PRIVITAR

Privitar Privacy Pulse 2019

How businesses harness the power of data and earn consumer trust

www.privitar.com

Methodology

Online survey in US, UK and France

5,000+ respondents

Fieldwork conducted January 2019 – February 2019

Consumers
Nationally representative on age, gender, region and income

US: 2,000+ respondents
UK: 2,000+ respondents
France: 1,000+ respondents

Business
Influencers in decisions about data management, policy and technology

Job roles: Business Lines, IT, Data Analytics, Data Management, Security

Sectors: Banking and Financial Services, Telecommunications, Healthcare, Civil and Social Services, Local Government, Retail, Utilities

US: 250 respondents
UK: 250 respondents
France: 250 respondents

Contents

We have the opportunity to make data privacy a significant competitive advantage

Jason du Preez,
Privitar CEO and Co-Founder

With nothing more than the geolocation trace from our mobile phones, organizations can infer very personal and intimate details in our lives: our friendship circles, our buying habits, our political affiliations – even our sexual orientation.

This data about us can be put to work for good. Everywhere, data is being used to deliver breakthroughs in fields as diverse as medicine and customer experience. But our data can be used for more insidious means – such as using curated information inside filter bubbles to manipulate election results.

I believe there is clearly a greater need now than ever before for measures that protect our privacy on the one hand and ensure transparency over how data insight is being used on the other. We must not forget that data points and statistics relate to people – to individuals with personal lives and a right to self-determination.

This is why we have undertaken this crucial piece of research into the state of data privacy.

We see notable consumer concerns and fears around sharing their data. We also see the challenges businesses are facing concerning their ability to embrace making data-driven decisions while complying with rapidly emerging regulations and maintaining consumer trust.

In the pages that follow, we identify practical steps that organizations can take to unlock the true power of their data; consider the challenges holding them back; and explore the opportunities awaiting those who get it right.

By embracing privacy-by-design principles and ensuring that ethical data practices are made intrinsic to the way we process data, we have the opportunity to make data privacy a significant competitive advantage.

I know you will find the insights valuable on your journey to becoming a responsible, trusted and successful data-driven organization.

The data trust deficit

The strength of public feeling about data privacy is reaching fever pitch. Increasingly, a privacy or data breach will not only erode trust in the source of the breach, but will also erode trust in the entire industry. Before looking at ways in which the world's businesses can tackle the loss of trust in data privacy, it's necessary to examine the nature of that deficit and the impact it can have – or rather, *is having* – on companies' success.

A collective concern

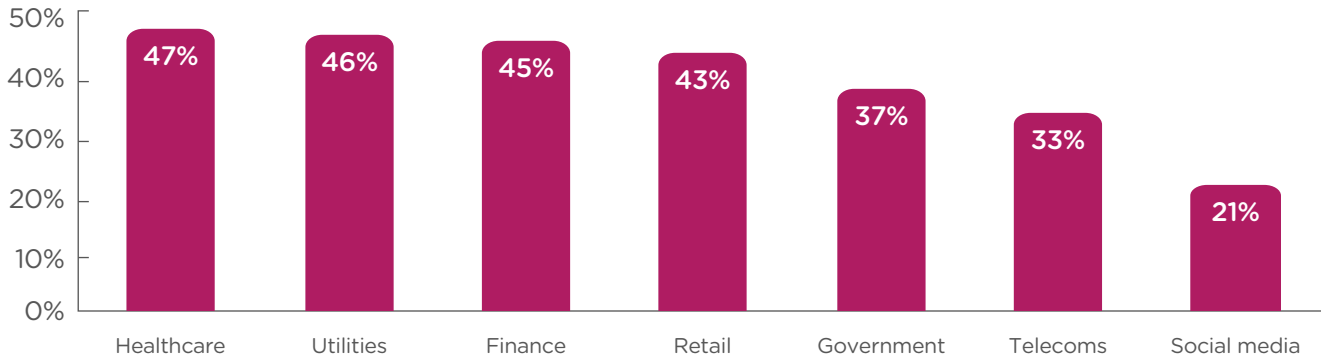
As we see in Figure 1, the lack of faith in organizations' ability to protect people's data reaches across sectors and countries. Perhaps unsurprisingly given events such as the ongoing criminal investigation against Facebook, social media is particularly distrusted as a custodian of data. Yet even in other, more established industries, levels of confidence remain noticeably low.

Emotions around data privacy run high. Over three-quarters (76%) of consumers agree they feel violated if their data isn't secure; and 74% think companies are not transparent in how they get permission for gathering and using their customers' data.

Public tolerance for mistakes is decreasing. When asked to describe how they would react to a company inappropriately using their data, half (50%) of consumers say they would trust the company less, an increase of five points since 2018. What's more, a quarter (25%) claim they would trust all companies less, further underlining that the actions of relatively few companies can have outsize impact on the rest of their industries.

As well as the reputational damage such data incidents cause – 42% of people say they would tell their friends and families if their personal information was misused – these figures threaten businesses' ability to harness the potential of their data by limiting the scale and scope of information available. Data misuse erodes the loyalty of current customers and cuts off the supply of new customers. As well as the immediate impact on the bottom line, this means less data – and less scope for innovation based on the insights and patterns therein – for companies who don't respect customer privacy.

Figure 1. Trust in industries to protect data



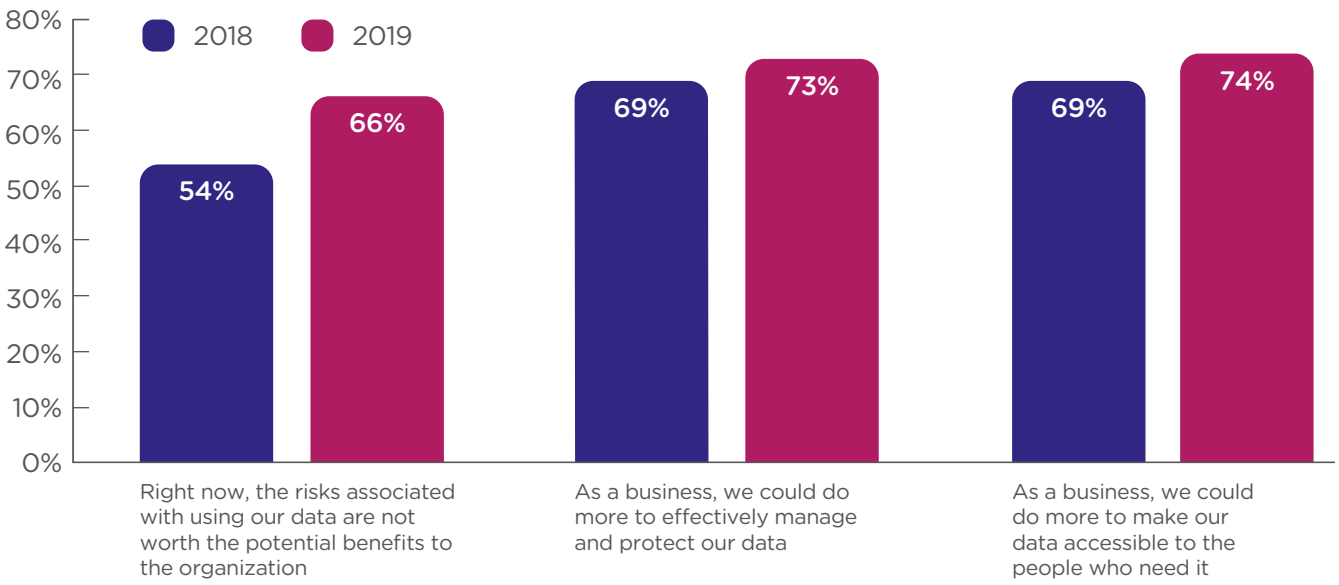
Nothing comes from nothing

The good news is that businesses recognize this trust deficit. More than three-quarters (77%) of those we surveyed citing the need to clearly explain to customers the value of sharing their data. A further 78% claim it's important to them to ensure their customers understand how they are using their data.

Belief is not the same as action. Businesses need to rise to the challenge the trust deficit presents, rather than burying their heads in the sand. Instead, many companies are retreating from using their data at all rather than risk the potential aftershock of something going wrong. Two-thirds (66%) of businesses believe the risks associated with using company data are not worth the potential benefits, an increase of 12 points since 2018. 73% admit they could be doing more to effectively manage and protect their data.

Yet the reality is that doing nothing carries nearly the same threat as getting it wrong. Failure to act places companies at a very real risk of being left behind. Firstly, by missing out on the opportunities data utilization can offer – from improved customer experiences and better staff retention to stronger financial performance. And secondly by finding themselves outgunned and outperformed by more data-savvy competitors.

Figure 2. Opinions on your organization's data management



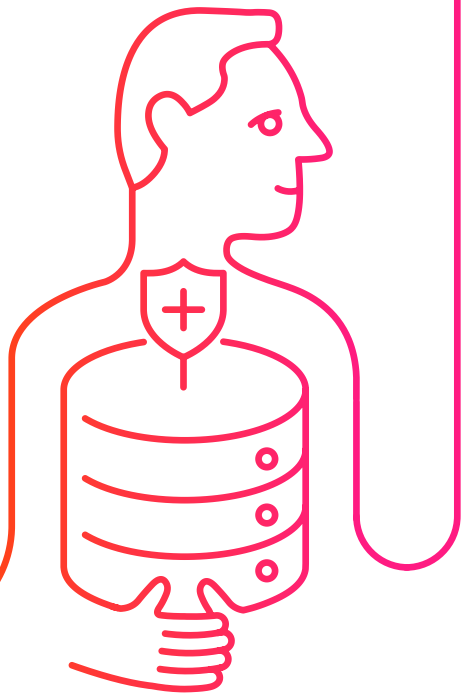
Time for action

The need for organizations across sectors to reassure customers and unlock the value of their data cannot be ignored. Nearly two-thirds (64%) of companies admit they have seen organizations in their industry miss out on a competitive advantage by not making the most of their data.

This is not an issue to 'get around to'. It's a ticking bomb. Our 2018 and 2019 Privacy Pulse studies show that the strength of negative consumer sentiment around data privacy is growing – and so is the public perception that businesses are failing to address their concerns.

64% of businesses have seen organizations in their industry miss out on a competitive advantage by not making the most of their data.

Now is the time for companies to step up and convince customers of the benefits of sharing their personal information and, in doing so, harness the power of that data for the good of their business.



Unlocking the value of data

Of course, unlocking the value of their data is not something businesses can, or will, do overnight. But there are immediate steps organizations can take to get the right processes and technologies in place – and demonstrate that commitment to customers.

The need for greater transparency and control

As we have seen already, chief among these is persuading customers they can be trusted with their data – from the moment it's collected to the way it's stored, accessed and used.

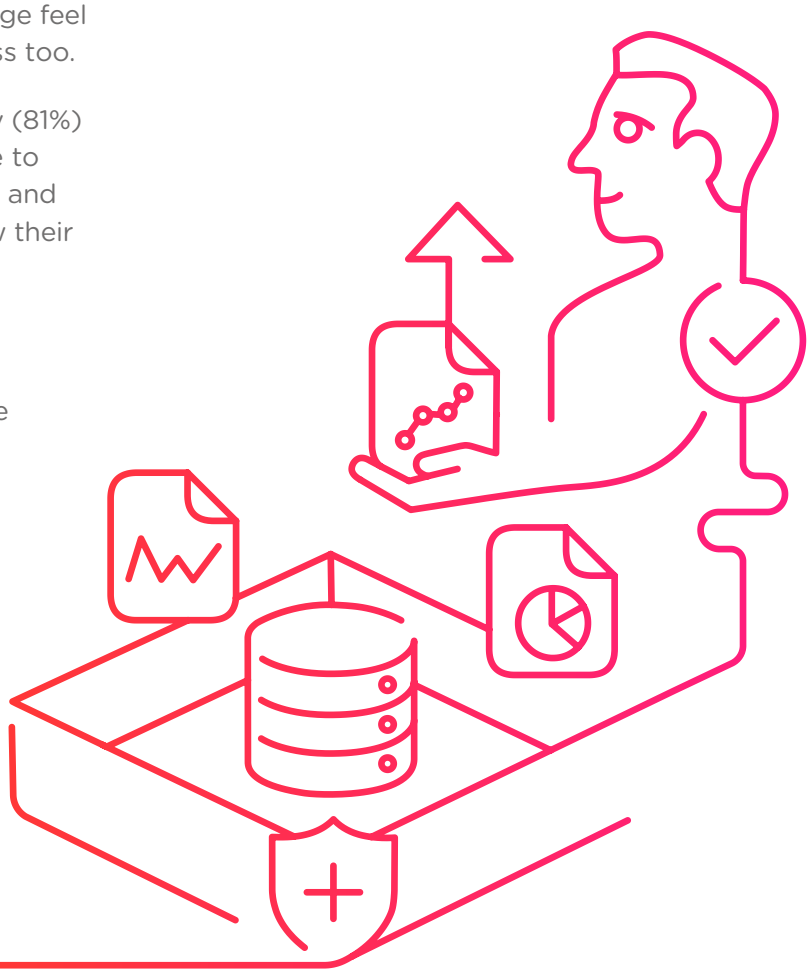
Many companies believe they are already doing a good job here. Over three-quarters (79%) claim they empower their customers to decide how their data is used, while the same percentage feel they are adequately explaining this process too.

Consumers do not agree. The vast majority (81%) want more control over when they choose to share their personal data with businesses – and two-thirds (66%) are concerned about how their data is being used without their consent.

There is a clear disconnect between what businesses think they are doing and what customers experience. It's imperative that businesses act now to close this gap, offering people the level of transparency and control they need to feel comfortable in sharing their personal information.

81%

of consumers say they would like more control over when they choose to share their personal data with businesses.



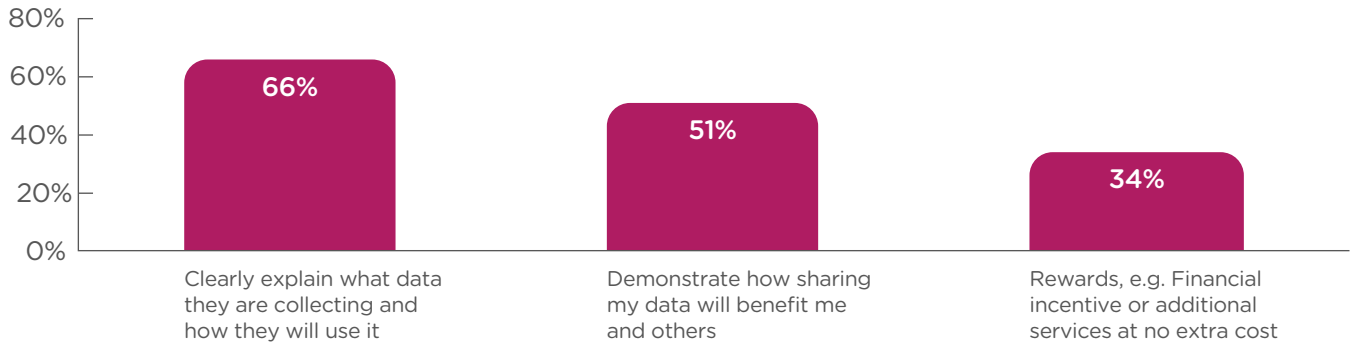
Education, education, education

Much of this comes down to education. For consumers, the level of understanding around how to protect their personal information remains low. More than half (58%) admit they do not feel knowledgeable about data privacy and 61% consider themselves uninformed about data security.

Increasing consumers' levels of understanding will go a long way to restoring their faith in the safety of their data. Over half (52%) of people who feel knowledgeable about data privacy say they trust organizations to handle their data, compared to just 30% of those who feel uninformed.

There is also a noticeable rise in people's readiness to share data when they receive an explanation of how it will be used. People are more motivated by knowing what data is being collected and why than they are by the benefits of sharing it or, even, the prospect of receiving a financial reward. (See Figure 3.)

Figure 3. Actions businesses can take to make consumers feel more comfortable sharing their data



Simply by taking the time to clearly explain to people what, when and why data is required, businesses can dramatically increase the likelihood of them being willing to share it.

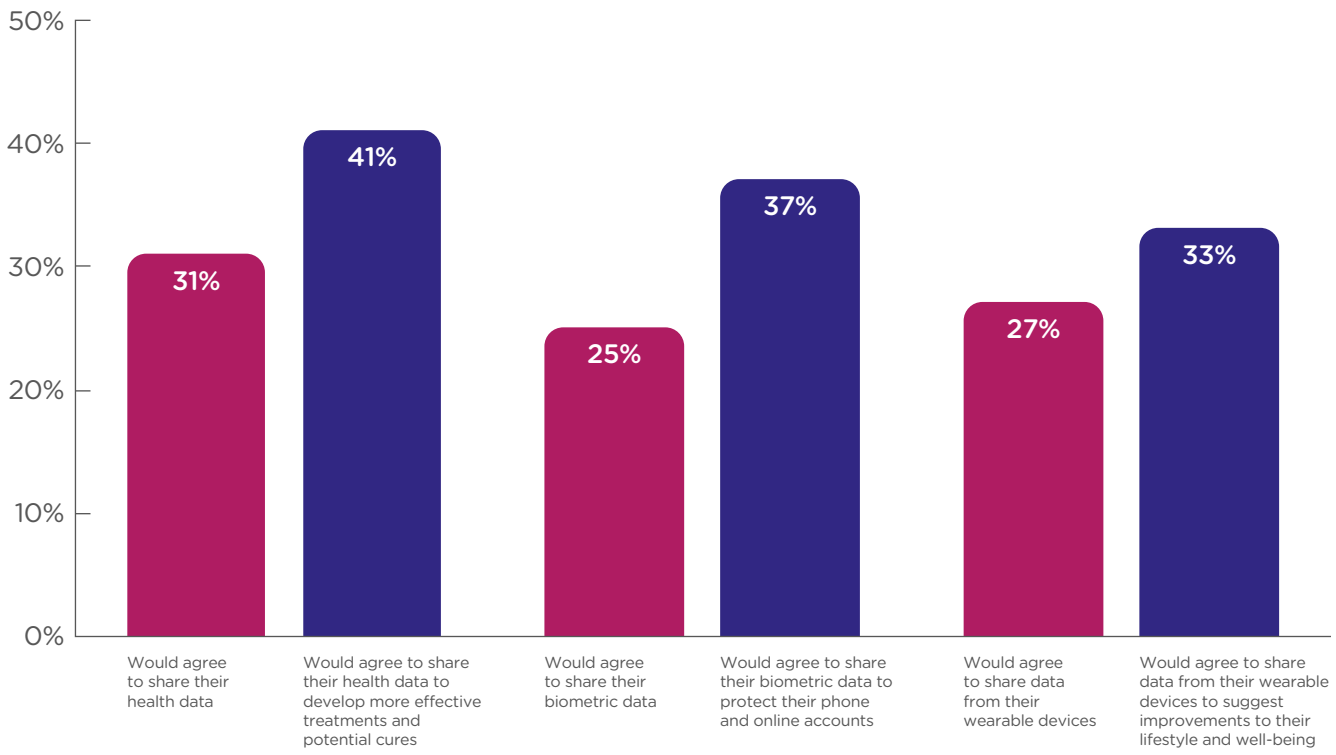
Showcase the benefits

While increasing public understanding of data privacy is important, it's equally vital for businesses to openly communicate the advantages of data sharing. Three in five consumers say they are more willing to share personal information when the benefits of doing so are made clear to them. (See Figure 4.)

There is also a marked discrepancy in what makes people happy to disclose personal information. For example, while half of consumers are willing to share data in order to aid the search for cures for preventable diseases or improve patient diagnoses and treatments, only 13% would do so to get personalised advertising.

This reinforces the need for greater transparency from businesses when it comes to communicating how collecting data can have a positive impact – either for individuals, communities or society as a whole. TfL's WiFi data collection pilot is a notable example. TfL took care to inform the public about not only what data they would collect, but also what would be done with it and why – and while advertising was a part of how the data would be used, another was improving the (literal!) customer journey.

Figure 4. Opinions on your organization's data management



Mind the gap

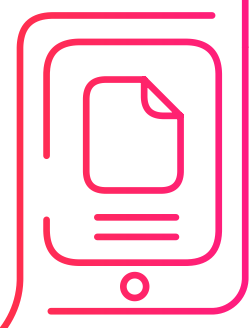
An emphasis on how businesses interact with the wider world around the issues of privacy and protection is critical. But there is also work for companies to do inside their own four walls if they are to make the most of their data.

More than three-quarters (78%) of business believe they can get useful answers from their data while still protecting their customers privacy. Yet many remain paralyzed by the fear of getting it wrong – whether that's the reputational impact of failing to properly protect customers' information or the financial penalties that come with falling foul of ever-more stringent regulations.

81%

of senior executives consider protecting customer privacy of paramount importance in making use of their own data.

Similarly, while 81% of senior executives consider protecting customer privacy of paramount importance in making use of their own data, three quarters (73%) say they could do more to effectively manage and protect that data. This gap between aspiration and action must be bridged – and quickly.



People power

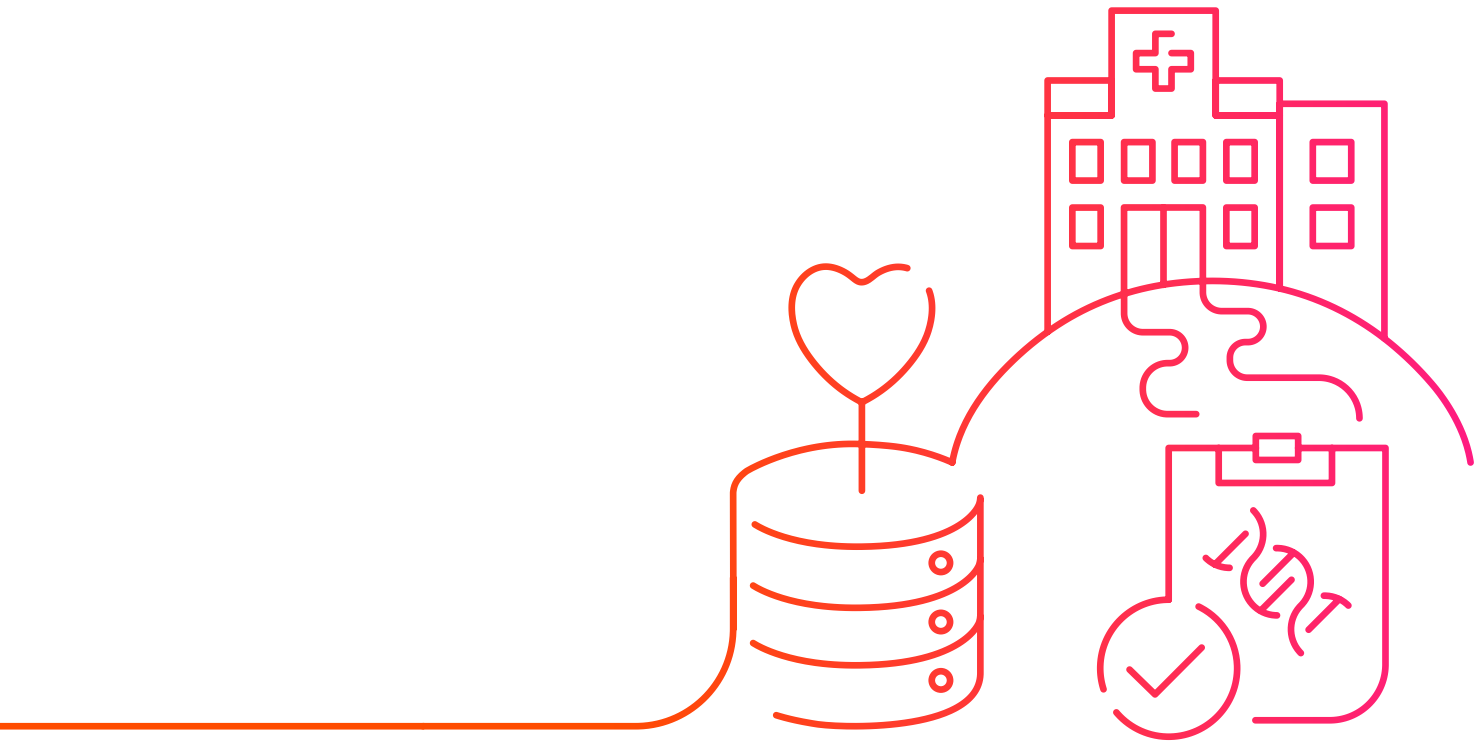
As the role of data in business operations grows in importance, so does the role of those charged with protecting and managing it. Whatever their sector, companies must invest now in building a dedicated data protection team from across their company.

Naturally, the size and shape of that team will vary depending on the size and shape of the business. In large companies, a data protection center of excellence can be a powerful tool in establishing and maintaining rigorous standards of data storage, access and use. In other situations, a small team – or even one person – can be supported by a network of data privacy champions around the business.

What's true in every case, however, is that this cross-functional team needs to take a strong leadership role when it comes to their company's data, leading technical and process changes to guarantee the integrity and security of all sensitive data – not just in the short term, as the nature of their task evolves and expands in the future.

> "Data privacy is the responsibility of every person in the company. Upholding data privacy for our current position is not enough. It needs to be robust enough to stand up to future changes and inclusive enough to guarantee each individual's privacy."

Russell Goom,
Data Engineer, Ieso Digital Health



A vital role

Along with this functional aspect of their job, those charged with managing company data also play a crucial educational role.

In the same way consumers are expressing a desire to better understand how, when and why their data personal information is used, 71% of employees say they wish they could get more support from their IT and data teams in making the most of their data – both in realizing their own career aspirations and in helping drive their business forward.

Top management are increasingly looking to Chief Data Officers and their team for help. Nearly three-quarters (72%) of business leaders say they need more support to improve their organization's data management.

This represents a great opportunity for internal data experts to put themselves at the heart of the business, whether by showing senior executives the benefits of increased data, counseling them on how to mitigate the inherent risks or offering ongoing training for other employees.

A strong reputation for looking after customer data is among the most important factors in making consumers feel comfortable about sharing their information. Being able to highlight the concrete actions their dedicated, expert team are taking is a powerful tool for businesses who are building their reputation and reassuring people they can be trusted to look after their data responsibly.

> "Privitar's 2019 Privacy Pulse demonstrates that privacy isn't optional. Businesses need to act now and protect their customers' privacy in order to retain them and build a sustainable reputation. Data protection must be an integral component of their business models. Executives, CDO and DPO, it is the perfect time for you to step up and be at the heart of the business strategy."
>
> Jason du Preez,
> Privitar CEO and Co-Founder

The right technologies

Just as it's important for businesses to change their processes and culture to better protect their customers' data, they must also invest in the tools and technologies that help keep sensitive data secure while getting the right information in the hands of the right people at the right time.

Three-quarters (74%) of business leaders agree their company could do more to make data available to the people who need it – the analysts and developers who can use it to build smarter operating models, deliver better customer experiences and foster greater innovation across the business.

Among employees, a lack of awareness of the options available for protecting or managing information was rated as one of the key barriers to making the most of company data.

74%

of business leaders agree their company could do more to make data available to the people who need it.

To truly enable safer – and wider – data utilization, companies must put in place the systems that let them transform a dataset containing highly sensitive information into a privacy-preserving, low-risk set of records that can be used for analytics and be shared with researchers and corporate partners.

From data de-identification and anonymization to secure multi-party computation, homomorphic encryption and differential privacy, this means finding the right privacy tools for them. Ones that not only meet their specific objectives but that can be easily used, managed, configured and deployed.

Crucially, data privacy governance must be centralized rather than applied piecemeal across the organization. This ensures consistency, while making it easier to stay on top of an evolving data privacy landscape and ever-changing regulations. It allows data and compliance teams to better track the movement of protected information around the company, between partner organizations and across borders.

After a data incident occurs, the right tools and infrastructure will prompt a swift, accurate and effective response. It will protect the sanctity of customers' personal information and prevent long-term damage to the business itself - reputationally and financially.

Five steps to building trust and unlocking the power of data

1. Be transparent with customers about when, how and why their data is collected
2. Clearly communicate to customers the benefits of sharing their data, whether that be for them individually, their community or society as a whole
3. Recruit, retain and train a dedicated in-house team of data privacy experts – and empower them to establish the right infrastructure across the business
4. Equip the business with the right data privacy solutions to enable safer and wider data utilization while adhering to local and/or international regulation
5. Centralize and automate data privacy governance to ensure greater consistency, compliance and control

"For data-driven businesses, the consequences of a privacy breach pose numerous existential threats. These include severe regulatory penalties, legal action and most damaging of all, loss of customer trust which leads to lost business."

Jason du Preez,
Privitar CEO and Co-Founder

Data privacy at Ieso

An interview with Russell Goom, Data Engineer, Ieso Digital Health

Describe your role and what you do for your company

I am the research and development department's Data Engineer, tasked with defining, refining and developing the data platform to serve the entire company. I come from a background of data quality engineering and data management for large companies, such as Oracle.

Why is data important to your company?

Our aim is to change the future of mental healthcare. In order to do that we need to optimize the assessment and treatment of mental health conditions to increase the likelihood of recovery and prevent relapse. This is all made possible through carefully analyzing our treatment data with skilled clinicians and scientists, and developing models, analytics and operations that improve our ability in all these areas.

Why is data privacy important to you?

We place utmost priority on our patient's data privacy. We are first and foremost providing a mental healthcare service to them – their well-being is our responsibility. We need to ensure that where we are using the power of the knowledge hidden within the patterns of our treatment data, **we never lose sight of the fact that we are dealing with individuals**. We take the responsibility for data privacy extremely seriously, not just so as to respect the law, but also to respect the security of our patient's information.

What's the most important thing to think about as you look to do more with sensitive data?

Patient safety and data security need to be top priority. At Ieso, data we use to analyze and model patient behavior has all been securely de-identified and cannot be accessed by anybody outside the small number of authorized staff in the company.

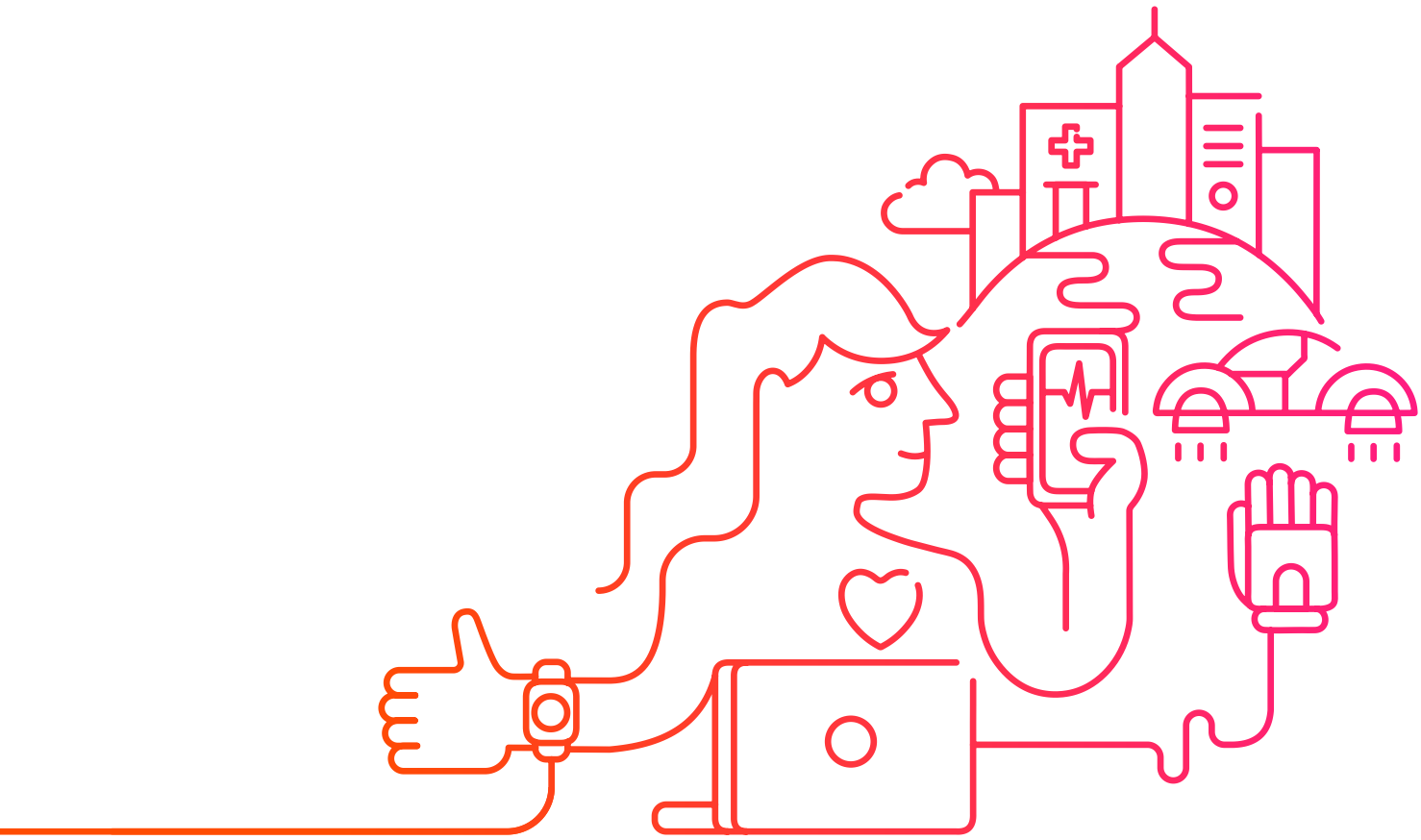
By reinforcing our approach of 'privacy by design', and ensuring robust procedures were an easily auditable part of the data pipeline, advances in mental health science can occur more smoothly and take away privacy concerns from the scientific effort.

What steps did you take to embed data privacy in your company?

Data privacy was already deeply embedded in our company with multiple layers of encryption and tight control on data access. What we wanted was to speed data privacy policy application, especially when we are considering new markets for our service. Privitar enabled us to slot in a user-friendly policy creation element into our existing processes. This enables a greatly decreased time to make new data pipelines using best practice privacy policies and differing infrastructures, putting the power of big-data into our hands without risking patient privacy.

Who needs to be involved in data privacy? Is there anyone you wish you had involved sooner?

Data privacy is the responsibility of every person in the company, not just the compliance and data teams. We take a holistic approach with every team being involved in data governance. Upholding data privacy for our current position is not enough. It needs to be robust enough to stand up to future changes without massive re-engineering, and inclusive enough to be able to guarantee each identifiable individual's privacy.



Looking forward

What changes have you been able to make for your customers?

As a data engineer, my customers are the teams in the company. I have been able to assure them that the data platform will meet their team's needs, taking the data pipeline and associated privacy concerns away from their list of responsibilities so they can concentrate on their main job.

For our patients, it has been the ability to underline our commitment to privacy. No matter how much data work we perform or what form it takes, we are able to reassure each individual that their data is safe, monitored and de-identified for analysis use.

What are the main opportunities you have been able to take advantage of, or seen for the future?

We look forward to taking advantage of current and future technologies to analyze our safely de-identified data to improve patient recovery, prevent relapse and even prevent mental illness occurring in the first place. We will be well equipped to protect our patients' data no matter what direction we pursue to achieve our aim of helping more people get better.

What advice do you have for leaders looking to do more with their sensitive data?

I cannot stress enough that **any data effort must include 'privacy by design'**. Sensitive data is a precious asset that should be protected at all stages of an initiative, whether it is re-engineering legacy systems or processes, or a brand new effort.

How do you see data privacy changing in the next five years?

As healthcare in particular moves into using the power of artificial intelligence and machine learning to process enormous data sets, the culture throughout the industry needs to acknowledge their role in not only respecting law and patient privacy, but the obligation to ensure that the data they hold can be used to improve healthcare in a privacy-centric manner. There needs to exist a framework and understanding that enable the knowledge potential stored in healthcare and behavioral data to be shared and collaborated upon in an accessible, secure and enabling manner.

“Privacy as a discipline will continue to advance and be recognized not as a part of someone’s role, or an afterthought, but as a key part of unlocking the value of data and, as such, a discipline in itself. As AI, machine learning and analysis of big data become the norm, it will become increasingly important to develop a position of trust and collaboration with patients and other stakeholders.”

Russell Goom,
Data Engineer, Ieso Digital Health

We're Privitar

We help organizations engineer privacy-preserving data operations, using advanced data privacy techniques that protect sensitive information while retaining data utility. Our software accelerates and automates privacy-safe data provisioning, helping our customers get more business value from their data, generate data-driven insights, and drive innovation.

Contact us:

e: info@privitar.com
t: +44 203 282 7136
w: www.privitar.com