iGrant.io®
Your data, your choice.

A Sustainable Data Exchange

An ethical approach to sharing personal data

July 2021

Acknowledgements

iGrant.io acknowledges the following organisations in the development of concepts outlined in this white paper:

Make it happen, make it right! mydata.org

NGI ESSIF-LAB

Executive summary

This white paper looks at how businesses can leverage and legally capture data beyond what is accessible within their own data sources. It delves into a decentralised data exchange model based on self-sovereign identity (SSI) that enables companies to exchange data in a transparent, secure and privacy-centric manner using verifiable data agreements.

The paper addresses how businesses can:

- Increase access to high quality personal data for personalisation and successful digital transformation
- Expand personal data assets using a scalable platform that is compliant to data regulation and enables timely access to relevant data
- Enable a transparent and human-centric data economy in which both individuals and businesses benefit

If you are a CxO or business developer seeking new business opportunities, a product manager, a security or privacy professional, an investor or company director with risk management or sustainability concerns regarding the use of data, the iGrant.io Data Exchange Platform should be of interest to you.

Data is not oil

“

*Data is **not** oil - it is a renewable resource that can be pooled, shared, reused ... we want to enable businesses to make the most of data - while securing that we can trust that we are protected from misuse*

In 2006, Clive Humby, a British mathematician and entrepreneur in the field of data science and customer-centric business strategies, coined the phrase *“Data is the new oil”.*

Later, Michael Palmer expanded on Humby's quote:

> *[Data is] valuable, but if unrefined it cannot really be used. [Oil] has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so, data must be broken down and analysed for it to have value.*

In May 2021, Margrethe Vestager, Executive Vice-President European Commission, tweeted:

> *Data is not oil - it is a renewable resource that can be pooled, shared, reused ... we want to enable businesses to make the most of data - while securing that we can trust that we are protected from misuse*

This statement heralds a new approach to the use and re-use of data, one that is greener, more secure, fairer and altogether more sustainable.

Contents

Introduction

> *The idea that many businesses rely heavily on data to produce or market goods and services is not new.[1] Indeed, even in 2018, four of the six top companies in market valuation — Amazon, Alphabet, Facebook, and Alibaba[2] — based their business models on the use of data to optimize advertising.[3]*

> *Digital advertising spending worldwide – which includes both desktop and laptop computers as well as mobile devices – stood at an estimated **378 billion U.S. dollars** in 2020. This figure is forecast to constantly increase in the coming years, reaching a total of **646 billion US dollars** by 2024.*

Business executives are unanimous in recognising data as one of the most strategic assets in the digitalisation journey that will enables companies to monetise their data assets in a legal, ethical and sustainable manner.

Companies invest in digitalisation to enhance decision making, improve operational efficiency and create new business opportunities. As digital systems are adopted for everyday transactions, companies are improving their engagement and relationship with the customers who share their data with them. It is immensely valuable for businesses to better understand known and anticipated consumer preferences derived from insights provided by consumers themselves. These can drive the development of new product and service strategies, such as the improved personalisation of marketing campaigns.

Digitalisation and business transformation is expected to attract 6.8 trillion USD of investment[4] between 2020 and 2023 which will go a long way towards driving the new data driven economy. A digitalisation programme requires data – not just any data or big data but access to the right data, much of which is personal. Access to the right data helps progress a company's digital transformation legally and ethically as well as showing customers human-centric responsibility, reliability and respect for their personal data.

This paper describes the requirements for a sustainable data exchange and outlines its key characteristics.

[1] S. Gandhi, B. Thota, R. Kuchembuck, et al., “Demystifying Data Monetization,” MIT Sloan Management Review, Nov. 27, 2018, https://sloanreview.mit.edu; J. Akred and A. Samani, “Your Data Is Worth More Than You Think,” MIT Sloan Management Review, Jan. 18, 2018, https://sloanreview.mit.edu; and M. Farboodi, R. Mihet, T. Philippon, et al., “Big Data and Firm Dynamics,” Centre for Economic Policy Research, January 2019, https://cepr.org.

[2] “The 100 Largest Companies in the World by Market Value in 2018,” Statista, www.statista.com

[3] José Parra-Moyano, Karl Schmedders, and Alex “Sandy” Pentland, 9 June 2020, What Managers Need to Know About Data Exchanges: https://sloanreview.mit.edu/article/what-managers-need-to-know-about-data-exchanges/

[4] https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/

The data access challenges

> *The IDC FutureScape for Worldwide Digital Transformation predicts:*
>
> *Accelerated DX Investments Create Economic Gravity.*
>
> *The course to its digital destiny with **65%** of global GDO digitalized by 2022 and will drive over **$6.8 trillion** of direct DX investments from 2020 to 2023.*[5]

The process of personalising a service, involving even the most basic data set, may not have either access to the relevant data or have the requisite legal basis for usage. Any business wishing to protect their digitalisation investment must make sure that they are on the right side of the law in their use of personal data. To ensure that people continue to say 'yes' to sharing their data, there are three principal challenges that need to be addressed

(1) Regulatory compliance

Global data protection and privacy regulations, such as the GDPR, are specific about the terms and conditions that determine how businesses are allowed to make use of personal data. For example, a common aspect of all legislations is that only business relevant data may be processed; data that falls outside that definition must be deleted or the company must seek additional consents from the individuals whose data is being processed.

(2) Lack of consumer trust

Consumer trust is vital to the success of any business. Today, most companies either collect and process data from their customers and employees, or buy data from aggregators with no involvement of the individuals whose data is being traded - or both. Neither situation is satisfactory and from socio-economic and legal perspectives, this process can be considered as broken and one of the reasons for the gradual erosion of consumer trust.

[5] IDC FutureScape: Worldwide Digital Transformation 2021 Predictions, 29 October 2020

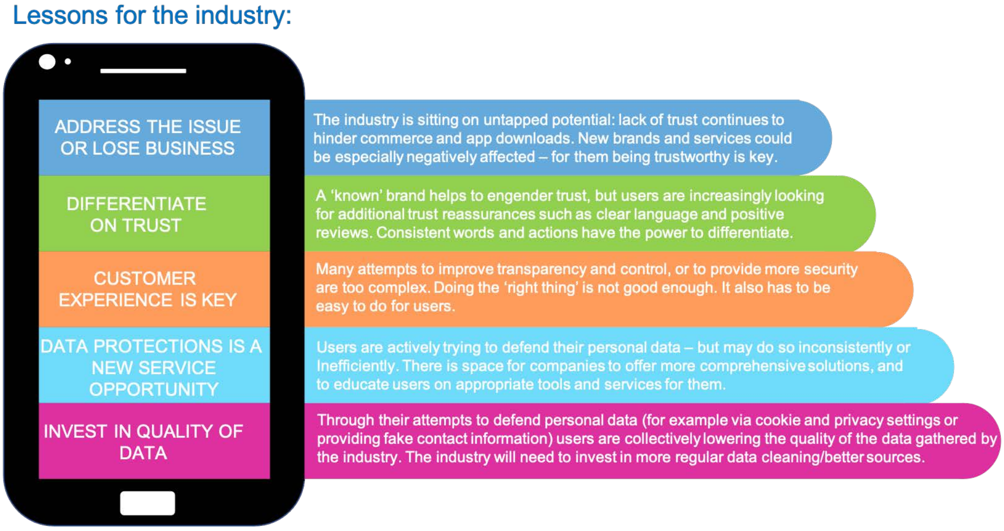
> “
> *Consumer trust is vital to the success of any business. However, research shows that a majority of people do not trust companies, large or small, with their data and, when given the chance, they may opt out from providing consent to data sharing or simply provide fake data to avoid the issue altogether.*

Another factor is the backlash against corporate misuse of data and the lack of transparency in the way personal data is used. Research shows that a majority of people do not trust companies, large or small, with their data and, when given the chance, may opt out from providing consent to data sharing or, lamentably, provide fake data to avoid the issue altogether.

(3) Data quality

One of the responsibilities incumbent on data-centric businesses is to ensure the quality of the data held. Relying or, worse still, propagating inaccurate data is not only illegal but also has the potential to be extremely harmful to both the business and the individual affected. Knowing that data comes from a trusted source and has not been tampered with goes a long way to assuaging those issues of misrepresentation.

For any business, new types of personalised services with advanced analytics building new AI-driven digital actionable insights further underpins the need to ensure high data quality. Major investments in accumulating, storing and processing big data goes haywire if businesses fail to ensure the data that goes in is fake or is wrong.



Lessons for the industry:

ADDRESS THE ISSUE OR LOSE BUSINESS

The industry is sitting on untapped potential: lack of trust continues to hinder commerce and app downloads. New brands and services could be especially negatively affected – for them being trustworthy is key.

DIFFERENTIATE ON TRUST

A ‘known’ brand helps to engender trust, but users are increasingly looking for additional trust reassurances such as clear language and positive reviews. Consistent words and actions have the power to differentiate.

CUSTOMER EXPERIENCE IS KEY

Many attempts to improve transparency and control, or to provide more security are too complex. Doing the ‘right thing’ is not good enough. It also has to be easy to do for users.

DATA PROTECTIONS IS A NEW SERVICE OPPORTUNITY

Users are actively trying to defend their personal data – but may do so inconsistently or Inefficiently. There is space for companies to offer more comprehensive solutions, and to educate users on appropriate tools and services for them.

INVEST IN QUALITY OF DATA

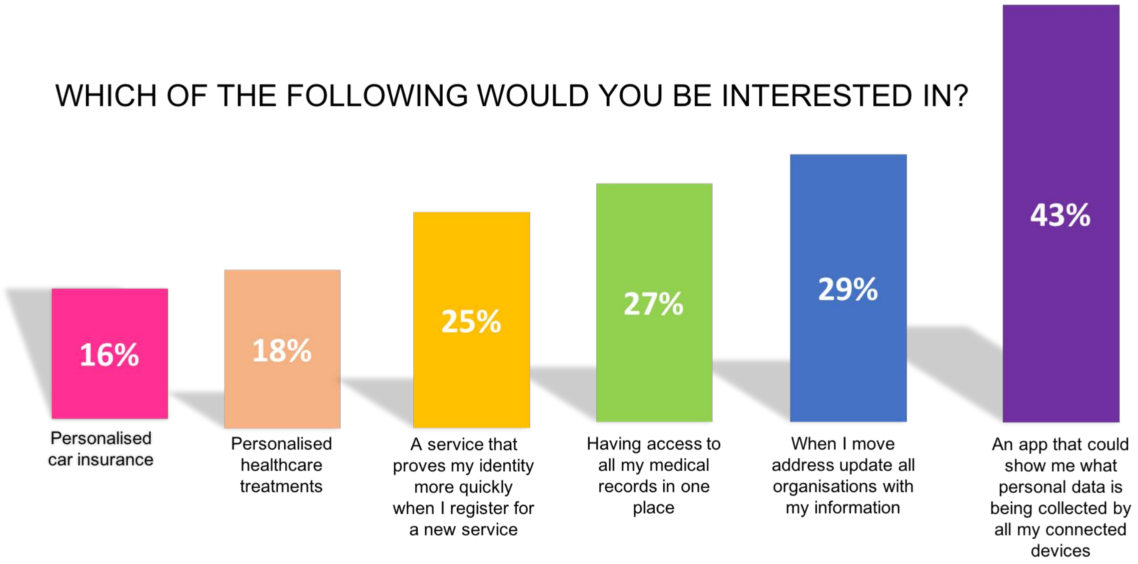
Through their attempts to defend personal data (for example via cookie and privacy settings or providing fake contact information) users are collectively lowering the quality of the data gathered by the industry. The industry will need to invest in more regular data cleaning/better sources.

Figure 1: Lessons for the industry

Source: MEF's Global Consumer Trust 6th Annual Report

Risk of data misuse accelerated post pandemic

Post-pandemic, the world is waking up to new levels of awareness about the digital world and personal freedoms. For both businesses and individuals, COVID-19 restrictions highlighted core digital dependencies and accelerated the pace of digital transformation[6]. As a result of the recent periods of enforced isolation through lockdown and quarantine, online transactions soared as did the consequent volume of data sharing. This further increased the risk of data misuse and exacerbated the need for privacy-centric solutions. For example, online or contactless identity verification procedures carry a much greater risk of important personal data being intercepted and captured, compared with a similar in-person verification process, such as during a hotel check-in.



Source: MEF, Global Consumer Trust Report 2017

Figure 2: Strong demand for data-driven products and services

[6] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Exchange data for new business opportunities

“

The era of big-data silos is fading. Shared data is the future.[3]

The business reliance on obtaining personally identifiable information, particularly with the growing variety of rich data sources, has dramatically increased in recent years. This has been one of the key drivers of the emerging data exchange solutions that enable access to business-critical data at low risk. A sustainable data exchange platform reduces risk of non-compliance, engages and empowers individuals or consumers and is able to leverage quality data for advanced personalisation and to create new services.

Reduced risk of non-compliance

“

... the conception of big data as a silo managed by single entities is giving way to the notion of shared data.
... data exchanges — shared platforms where data is gathered and curated from many different sources (all the individuals and organizations that voluntarily share it), allowing third parties to gain insights from it.[3]

With the potential reward of accessing more data for personalised services comes the risk of non-compliance to data protection and privacy regulations as well as the ethical responsibilities associated with collecting and processing personal data. A data exchange service can greatly reduce the risk factors of the businesses it supports by going beyond what is required by the relevant data protection regulations. By seamlessly navigating between the concepts defined by MyData principles, the European Data Governance Act[6] and self-sovereign identity (SSI) technologies, businesses also gain better access to the data they require[7].

[6] The Data Governance Act: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[7] In addition, the EU’s recently proposed legal framework on AI puts additional emphasis on compliant data governance: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

A data exchange service should also support data minimisation techniques (e.g., concepts like zero-knowledge proof and zero-copy integrations) which focus on the insights instead of the data itself. This type of service only provides 'just enough' information required to fulfill a particular data request, such as confirming that an individual is old enough to buy alcohol without having to reveal her age.

Combining regulatory compliant data usage with auditable data agreements is another essential aspect to minimising risk.

Engaged and empowered individuals

At the heart of the data exchange vision on how personal data should be managed and shared is to provide complete transparency and privacy-centricity to the individual whose data is being used. It is of supreme importance for businesses to ensure that individuals are not in any way disadvantaged or even harmed by the use or potential misuse of their personal data from an ethical or moral standpoint. It is for that reason that individuals today have a comprehensive set of data-centric rights enshrined in most if not all of the global data protection regulations.

> “*The backlash against corporate misuse of data provides forward-looking businesses a great opening to differentiate their offerings and gain a competitive advantage*

The right to have a say in determining how personal data is used has the added advantage of getting individual users engaged with your business and to further cement a trust relationship based on what they observe. For example, being selective about what and how much data to disclose is a good demonstration of a business's approach to privacy that can in itself engender a favourable degree of trust and loyalty.

> *At the heart of the data exchange vision on how personal data should be managed and shared is to provide complete transparency to the individual whose data a business is negotiating with the individual or with other organisations.*

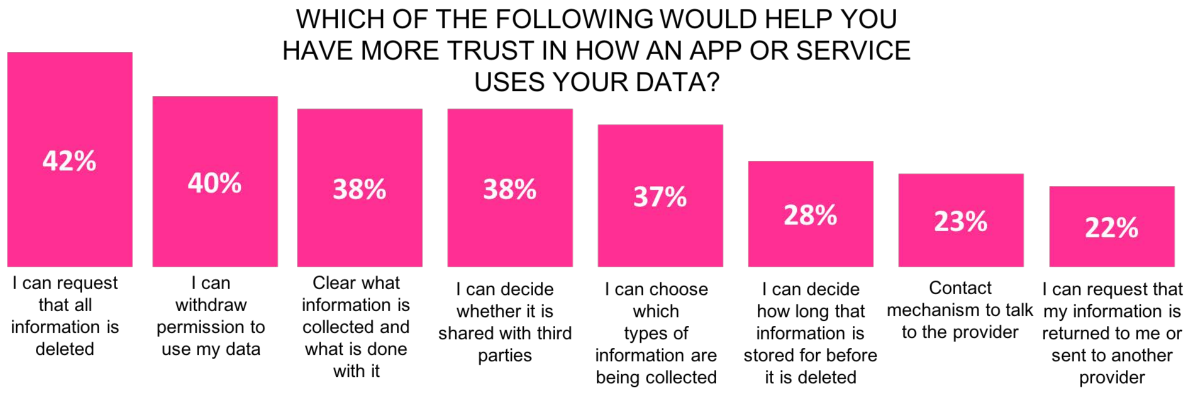
> *Obtaining consent to use consumer data is not a licence to use any of that information in a way that would contravene a user's personal principles*

New services with access to quality data

By using a scalable data exchange service, businesses can leverage and legally capture data beyond what is accessible within their organisation as part of a data marketplace[8].

Alternative methods of data exchange create immense integration challenges on businesses. With the use of new protocols, companies can onboard and leverage data within a decentralised and secure ecosystem, enabling them to legally expose and consume personal data.

Combining data from multiple sources with guaranteed authenticity of that data using advanced tamper-proof mechanisms will contribute to the speedy roll-out of new, 'just in time' services.



Source: MEF, Global Consumer Trust Report 2017

Figure 3: Consumers trust services that put them in control

[8] In a data marketplace, a data exchange platform would play the role of a data intermediary.

A sustainable data exchange

Simply put, a data exchange[9] provides access to as many data points as are needed to complete a data-oriented task or to fulfil a customer interaction or transaction.

The underlying assumption is that a process of personalising a service requiring even the most basic data set may not have either access to the relevant data or the requisite user consent – or both – and that data elements have to be obtained from a multiplicity of sources.

There is no global market that allows data to be moved transparently between companies or from individuals to companies. Many businesses are currently reliant on collecting and processing data from their customers, suppliers and employees or buying data from aggregators. The benefits that data exchanges bring are in structuring, aggregating and anonymising data. Once shared by consent and subject to legally-binding agreements, individuals are provided with a greater degree of control as well as confidence than they have today. Participating companies are able to carry out any number of simple or complex data-oriented activities without fear of breaking the law or compromising the privacy of their customers, suppliers or employees.

A sustainable and trustworthy data exchange should be transparent, regulatory compliant and auditable. This is what differentiates iGrant.io from many other data exchanges.

[9] José Parra-Moyano, Karl Schmedders, and Alex “Sandy” Pentland, 9 June 2020, What Managers Need to Know About Data Exchanges: https://sloanreview.mit.edu/article/what-managers-need-to-know-about-data-exchanges/

Example: A healthcare data exchange

This healthcare scenario provides a good example of data sharing and exchange involving multiple parties.

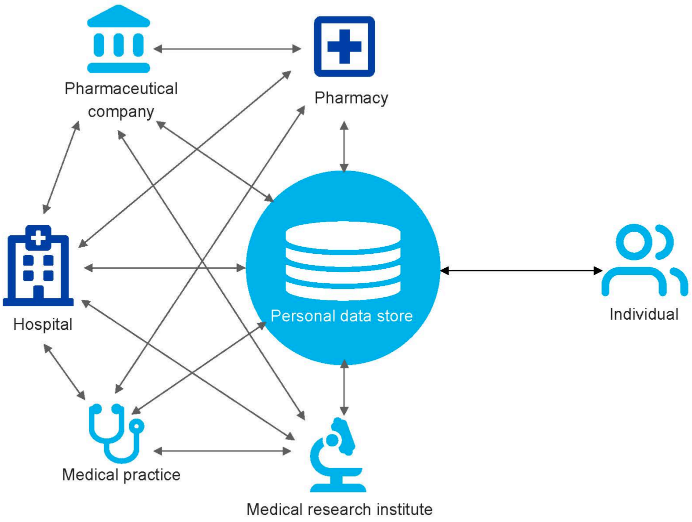


Figure 4: A data sharing environment for patient medical records which is neither sustainable nor human-centric

In*figure 4*, the individual enters some personal information into her medical records where sensitive information is gathered from her medical practitioner and any hospital she's had occasion to visit. Another actor in this scenario is the pharmacy that dispense her medicines. The pharmaceutical companies and research institutes also have a role to play in seeking to get hold of as much real-world information about incidents of disease or disabilities as possible. The efficacy of the medical solutions recommended by medical experts contributes to the furtherance of medical research as well as the modification of existing pharmaceuticals or even the creation of new medicines altogether. In this picture, the individual concerned has little or no idea about what any one of these actors knows about her and even less idea about how that information may be being exchanged. Her consent is not requested or required, an approach that is neither sustainable nor human-centric.

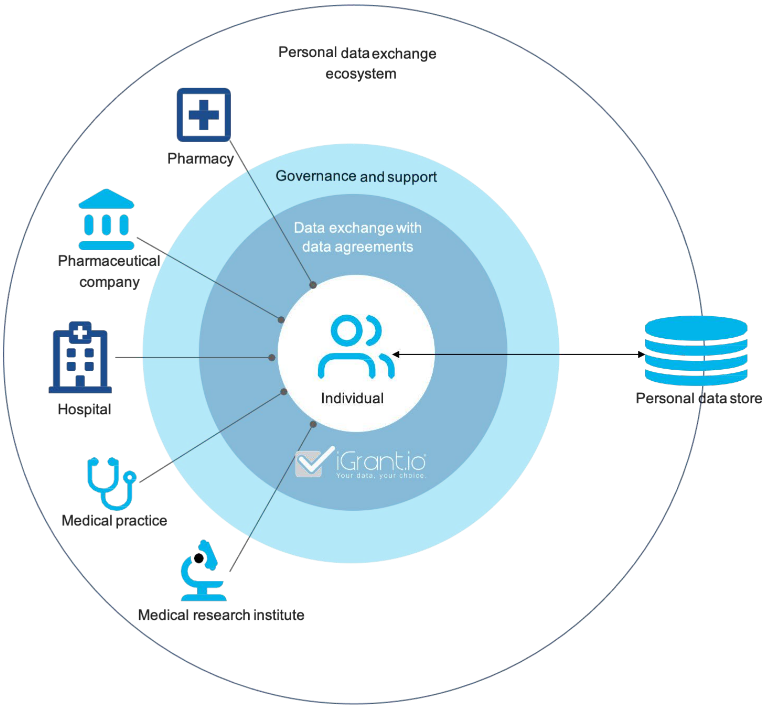


Figure 5: A data sharing of patient medical records with a data exchange

Figure 5 represents the role a data exchange, trusted by all the actors involved, can play in ensuring that the data concerning the individual is shared with her consent and subject to legally binding agreements. Examples of the role of the data exchange, how data is actually shared and the types of agreements they are subject to can be found in the next section.

Introducing iGrant.io

Towards a ubiquitous data exchange

As a provider of solutions for businesses to work with their customers, in 2020 iGrant.io was recognised as one of the first group of MyData Operators[10]. That is, a company:

> *… responsible for operating infrastructure and providing tools for individuals in a human-centric system of personal data exchange.*

In addition, a MyData Operator enables a business's customers:

> *… to securely access, manage, and use personal data about themselves as well as to control the flow of personal data within and between data sources and data using services.*

According to MyData Global[11]:

> *The human-centric paradigm is aimed at a fair, sustainable, and prosperous digital society, where the sharing of personal data is based on trust as well as balanced relationships between individuals and organisations.*

“

The objective of the MyData Operator initiative is that competing service providers should work together to create a global network for human-centric personal data transfer

There are a large and growing number of actors providing personal data management services, which should as far as possible be interoperable and substitutable as well as technology agnostic. The objective of the MyData Operator initiative is that competing service providers should work together to create a global network for human-centric personal data transfer just as a group of banks form a network for payments or mobile operators for phone calls. This kind of interoperability is recognised as having positive impacts for all stakeholders in a data driven economy.

[10] MyData Operator white paper: https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf

[11] MyData Global: https://mydata.org/

Until recently the various industry-led efforts to collect, store and manage personal data were poorly coordinated and, where there were attempts at interoperability, they tended to be cumbersome, involving complex integrations and suffering from lack of comprehensive standardisation to back them up. In addition, even if regulatory compliance was included as a design point, little consideration was given to the auditability of every end-to-end transaction undertaken.

Data agreements

With the iGrant.io data exchange solution, as a means to formalise trusted personal data flows from a data source to a data using service are based on data agreements. iGrant.io was one of the first MyData Operators to have data agreements which can be based on consent or any other lawful basis such as contract, legal obligation, vital interests, public task and legitimate interests (as per the GDPR.

If agreements are made without legally based consents, individuals have few means of influencing data usage, although they can still follow what data is processed and why. They can also exercise other rights such as the right to rectification, objection and portability. The value of a data agreement can be described as:

- End-user empowerment: Giving individuals control over how data pertaining to them is used and allowing them to exercise their rights as data subjects; and in addition, enabling companies to legally re-use that data.
- Data usage transparency: Enabling businesses to be both transparent about their use of personal data down to the attribute level and compliant with data protection regulations
- Data collection limited to the purpose selected: Making it safer for both individuals and companies to share data by limiting the amount of data shared to what is relevant for the intended purpose .

> “
> *As a means to formalise trust, a MyData Operator enables a data exchange whereby personal data flows from a data source to a data using service based on data agreements.*

- Paperless, all digital: Information can be automatically populated in a form based on data that individuals already have in their possession or consent to retrieve from another source.
- Privacy by design: Apart from contributing to data reuse and adherence to data minimisation requirements, every agreement-based transaction is independently verifiable which significantly reduces the risk of privacy violations.

Terminology

The terminology used by MyData Operators to describe the actors in a data exchange is precise and intended to avoid confusion, and similar to the language used in the GDPR

- a Data Source, the organisation collecting private data, (typically a data controller) [SSI: Issuer]
- a Data Subject or Individual [SSI: data holder]
- a Data Using Service is typically a data controller when using data from a data source, [SSI: data verifier]. There are also certain cases in which a data controller becomes a co-controller [SSI: data issuer]
- an Assessor reviews the practices of a business, conducts a data protection impact assessment (DPIA) and drafts data agreements and inter-company agreements for third parties
- an Auditor may be called in to review the data agreements and ensure they fulfil all legal requirements in case of data breaches or regular inspection.

With iGrant.io, a data using service can engage in agreements with various data sources, facilitating the relationship between a data controller or data processor (as defined in the GDPR). iGrant.io takes a data minimisation approach to personal data transfer where only the consent and transaction logs are stored as well as identity data. iGrant.io does not store the actual data that is being exchanged.

Active and passive data exchanges

A data exchange can be of two types:

A demonstration of the iGrant.io data wallet with a reference case (Data4Travel) can be found at: https://igrant.io/datawallet.html

(1) Active Data Exchange: an individual is actively involved in the data exchange flow. This can be of two types:

A. Using a data wallet, the individual holds the data and shares the data with any data using service in real-time.

B. Using notifications, an individual is notified of a request to use her data by the data using service and agrees to a data exchange from a given data source.

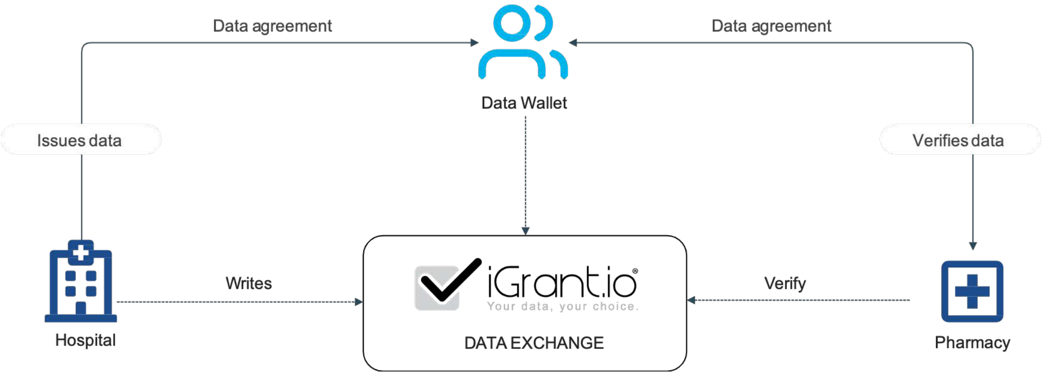


Figure 6: An Active Data Exchange

In *figure 6*, data is being exchanged between a hospital and a pharmacy both of which are data controllers. This workflow occurs in two phases:

(1) The hospital issues data based on a template to an individual

(2) The individual shares the requested data from her data wallet to the pharmacy

In order for this data exchange to take place each of the organisations are separately required to seek the consent of the individual whose data is being exchanged and to safeguard that consent through a data agreement with the individual. All the transactions involving the individual are stored in a data wallet, typically represented as an app on a mobile phone. The wallet stores data receipts and programs installed to make monitoring as easy as possible.

(2) Passive Data Exchange: data is exchanged between a data source and a data using service based on a data agreement that was mutually endorsed between the individual and the organisations involved.

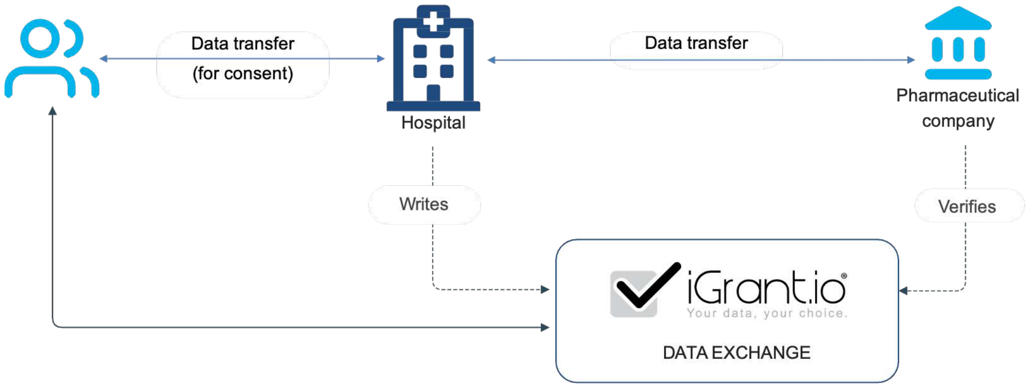
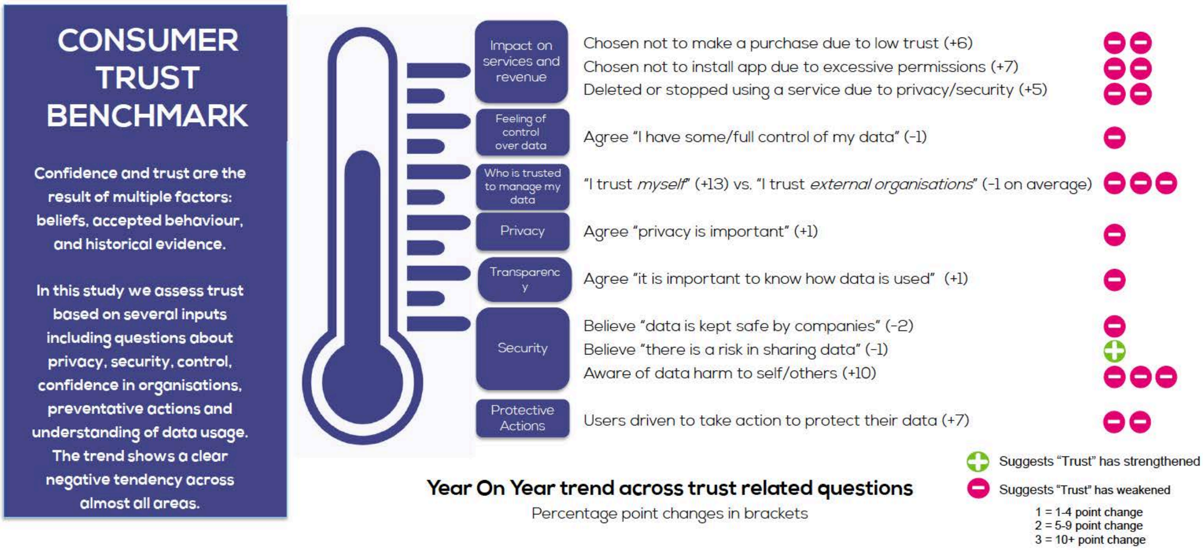


Figure 7: A Passive Data Exchange

In *figure 7*, although both organisations are involved in trading data, only the hospital has a direct relationship, in the form of a data agreement, with the individual who is asked to provide consent for the exchange of data between the hospital and the pharmaceutical company. As in the previous example, the ledger keeps an immutable record of the transactions and agreements.



CONSUMER TRUST BENCHMARK

Confidence and trust are the result of multiple factors: beliefs, accepted behaviour, and historical evidence.

In this study we assess trust based on several inputs including questions about privacy, security, control, confidence in organisations, preventative actions and understanding of data usage. The trend shows a clear negative tendency across almost all areas.

Impact on services and revenue	Chosen not to make a purchase due to low trust (+6) Chosen not to install app due to excessive permissions (+7) Deleted or stopped using a service due to privacy/security (+5)	− − − − − −
Feeling of control over data	Agree "I have some/full control of my data" (-1)	−
Who is trusted to manage my data	"I trust *myself*" (+13) vs. "I trust *external organisations*" (-1 on average)	− − −
Privacy	Agree "privacy is important" (+1)	−
Transparenc y	Agree "it is important to know how data is used" (+1)	−
Security	Believe "data is kept safe by companies" (-2) Believe "there is a risk in sharing data" (-1) Aware of data harm to self/others (+10)	− + − − −
Protective Actions	Users driven to take action to protect their data (+7)	− −

Year On Year trend across trust related questions

Percentage point changes in brackets

+ Suggests "Trust" has strengthened

− Suggests "Trust" has weakened

1 = 1-4 point change
2 = 5-9 point change
3 = 10+ point change

Source: MEF's Global Consumer Trust 6th Annual Report

Figure 8: User trust dropped again in the last 12 months

The growth of self-sovereign identity

Self-sovereign identity (SSI) describes a novel approach to digital identity that acknowledges that individuals should own and control their digital identities and personally identifiable information (PII) and be able to choose which companies they trust to collect, store, manage and re-use any personal data that concerns them.

To establish trust, one of the parties involved in an online transaction will present credentials to the other parties who can verify that the credentials came from a trusted issuer. In this way, the verifier's trust in the issuer is transferred to the credential holder. In a well-managed self-sovereign system, users control their verifiable credentials pertaining to a set of data assertions that they trust. Businesses which wish to make use of those credentials need a data agreement with the user legally based on consent, for example.

SSI systems are decentralised, using credentials that are verified based on public key cryptography which are often held in a distributed ledger. One of the main benefits in using a distributed ledger technology (DLT, such as blockchain, is that anything written to the ledger is immutable and consequently tamper-proof.

> *One of the main benefits in using distributed ledger technology (DLT), such as blockchain, is that anything written to the ledger is immutable and consequently tamper-proof.*

The European self-sovereign identity framework (eSSIF)[12] is part of the European blockchain service infrastructure (EBSI)[13] which is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology. iGrant.io is one of the few companies chosen to participate in the second eSSIF-Lab Infrastructure open call addressing automated data agreements (ADA) and so is part of the European SSI Framework.

Hyperledger[14] Aries is a multi-project open-source collaborative effort, hosted by The Linux Foundation created to advance cross-industry distributed ledger technologies. iGrant.io uses Hyperledger Indy[15]as a distributed ledger for publishing decentralised identifiers that are interoperable across administrative domains, applications, and any other data source, but businesses have the option to choose another instance of Hyperledger Indy.

[12] NGI eSSIF-LAB, European Self-Sovereign Identity Framework Lab, https://essif-lab.eu/

[13] European Blockchain Services Infrastructure (EBSI): https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

[14] Hyperledger: https://www.hyperledger.org/

[15] Hyperledger Indy: https://www.hyperledger.org/use/hyperledger-indy

Pioneering secure digital transformation

iGrant.io is pioneering the ground-breaking technologies that are transforming the way that businesses and their customers can interact over personal data, securely and with mutual respect, realising a clear and sustainable way forward.

The critical confluence

The iGrant.io proposition addresses the key challenges that have dogged the data economy and privacy professionals for years. It represents and demonstrates the confluence of a number of factors:

- Public awareness: The drip feed of headline stories concerning data breaches at well-known brands, in both the public and the private sectors, has forced a reluctant public to acknowledge the volume of data that is being held about them and how vulnerable they are to third parties, known and unknown.
- Cybersecurity: The general public's casual unwillingness to confront issues of how data is managed is perfectly understandable, human nature in fact. As long as using the Internet is a simple, easy-to-use, inexpensive, rich and rewarding experience, why worry? It's only when the repeated stories about the loss of data and the potential that such vulnerabilities may impact not just one but many of the services they are accustomed to using on a daily basis does it start to make sense to be more circumspect about sharing any kind of personal data.
- Data protection and privacy regulations: European policymakers took the lead in laying the groundwork for best practices with the introduction of the GDPR and the e-Privacy regulation which

> “
> *The general public's casual unwillingness to confront issues of how data is managed is perfectly understandable, human nature in fact.*
> *As long as using the Internet is a simple, easy-to-use, inexpensive, rich and rewarding experience, why worry?*

are being adopted in similar forms worldwide. The GDPR outlines the basic rights of an individual to exercise control over the use of their personal data held online which puts tremendous responsibilities at the door of companies in possession of such data.

- Regulatory compliance: As policy on data protection is no longer subject to a directive but a regulation, regional, national and, in the case of Europe, supranational authorities have been set up to police how well companies are observing the spirit if not the letter of the law. They also have the statutory powers not only to name and shame but also to impose significant fines. Given the length of time the GDPR in particular has been in force, it is no longer acceptable to claim ignorance or lack of time to prepare.

> *Given the length of time the GDPR in particular has been in force, it is no longer acceptable to claim ignorance or lack of time to prepare.*

- Technology: Distributed databases have been available for well over thirty years and are characterised by replicating, sharing and synchronising data across multiple sites, which could be in different countries. Distributed ledger technologies (DLTs), of which blockchain is the most well-known, have also been available for many years and are very similar to distributed databases, with the notable difference being that there is no central administrator or authority. As long as cryptocurrencies were the main blockchain applications, it was doubtful whether DLTs would be accepted in traditional industry sectors. However, over the last five-six years the Hyperledger project has advanced cross-industry collaboration by developing distributed ledgers, with a particular focus on improving the performance and reliability of these systems, so that they are capable of supporting global business transactions by major technological, financial and supply chain companies.
- Self-Sovereign Identities (SSI): The concepts underpinning SSI have been in circulation amongst the so-called *identirati* for at least the last twenty years and probably longer. The idea that individuals should be masters of their own digital fate, once articulated, seems self-evident. However, until relatively recently, the time was not right to put in place large scale systems and infrastructure due to the lack of sufficient public and corporate awareness of any ‘burning business problem’. The tide has now demonstrably changed.

- **MyData Global:** The mission of this international non-profit organisation is to empower individuals by improving their right to self-determination regarding their personal data. It is based on the MyData Declaration. The organisation has over 100 organisational and 400 individual members from over 40 countries, on six continents working on the ethical use of personal data. MyData provides both a vision and set of guiding technical principles, including those associated with MyData Operators.

Meeting the challenges

As a MyData Operator utilising SSI-based DLT technology, iGrant.io's data exchange solution fulfils the confluence of conditions identified above by providing transparency in the usage and exchange of data. The key risk to all the stakeholders involved is that data records or credentials may be tampered with or altered, irrespective of whether it is through malice or by accident. Consumers today have to rely on a company's policies and there is little or no way for the company to justify their position in a court of law when there are data misuse concerns, unless it can be proven through an audit.

By involving customers, consumers and citizens in these transactions through legally-binding agreements, not only is data regulatory compliance ensured but just as critically consumer trust can be maintained – or, if necessary, restored. In addition, iGrant.io is participating directly with the organisations and bodies driving standards on preference mechanisms, secure data exchange and automating data agreements.

> “*By involving customers, consumers and citizens in these transactions through legally-binding agreements, not only is data regulatory compliance ensured but just as critically consumer trust can be maintained - or, if necessary, restored.*

A trustworthy partner

iGrant.io is ideally placed to partner both public and private organisations who are in the business of exchanging personal data with other organisations and who are concerned about doing so in a human-centric and privacy-sensitive manner.

iGrant.io's solution ensures that transactions involving the exchange of personal data are secure and regulatorily compliant and have the consent of the individuals whose data is being transacted through legally binding data agreements. It guarantees that the integrity of the data received by a data using service is protected and tamper-proof, ensuring the reliability and validity of data at the time of use, thereby reducing fraud. iGrant.io provides a platform and a mobile client SDK that can be customised to suit the needs of any company, large or small.

The management and governance of data held by all types of companies is going to be increasingly scrutinised by the authorities and the public over the coming months and years.

Getting a solution that enables firms to carry on their business with confidence and inspiring trustworthiness is not only sound commercial sense but also a competitive advantage.

iGrant.io's trusted data exchange solution enables your business to balance honouring and respecting your customers' privacy while leveraging the data they submit. iGrant.io both reduces the risk of non-compliance and increases customer satisfaction and loyalty. In addition, getting greater access to personal data for personalised services provides a competitive advantage.

iGrant.io is one of the leaders promoting this new wave of human-centric data management. We have explained in this white paper how businesses can navigate the regulatory landscape with confidence while still providing highly valuable personalised services.

Annex: The transformation of personal data processing

The digital transformation underway today was initially triggered by the commercial adoption of the Internet in the 1990's which started the significant shift in the way in which companies interact with their customers and employees; and in particular the collection, storage, management and re-use of personally identifiable information or simply personal data.

During that time, businesses learnt to use the web to showcase their products and services. Within a few years, new companies emerged that were building businesses on the data that was being generated on the back of the nascent digital economy. Companies like eBay, Airbnb, Amazon and many others like them were gaining significant global attention by making data-related business decisions and introducing user profiling, in return for which they provided their customers with personalised services based on behaviour, location and personal choices.

Later Google, Facebook and others successfully leveraged the data opportunity, and fundamentally disrupted traditional business models, and, unimpeded by poor data protection regulations, were able to aggregate all the data they had access to. The era of big data, and, with it, data analytics, had arrived.

In this brave new world, user data became an asset to be packaged and sold on to any number of third parties, undisclosed to the users themselves, who rarely complained. Even if they were made aware that the data they had provided about themselves was being traded commercially, as long as they continued to be able to make use of free services, they were getting a good deal. Even though online transactions could now be tracked with ease, the individuals whose data was involved were not offered the option to find out how their accumulated profile data would be collected, managed, stored or sold on to third parties for purposes unknown.

For years the unregulated nature of the new technology-based sectors provided an unfair advantage over companies in highly regulated industries, such as telecoms and healthcare, which were hindered from free exploitation of the personal data they had access to and fuelled the growth of the new sector.

Fast forward ten-fifteen years and eventually the penny dropped that the business practices of data aggregators had got out of control. The revelations concerning how the political data analytics firm Cambridge Analytica had improperly obtained the personal data of millions of users reverberated far and wide. That a developer was able to legitimately access Facebook's platform with the express purpose of profiling voters in the UK and the US without their knowledge or proper consent came as a major wake-up call both to the authorities and Internet users the world over.

> “
> *... over **80%** of Internet users in the US feel that they have little or no control over their personal information online ...*

> “
> *... **91%** of consumers say that they are more likely to shop with brands that send them personalised offers and recommendations ...*

> “
> *... **81%** want brands to get to know them better and to understand when to approach them and when not to..*

It's hardly surprising then that over 80% of Internet users in the US feel that they have little or no control over their personal information online. Nevertheless 91% of consumers say that they are more likely to shop with brands that send them personalised offers and recommendations and 81% want brands to get to know them better and to understand when to approach them and when not to. Hence, consumers clearly want to trust the brands that they transact with, even though at the same time they lack any say in what happens to the information they provide to carry out those transactions[16].

With the sobering realisation that the general public has a more heightened awareness about potential personal data misuse than ever before, businesses are increasingly seeking to strike the right balance between protecting the data they are responsible for and

[16] State of connected customer, Salesforce (4th Edition): https://www.salesforce.com/content/dam/web/en_us/www/documents/research/salesforce-state-of-the-connected-customer-4th-ed.pdf

personalisation or profiling. The key to successful marketing means being able to continue to provide rich and personalised offerings to customers and prospects while staying on the right side of the law and building trust-based relationships. Legal frameworks to monitor the use of personal data are emerging in the form of data protection and privacy regulations across a growing number of jurisdictions worldwide, alongside which are the national and supranational supervisory bodies to monitor them.

Consequently, and in the wake of a growing number of data misuse incidents, the tech giants, now very much in the public spotlight, have reined back from their unbridled approach to personal data aggregation with self-governing mechanisms. On closer inspection however, those that have adopted, for example, an opt-out approach to data sharing with their users bury the set of choice options deep within their applications. Turning them off is often cumbersome or difficult to access, which, one might conclude, is more akin to 'data collection by default' rather than 'privacy by default'. Although Apple's Tim Cook has shown that it is even cool and business-savvy to become a public champion of data protection and privacy-preserving approaches, there is still a long way to go.

The mechanisms for managing the sweeping changes in attitudes, behaviours and practices have been relatively slow to evolve, but are gradually crystallising around a human-centric approach to data management that aligns the rights and preferences of the individual with the business purposes of companies, large and small. It calls for a shift away from companies' hoarding mountains of big data for their own exclusive use to sharing right data from multiple sources and involving the individuals whose data is being traded. Needless to say, but nevertheless important, the whole process has to be transparent, secure and privacy-centric, based on verifiable agreements.

> “
>
> *The mechanisms for managing the sweeping changes in attitudes, behaviours and practices have been relatively slow to evolve, but are gradually crystallising around a human-centric approach to data management that aligns the rights and preferences of the individual with the business purposes of companies, large and small.*

iGrant.io is promoting a new wave of human-centric data management aligned with the behavioural shift of businesses and individuals

The iGrant.io data exchange platform is a trust-based solution to the problem of business use of personal and sensitive data, enabling businesses to navigate the regulatory landscape with confidence while providing new highly valuable personalised services to their customers, based on existing and new technologies

MyData
Operator
2020

Bössvägen 28
Sollentuna - 192
55 Sweden

info@igrant. io

www.igrant.io

iGrant.io®
Your data, your choice.