PRIVITAR

6 Steps to Creating a Privacy-Centric Data Culture

No longer a niche subject for backroom discussions, data by design is now on the mainstream agenda.

Increasingly, people are waking up to the realization that data protection needs to be intrinsic to the entire business and consistently applied at all points of use.

The best way to drive better privacy protection is to move beyond a compliance mindset into a culture of data privacy.

Because once you adopt a culture that protects privacy by default, you can offer safe data on demand, and avoid fines, reputational damage, and loss of customer trust in the process.

Since enforcement began in 2020

$13.5

million paid in HIPAA in fines in 2020

40%

increase in GDPR fines

76+

lawsuits

Every $1 spent on analytics earns $9.00 in returns from improved productivity and avoided costs to increased profitability

Source: Nucleus Research, "Investing in Analytics returns $9.01 per dollar spent," January 2019

It takes a village to change a culture

For many organizations, data privacy starts with an alliance between the central data or IT team that implements the systems, and the compliance function — the data guardians — whose job it is to keep the regulators from the door. But this is not solely a legal issue, nor is it an IT issue.

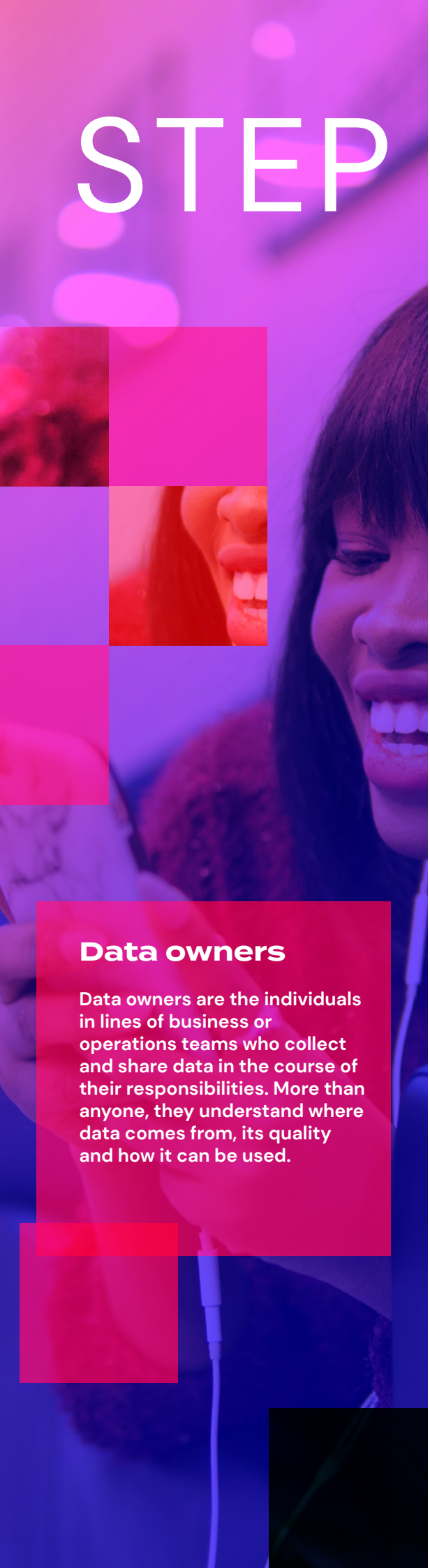
It's a cross-functional mandate: all stakeholders have their part to play.

In a digitally transformed world, everybody understands how important it is to be "together in data" — but this extends far beyond simply automating existing data processes to ensure privacy protection is built in. As privacy leader Michelle Dennedy believes, it's about different business units and leaders forming partnerships based on shared purpose.

So, if you're looking to put data privacy at the core of everything your organization does, embedding a privacy-centric data culture across the whole business and not just your data teams, here are six steps you should take.

Data guardians

Data guardians are responsible for the policies and rules that govern safe data use across their organization. Whether legal counsel, data protection officer or compliance professional, they must ensure those standards are up to date with legal requirements, regulatory guidance and the organization's changing attitude to risk.



STEP 1

Engage the Data Owners

We know there are a variety of teams who generate and/or use data for faster and improved decision-making. From sales and marketing, to product and ecommerce, along with finance and risk teams. Even HR departments are embracing predictive analytics.

To get the full support from the leaders of these teams — the data owners — in fostering a privacy-centric culture, it's important you make an effort to understand their individual goals and how you can use data to meet them. You want to encourage their appetite for using multiple data sources to learn more about customers, without having to worry about compliance and regulation. You also want them to pass that enthusiasm on to their departmental data analysts.

Some leaders might have dreamt of the potential but given up; others might be trying to achieve it already through "gray market" means. It's important to work with these leaders to identify what their concerns are. It will likely involve conducting trial runs with their analysts, showing how much more usable data can be compared to the unfiltered, risky data of years gone by.

Data owners

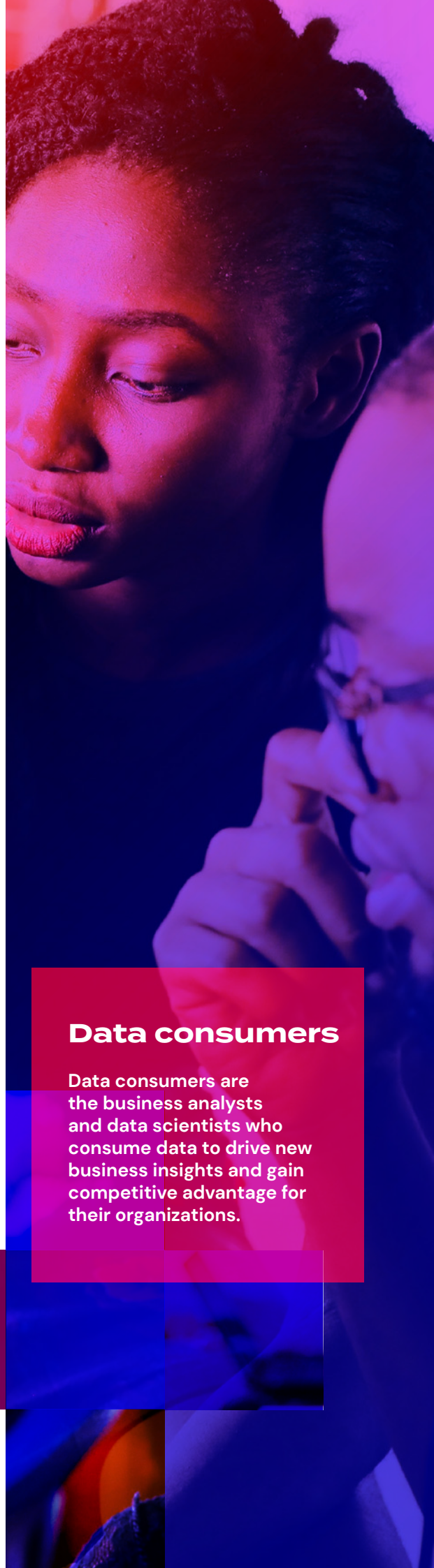
Data owners are the individuals in lines of business or operations teams who collect and share data in the course of their responsibilities. More than anyone, they understand where data comes from, its quality and how it can be used.

STEP 2

Involve Your Superstar Data Scientists

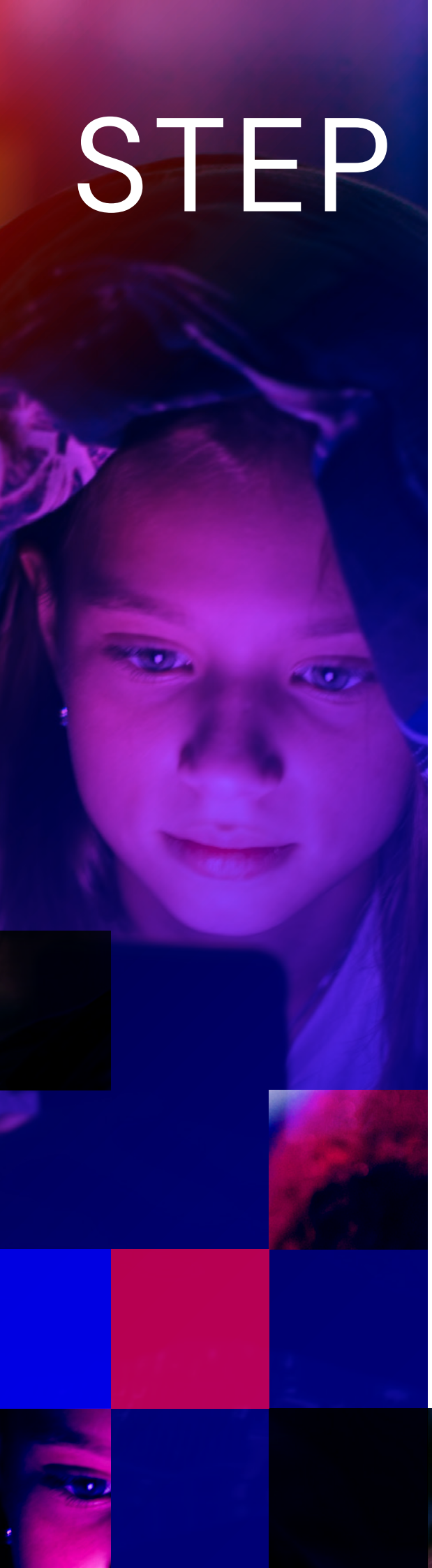
If you're looking for ways to get more attention on your data privacy projects, consider working with a broader group of data consumers from across the company.

These data scientists and analysts come in many guises, whether they're people analysts looking at employee data, marketing operations looking at prospect behavior data or business analysts looking at customer data. Joining different data sets together or building new models using cross-functional data in order to grow the business will only strengthen a privacy-centric culture. And you'll uncover insights you may not have been able to pull before.



Data consumers

Data consumers are the business analysts and data scientists who consume data to drive new business insights and gain competitive advantage for their organizations.



STEP 3

Inspire Communication from the Top

If you're a data leader looking to embed data privacy across your business, it's a given that your relationships with key executives will be paramount in achieving buy-in. They are instrumental in communicating clearly and consistently to the *whole* workforce.

Seemingly obvious, it's often the hardest thing to do. But there are different tactics you can use to ensure your people engage with what you're driving, culturally.

Messaging could come as part of a bigger data initiative, for example. Or if your business has quarterly themes or goals, you could align privacy to each of these. Whether driving revenue or customer satisfaction, this approach puts a sustained focus on data to achieve those aims.

In all these scenarios, it's about increased availability - and usability - of safe data. That's what will excite your people.

STEP 4

Align with the Customer-Centric Imperative

Forward-thinking organizations are as customer centric as possible. Quite simply, if businesses don't acquire and retain customers, they won't survive. So aligning data privacy with customer centricity can also help on your journey to becoming a privacy-centric company.

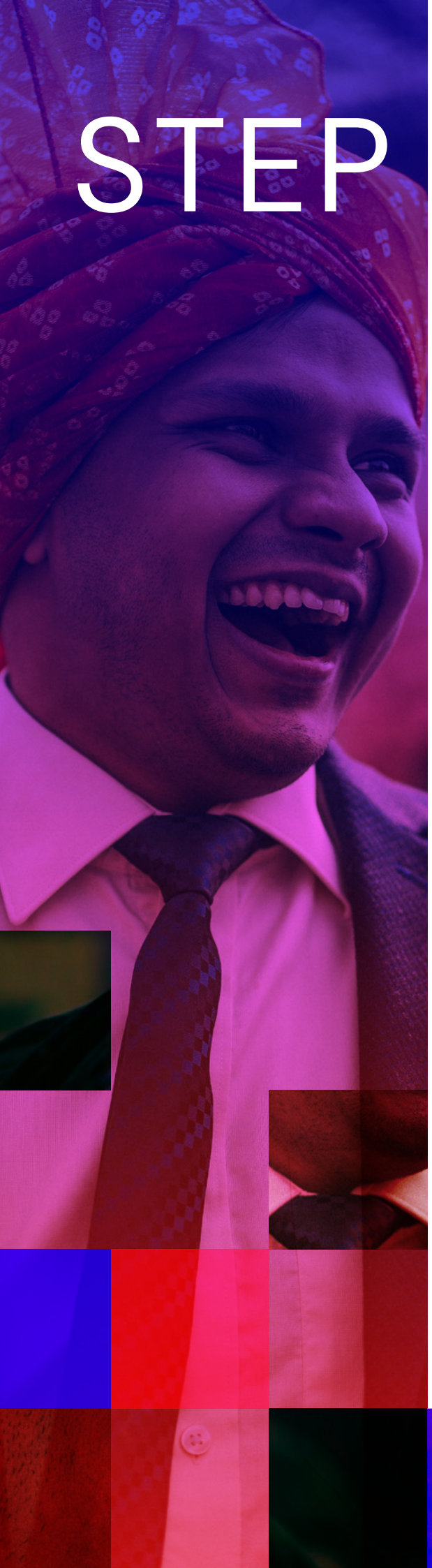
After all, the work your people do regardless of function, is for your customer. You build products that meet customer needs, you anticipate customer wants and you provide a level of service that keeps customers onboard.

Protected data plays a big part in driving this. Having easily accessible and usable data that helps make the right decisions for customers, shows customer centricity in action.

If you can identify the customer-first employees in your organization, the go-getters who are passionate about the customer-centricity agenda, you can also leverage them to help build your privacy-centric culture and build out those champions.

We want to give our customers the best possible service through the use of analytics but we need to ensure that we have the appropriate controls. To be a truly data-driven organization, we need to generate valuable insights, through well-managed data assets.

Steve Suarez
Global Head of Innovation – Finance & Risk
HSBC



STEP 5

Get Company-Wide Buy-In and Strengthen your Brand

When we accept that data privacy is greater than just the Chief Data Officer's organization, then the responsibility to pursue a data privacy culture lies with everyone across the company.

From a practical point of view, it's always better to have a groundswell of support and a shared vision that permeates the entire organization. It's useful to have people reiterating a mantra and create that force multiplier effect for the efforts of your core privacy team.

Safe data can also become something for all businesses to shout from the rooftops. Respect for citizens' data is as important to your brand as being sustainable or good citizens in the community. Data privacy can affect not only how customers view your brand, but also how prospective and current employees view their workplace.

STEP 6

Make Safe Data Provisioning Easier Than Any Other Route

For a company to be doing more than paying lip service to a culture of data privacy, it must make data so easy to access that the data scientists and analysts won't want to do it any other way.

Streaming services provide a useful metaphor here. It used to be easier to download movies and television shows illegally than to pay for them. Now consumers happily subscribe to one or more services — sometimes just for a month to get the one program they want to watch — because it's easier than pirating it.

It's a huge cultural shift in entertainment, and it's pertinent to a culture of data privacy. On the occasions when data professionals don't follow prescribed processes, they're usually not doing it just to be bad – it's a means to an end. Your data provisioning system of choice needs to be the fastest and safest way to get access to what they need, and everyone needs to be able to use it.

Are we there yet?

What would your organization look like if data privacy was genuinely part of its DNA?

First, your IT infrastructure team would see an increasing volume of data running through its central clearing house, as people begin to understand the power of the system and what they can do with their company's data.

IT would see a steady growth in the number of data requests they receive over the course of a year. Using a modern approach to data provisioning, with data guardians' policies embedded into systems, requests could be quickly and automatically approved, giving consumers easier and faster access to data - all without adding to the workload or stress of their IT colleagues.

The compliance team would have increased visibility into what's happening with data, and they would see a reduced number of interventions and awkward conversations with data analysts.

With data consumers and the marketing, ecommerce, sales teams they serve getting faster data access, your organization would be making better business decisions, engaging more effectively with customers, and innovating more quickly.

And at an even more basic level, your teams would be able to answer those simple questions that make the difference between success and disappointment in any given period. Knowing when a customer is ready for an upsell or a cross-sell and what useful interventions can be made – that's the power of safe data.

Talk to Privitar

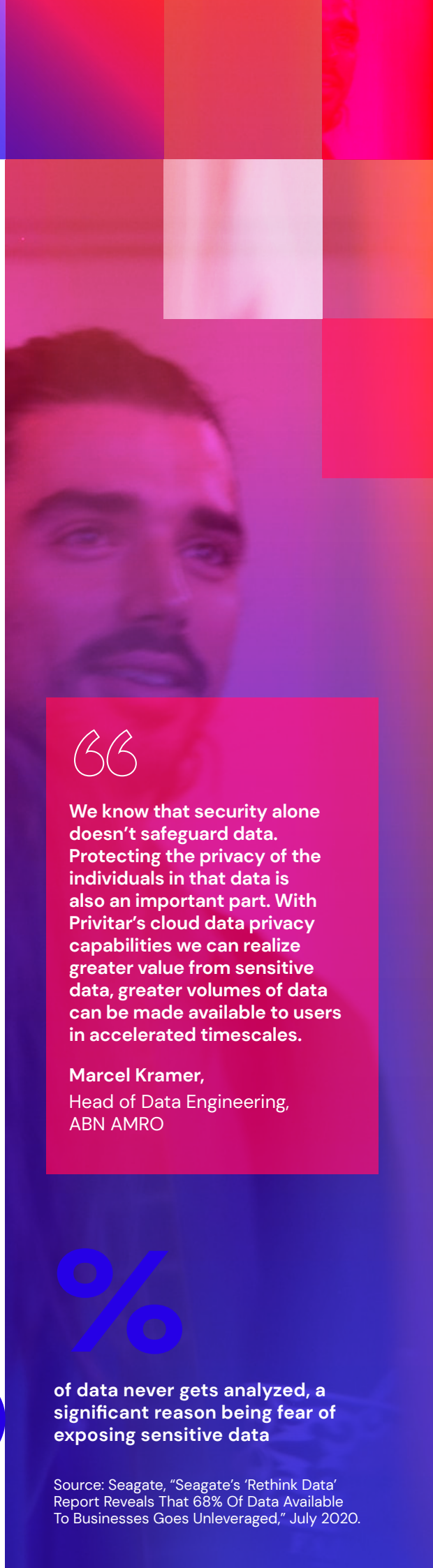
There's no turning back — privacy by design is the future. You need a platform that protects and manages sensitive data while optimizing its utility for business benefit. One that defines, manages, and systematically applies consistent data privacy policies across locations and data environments, fine-tuning policies applied directly to data according to context.

Privitar enables organizations to leverage safe data for analytics through its comprehensive technology platform and expert advisory services.

Your data scientists and business analysts can access de-identified, safe datasets quickly, using their choice of tools and frameworks, including analytics and machine learning services.

And never again will you experience the cost of lost opportunity due to an inability to use data where the risk is deemed too high.

Visit the Safe Analytics Resource Hub for more information on how to power your organization with safe analytics.



> **We know that security alone doesn't safeguard data. Protecting the privacy of the individuals in that data is also an important part. With Privitar's cloud data privacy capabilities we can realize greater value from sensitive data, greater volumes of data can be made available to users in accelerated timescales.**
>
> **Marcel Kramer,**
> Head of Data Engineering,
> ABN AMRO

68%

of data never gets analyzed, a significant reason being fear of exposing sensitive data

Source: Seagate, "Seagate's 'Rethink Data' Report Reveals That 68% Of Data Available To Businesses Goes Unleveraged," July 2020.

About Privitar

Privitar is the leader in modern data provisioning, empowering organizations to use data responsibly, effectively and efficiently. We make data highly accessible by using the latest advances in privacy enhancing technology and integrating robust best-practice processes so that high-utility data reaches those who need it, at the right time, while managing risks and demonstrating compliance with relevant laws. Only Privitar has the right combination of technology and expertise to create a safe data provisioning ecosystem that enables clients to share data and unlock new data insights while keeping data safe and businesses compliant.

Founded in 2014, Privitar is headquartered in London, with regional headquarters in Boston and locations throughout the US and Europe.

For more information, please visit www.privitar.com.

PRIVITAR

Published 2/22. Reference: P1005_GU_6-Steps-to-a-Privacy-Centric-Culture_DP.

Privitar believes the information in this document to be accurate as of its publication date. This information is subject to change without notice.