
# Data Sharing and Consent Management:

## Making consumer choice a business opportunity

June 2018

# Contents

# Introduction

It is widely acknowledged that the collection, storage and processing of data is at the heart of the digital economy. Much of this information is about people and the key to making the digital economy work relies on getting their consent to the use of data held about them.

The Internet and mobile devices have given everyone unlimited access to services and social engagement that were undreamt of twenty years ago. What was also unanticipated was the way in which companies would hour-by-hour, day-by-day stockpile consumer preferences and other personal data derived from machine-learnt algorithms which could then be sold on to third parties. The emergence of a handful of powerful data-driven companies has distracted from the complicity of most organisations in the erosion of consumer trust in the digital world, particularly when a data breach or an incidence of data misuse comes to light. Europe has become increasingly vigilant in challenging through the courts global enterprises that abuse their right to use their consumers' data. With the GDPR in force, the net will be spread much wider, giving EU citizens significantly more control than ever before over how their data is collected, stored, processed and shared.

# Consumer attitudes

Before analysing what organisations should do next, it is worth considering what consumer attitudes and concerns are to the key issues of data usage and perceptions of trustworthiness. According to a recent report[1], these were the significant findings:

- Consumer caution is generally increasing across age groups and countries: when asked whether they should be cautious about sharing their personal data online, all age groups across all countries surveyed strongly agreed, although millennials slightly less so.
- Data type is critical to understanding and contextualizing consumer sentiment: financial information was considered the most private, surprisingly more so than information about health, family members and communication data. Purchasing preferences and commonly held information such as name, gender and age were much lower on the list. There was a significant divergence between attitudes across Europe with France and Germany being the most private.
- Consumer concerns vary widely by industry: the concerns about the companies that are least trusted reflects a degree of savviness about the type of data they might hold or have access to. Online companies, the finance sector and government agencies fall into this category.
- Consumers are primed to suspect companies of misusing their data: a majority of consumers do not believe that companies are honest about data relating to them is used, with only a very few trusting companies 'to do the right thing'.
- Companies are failing to use data for new purposes that most consumers find acceptable: there is a discernible discrepancy between what companies and consumers believe is the appropriate use of personal data. Significantly, consumers are more concerned about being asked for permission than about the actual purpose to which consumer data is being used.

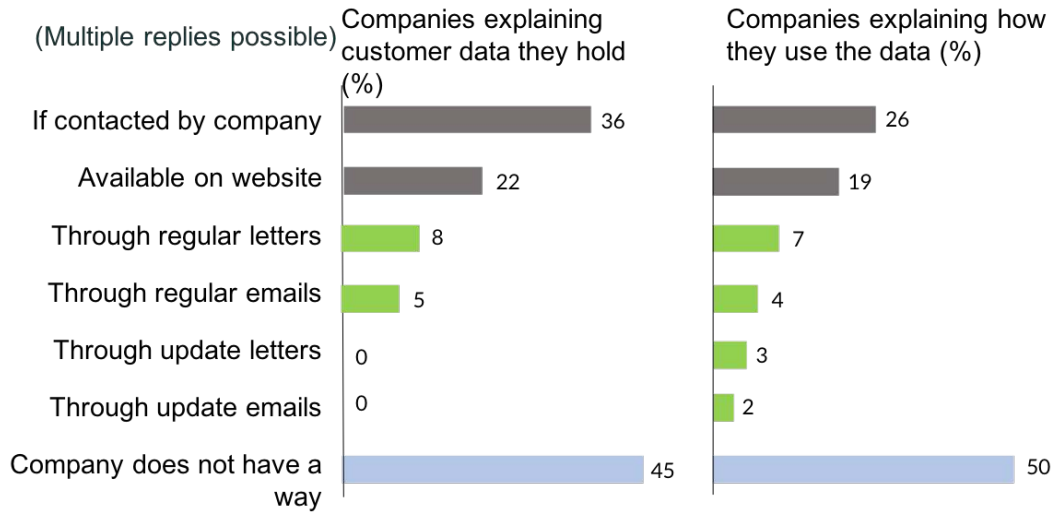
*Significantly, consumers are more concerned about being asked for permission than about the actual purpose to which consumer data is being used.*

*A majority of consumers do not believe that companies are honest about data relating to them is used, with only a very few trusting companies 'to do the right thing'.*

1 *Leveraging GDPR to Become a Trusted Data Steward*, The Boston Consulting Group, March 2018

*There needs to be a solution that meets the need of both people and companies that makes life better and easier for both*

- **Distrust radically reduces the amount of data consumers are willing to share with a company:** once consumer trust is lost through the misuse of data, whether intentional or accidental, it is difficult to restore with a negative impact on marketing revenue potential
- **Many companies either use passive methods of data-related communication or have no way to communicate:** with the advent of GDPR, companies will have to learn to be pro-active in how and when they communicate with their customers in all matters related to the handling of personal data *(see figure 1)*




Source: BCG Big Data & Trust Consumer Survey
Note: Survey questions: "With regard to engaging with customers about the data your company holds about them, which of the following statements are true?" and "With regard to engaging with customers about how you use their data, which of the following statements are true?"

*Figure 1: Many companies either use passive methods of data-related communication or have no way to communicate*

Despite these apparently negative trends and perceptions, the high visibility of data protection and privacy issues in the public eye today provides a great opportunity for companies to embrace the principles of privacy regulations and thereby earn the trust of their customers and in addition derive more value from the appropriate use of personal data. Consider the success of companies like Amazon, Netflix and other retailers which deliver highly personalised recommendations based upon previous search and purchase histories.

# Refresh the business model

*Companies will be in the hands of their customers by having to rely on their explicit consent for sharing personal data, which applies equally to data from a partner application or when data is shared between entities.*

So how can organisations avoid falling foul of the authorities, as well as their customer base, and seize the opportunity to take advantage of the new regulation? The way to make this happen is through designing and offering new privacy-preserving services, re-appraising existing business models including transparency on data storage and processing policies as well as creating a heightened sense of employee awareness and responsibility. In itself, this should motivate and inspire companies to enrich the user experience, and in so doing build and maintain customer loyalty as well as remain competitive. But it's not enough to simply tick all the regulation boxes: the challenge is to get and retain customer trust and the key to achieving that is by creating a consent trust framework.

For many companies, digital transformation simply involves applying IT tools in a smarter way, to improve cost effectiveness and operational efficiency. A strengthened relationship with the consumer should always be a core outcome of a digital transformation. So, in order not to miss a great opportunity to be successful, the process has to include re-appraising how best to re-engage with customers, suppliers and partners. In the data sharing economy, companies can expect to have to regularly analyse the entire customer journey, in terms of providing secure access to personal data that is relevant and based on transparent and unambiguous policies for how that data is collected, for what purpose and how it is to be processed. Companies will be in the hands of their customers by having to rely on their explicit consent for sharing personal data, which applies equally to data from a partner application or when data is shared between entities.

# Overcome the privacy paradox

The Mobile Ecosystem Forum's annual Global Consumer Trust Survey canvassed the behaviours and attitudes of over 5,000 consumers in eight countries including both developed and growth markets[2].

- Reluctant sharers, who share data only because they have no other choice if they want to use the app, account for half US and German mobile users
- Concern around data privacy and security is greatest in China, the USA and Germany. Chinese consumers have the highest security concerns, whereas Americans are most put off by data-hungry apps.
- In Brazil, consumers currently assign greater sensitivity to their photos than their financial information whereas in India, contact information is considered most sensitive.
- Although consumers rarely read data usage agreements, they agree to the terms (non-informed consent).

Research also shows that many consumers often continue to use services that can be very intrusive, while at the same time express concerns about data being collected from their service providers. This is the privacy paradox.

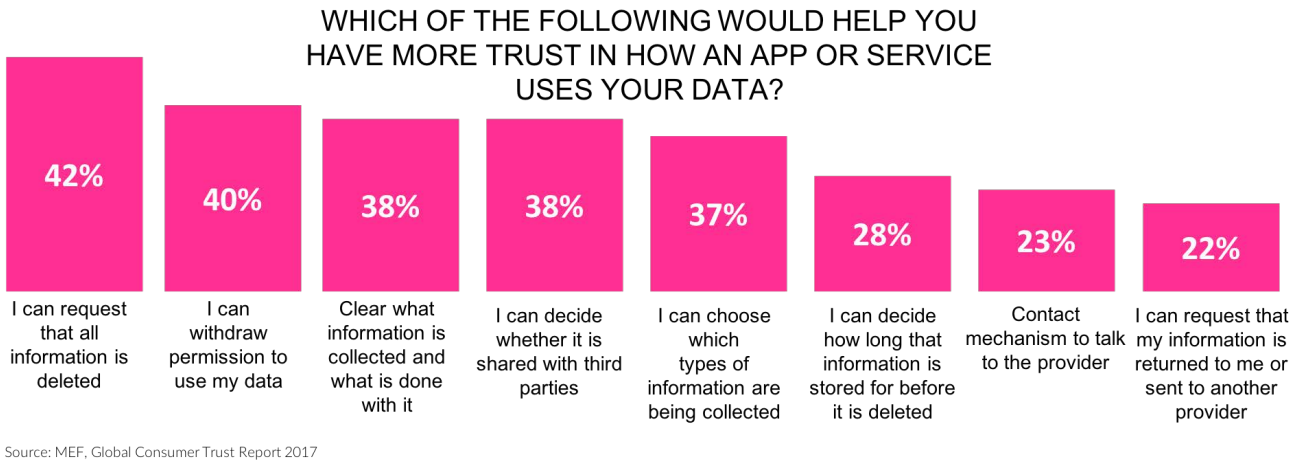



*Figure 2: Consumers trust services that put them in control*

A recognition of the privacy paradox is a worthwhile consideration in formulating data policies for any consumer-oriented business.

Establishing a high degree of respect for customer misgivings is essential when aiming for satisfaction and loyalty. Clearly, the business might be at risk when individuals start saying "no" to a consent request if they don't see the value in saying "yes". On the other hand, a data policy built on consumers agreeing to a service, despite the perception that it is intrusive for example, is unlikely to be successful.

The GDPR has made all-or-nothing data privacy policy statements or user agreements outdated. From now on, the scope of a data policy, in terms of coverage and governance, requires a clear and transparent statement of consent that applies to the:

- use of information for delivering a service;
- access to data for the sales and marketing department for enhanced/enriched services including data sharing; and
- sharing of information to a call centre and other partners if there is an intention of transferring personal data

As the data sharing economy evolves, customers will be able to build up and sell their own data to the companies they want to, rather than the data being purely exploited by those brand partners.

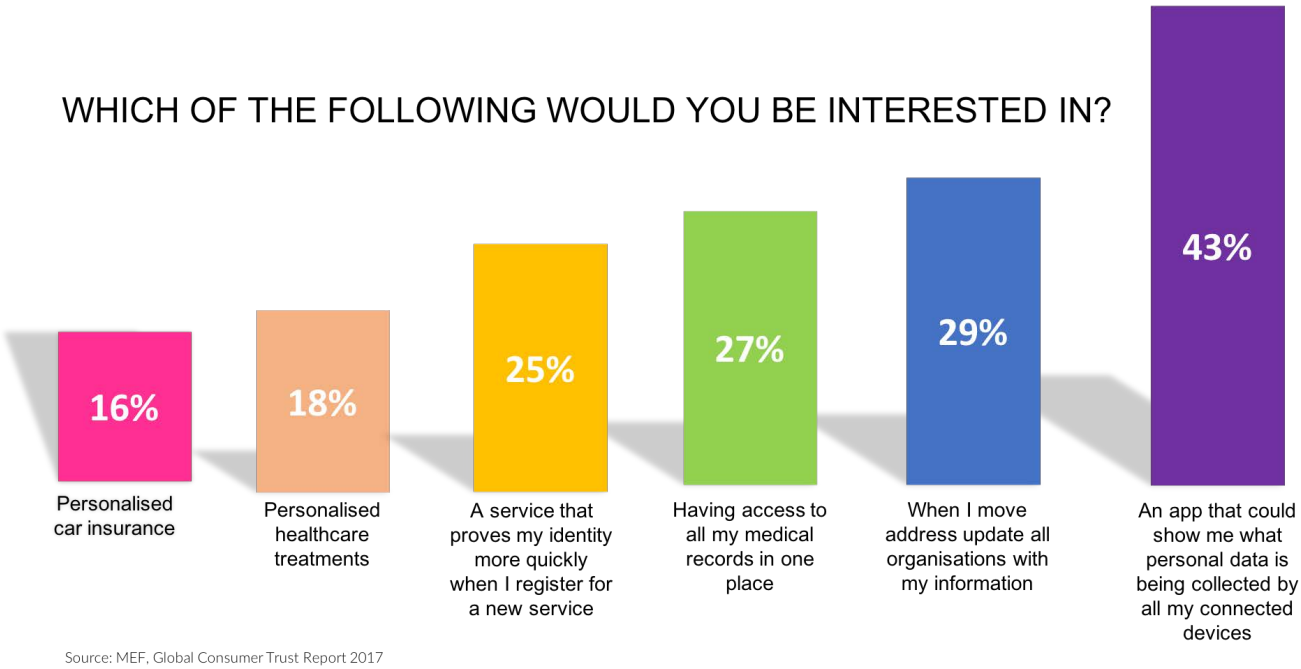



*Figure 3: Strong demand for data-driven products and services*

2 *Global Consumer Trust Report*, Mobile Ecosystem Forum, March 2017 - https://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-survey-2017/

# Avoid crossing red lines

Online stores, search engines and social media collect, analyse, acquire and share a large amount of personal data. The objective is simple and logical: when consumers' online behaviour can be tracked, logged and analysed their buying preferences can be predicted. Personal data has become a traded resource, a commodity or a "currency" in the digital economy.

Screening and algorithm-controlled processes are also used for customer segmentation and are invariably driven by profit and/or productivity motives. As long as there is a match between a company's products and services and their declared values, both parties will benefit. However, as and when there is a disconnect, such as when individuals' personal finances, lifestyle and health status are used to derive tariff settings, insurance premiums or interest rates, consumers and society at large will react by questioning the company's ethics and the line that has been crossed.

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

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

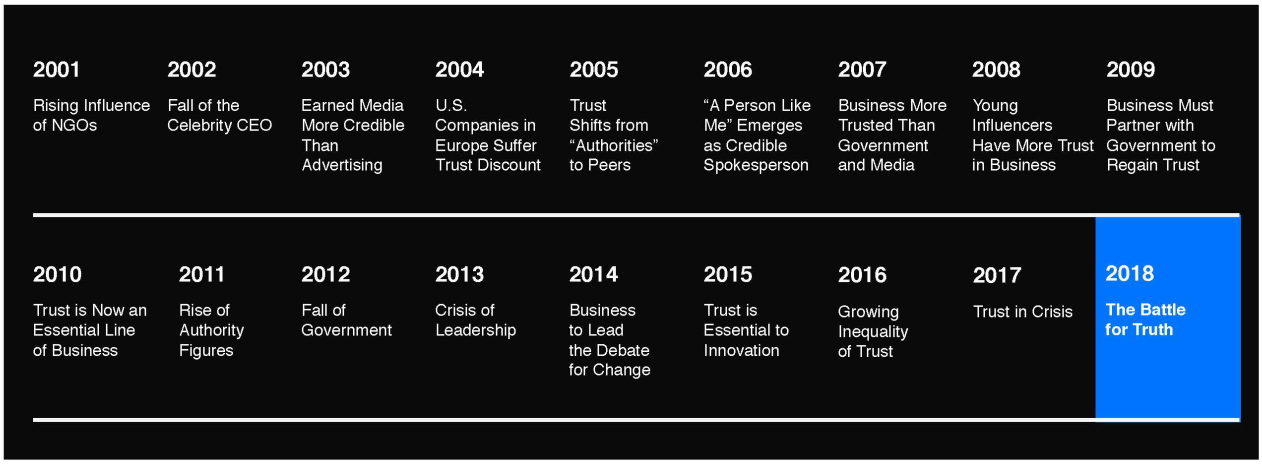
So, even if getting consent was compliant and transparent, there is no guarantee companies will meet consumers ethical expectations. The recent exposé involving Facebook and Cambridge Analytica demonstrated very forcibly how algorithms can be constructed to imperceptibly effect individuals' preferences. What was most disturbing was not so much how the data was acquired but how sophisticated algorithms were used to influence the hearts and minds of millions of voters.

How does an individual build and maintain a trust relationship with a company that knows things about the individual that no one else knows? For example, a company crosses a red line when an algorithm correctly 'guesses' that you have a serious illness based on healthcare app feedback and informs your healthcare provider, if you haven't indicated that you wanted that level of intrusion?

The dependence on a consumer's explicit consent can also lead to a risk-reward dilemma when offering new services. A company may decide not to unlock the value of data in situations where the ownership of personal data is either unclear or there is no strategy for getting consent. One company may draw a red line and say "no" to service development due to a fear of violating data privacy regulations and incurring high fines. Conversely, a competitor may balance risk and reward differently for similar services.

Where does a defensive strategy pay off and could an offensive move lead to fines and a stranded investment? It is a tricky balancing act and companies need to be sensitive to consumers' likelihood to provide consent.

Trust between two parties is based on a complex cocktail of confidence, respect and observable actions. Generation Y and Z, tomorrow's consumers, will be focusing on companies and brands that have a clear purpose and a vision on corporate social responsibility that goes beyond high-quality products and services when they make a purchase.




*Source: 2018 Edelman Trust_Barometer Global_Report*

*Figure 4: Trust in retrospect*

# Leverage the value of trust

*According to Amazon's Jeff Bezos, "Your brand is what other people say about you when you are not in the room".*

*A company cannot simply announce to its customers, "We are trustworthy": trust has to be earned.*

In the latest report from the Edelman Trust Barometer, that has been measuring trust in institutions across government, business, media and NGOs in 28 countries since 2001, the United States is seen to be suffering from the largest ever recorded drop in trust in the survey's history among the general population[3]. Not surprisingly this is a trend that is reflected elsewhere in the world.

At a time of declining trust, maintaining credibility and transparency is essential for a company's brand. Successful brands recognise that they are not fully in control of the brand themselves. According to Amazon's Jeff Bezos, "Your brand is what other people say about you when you are not in the room". A company cannot simply announce to its customers, "We are trustworthy": trust has to be earned.

Companies can prove their credibility and transparency through concrete actions. In the data sharing economy being transparent means letting customers know how services are designed, including what data goes in to them and where it is sourced. When businesses are consistently transparent, they are much less likely to have problems.

PR agency Cohn & Wolfe has been conducting brand and authenticity surveys since 2012[4] to determine which brands are held in the highest esteem. Acknowledging that "brand authenticity is hard to define, but it's something consumers know when they see it", the survey's measurements are based on:

- Reliability: a brand delivers on promises;
- Respectfulness: a brand treats customers well and protects data;
- Reality: the brand communicates honestly and acts with integrity.

The study shows that authenticity depends mostly on customer experience — reliability and respect don't come from advertising.

3 All fieldwork was conducted between October 28 and November 20, 2017

4 https://www.campaignlive.co.uk/article/cohn-wolfes-authentic-100-reveals-global-brand-trust/1445935 and http://authentic100.com/

The value of trust is apparent in the case of Verizon's decision to offer $350 million less than originally planned to acquire Yahoo after the disclosure of two massive data breaches in 2017 .

A study on Fortune 500 companies' data policy transparency and consumer control[5] concluded that companies that scored low on both transparency and control suffered more severely than those that scored medium to high, when affected by a data breach within their company or even a close industry rival, due to a spillover effect.

Even before GDPR, the authorities in Europe were taking strong action against companies flaunting the rights of their users. For example, following Facebook's amendment of its privacy policy in 2015, the French data protection authority performed on site and online inspections, as well as a documentary audit, to verify that Facebook was acting in compliance with French law.

The investigations revealed several failures that included Facebook's massive compilation of personal data for targeted advertising and the collection of data on users' browsing activity on third-party websites, in both cases without users' knowledge or consent. After being issued with a formal notice to comply, Facebook were unable to provide adequate responses which eventually resulted in a public sanction of 150,000 euros. Today, under the GDPR, the sanctions imposed as well as the negative impact on brand and public perceptions of trustworthiness would be significantly higher.

The prerequisites for trust which has a high tangible value are far more likely to be determined by astute customer-oriented policies than security software. There is a business logic and branding opportunity to go from a blind, non-informed agreement to mindful and educated consent[6]. It's a belief that people will prefer to deal and interact with companies that honour integrity and act with transparency.

5 *A Strong Privacy Policy Can Save Your Company Millions*, Kelly D. Martin et al. Harvard Business Review, February 2018 - https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions

6 *The quantified consumer: blind, non-informed and manipulated?* Stefan Larsson, Internet Policy Review, July 2017 - https://lup.lub.lu.se/search/publication/32a9da75-bacf-47bb-bf1f-97c5db782c69

# Partners in trust


*Create a consent trust framework that works at the speed of business*

*Do business in a data driven world with no risk, maximum speed and best quality*

iGrant.io[7] provides consent management products and services for organisations and individuals. In the data sharing economy, consent agreements are complex, often requiring real-time access to several partners. Our privacy-preserving SaaS-based platform provides solutions that facilitate regulatory compliance for all types of organisations and offer users ease of use to manage consent agreements.

Today, iGrant.io can easily be adopted and integrated as an API into an organisation's IT environment. Consumers are able to sign consent agreements on the organisational website or via the iGrant.io mobile app. The advantage of iGrant.io's API, even for a peer-to-peer consent agreement, is that no personal data is exchanged or shared with iGrant.io, only a record of the transaction. iGrant.io services are not intrusive for companies that make consent requests nor for the responding users.

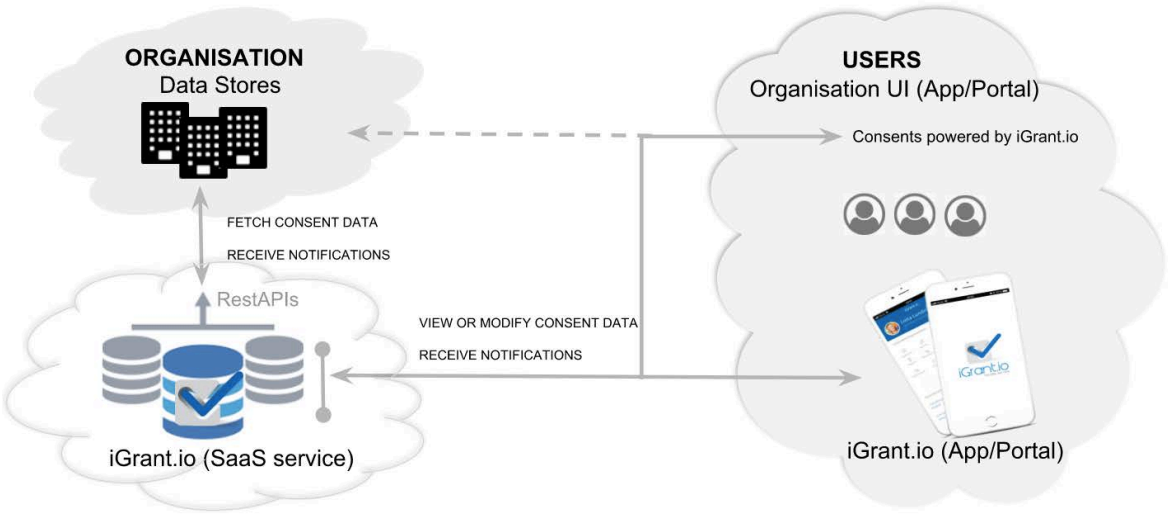
iGrant.io does not use incentives for users to sign up to use the app or web services. Consent and/or loyalty schemes based on financial rewards and other gratifications and monetization on personal data do not replace or change the requirements of an informed user consent. GDPR prescribes a strict and mandatory right for users to revoke a consent and to erase personal data regardless of whether or not they had agreed otherwise with any third party.

The services provided under iGrant.io are associated with a high degree of transparency and control of personal data. Our brand is based on trust that our enterprise customers benefit from. Wherever the iGrant.io logo is visible, it symbolizes trust and respect for privacy. Although some organisations will be confident about managing their peer-to-peer agreements, iGrant.io provides an independent and trustworthy solution for organisations to engage with their end-users and also to manage more complex one-to-many and many-to-many transactions.

7 iGrant.io is wholly owned by LCubed AB

Unlike some other commercially-available solutions, iGrant.io is designed for industrial scalability in terms of enterprises and users, provides real-time functionality. iGrant.io does not store any personal data itself, as this is the responsibility of the organisations it is transacting with.

The iGrant.io app available on iOS and Android is freely available. For organisations, there is an initial fee for installation/subscription (including support) with a subsequent transaction-based business model.



**iGrant.io is a cloud-based personal data and consent mediation platform that enables a fully transparent and trustable data sharing economy.**

**It helps institutions, both private and public, unlock the value of personal data in a fully compliant manner. Apart from lowering the cost of legal compliance to, for example, Europe's General Data Protection Regulation, iGrant.io helps companies establish and maintain trust with their customers by demonstrating transparency and respect in how personal data is used.**

Bössvägen 28
Sollentuna - 192 55
Sweden

info@igrant. io
www.igrant.io