advanced stage in terms of knowledge and capabilities related to data technology, it has been less successful at commercialising data technologies. This has resulted in the region lagging behind some other parts of the world in terms of the contribution to the economy. In order to close that gap, the European data economy and its ecosystems need new kinds of data-enabled business models that create new services. Data sovereignty can provide the necessary direction for this. However, it will require the efforts to be prioritised; all activities (and funds) should be channelled towards the same goals rather than taking a fragmented approach. Moreover, the focus should be more firmly on facilitating and stimulating its adoption and less on the underlying legal or governance-related discussions.

Resist the temptation to focus on legal issues

We feel it is important to emphasise here that legal frameworks are not the most urgent issue in this process. After all, frameworks such as eIDAS, PSD2 and GDPR already exist. Using such legislation as a starting point, and provided that the 'how' (interoperability, trust, standards, governance, level playing field, certification, adherence, etc.) is clearly distinguished from the 'what' (sector use cases/applications), means that only the application is sector-specific and will require additional implementation guidelines and associated governance.

Resist the temptation to focus on technology

A common pitfall with initiatives of this kind is that the focus is immediately directed towards the development of new technologies (e.g. blockchain, etc.). On the one hand, policymakers think these technologies are necessary to solve the issue, and on the other hand the available funds are often gobbled up by 'next big thing' projects piggybacking on the latest hype. However this is not only a technology issue; it is equally about functional, legal and operational agreements.

iSHARE and IHAN have already shown that building such a soft infrastructure can be done today. It is primarily a matter of extending current internet standards with a standardised way to handle identity, data semantics and consent management. This is what has been missing from the HTTP stack from its very beginnings.

Resist the temptation to focus too narrowly on governance

It is difficult to create a common governance framework when there is a lack of common concepts and semantics. Therefore, it is our view that the EC should wherever possible try to avoid regulating per sector ('point regulation' or regulation per use case) and focus on principle-based regulation instead. After all, the adoption of telecoms, payments and internet is not defined per sector. What is needed is a more holistic view of data governance from an EU-wide perspective – across all business services, business processes, information, applications and technology.

In the European data spaces discussion, we've noticed that the focus rapidly shifts to 'new entities' (the 'intermediaries') that will provide data services in the new European data ecosystem, and how they will need to be certified. We strongly advise against focusing on regulating specific roles and responsibilities of these intermediaries at such an early stage, firstly because it

diverts attention from the real aim: to co-create, organise and stimulate adoption of decentralised access to and exchange of data while maintaining trust, security and interoperability.

Secondly, we know from first-hand experience that creating a soft infrastructure results in the description of certain (certified) roles in the data ecosystems. Some of these roles are fluid and can be fulfilled by different participants at different times in the same data ecosystem. Once a soft infrastructure is in place, it is a clear framework enabling all concerned to either use the framework, choose to play a certified role within the framework, or build intermediary services on top of it. Moreover, intermediaries will eventually be required to comply with the mandated data sovereignty and become interoperable by default. This will result in a much more organic and fair system and will create a level playing field for all involved.

In other words, governance efforts should be directed at organising a viable ecosystem of public and private organisations in order to create and maintain such a soft infrastructure holistically, on an EU level.

An example of how an *afsprakenstelsel* supports the roles and the governance

An organisation can be a data provider one moment and a data consumer the next. Other roles serve a formal function throughout the ecosystem and are thus subject to strict certification, e.g. the role of an 'Authorisation Registry' in the iSHARE (www.ishareworks.org) *afsprakenstelsel* or 'trust scheme'.

Communication is key

Data is the new fabric of society and we are still learning how to deal with it. A crucial, yet often undervalued aspect of new advancements is how to communicate them and build awareness among end users, and this holds very strongly for the European data sovereignty infrastructure. After all, this is a new concept which will manifest itself in lots of B2C, B2B and B2G services.

We believe that it is possible to educate businesses and the global population on the benefits of new data-related behaviour, just as has been done before with mobile telephony, payments and messaging, for instance. In order to do this, it is important to showcase the trustworthiness, relevance and value of services made possible by data sovereignty. Governments can play a significant part in this by supporting and accelerating the creation of innovative business models and ecosystems offering new data sovereignty-related services, particularly in sectors with existing demand, regulation and public involvement.

According to Sitra's 2019 report, European businesses are hesitant about the opportunities afforded to them by the data economy. Likewise, a lack of expertise is deemed to be an obstacle to making use of data. Therefore, it is essential to support businesses in renewing their business models and helping them to understand that data sharing is the key that will enable them to become part of data ecosystems which will generate future growth. Digital Innovation Hubs (DIHs) and common European data spaces can play a role in this and collectively provide relevant training, prototyping and funding, especially for SMEs.

Trustworthiness of a soft infrastructure will be safeguarded via external certified parties, authorised and trusted bodies who can give access to data services.

Conclusion: The European Commission can play a role in enabling the next phase of the data economy

The European Commission wants to unleash the full benefits of better data usage in the EU and create a thriving human-centric data economy. Based on European values and the concept of data sovereignty, the European data strategy provides the necessary direction for achieving this.

The task now is to create a soft infrastructure for data sharing based on sound consent, data transfer and trust mechanisms. The infrastructure must work for every person, business and government in the EU, and in terms of standardisation must go beyond regulation and governance alone. In our opinion, we have today reached a similarly pivotal point in history as in the early days of the internet, just before standards such as TCP/IP were agreed.

We believe that the EC can play a key role by establishing this EU soft infrastructure or trust framework for cross-sectoral data governance. This should be built around easy-to-grasp and actionable guidelines encompassing all relevant aspects: business, legal, ethical and technical.

The quickest and most effective regulatory intervention in order to ensure this succeeds in practice is for the EC to make data sovereignty mandatory for businesses and the public sector in the EU over the coming decade. The aim should be to nudge businesses and governments (and their IT providers) into giving their users, customers and people tools to manage, share and exploit their data. Only then will the goals and objectives be addressed holistically across all application development projects and their deployment into production. This will stimulate data sharing not only within sectors, but also across sectors.

Ultimately, this will accelerate the execution of the European data strategy and ensure that the EU becomes a leading role model as a society empowered by data.

Glossary of data sharing

Afsprakenstelsel
A uniform set of agreements or scheme (functional, legal, operational, technical) that enables organisations and individuals to give each other access to their data.

Authentication
A process that is used to confirm that a claimed attribute of an entity is actually correct.

Authenticity
In the context of information security, authenticity refers to the truthfulness of information and whether it has been transmitted or created by an authentic sender. Authenticity can be achieved, e.g. by digitally signing a message with the sender's private key. The recipient can verify the digital signature with the matching public key.

Authorisation
The process of giving someone or something permission to do something, for example to gain access to services, data or other functionalities.

Authorisation Registry (AR)
An authorisation registry manages Records of Authorisation (and, if relevant, Records of Delegation) so that Participants in the Collaborative Solution can verify whether a Data Consumer is authorised to access a specific Data Asset.

Bilateral Agreement
Covers agreements between two data-sharing actors, ranging from legal obligations to non-binding agreements of principle allowing them to share data.

Certificate Authority
A trusted third-party entity issuing digital certificates (e.g. X509-certificates) or host services to validate certificates issued.

Collaborative Solution
A solution in which multiple stakeholders work together to facilitate many-to-many data sharing. The solution can make use of multiple models (i.e. platform and scheme).

Consent
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Credentials
In the context of information security, credentials are used to control access of someone or something to something, for example to services, data or other functionalities. The right credentials validate (i.e. Authentication) the identity claimed during Identification.

Data Asset
A data resource, controlled by an organisation to generate revenue, e.g. a system, application output file, document, database, web page.

Data Consumer
An individual, group or application that receives data in the form of a collection. The data is used for query, analysis and reporting.

Data Governance
A system that employs interoperability components (standards and policies) to ensure the acceptable use and high quality of data within a specific ecosystem. Manages the availability, usability, consistency, integrity and security of the data used.

Data Portability
The ability of data to be easily moved across interoperable applications and domains. The legal right to data portability, granted in some jurisdictions to individuals, can be delivered through a range of technical mechanisms and varies in scope according to the jurisdiction. Our principle of data portability encompasses the ease of both access to and reuse of data.

Data Product
A pre-defined set of information required for providing a service. May consist of attributes of one or several data sources.

Data Provider
Any person or organisation that makes data available.

Data Self-determination
The capacity of an individual or organisation to control who has access to their personal and business data and under what conditions (see also: Data Sovereignty). This includes data in machines and other 'things'.

Data Source
A source of data assets that is being exposed to data consumers by data providers. The role responsible for collecting, storing and controlling personal data which persons, operators and data-using services may wish to access and use.

Data Sovereignty
The capability of an individual or organisation to be entirely self-determining with regard to their personal and business data (see also: Data Self-determination). This includes data in machines and other 'things'.

Delegation
The act of designating someone or something to act for another or to represent others. In a data-sharing scheme, this means that one party designates another party to share or consume data or to issue authorisations on their behalf.

Ecosystem
The overall system created by the activities and connections of a set of actors and infrastructure interacting according to a common set of rules. Multiple ecosystems can exist, overlap, and collaborate.

eIDAS
An EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. This regulation covers important aspects related to electronic transactions, such as qualified electronic certificates. eIDAS provides a safe way for users to conduct business online.

Governance
A system of rules, practices and processes used to direct and manage an ecosystem. The four pillars of good governance are transparency, fairness, accountability and security.

Identity Provider
An intermediary party offering services to create, maintain, manage and validate identity information for parties that share data within a collaborative solution (See also: Collaborative Solution).

Individual
A natural, living human being.

Interoperability
The ability of different systems to work in conjunction with each other and for devices, applications or products to connect and communicate in a coordinated way, without effort from the person.

Levels of Assurance
Within online authentication, depending on the authentication protocol used, different levels of assurance give the server different degrees of certainty about the client's identity. Depending on parameters such as the quality of the registration process, quality of credentials, use of biometrics or multiple authentication factors and information security, an authentication protocol can provide a server with high or low confidence in the claimed identity of the client. For low-interest products, a low level of assurance might be sufficient, while for sensitive data it is essential that a server is confident that the client's claimed identity is valid.

Metadata
Information about data that helps describe, structure or administer that data.

Person
The role of data subject as represented digitally in the ecosystem. Persons manage the use of personal data about themselves, for their own purposes, and maintain relationships with other roles.

Platform
A platform facilitates the exchange of value between two or more parties, with multiple parties interacting through the platform.

Role
function or set of responsibilities for a particular purpose.

Scheme
A common set of multilateral agreements that facilitates standardised and decentralised data sharing directly amongst participants.

Self-sovereign Identity (SSI)
A model for managing digital identities in which an individual or organisation has sole ownership over the ability to control their accounts and personal data without the need for intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.

Structured Data Assets
Data that adheres to a predefined data model which is primarily useful for interpretation by machines.

Trust Framework
A structure that lets people and organisations do business securely and reliably online.

Unstructured Data Assets
Data that does not have a pre-defined data model or is not organised in a pre-defined way, making it primarily interpretable by humans.

About Sitra

Sitra is a future fund and an agent for societal change, with deep roots in the Finnish innovation field. Sitra collaborates with partners from different sectors to research, trial and implement bold new ideas that shape the future. The independent fund has been commissioned with the task of probing the future and promoting qualitative and quantitative economic growth.

This paper has been compiled as a part of Sitra's IHAN® project, which lays the foundation for a fair data economy in which successful digital services are based on trust and create value for everyone.

About INNOPAY

INNOPAY is an international consultancy firm specialised in digital transactions. We help companies anywhere in the world to harness the full potential of the digital transactions era.

We do this by delivering strategy, product development and implementation support in the domain of Digital Identity, Data Sharing and Payments. Our services capture the entire strategic and operational spectrum of our client's business, the technology they deploy, and the way they respond to local and international regulations.

We have grown from strength to strength since our foundation in 2002 and operate from our offices in Amsterdam, Frankfurt and Berlin. Our head office is located in The Netherlands, where we have the #1 market position.

We are a founding member of Holland FinTech, a financial technology hub with links to the rest of Europe, the US, the Middle East and Asia. Our team consists of over 60 experienced domain experts who regularly advise a wide range of global organisations.

INNOPAY

World Trade Center F-tower
Strawinskylaan 381
1077 XX AMSTERDAM
The Netherlands
T: +31 20 65 80 651

Taunustor 1
(TaunusTurm)
60310 Frankfurt a.M.
Germany
T: +49 (0) 69 50 50 60 4350

info@innopay.com
www.innopay.com