WHITEPAPER

Trust in the Personal Data Economy

From GDPR compliance to opportunity: How giving individuals control over their personal data unlocks new business opportunities.

EVRY

Table of Contents

Executive summary

"People don't trust the banking sector anymore" is an oft-repeated statement. Yet survey data shows that banks have the highest trust of all institutions to store personal data. Nordic banks are more trusted to handle personal data than banks in any other region in Europe. Customer satisfaction with banks, however, is languishing. People are increasingly expecting banking services tailored to their personal needs. These expectations are largely going unmet. Nordic banks therefore have an opportunity to leverage their trust to provide new services from personal data.

The General Data Protection Regulation comes into force in 2018, and will give EU/EEA citizens the most complete data protection rights in the world. This includes the right to access any personal data a company might hold on them. They also have the right to delete their personal data, or transfer it between companies.

Despite new regulatory burdens, there are also opportunities to be found in the GDPR. **The right to data portability unlocks the possibility for a new model for personal data management:** 'Personal

Information Management Systems' (PIMS). PIMS are technologies and ecosystems which give individuals a singular view over their personal data from a variety of sources, which could include companies and organisations from both the private and the public sector. From here, individuals can analyse, delete, or transfer data between data controllers, as well as gain access to new services based on their personal data. Not only could such a platform afford GDPR compliance, it would also bring data sources together which are usually kept apart, leading to new opportunities within analytics, cognitive technologies, CRM, and innovation.

We argue that Nordic banks are particularly well-suited to hosting such a platform. Cooperation is necessary - particularly with the government, regulatory authorities, companies, and digital service providers. Nevertheless, as PIMS facilitates the free flow of personal data while strengthening the rights of consumers, it could be a win-win-win deal for consumers, companies, and regulatory authorities.

Data serfdom

Today, it is companies, and not people, who control personal data. Yet many companies lack the resources to analyse or make use of this data. After 2018, people will be in control of their own data. To explain why innovation and privacy are not mutually exclusive, and why both companies and individuals have cause for optimism, we go far back into early European history.

In the Middle Ages, serfs were bound to labour the land of an aristocrat in exchange for shelter and a small plot of land. Because of this living arrangement, neither serf nor landlord had much interest in technological innovation. Due to a series of crises, serfs eventually gained more rights, including wages and the right to offer their labour elsewhere. As a consequence, the labouring class was incentivised to improve their lives. This led to greater efficiency in agriculture, new technology, and the development of a market economy and early capitalism. In the long run, this was something both parties benefited from.

The ongoing expansion of the data economy has been called 'the fourth industrial revolution'. Today, personal data is monetised. However, people are far from having ownership over their data. Arguably, we still live in a state of 'data serfdom'. We trade our personal data for services, many of which we are utterly dependent on. It is hard, if not downright impossible, to transfer data from one service provider to another.

Data portability would benefit more than just the individual. Although more data is being collected than ever, companies can also have the paradoxical problem of not having the right data. The situation today is intrusive data collection, customers endlessly filling out the same forms, and data brokers selling data of questionable validity. If service-providers are given permission by the individual to access their personal data in a secure and easy way, this might significantly lower the barrier for innovation and the creation of new services.

Upcoming regulations will give people control over their data, including the right to transfer it between companies. In other words, the serfs are about to get paid.

They will need a bank.

Chapter 1:

The trust mindset

How trust makes everything possible.

1.1 Introduction to the whitepaper

The word 'data' comes from *datum*, which is Latin for 'a thing given'. The definition reflects to a certain extent how things are today, and even more how things could be in the future. People want to give away their data - as long as they feel they can trust the recipient, and get something in return. In this way, data is similar to money. Only when trust is violated do people withhold their data, proverbially "stuffing it under their mattress".

This is perhaps the clearest reason why the personal data economy cannot reach its full potential without the full trust and participation of the people. Trust lays the foundation for the personal data economy.

In this chapter, we will explore institutional trust more fully, and how it relates to demand for data-driven services. This lays the groundwork for Chapter 2, where the effects of the upcoming General Data Protection Regulation will be analysed. Finally, in Chapter 3, we outline the innovation opportunities to be found in the regulation, and strategies for entering the personal data economy.

1.2 Methodology

- This whitepaper is primarily addressed to the financial services industry in the Nordic market.

- When referring to 'the EU' and 'Europe', this includes the 28 EU member states as well as non-EU EEA states Iceland, Norway, and Liechtenstein.

- This paper will focus on psychological attitudes among people, the expected effects of the GDPR, and strategies to create opportunities out of regulatory changes.

- The role of technology is not addressed in this paper. Nor should this be considered a comprehensive guide to GDPR compliance.

- To support the paper's goal of investigating Nordic attitudes to personal data, the research team conducted a survey in September 2016 (161 participants, 60 % men, 52 % aged 22 - 35). The respondents were predominantly Norwegian-speaking (81 %).

1.3 Untapped Big Data potential

Companies are collecting increasingly larger volumes of customer data, under the mantra of 'more is better'. However, creating value from collected data continues to be a problem for many companies. Much of the data will be messy and unstructured - so-called 'dark data'. External data is often necessary to understand the customer, but information provided by data brokers will vary in reliability.

The banking industry holds some of the most valuable customer data of all industries. Despite the industry's tremendous resources, most banks are currently unable to maximise the full potential of their data.

Some financial institutions lack the proper technology, others haven't embraced a data-driven culture, and for many others the barrier is more fundamental. Complex, outdated banking technology and siloed data are contributing factors to why banks are unable to use the full breadth and depth of data at their disposal. Overall, the financial services industry has lacked the ability to achieve practical insight from the data, and to use the insights for the direct benefit of the customer.

There has been increased interest in how to monetise customer data. Some banks have adopted direct monetisation models, selling their customer data to third parties. In the Nordic countries, strong regulations protecting user data have made it harder to adopt such a model. Other banks indirectly monetise customer data through analysing transaction history to leverage up- and cross-selling new services. Unfortunately, much of this data is stripped of a fair amount of information due to regulations that enforce customer anonymisation and permission for use. This makes it a challenge for banks to personalise the services on an individual level.

1.4 Attitudes towards banks

There is a common perception of low consumer trust in the banking sector. Survey data shows that people seem to trust the banking industry less than just about any other industry, and none more so than Europeans[1][2]. These statistics give room for pause. 'Trust' is not a uniform concept, and there are many different kinds of trust.

The perception of low trust is further propagated by the fact that 'trust' and 'customer satisfaction' are sometimes used interchangeably. Whether customers *like* their banks is an entirely different question from whether they *trust* them.

Trust is not dead

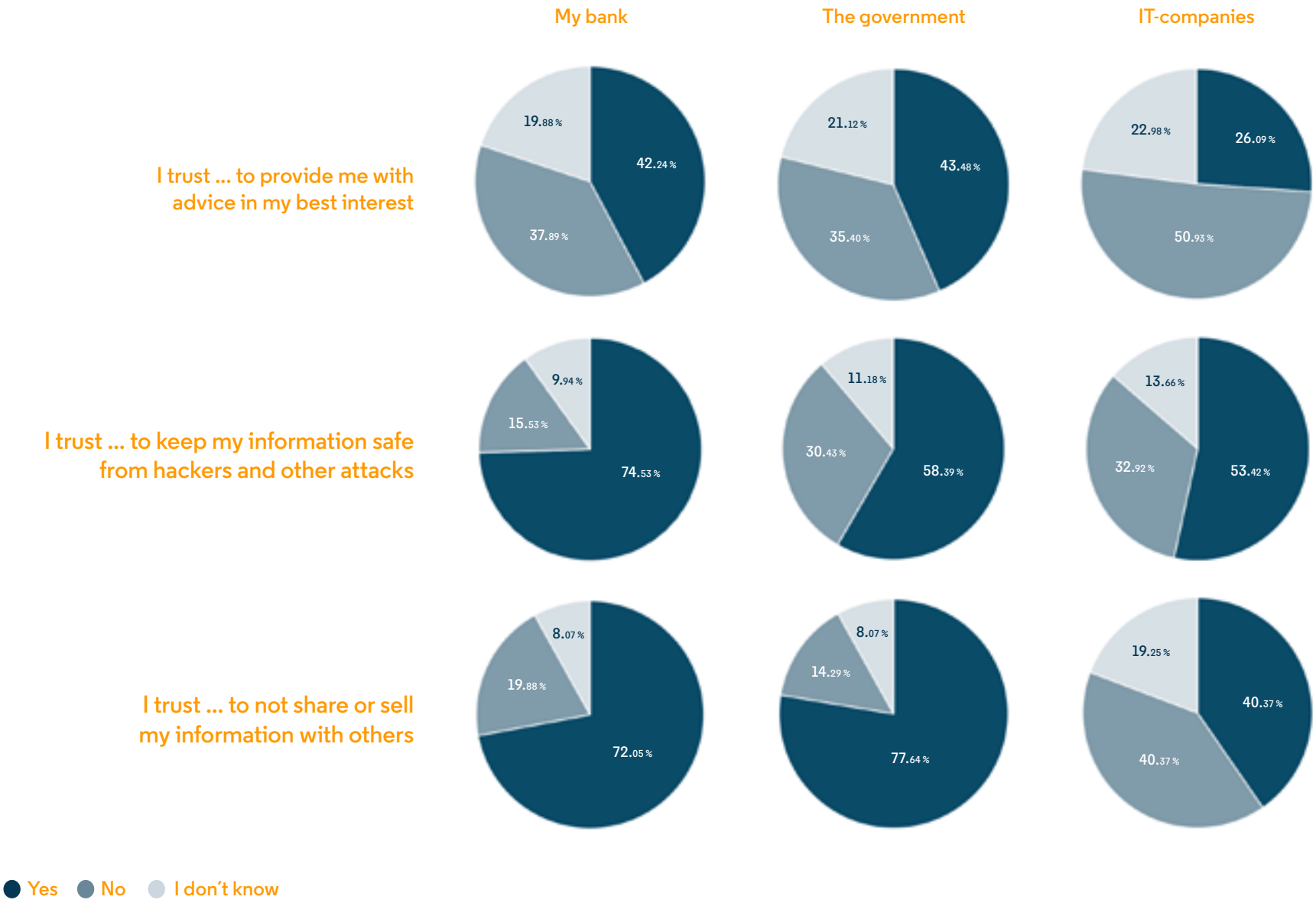
In a world-wide poll by Edelman, the financial services sector has among the lowest trust ratings of all industry sectors, whereas the technology industry is the most trusted[2].

The picture becomes more nuanced when we ask, *trust to do what?*

In our own survey (see next page), we were interested in delineating different kinds of trust between different sectors. Banks were the most trusted to keep personal data safe. Banks and governments enjoyed similarly high levels of trust to not re-sell information, and provide advice in the customer's best interest. In all cases, banks are trusted significantly more than IT companies.

This may seem paradoxical when considering the lower overall trust in financial services relative to the technology sector. Nevertheless, an Accenture report showed that 86 % of respondents trusted banks the most to securely manage their personal data over all other industries[3].

Citizens in Nordic countries trust their banks and national public authorities to protect their personal data more than citizens in any other European country[4]. As this chapter will argue, a strong fundament of trust is the keystone to engaging participants in the personal data economy. Therefore, high levels of trust give Nordic companies an advantage when it comes to providing data-driven services.


My bank
The government
IT-companies
I trust ... to provide me with advice in my best interest
I trust ... to keep my information safe from hackers and other attacks
I trust ... to not share or sell my information with others
42.24 %
37.89 %
19.88 %
43.48 %
35.40 %
21.12 %
26.09 %
50.93 %
22.98 %
74.53 %
15.53 %
9.94 %
58.39 %
30.43 %
11.18 %
53.42 %
32.92 %
13.66 %
72.05 %
19.88 %
8.07 %
77.64 %
14.29 %
8.07 %
40.37 %
40.37 %
19.25 %
Yes
No
I don't know

Source: EVRY

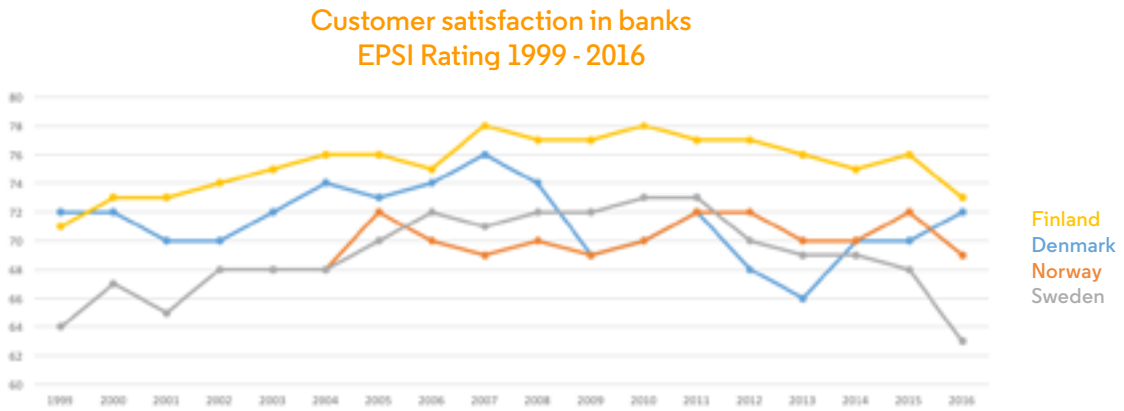
Declining customer satisfaction

One area for improvement in Nordic banking is customer satisfaction. Data from EPSI shows that customer satisfaction has largely been unaffected by the financial crisis of 2008*. Nevertheless, customer satisfaction in Nordic banks has been slowly declining over the past 10 years[5].

Even though banking services are available at any time through online platforms, banks are mostly perceived as distant for the customer. The closure of local branches, dismantling of personal service in rural areas, as well as neglecting customer promises are all contributing factors to the decline. The winners of customer satisfaction are for the most part small regional banks who operate with local branches[5].

However, Skandiabanken with its online-only business model, is ranked as number one in customer satisfaction and loyalty in Norway[6]. Simple and user-friendly services, as well as strong internal investments in IT, have been attributed as the reasons for Skandiabanken's success[7 8].

**The exception being Denmark, where customer satisfaction with banks dropped rapidly between 2007 and 2009 due to the collapse of the Roskilde Bank and the following aftermath[9].*



Source: EPSI

Dwindling loyalty

Customers increasingly view their relationship with banks as transactional as opposed to advice-based[3]. Today, customers can obtain basic banking advice from the internet. Users are tech-savvy, and research credit cards, mortgages, and loans online rather than in their local bank branch. This leads them to diversify their bank portfolio, picking and choosing products from different banks.

However, customers spend enormous amounts of time researching difficult financial decisions on their own[10]. If given the offer, customers would still appreciate help making difficult and complex decisions. Receiving additional advice would also make them more loyal. Almost half of Accenture's survey respondents state that they would be more loyal to their bank if they received assistance in buying a car or a home. Even if a bank did not offer the most favourable mortgage rates, nearly a third of consumers would be willing to apply for a mortgage with their current bank if they also received end-to-end customer service[3].

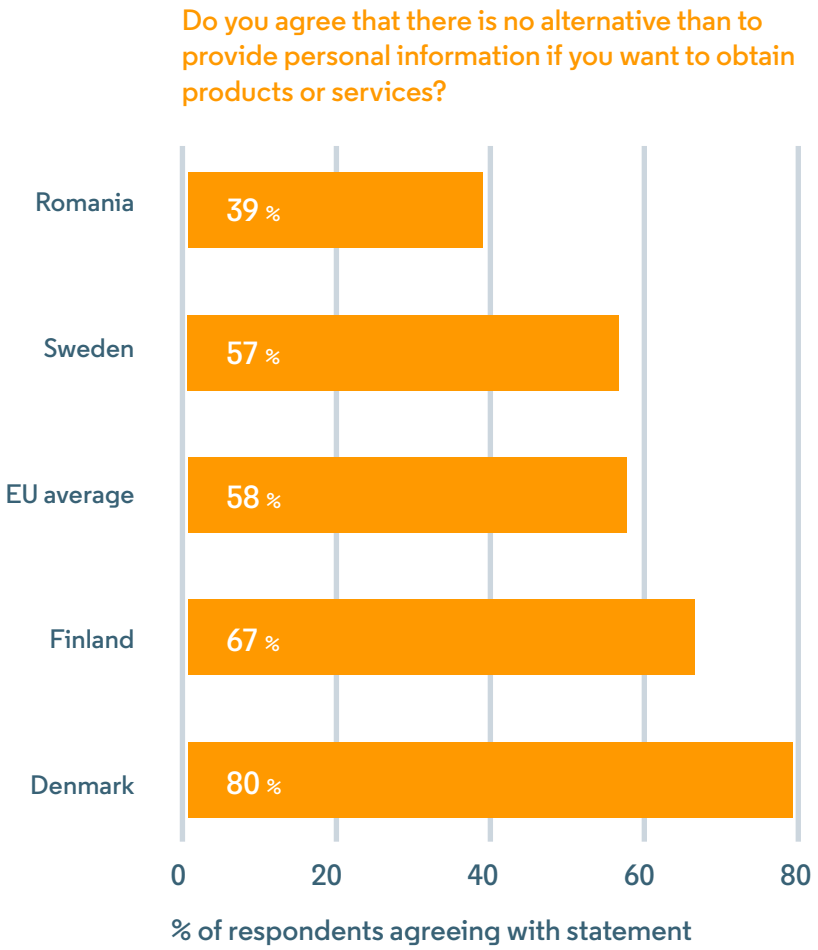
In short, people want services which will simplify their lives. By providing these services, banks can bolster customer loyalty.

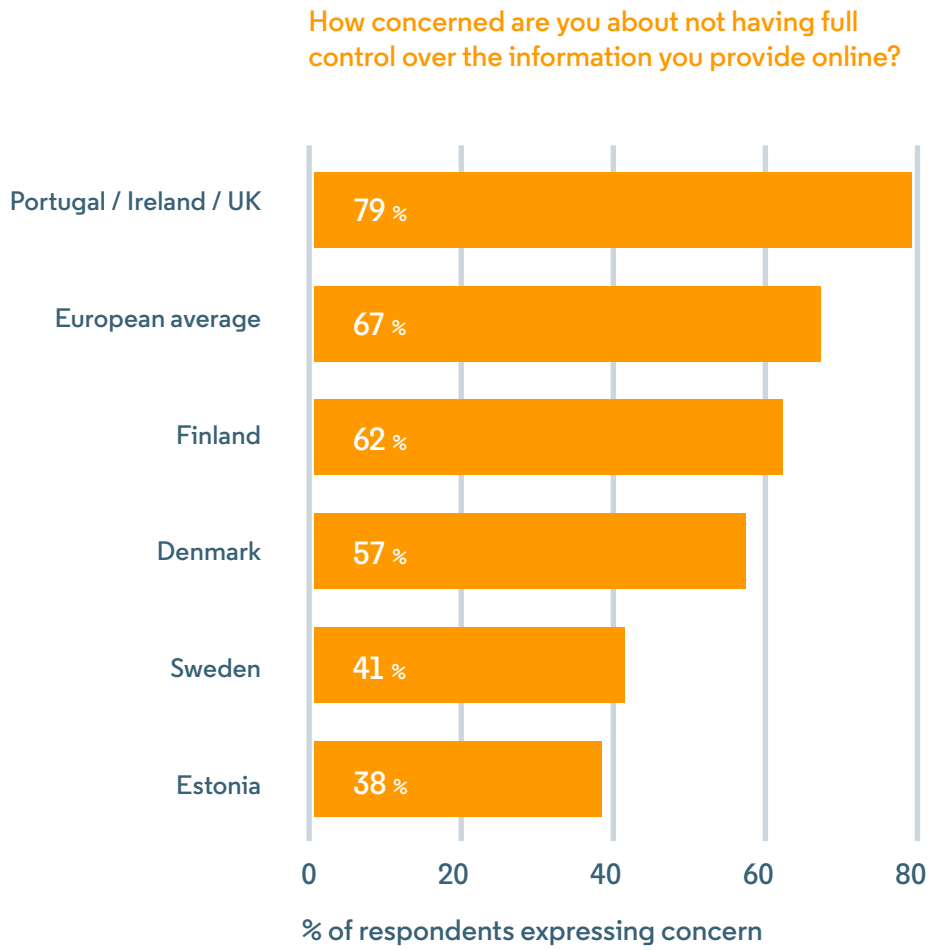
1.5 A question of control

People also find the idea of trading personal data for services natural. According to a survey by Fujitsu, **97 % of European respondents were happy for their personal data to be used to inform, make recommendations or add value to their financial services**[11]. Some of the most popular services people would be willing to trade their data for were lower mortgage or insurance premiums, relevant product and service recommendations, and information on their spendings and savings.

It is legitimate to ask how much control people are willing to sacrifice in order to receive services. It is well-known that people take risks for the sake of convenience, such as using public WiFis and passwords that are easily cracked[12] [13]. A Europe- wide survey by the European Commission (the Eurobarometer) shows that Norwegians are the worst at reading Terms and Conditions carefully and completely, with other Nordic countries all below average[14]. In another Eurobarometer report, which did not include Norway, Nordic individuals were relatively unconcerned about not having full control over their data, with only Estonians being less concerned[4]. Disclosing personal information was also not a big deal. Denmark believed more than any other country in Europe that there is "no alternative than to provide personal information if you want to obtain products or services".

So although a fair proportion of Nordic respondents do care about controlling their personal data, the region as a whole appears less worried than the rest of Europe.





Both charts show responses at the extremes; the EU average; as well as the three Nordic EU-countries, Denmark, Sweden, and Finland.

Source: Eurobarometer

Across the countries, there was a correlation between high trust in authorities and institutions, and low need for control, as well as belief that providing personal information is a part of modern life. Among all European countries, the Nordic countries trusted their banks and national authorities the most to protect their personal information. Source: *Eurobarometer*

1.6 Paying the price with data

The authors of the last Eurobarometer report describe a trend across European countries: the more institutional trust a country has, the less concern there is with control, and the greater the willingness to provide personal data in exchange for services. With trust, people willingly engage in the data-driven economy. Without trust, they withdraw.

Banks are, more than any other sector, trusted to handle personal data. Institutional trust in banks is particularly high in the Nordic region. Nevertheless, customer satisfaction is declining, as banks are perceived to be distant and impersonal. There is currently an unmet desire for more financial services, particularly those which make life easier or aid difficult decision-making. Providing these valued services may be a way to boost customer loyalty. Furthermore, Nordic customers are more willing than most to pay for services with personal data. Nordic banks are therefore well-positioned to handle personal data, and have a strong incentive to do so.

Chapter 2:

The General Data Protection Regulation

Regulatory tsunami or wave of opportunity?

2.1 Introduction

Two regulatory waves are approaching the sleepy beach of traditional banking in 2018.

The revised Directive on Payment Services (PSD2), which comes into force 13 January 2018, will facilitate the free flow of financial data by relieving banks of their monopoly on customer account data[15]. European banks will be forced to share the data with certified third parties looking to create value from it. Additionally, the threat from financial technology companies (fintechs), which challenge banks on basic and innovative financial services, has been apparent for some time. Already some banks are turning these supposed disadvantages into opportunity by launching themselves as service-oriented platforms via 'Open Banking', thus bringing third party services into the bank's own ecosystem.

The General Data Protection Regulation (GDPR) enters into application 25 May 2018, and affects all industries[16]. The aim of the GDPR is to create a unified framework for personal data protection across Europe. People will have the right to access their personal data across companies, request its deletion, and transfer it from one company to another. There will be strict requirements for data security, and organisations will be severely fined if they fail to meet compliance requirements.

Just like some banks are creating opportunity from the PSD2's requirement for data sharing, so might the GDPR offer new opportunities in the personal data economy.

The main focus of this chapter will be GDPR. For more information of the implications of PSD2, see EVRY's whitepaper on the topic[17].

2.2 GDPR

The GDPR is the most lobbied-against legislation in European history, with almost 4,000 amendments[18]. In a nutshell, the GDPR increases the control data subjects have over their personal data, and is expected to set the global standard for data privacy. It will replace the Data Protection Directive from 1995.

There has been a recognised need to update data privacy legislature in the current technological and political climate. As mobile technology, wearables, and the Internet of Things (IoT) are increasingly becoming mainstream; huge amounts of personal data are circulating the personal data economy. We have seen the rise of 'bigtechs' - huge technological companies such as Google and Facebook - which may know more about you than you do yourself. Following the Snowden revelations, European citizens have become increasingly fed up with 'Big Brother'-style monitoring.

All companies in all sectors who offer goods or services to EU residents, monitor their behaviour, or process their personal data, must comply with the GDPR. This includes both data controllers and data processors.

A major change of the GDPR from the existing Data Protection Directive is that data processors can also be held accountable in the case of non-compliance. Extended accountability, together with prohibitive fines, is expected to significantly decrease the occurrence of security breaches.

Another goal of the regulation is to cut bureaucratic costs for companies currently having to comply with different privacy legislation and different data protection authorities (DPAs) in different European countries. With the GDPR, the same rules will apply across Europe, and a company will only have to deal with the data protection authorities (DPA) in the country where they are headquartered.

Most companies will have to make operational reforms. Some of the most important changes are outlined in the following pages.

Data controllers and data processors

A data controller is any entity which decides the purpose and manner of data collection (e.g. an organisation, company, or business, etc.).

A data processor is any entity which processes data on behalf of the controller (e.g. data warehouses, market research companies, accounting firms, external cloud storage, etc.).


COMPONENTS OF THE
GDPR
DATA PORTABILITY
BREACH NOTIFICATIONS
PSEUDO-NYMISATION
PRIVACY BY DESIGN
APPOINT DATA PROTECTOR OFFICER
FINES
CONSENT
RIGHT TO ACCESS
PROFILING RESTRICTIONS
PURPOSE LIMITATION
RIGHT TO ERASURE

The GDPR means expanded data rights

- **Right to access:** Data subjects have the right to access their data, and rectify it if incorrect. Controllers have one month to respond to the customer's request for access.

- **Right to erasure:** Data subjects have the right to have their data deleted.

- **Data portability:** Data subjects have the right to receive their personal data in a "machine-readable format" and transfer it between data controllers.

- **Consent:** Consent will be required for the collection and processing of personal data. In the GDPR, consent is defined as the signalling of agreement through "a statement or a clear affirmative action". Pre-ticked boxes or inactivity do not count as consent. Consent should be communicated in clear and simple language, and be distinguishable from other terms and conditions. Ambiguous language will not be accepted. It should be as easy to withdraw consent as it is to give it.

- **Purpose limitation:** Data may only be used for the purpose consented to. If the data controller wishes to use the data in new ways, new consent must be acquired.

- **Profiling restrictions:** The GDPR places new restrictions on 'profiling', defined as automated processing of personal data to assess certain aspects of a person. Data subjects have a right to be informed about the consequences of profiling, and will have a right to object.

What is personal data?

The GDPR defines personal data as "any information relating to an identified or identifiable natural person". This includes both direct identification, such as name, as well as indirect identification through description.

Clearing up previous ambiguities, personal data specifically includes online identifiers such as location, IP address, cookie strings, and device IDs.

Consent must be "explicit" for the processing of "special" personal data, also known as "sensitive personal data". This specifically includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual life. Biometric or genetic information are also treated as special data.

The GDPR means more security

- **Privacy by design:** The GDPR's requirement for 'privacy by design' means that privacy must always be taken into account when planning any new company operation, and not slapped on later.

- **Breach notifications:** The GDPR places new demands on security. Importantly, data breaches must be reported to the DPA within 72 hours. If the data breach is likely to result in a high risk to the data privacy of any individual, they too must be notified immediately. For the financial sector in most European countries, including the Nordic region, this represents a new requirement.

- **Data Protection Officer:** Both data controllers and processors will be required to appoint a data protection officer (DPO), tasked with monitoring compliance and cooperating with the DPA.

- **Fines:** Fines will be imposed for non-compliance. The highest level of fines for non-compliance is €20 million or 4 % of annual global turnover, whichever is greater. Data subjects will also have the right to claim compensation.

- **Pseudonymisation:** Although the GDPR does not make any specific technical requirements, it advocates pseudonymisation as a security measure. Pseudonymisation is the process whereby personally identifiable information is replaced by an artificial identifier, and a separately kept security key. Data breaches involving pseudonymised data need usually not be reported to the individual if the key is not compromised. Data pseudonymisation may also allow the data processor to further analyse data without consent for "scientific, historical, or statistical" research purposes.

2.3 Short-term challenges

In the short term, handling personal data will be a compliance burden for many companies. This is evidenced in the fact that the market opportunity for security and storage software vendors following the GDPR is expected to surpass $3 billion[19]. Furthermore, there is great uncertainty about how to proceed, and many companies do not currently possess the tools to comply with the GDPR[20]. The GDPR will in some cases require the rewriting of industry standards, and it is in the best interests of industries to immediately assess whether existing standards contradict the GDPR. Standardised procedures are needed for handling requests for data erasure, fines, damages claims, and data portability. For example, it is not clear how laws concerning bookkeeping will interact with the GDPR's right to erasure.

The greatest challenge for Nordic banks with regards to GDPR compliance will likely be the right to erasure, data portability, and requirements for data breach notifications.

Today, legacy IT systems make it cumbersome to provide data access, transfer, and erasure when customer data is spread across silos. In the long run, renewing core systems may relieve compliance burdens by affording easy access to user data, and making processes more efficient and less prone to human error.

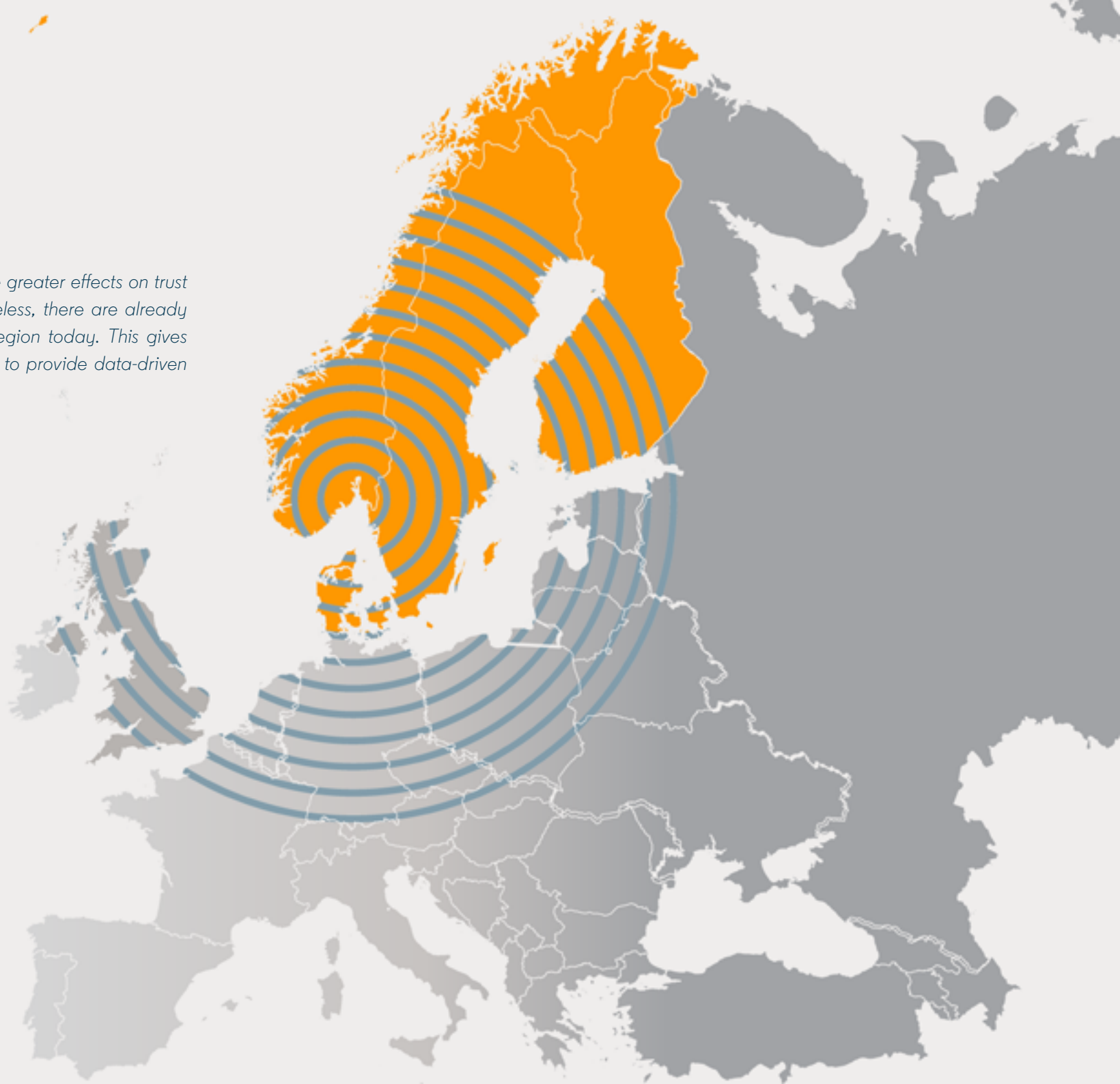
2.4 Data portability

The Article 29 Data Protection Working Party (WP29) is tasked with creating guidelines, tools, and procedures for the right to data portability, and other aspects of the GDPR.

Data portability is more likely to be a burden for businesses who own valuable or unique data, as customers will be able to transport this data to competitors. Startups and small businesses could also be at a disadvantage, since they may not have the immediate ability to fully leverage their data. The winners will likely be those who are able to create the most valuable services for their customers, not those who hold the most valuable data.

GDPR does not impose data controllers to share data in a format which is compatible to the recipient, though it must be "structured, commonly used and machine-readable". Today, most companies do not have the capabilities to make use of data from other controllers. This will probably change quite rapidly once data portability becomes a reality.

We believe that the GDPR will have greater effects on trust outside the Nordic region. Nevertheless, there are already high levels of trust in the Nordic region today. This gives the region immediate opportunities to provide data-driven services.



2.5 Renewed trust across Europe

How will the GDPR impact the behaviour of European citizens? Ultimately, this depends on how well companies comply with the GDPR, and the level of awareness in the population around the regulation.

Nevertheless, we expect to see different impacts in different regions in Europe. As we saw earlier, many Europeans outside the Nordic region are concerned about not having enough control over their data. We believe that the GDPR will go some way to build consumer trust in data-driven services in these countries.

Although the GDPR will have important consequences also in the Nordic region, we expect to see a smaller impact on trust. Regulatory frameworks are already very protective of user privacy, especially in the financial services industry. In the Nordic region, there already is high trust in banks and governments to protect personal data, and consumers have a lower need for control.

Companies may do well to choose different strategies for advertising GDPR compliance across Europe. Emphasising control of personal data may be more relevant in countries where there is a high need for control. In the Nordic region, less focus should be placed on control, and more on the benefits of new data-driven services.

The GDPR may in the long run bolster trust across Europe. However, this could take years, and the Nordic region already have the advantages of trust, and people who are to a large extent willing to trade personal data for services. **Therefore, we believe that the Nordic region will continue to provide an advantageous environment for the personal data economy.**

Chapter 3:

Sailing the regulatory wave

"It's not privacy or innovation – it's privacy and innovation. The personal information economy can be a win-win situation for everyone. Get it right, and consumers and business benefits."

- Elizabeth Denham, UK Information Commissioner

We will work with industry and civil society to build this up from the ground. We must associate all stakeholders.

Isabelle Falque-Pierrotin,
Chair of the Article 29 Working Party

3.1 From compliance to opportunity

Regulatory changes will lay the cornerstone for ground-breaking changes in the use of private data. This presents several opportunities for banks and companies to leverage regulatory demands to position themselves within the new personal data economy.

> *Don't just engage in individual dialogue; bring solutions. We don't have time.*
>
> *Jacob Kohnstamm, Chair of the Dutch DPA*

Evaluate capacities for meeting the regulatory requirements

How easy is it for your financial institution to delete and transfer data? Can customer requests be responded to within the one-month deadline? Consider obtaining external help with compliance. Also evaluate current data collection practices, and the objectives for data collection. Unnecessary personal data may pose a security risk, and the prevailing notion that "more is better" will no longer apply when data becomes more available.

Give customers transparent access to their data

Create a "dashboard" where customers can access the personal data the company holds on them. From the same dashboard customers can also erase data, and manage consent for different services. Data access is a requirement for the GDPR, but creating a transparent and easy-to-use interface further promotes trust (see next page: "The Creepiness Conundrum").

Expand compliance

Compliance should be extended into all branches of the company, especially public relations, IT, and customer service. Similarly, representatives for different branches, operations, and interests within the company should be included in the compliance division. This will minimise the risk of acting in noncompliance, but also allow the company to more freely use personal data without fear of accidental noncompliance.

Shape industry standards with concrete solutions

The Chair of WP29 has specifically requested that industries collaborate closely with WP29 to interpret the GDPR[21]. Specifically, concrete and usable solutions are requested. Companies should appoint a DPO as soon as possible to stay informed about the workings of the WP29. Companies should also work with the national DPA to create new standardised procedures where previous procedures fall outside GDPR compliance.

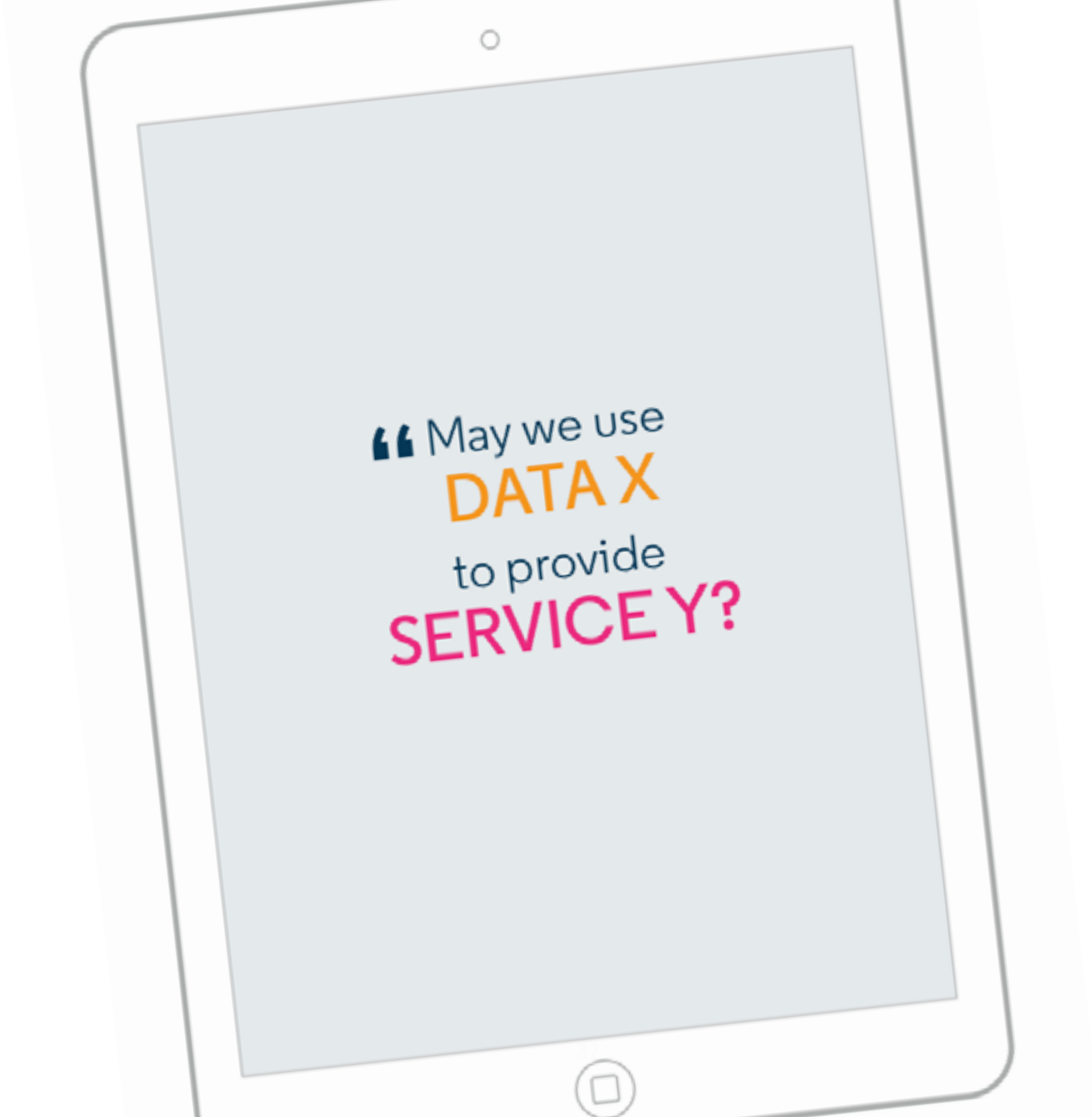
3.2 The creepiness conundrum

A few years ago, Target started sending a teenage girl baby-related products in the mail. By analysing her spending habits, Target had figured out that she was pregnant before she had even told her parents. While customers want services tailored to their individual needs, the prospect of companies knowing too much is considered creepy. Therefore, companies are wrestling with the conundrum of giving customers what they want, without appearing to know too much about the customer.

Targeted ads may feel creepy when the customer has not consented to the collection and analysis of their personal data. When companies reveal that they know very personal details about their customers, this often comes as an unwelcome surprise, because it reveals how little control the customer actually has over their data. As a consequence, customers may limit their interactions with the company[22].

There are two problems here: a lack of **transparency** and a lack of **consent**. The GDPR's requirement for purpose limitation - i.e., consent must be obtained for each new use of data - presents an opportunity to provide services in a way which improves customer relations (and doesn't feel creepy).

Always ask "may we use **data X** to provide **service Y**?" before each new service. Remind the user that the company is bound by law to only use the data for the purposes they originally obtained consent for.


“ May we use
DATA X
to provide
SERVICE Y?

3.3 Personal Information Management Systems

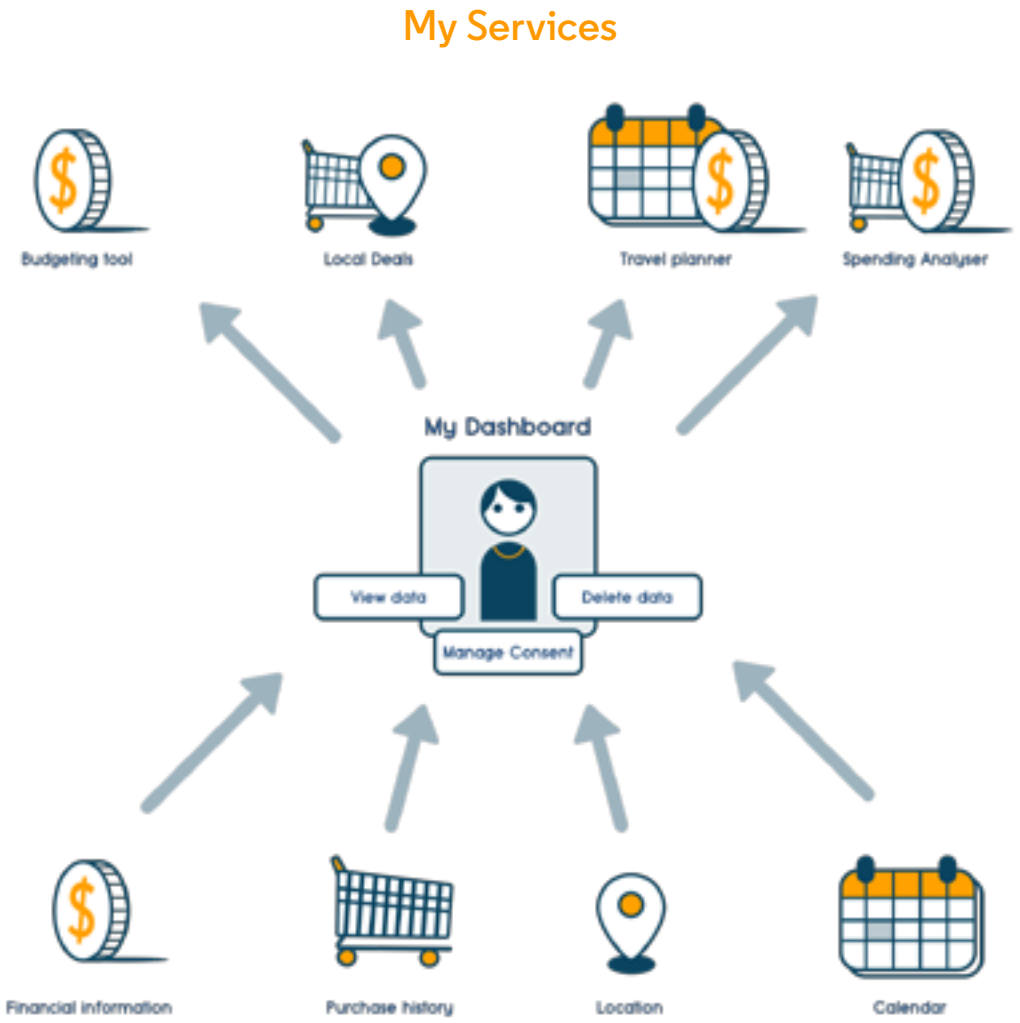
Currently, there is no platform giving a single view access to personal data across sectors and industries. Not only do customers not have full control over their data, they are also unable to reap the full benefits of Big Data. If an individual has access to all their personal data in a single place, it could be analysed in a myriad of new ways to benefit the individual. For example, a 'personal assistant' might provide insight based on direct analysis of personal data. Companies, for their part, are increasingly under pressure to gain access to new quality information on the customer in order to improve their analytics capacities. Due to technological innovations - such as mobile technology, IoT, and cloud computing, several organisations have predicted that a new class of services will fill this value gap[23]. Different organisations have used different names, though we use the name 'Personal Information Management Systems' (PIMS). The essential features are:

- **Single-person consolidated view:** From a single platform, an individual gets access to their personal data from multiple companies across industries, including the public and private sector.

- **Individual control over their data:** From a "dashboard", the individual can access, delete, transfer, and manage third party access to their data.

- **Value generation:** A PIMS gives companies permissioned access "traditional" customer data, as well as previously unavailable data sources. This may be used to improve existing services, or create entirely new services.

It is important to note that PIMS are not the same as data vaults or data warehouses. Storage is an optional, but not necessary feature of a PIMS.


My Services
Budgeting tool
Local Deals
Travel planner
Spending Analyser
My Dashboard
View data
Delete data
Manage Consent
Financial information
Purchase history
Location
Calendar
My Data Sources

3.4 The Nordic bank advantage

In anticipation of PSD2, some banks are reorganising their business models towards a future where customers' data will be open to third parties, by launching Open Banking platforms. There is considerably less attention to the fact that open data may be a reality for all industries, thanks to the GDPR's right to data portability. This gives banks a first-mover advantage in developing a PIMS. Leading up to 2018, banks have the opportunity to build up a systems architecture accommodating services based on financial and non-financial data.

In fact, banks have more than just the first-mover advantage. Banks are the most trusted institution to keep personal data safe. Nordic banks are also pioneers in providing digital identity verification. BankID in Norway and Sweden, though not identical, both provide digital ID to both the public and private sector. This may make banks well-suited to orchestrate personal data transfers as well. Digital identity verification can be a major challenge, and federated identification via Facebook or Google is not always suitable. You can't sign official digital documents with your Facebook account.

Today, bigtechs have come the farthest in acting as personal data platforms, integrating huge amounts of information and allowing onboarding to services. **Vis-à-vis bigtechs, Nordic banks have four major advantages in becoming platform managers of personal data:**

Banks are the most trusted to manage personal data

Bigtech's path towards acquiring personal financial information in the EU is not yet clear

"Everyone" has a bank

Nordic banks already act as digital identity verifiers

3.5 Paradigm shift – from company to individual

Today, companies manage data for their customers. In the future, people may be managing data for their service providers. This is a complete change in paradigm, shifting control of data from companies to the individual.

Loss of control over customer data may seem like an unwelcome change to many companies. However, customer control may be better for both companies and individuals. This is because it allows a more direct matching between supply and demand. If customers trust the platform, they may be happy to give away the necessary data to receive valued services. Customers will be sure that their data is only used for the purpose for which consent was given. Gratuitous data collection on the part of companies will become a thing of the past. Nevertheless, with a PIMS, companies would have access to rich and accurate data, without the need to be intrusive or rely on data brokers. The author Doc Searls has labelled this 'vendor relationship management' (VRM), in contrast to 'customer relationship management' (CRM)[24].

3.6 Why the time is right

Currently there are several hundred commercial startups acting as PIMS[25]. However, these are mainly research projects, in the pilot phase, or are only allowing the management of a limited amount of data. Nevertheless, these companies are counting down the days until 25 May 2018, and the new opportunites this will bring.

Previous attempts to create large-scale platform for banks and other industries to exchange information have also fallen through[26]. Voluntary initiatives of data portability, such as the UK Midata Initiative, have had mixed success, with only a few banks signing on[27].

Without legislation making data portability a right, few companies will take the bold step of voluntarily offering it. Data portability has network effects, as it encourages more service providers to accept external data, and more innovation based on new data sources. Yet when only a few companies offer data access and portability, the potential value is limited.

Up until now, restricted data portability has been a bottleneck for the personal data economy. After 2018 when both PSD2 and GDPR come into force, this bottleneck will start to loosen for both financial and personal data.

3.7 Converging Interests

The plausibility of the PIMS concept lies not in its idealism. The plausibility lies in the monetary interests inherent in the service. Boston Consultancy Group predicts that the value created through digital identity in Europe could be worth as much as €1 trillion by 2020[28]. They also predict that two-thirds of potential value generation will be at risk if stakeholders fail to establish trust with consumers. Therefore, there should be an overarching interest in building trust when monetising personal data.

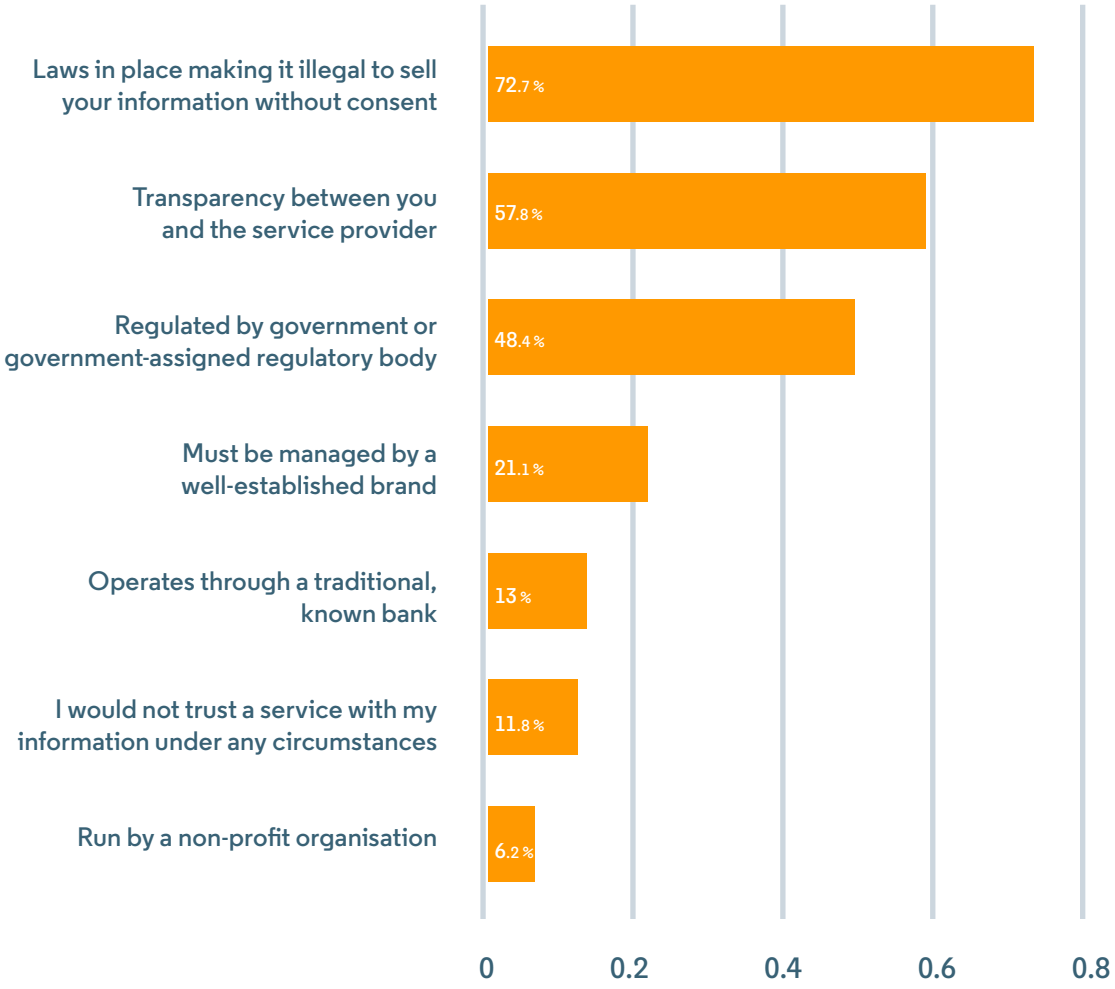
The economy as a whole may benefit from PIMS. However, major stakeholders - including individuals, companies, banks, and governments - all have an interest in the creation of PIMS.

Individuals

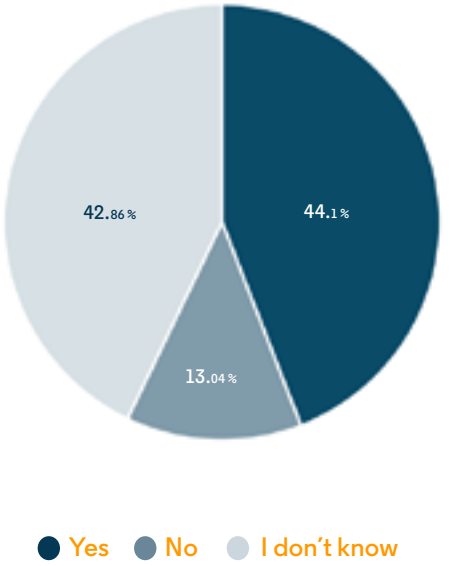
People want to trade their data for services, especially in the Nordic region. With the GDPR's right to data portability, individuals may demand that service providers create value from new data sources.

In our survey (see next page), we asked which requirements would have to be in place for customers to trust a service which stores and handles your personal information. The most important prerequisites were central tenants of the GDPR, such as regulation, transparency, and laws preventing resale of data without consent. If these requirements were met, consumers were overwhelmingly positive to adopting such a service.

What would be required for you to trust a service to store and manage your personal information?



If there were such a service meeting all these requirements, would you use it?



Source: EVRY

Companies

Companies and other service providers have perhaps the greatest incentive for PIMS. Most companies have difficulty analysing and creating value from their existing personal data. By connecting customer data to new and accurate data sources, companies can improve existing services, and lower the threshold for further innovation. A PIMS, which facilitates data access through consent, could be a tool for GDPR compliance, as well as improving customer relations and reducing costs for call centres and mass marketing.

Banks

Banks are looking for ways to combat decreasing margins due to fintech competition and diminishing loyalty. Permissioned access to more customer information allows the improvement of existing services. There is also high demand for personalised financial services, and a PIMS could facilitate this. A centralised view of the customer could lead to more automation, less human error, and greater efficiency of operations. As with companies, a PIMS would make GDPR compliance easier, especially the right to erasure. Access to more data points could also improve fraud detection capabilities.

Governments and DPAs

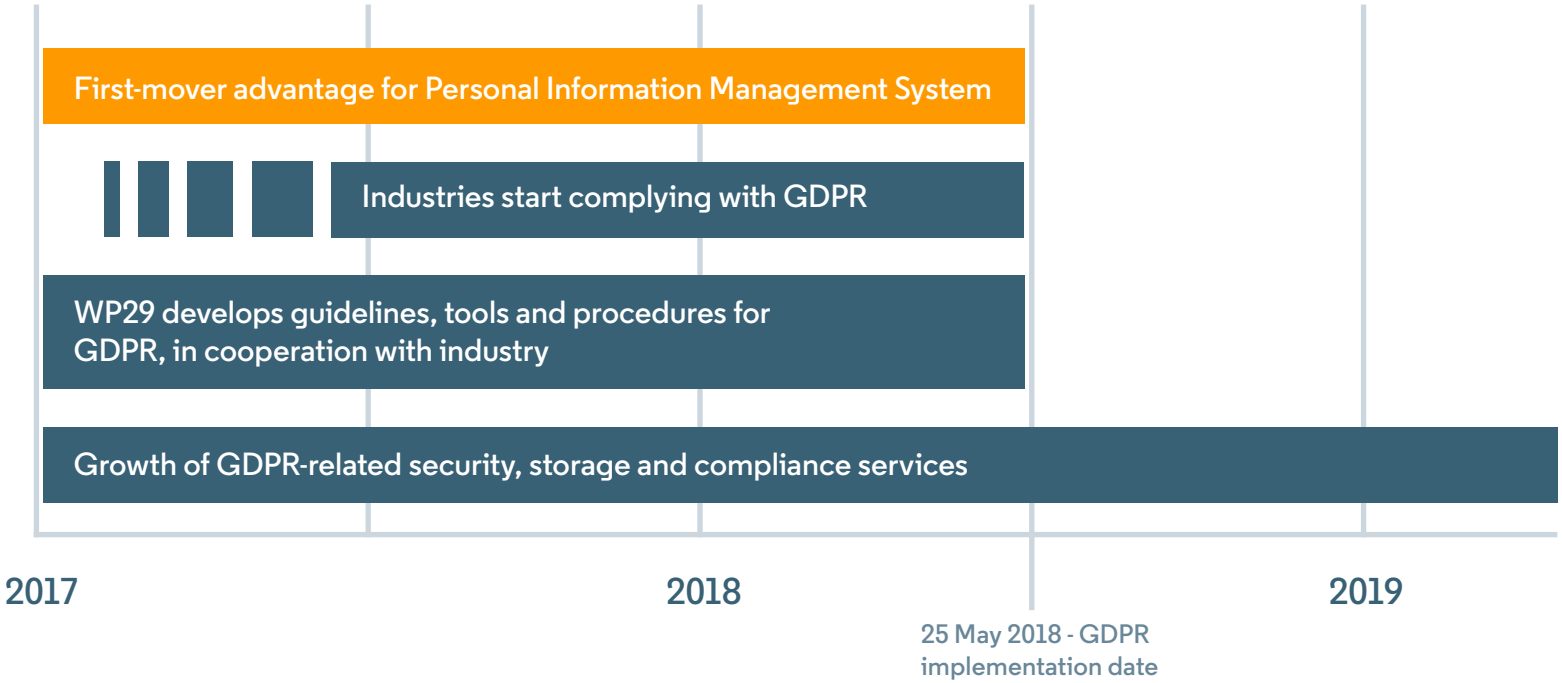
Governments have an overarching interest in the well-being of all sectors and stakeholders in society. A platform which facilitates the exchange of data could boost the economy. With a PIMS, the government can also make their operations more efficient, and more tailored to the needs of the citizens. A PIMS could also significantly streamline the work of DPAs. As recently as October 2016, the European Data Protection Supervisor wrote an opinion piece advocating the use of PIMS[29].

3.8 Two entry points for PIMS

From the viewpoint of banks, we suggest two different entry points for establishing a PIMS. These are both part of the same strategy, and differ chiefly in when banks start cooperation with other stakeholders.

- **Entry point 1: Transition to Open Banking:** Many banks are already exploring the options for Open Banking. An Open Banking platform can later be expanded to give permissioned access to non-financial data for a multitude of services across public and private sectors.

- **Entry point 2: Cooperate with stakeholders:** Early on, banks enter into cooperation with major stakeholders, such as the government and the DPA, trade organisations, companies, and financial authorities, to co-create a PIMS.



While industry norms remain unclear, there is an opportunity for leadership in offering practical solutions for GDPR compliance. Different industries will increasingly be seeking help for GDPR compliance. Prior to the implementation date for the GDPR, there is a window of opportunity for launching a Personal Information Management System.

Entry point 1: **Transition to Open Banking**

(see EVRY's whitepaper on Open Banking)

With PSD2, third parties will be able to enact payments on behalf of banks, and with the customer's consent, gain access to their account information in order to provide services. Banks can stand passively by and give fintechs the necessary information. Alternatively, they can create an Open Banking platform business, which encourages third parties to create new valued services, and places banks in the centre of this ecosystem. Many larger banks such as Citi, Capital One, and Deutsche Bank, are already in the process of doing so.

Once in place, Open Banking can be expanded to handle non-financial data on behalf of the customer, as well as facilitate permissioned access to third parties - while maintaining the central role as proprietors of the platform. Open Banking can therefore be the first step towards a PIMS. As this transition takes place, cooperation will become increasingly necessary, especially if a PIMS is to include public sector services.

Such a strategic transformation is not available for everyone. Banks who are transitioning towards Open Banking have also implemented costly updates to their core architecture[30]. Open Banking ecosystems may even be a "winner takes all" concept, with only a few actors at the top, and not something every single bank can, or should, try to win. Although smaller banks may be unable to create a large financial, commercial, and social ecosystem themselves, they might be able to become service providers on a larger bank's platform.

Benefits of transitioning to Open Banking

Implement quickly

Many banks are already transitioning towards Open Banking, and we know that it is something we can expect to see within a couple of years. Adopting aspects of Open Banking is, in theory, something any bank can decide to do on their own tomorrow.

Locking in the market

By providing a few simple and valued services, banks have a chance of quickly capturing the market. To maintain lock-in, they will have to continuously improve their services, but it will also be more difficult for new entries to replace them.

Entry point 2: **Cooperate with stakeholders**

Here, the focus is on creating a PIMS in cooperation with key stakeholders. Relevant parties would be the government and government agencies, the European Commission, trade organisations, companies, financial authorities, digital service providers, and the DPA. This approach is suited for banks of any size who want to participate in the personal data economy. It is also suited to the Nordic environment where there is high trust in the government. Although banks have stated advantages in hosting the platform, any stakeholder might take this role. A basic PIMS, which affords control over a few personal data sources and offers a few valued services, is a realistic starting point.

Benefits of cooperating with stakeholders

Open to all banks

Not every single bank has the capability to transition to Open Banking. However, these banks do not want to be left behind when Open Banking becomes a reality. By not providing up-to-date services, they risk losing market share to fintechs and banks who have adopted aspects of Open Banking. For many banks, the only way to stay ahead may be to divide the bill with several other stakeholders.

Maximise goodwill

Getting other stakeholders on board may be easier if they are equal players in the decision-making process from an early stage. It will also be easier to cooperate with the government, as is necessary if the platform is to be connected to government services. Banks hold one of the most valuable information stores in society. Governments must balance the need to grow the economy with preventing a data monopoly. As such, they may be more supportive of an initiative where the banks aren't sole proprietors of the platform.

Use case: MyData (Finland)

The Finnish MyData[31] alliance offers a human-centred approach to personal data management, and has over 40 organizations, including retail chains, telecoms, banks, digital service providers, companies, government agencies and research institutes. There are several ongoing projects in Finland, with the common aim of giving individuals control over their personal data and the ability to benefit it, by offering new and innovative services. MyData is also an international collaborative project, and the term is used in Italy, Spain, Estonia, and France.

3.9 Closing remarks

This whitepaper presents a vision of how banks and other companies can meet the needs of individuals, beyond just regulatory compliance. However, a platform which gives individuals control and benefit from their personal data is not inevitable. It requires considerable cooperation, re-writing of established rules, and a strategic leap of faith.

A goal of this whitepaper has been to convey different perspectives and interests, and show where they converge. The GDPR is not just a burden, it is also an opportunity. While companies may see the GDPR as a regulatory tsunami, privacy advocates see it as a small wave facing the real tsunami: Big Data.

Here, it is in the interest of companies to understand the perspective of privacy advocates. Big Data and market power is gathered in fewer and fewer hands, and gravitates towards the largest players. A more level playing field within the personal data economy benefits everyone, consumer and company alike.

Big Data is a tsunami which cannot be stopped, but it can be sailed.


For more information, please visit www.evry.com/financialservices

Sources

1. Edelman (2016): Trust Barometer: Trust in Financial Services. Retrieved from Edelman Insights & Blogs: http://www.edelman.com/insights/intellectual-property/2016-edelman-trust-barometer/state-of-trust/trust-in-financial-services-trust-rebound/

2. Edelman (2016): Trust Barometer: Global Results. Retrieved from Edelman Insights & Blogs: http://www.edelman.com/insights/intellectual-property/2016-edelman-trust-barometer/global-results/

3. Accenture (2015): North America Consumer Banking Survey 2015. Retrieved from Accenture Corporate Web site: https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/Microsites/Documents17/Accenture-2015-North-America-Consumer-Banking-Survey.pdf#zoom=50

4. European Commission (2015, June): Special Eurobarometer 431 - Data Protection Report. Retrieved from European Commission - Public Opinion: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

5. EPSI Rating Group (2016, May 10): Nordic Banking Report 2016. Retrieved from Svenskt Kvalitetsindex: http://www.kvalitetsindex.se/wp-content/uploads/2016/06/Nordic-Banking-report-2016.pdf

6. BI Business School (2016, October 06): Norsk Kundebarometer - Bank og finans. Retrieved from Smarte Penger - Kundetilfredshet: http://www.smartepenger.no/forbruker/1339-kundetilfredshet-bank-og-forsikring

7. Njarga, B. (2011, October 3): Skandiabanken har fornøyde kunder. Retrieved from Dinside: http://www.dinside.no/okonomi/skandiabanken-har-fornoyde-kunder/61587576

8. Valle, M. (2015, December 7): IT-avdelingen er gullet vårt. Retrieved from digi.no: http://www.digi.no/artikler/it-avdelingen-er-gullet-vart/319998

9. Ministry of Business and Growth Denmark (2013, September 17): The financial crisis in Denmark - causes, consequenses and lessons. Retrieved from Ministry of Business and Growth Denmark: https://www.evm.dk/english/publications/2013/13-09-18-financial-crisis

10. King, B (2012): Bank 3.0 Why banking is no longer somewhere you go but something you do. John Wiley & Sons. p. 63.

11. Fujitsu (2016) The Fujitsu European Financial Services Survey 2016. Retrieved from Fujitsu Corporate Web site: http://newpaceofchange.com/

12. Fujitsu (2010): Personal Data in the Cloud. Retrieved from Fujtisu Corporate Web site: http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf

13. Kaspersky (2014, July): Consumer Security Risks Survey 2014: Multi Device Threats in a Multi-Device World. Retrieved from Kaspersky Corporate Web site: https://press.kaspersky.com/files/2014/08/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf

14. European Commission (2011, April): Special Eurobarometer 342 - Consumer Empowerment. Retrieved from European Commission - Consumers: http://ec.europa.eu/consumers/consumer_empowerment/docs/report_eurobarometer_342_en.pdf

15. European Parliament and The Council of European Union (2015, October 10): Revised Directive on Payment Services (PSD2). Retrieved from European Commission - Banking and Finance: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

16. European Parliament and the Council of European Union (2016, May 4): General Data Protection Regulation. Retrieved from European Commission - Justice: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

17. EVRY Financial Services (2015): PSD2 - Strategic Opportunities Beyond Compliance. Oslo: EVRY AS. URL: https://www.evry.com/globalassets/bransjer/financial-services/bank2020/wp_psd2/psd2_whitepaper.pdf

18. Lexology (2015, July 31): One small step for Europe; one giant leap for data protection? Retrieved from Lexology website: http://www.lexology.com/library/detail.aspx?g=981b312b-3c22-4631-b7d9-a390952efac1

19. International Data Cooperation (IDC) (2015, November 03): IDC Predicts GDPR Will Create a $3.5B Market Opportunity for Security and Storage Vendors. Retrieved from IDC - Press Release: https://www.idc.com/getdoc.jsp?containerId=prEMEA40551915

20. Baker & McKenzie (2016): Preparing for New Privacy Regimes: Privacy Professionals' Views on the General Data Protection Regulation and Privacy Shield. Retrieved from Baker & McKenzie: http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf

21. Pierrotin, I. (2016, March 16): Isabelle Falque Pierrotin's speech to the Centre for Information Policy Leadership (CIPL) - GDPR Amsterdam Workshop. Retrieved from Centre for Information Policy Leadership's archives: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/isabelle_falque_pierrotins_speech_-_amsterdam_-_cipl_-_march_2016.pdf

22. Rose, J., Lang, F., & Lawrence, A. (2016, June 21): Bridging the Trust Gap: The Hidden Landmine in Big Data. Retrieved from BCG Perspectives: https://www.bcgperspectives.com/content/articles/big-data-advanced-analytics-technology-digital-bridging-trust-gap-hidden-landmine-big-data/

23. Though using different names, these all describe similar concepts: World Economic Forum write about "Personal Data Services", Ctrl+Shift predict the rise of "Personal Information Management Services", Mydex writes about "Personal Data Stores", and KuppingerCole writes about "Life Management Platforms".

24. Searls, D. (2013): The intention economy: when customers take charge. Harvard Business Press.

25. e.g. Digi.me, meeco.me, Datacoup.com

26. e.g. The Digital Asset Grid by The Society for Worldwide Interbank Financial Telecommunications (SWIFT)

27. Out-law (2014, February 17): Midata initiative may have stalled due to poor data quality, says IT consultant. Retrieved from Out-law archives: http://www.out-law.com/en/articles/2014/february/midata-initiative-may-have-stalled-due-to-poor-data-quality-says-it-consultant/

28. Boston Consulting Group (2012): The value of our digital identity. Retrieved from BCG Perspectives: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

29. Buttarelli, G. (2016): EDPS Opinion on Personal Information Management Systems. Retrieved from The European Data Protection Supervisor Opinions: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

30. e.g. Nordea has spent €1 billion on renewal of core architecture; Nikel, D. (2015). *Nordea Bank signs Temenos and Accenture for core banking transformation*. Retrieved from: ComputerWeekly: http://www.computerweekly.com/news/4500254088/Nordea-Bank-signs-Temenos-and-Accenture-for-core-banking-transformation

31. Poikola, A., Kuikkaniemi, K., Honko, H. (2015): MyData – A Nordic Model for human-centered personal data management and processing. Retrieved from MyData Resources webpage: https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/2e9b4eb0-68d7-463b-9460-821493449a63?version=1.0