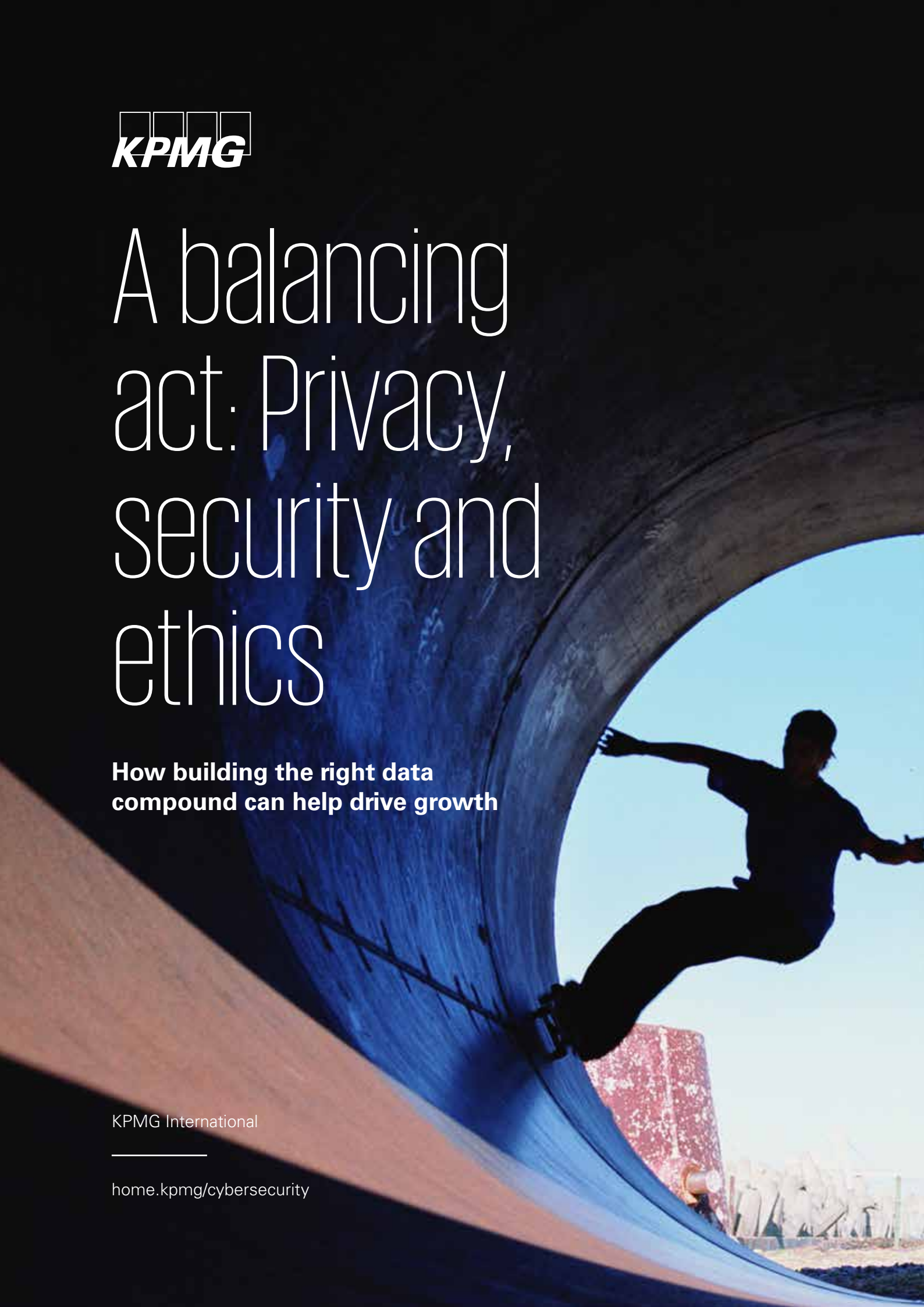


A balancing act: Privacy, security and ethics

How building the right data compound can help drive growth

KPMG International

home.kpmg/cybersecurity

Contents

Foreword

Organizations are striving to devise the perfect 'data compound' — the precise 'mix' of personal data elements that will unlock new opportunities for insight-based decision-making, innovation and revenue growth, all while ensuring that privacy, security and ethics concerns are effectively managed at all times.

Much like a digital 'chemistry set,' the 'elements' of any organization's data inventory can be strategically combined for game-changing success in the digital era. At the same time, the wrong mix or 'blend' of data assets can prove 'combustible' — even 'toxic' — amid rising consumer concerns and regulatory scrutiny regarding the appropriate use of personal data.

Those consumer concerns have been increased further by recent developments such as the use of personal data by countries battling to control the spread of COVID-19.

Compiling and analyzing data with today's remarkable tools and capabilities is certainly enabling data-driven businesses in every sector to enhance and personalize customer relationships, develop innovative new products and drive growth. And this is only the beginning. To capitalize on data as a source of competitive advantage, organizations are working hard to determine

— how personal data can be monetized to open new revenue streams

— how the public will perceive innovation in the use of their data

— how much to invest in privacy as privacy rights and the regulatory landscape evolve

— how to deal with the privacy paradox: the apparent inconsistency between customer concerns about privacy and actual online behavior

— how data-processing practices will be perceived from a security and ethics perspective by the growing number of watchdogs scrutinizing data use.

— how the pandemic may shift customer attitudes over the processing of their personal data.

A question of balance

As today's data ecosystem continues to expand exponentially, organizations have plenty to gain in their pursuit of data-driven business models. With the proliferation of cloud computing, (further accelerated by COVID-19) the globalization of business systems, processes and supply chains, and the ubiquity of mobile devices and social media, consumer data is being collected, analyzed and shared at unprecedented levels. At the same time, the rapid emergence of digital labor, the growing use of consumer IoT devices, artificial intelligence and predictive capabilities are already increasing the potential of data-driven organizations to embrace digital disruption, deliver new value to customers and enable businesses to emerge successfully in the new reality.

But when set against the backdrop of growing privacy, security and ethics concerns and regulatory scrutiny, leveraging consumer data wisely is becoming critical. The work of KPMG member firms, with clients globally, reveals that many businesses are recognizing the challenges in designing a balanced data compound — and many remain unsure about how to strategically manage data assets, mitigate liabilities and take action.

KPMG believes that placing *trust* at the center of every initiative involving personal data use is vital to turning potential risks into historic new opportunities for business differentiation and growth in the digital era.

Technology and it's accompanying data trails permeate so many aspects of our lives that companies must earn and sustain trust, or wary consumers will be reluctant to share the critical data that businesses need to become data-driven and customer-centric. Trust in the digital era goes beyond the quality of an organization's brand, products, services and people. It's also about the trustworthiness of data use and management. The challenge ahead is to prove that businesses are protecting the customer data they are using to create value and drive success.

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International

Designing the data compound

The race to capitalize on the immense promise of big data is having a game-changing impact on businesses that are boldly turning today's digital challenges into opportunities. As consumer purse strings tighten, and physical commerce becomes increasingly unreliable amidst the risk of future lockdowns, businesses have a growing need to become data-led and manage the exploding volume, depth and accessibility of data in the most cost effective way. All in an attempt to not fall behind their competitors and emerge successfully in the new reality.

Consider, for example, the rapid proliferation and ongoing evolution of internet-enabled devices over the past decade — and how businesses have responded to the hyper-connectivity trend. In 2010, we generated about 12 exabytes (EB) of internet traffic (1 EB is equal to 1 billion gigabytes) through our typical interactions, and data processing had limited information sets such as name, email address, phone number, home address and perhaps their work location.[1]

Today, the annual volume of data a user generates has increased 1,000 percent to over 136 EB of internet traffic. This is all before the pandemic forced consumers to digitize their shopping habits, and the extensive proliferation of super-fast 5G mobile — pure fiber internet connectivity which is going to transform our everyday lives even further.[2]

The explosion in personal data is leaving behind an endless trail of personal information that future-focused businesses are tapping into for the wealth of timely insights that will enhance customer relationships and drive growth.

Bringing trust into the strategic 'formula'

As the pandemic accelerates an already digitizing world and customer expectations for service, reliability and security grow amid the rush to exploit the data 'gold mine,' how do companies balance the proliferation of data and their drive for value with serious privacy and security concerns and increasing scrutiny from regulators?

An explosion of data

The amount of data individuals produce every day is staggering. Estimates vary but it's believed that roughly 2.5 quintillion bytes of data are created daily.[3]

More than

4.6 billion

people are estimated to use the internet daily[4]

5 billion

searches are made daily[5]

There are

3.9 billion

daily email users[6]

Per month, there are

2.74 billion

active users on Facebook[7], 1 billion+ on Instagram[8]

With the number of Internet of Things (IoT) devices expected to reach 35 billion next year, these numbers will only continue to increase.[9]

---

1 *Cisco Visual Networking Index: Forecast and Trends, 2017–2022,* 2019.
2 *Ibid.*
3 *Data Never Sleeps 8.0,* DOMO, 2020.
4 *Global digital population as of July 2020,* Statista, 2020.
5 *How much data is generated each day,* World Economic Forum, April 17, 2019.
6 *Number of e-mail users worldwide from 2017 to 2024,* Statista, 2020.
7 *Q3 2020 IR Statement,* Facebook, 2020.
8 Info Center, Instagram, 2020.
9 *The IoT Rundown for 2020,* Security Today, January 13, 2020.

While some firms are moving boldly forward to 'formulate' the right personal data compound, many more organizations are amassing huge volumes of digital information that they don't know what to do with — or where to even start. As today's ground-breaking companies are discovering, the effective use of personal data demands the strategic design of a comprehensive data compound. Organizations seeking a trusted strategic formula for a personal data compound that will transform customer data into a source of competitive advantage, face a careful and perhaps daunting balancing act.

— Which personal data elements need to be combined?

— How and in what proportion should data elements be mixed?

— How can the data compound's potential to produce positive or negative 'energies' — for example when addressing the inherent liabilities of privacy, security and compliance concerns — be effectively managed in order to turn personal data into a formidable and trusted new source of competitive advantage?

"Access to a pool of information that provides a unique opportunity to conduct in-depth market research — offering rich insight into recent sales trends, critical business improvements and gaps to exploit in the market — could be the solution to CEOs worries," says Koos Wolters, Privacy Lead, KPMG in the Netherlands.

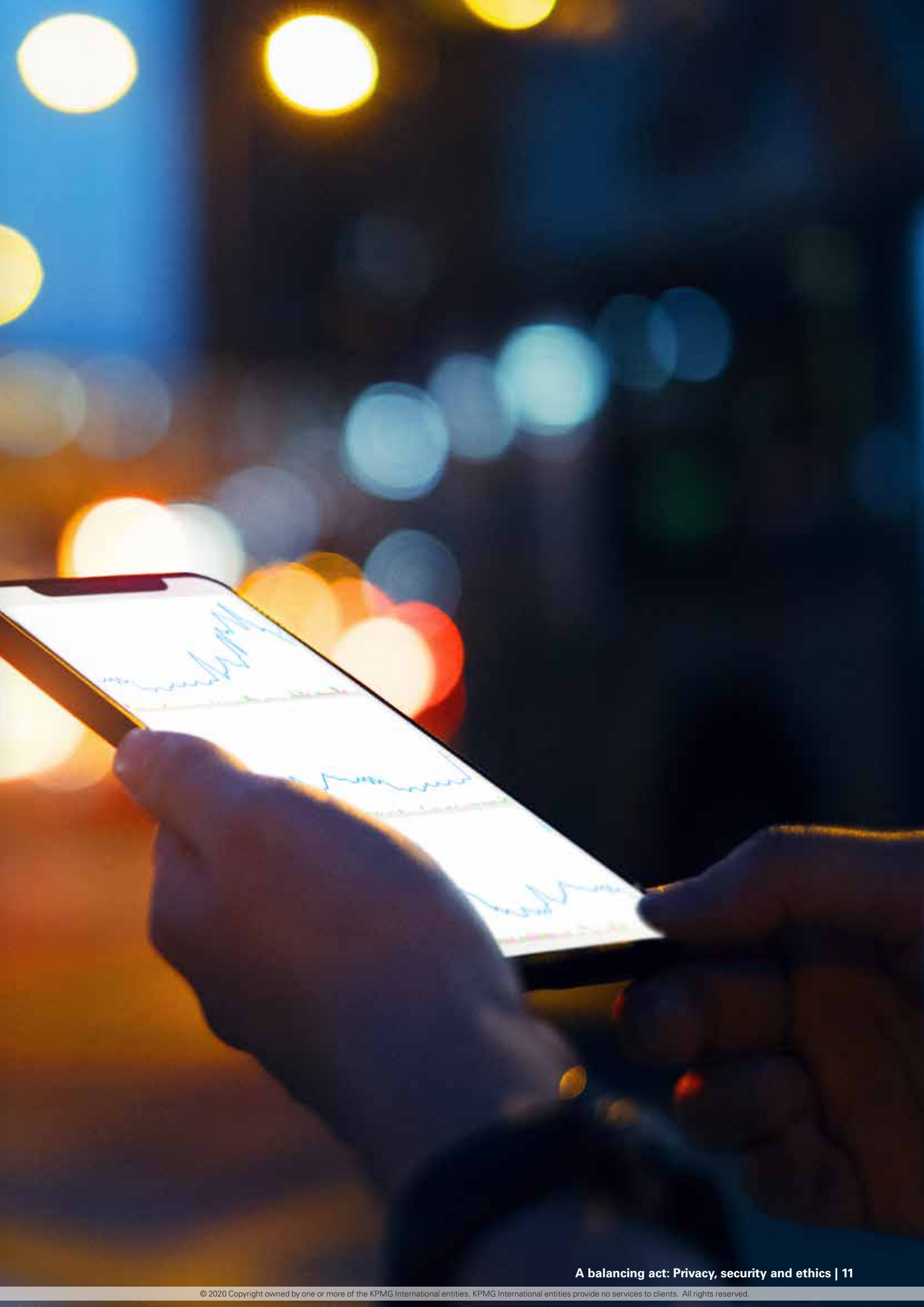
"Cut it and slice it in the right way and businesses can generate much value from data — understanding customer online activities, purchasing power, shopping habits, preferences and more. Companies can also gain insights into customer motivations and desires and combine these with more-sensitive aspects of a customer's personality, such as political and religious beliefs, educational background, gender and race. Companies will profile their customer base more effectively to strengthen brand perception, improve customer retention and increase sales."

"Access to a pool of information that provides a unique opportunity to conduct in-depth market research — offering rich insight into recent sales trends, critical business improvements and gaps to exploit in the market — could be the solution to CEO worries."

— Koos Wolters
Privacy Lead
KPMG in the Netherlands

Unlocking opportunity or unleashing challenges?

Strategic use of data can enable success for organizations in the new reality. Access to the right data at the right time to generate timely, accurate and actionable insights is critical to build brand trust and loyalty, identify new customer segments, capitalize on emerging market trends, deliver innovative new products and services, and achieve a competitive advantage in the post-pandemic world.



“Companies often operate under the misconception that personalization and data protection are conflicting efforts, not symbiotic opportunities.”

— Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International

Understanding how to compile the data compound, choosing, analyzing and capitalizing on quality data that adds real value to the business — while working well within privacy, security and compliance requirements — will be critical to success as businesses emerge in the new reality, in today’s hyper-competitive, customer-centric world, those businesses that know the most about their customers and markets are most likely to achieve the greatest success.

It’s no surprise then that future-focused organizations pursuing enhanced productivity and value are increasingly investing in the remarkably powerful capabilities that artificial intelligence (AI), machine learning, the Internet of Things (IoT) and augmented reality (AR) solutions can deliver when combined with data and analytics.

In healthcare, smart technologies and data analysis of patients’ genetic profiles is already allowing doctors to prescribe game-changing preventative and personalized treatments. In transportation, self-driving vehicle technology and traffic monitoring are improving traffic flow to reduce congestion and accidents. In financial services, rapidly emerging capabilities

are already being applied to risk management, portfolio management, trade clearing and more to improve business efficiency and drive growth. The list goes on.

Combine personalization and protection

Capitalizing on the vast potential of data analytics and the power of intelligent technologies assumes, of course, that privacy rights and data security will be strategically managed and protected.

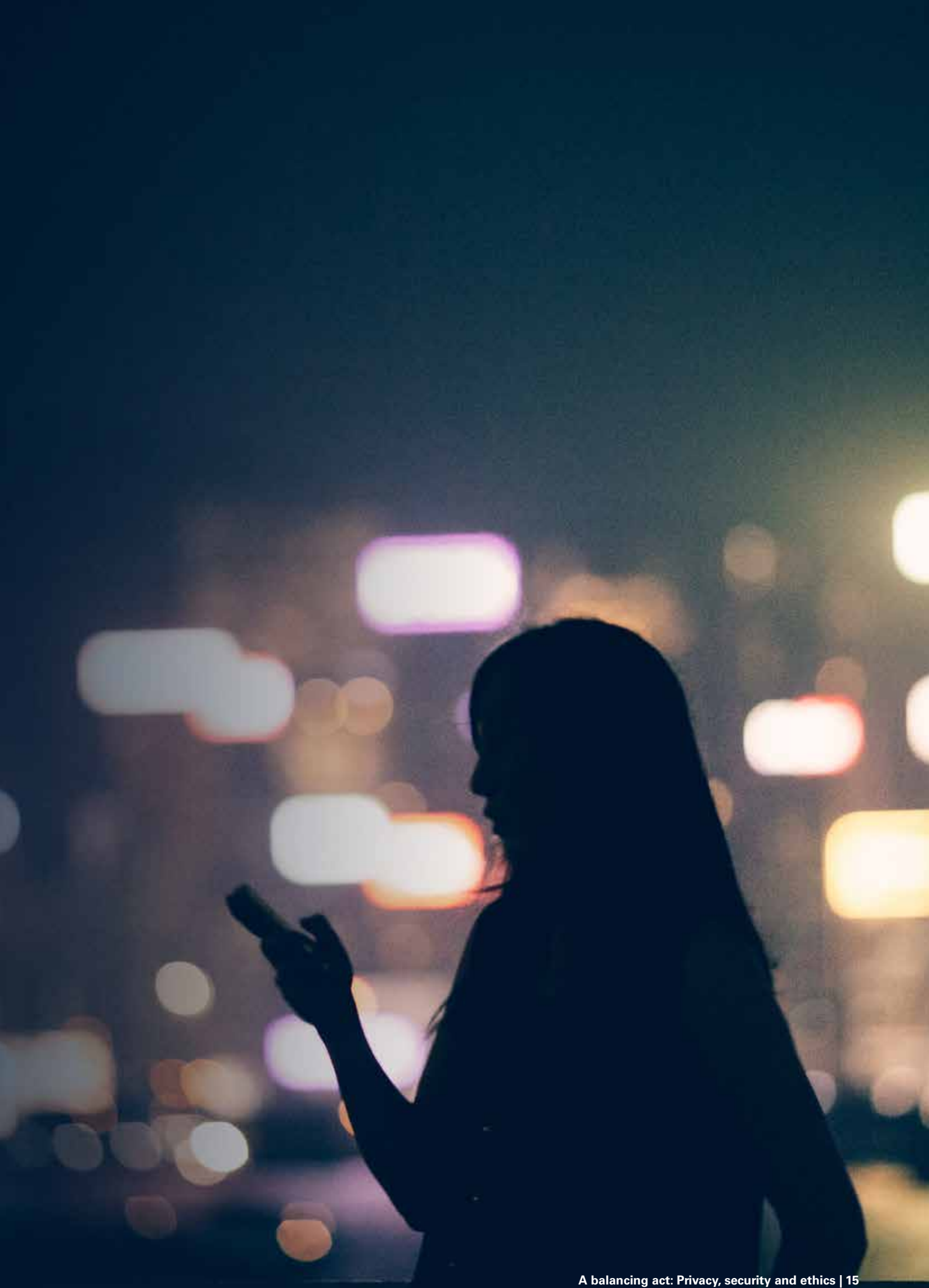
"Companies often operate under the misconception that personalization and data protection are conflicting efforts, not symbiotic opportunities," says Sylvia Kingsmill, Privacy Lead, KPMG in Canada. "The potential outcome of conflicts between data and analytics leaders, customer experience leaders, marketing leaders, security and risk professionals and other business and IT stakeholders is evident when data monetization efforts largely exceed and hinder data protection."

Organizations that fail to combine personalization efforts with data protection are undermining their chances to monetize personal data, she notes.

"They're frustrating customers and limiting new business values. Playbooks in response to the General Data Protection Regulation (GDPR) have helped to transform the way that personal information is collected, stored, used, disclosed and disposed of, while the NIST Cyber Security Framework in the US provides guidance on how businesses should detect, protect against and respond to cyber-attacks. These should be used to reframe business discussions and actions to focus on using personalization and data privacy to benefit customers, not frustrate them."

The question of ethical data use

Seeking the right data compound in the new reality raises ethical questions for careful consideration amid the increasing proliferation of cloud adoption, digital technologies and devices, and our growing reliance on their capabilities. Mobile phones, tablets, and laptops to enable remote working; the emergence of smart-watches, vehicles, homes, appliances; and not to mention the development of track and trace capabilities to control COVID-19, have all become an essential part of daily life.



64%

of consumers worldwide feel anxious about the authorized tracking of their online habits by companies, governments or criminals.

"Privacy is starting to collide with data ethics as organizations begin to explore if they should be using personal data and if so, how and for what? It's a new frontier which is going to strike hard at the bottom line for organizations that do not get it right."

— Mayuran Palanisamy
Privacy Lead
KPMG in India

Over time, of course, our digital devices are learning everything about our habits, preferences, communications, travels, purchases and more. Recent events have highlighted how critical those digital devices can be to controlling a global pandemic. Today's digital technology is designed to compile endless streams of personal data that's already being used, shared and monetized for analytics, customer profiling, targeted advertising and beyond. In today's digital world, not only are individuals a source of revenue for a company's core business — information generated about them is also a revenue stream in its own right, raising the question of when encroachment of personal data can be deemed unethical.

KPMG's *Me, my life, my wallet* report revealed that a majority (64 percent) of consumers worldwide feel anxious about the authorized tracking of their online habits by companies, governments or criminals, while even more feel anxious about identity theft (74 percent).[10] Recent evidence suggests that such concerns are on the rise, with 75 percent of US customers indicating they are thinking more about data privacy in the wake of COVID-19.[11]

Making data ethics a priority

Little wonder, perhaps, that data ethics is an emerging branch of applied ethics that focuses on the value judgments and approaches made when collecting, using, sharing, storing or destroying data. Data ethics includes a sound knowledge of data-protection law, other relevant legislation and the appropriate use of new technologies. It requires a holistic approach incorporating best practices in computing techniques, ethics and information assurance. Data ethics challenges that businesses face today include:

- violation of personal privacy or breach of trust due to inappropriate data processing
- processing personal data in a disproportionate or compromising manner that exposes the individual to harm or undermines trust
- profiling of individuals, potentially leading to discrimination based on age, ethnicity, health, religion or gender
- intrusive advertising that invades customer privacy or violates human rights.

The challenges and risks are real, but data ethics remains a new concept that many organizations are struggling to fully comprehend and respond to in their quest to design and embed robust ethics frameworks. This year the pandemic has highlighted how even countries can struggle to ethically use data when responding to COVID-19.

Technology that's enhancing the customer experience at the *front of the house* is also allowing organizations to analyze every granular detail of the customer experience and interaction at the *back*. A smart 'customer first' approach, therefore, also demands a 'data first' approach that includes an appropriate sustained focus on ethical privacy protection and security. With technology generating unprecedented insights that enhance decision-making traditionally handled by humans, data ethics should be near the top of every organization's digital transformation agenda.

Data ethics raises significant questions that address whether data use is legal, fair and balanced. Businesses that consider every ethical implication of their data management can be confident of maintaining public trust, brand loyalty, reputation and, ultimately, a competitive edge by meeting compliance and consumer privacy issues.

"Privacy is starting to collide with data ethics as organizations begin to explore if they should be using personal data and if so, how and for what? It's a new frontier which is going to strike hard at the bottom line for organizations that do not get it right," warns Mayuran Palanisamy, Privacy Lead, KPMG in India.

[10] *Me, my life, my wallet,* KPMG, 2019.
[11] *The new imperative for corporate data responsibility,* KPMG LLP, 2020.

What's your data worth?

Organizations, whether or not they accelerated or kickstarted their digital transformation journey to combat the impact of the pandemic, are grappling with the challenge of how to strategically manage consumer privacy while maximizing the value of the vast data assets they continue to amass. To understand how much to invest in managing liabilities involving data protection, security and ethics, businesses must first assess and understand the current and potential value of their data and data compound. For example, how much is a customer's email address worth — and how much more could it be worth when combined with other data sets?

Unfortunately, no formula exists to establish the value of the diverse data assets that are inundating businesses in every industry. But enterprises trying to establish what their data is worth and where its ultimate value resides should start by looking into their *data asset inventory* to determine precisely *which* data the organization is using and *why*. This will reveal how each data element is being used to provide value to the organization, how it does so and the monetary return it ultimately provides or enables.

"Organizations need to start understanding the value of their data assets to ensure they treat those assets in the right way. For example, an airline understands the value of a jet and will use, manage and protect it accordingly. As we continue on this digital revolution, ensuring personal information assets are understood and managed appropriately is going to become increasingly critical for organizations," says Matthew Quick, Cyber Privacy Lead, KPMG in Australia.

"As we continue on this digital revolution, ensuring personal information assets are understood and managed appropriately is going to become increasingly critical for organizations."

— Matthew Quick
Cyber Privacy Lead
KPMG in Australia

Regulators are sharpening their focus on data use

Organizations are operating in a precarious environment, which is increasingly impacting the data compound mix. On the one hand, they're pushing the boundaries of innovation and data use as never before. At the same time, however, they're carefully examining customer perception of privacy rights, which have heightened in sensitivity as a result of the pandemic, so as not to cross the line between what consumers consider 'cool' and what they dismiss as 'creepy' or potentially unethical — if not illegal.

The protection of personal data and data privacy are clear priorities for consumers. KPMG's recent survey in the US revealed a change in attitudes amongst consumers when it comes to their personal data — 87 percent of respondents now say that data privacy is a human right. Significant consumer mistrust was also reported — 68 percent of respondents said they don't trust companies to ethically sell data, and over half of respondents don't trust companies to collect or protect their data.[12]

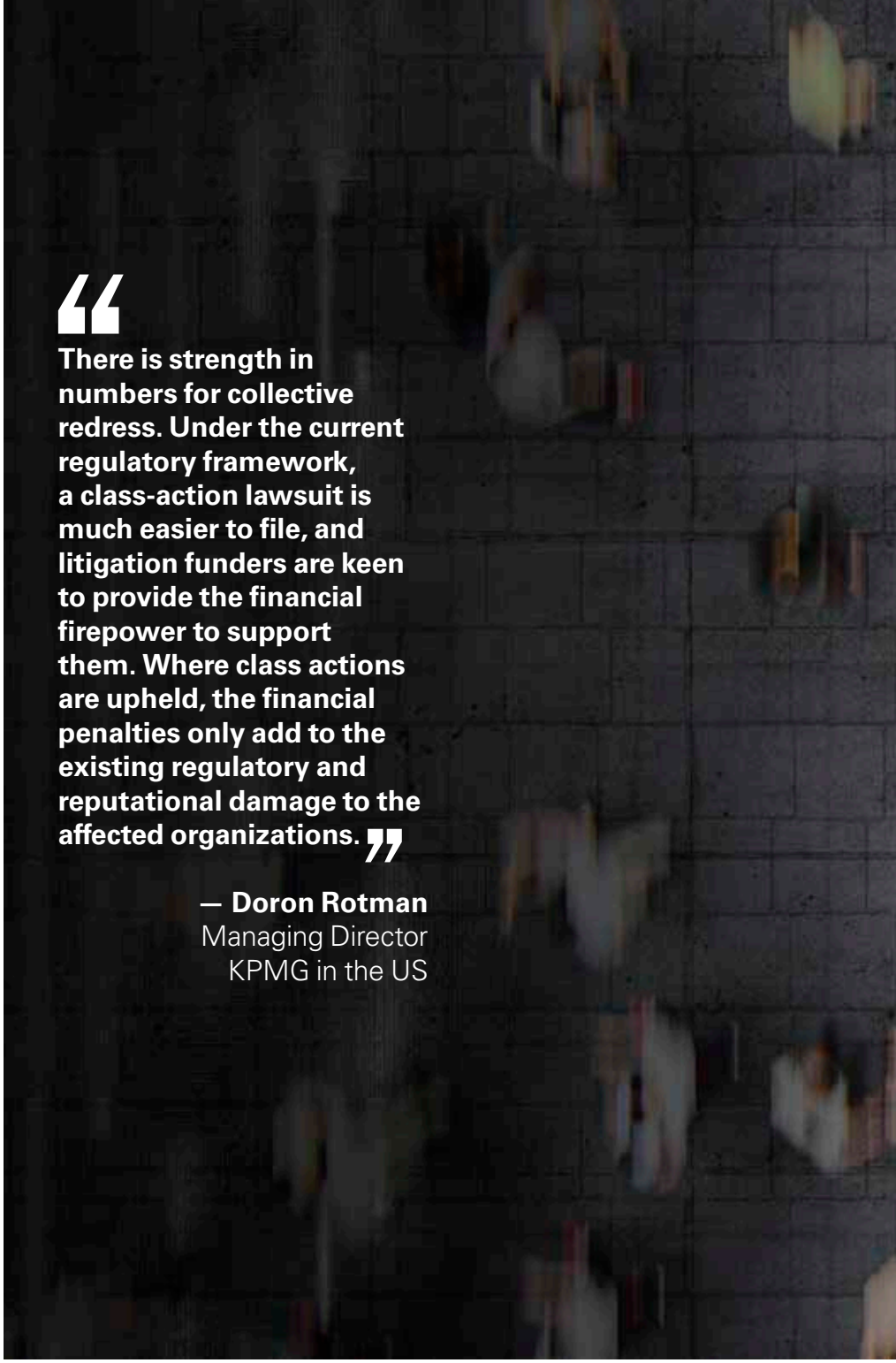
Regulators are taking notice, and the regulatory landscape is rapidly evolving to address public concerns over privacy, security and the legal use of data. In May 2018, the General Data Protection Regulation (GDPR) came into effect as perhaps the most rigorous and far-reaching data-protection regulation to date. It imposes tight data-protection requirements and hefty penalties for non-compliance by businesses around the world that fall within its scope.

The GDPR was the first wave in the trend toward new privacy regulation. As technology advances, new data-protection laws are emerging globally to:

— establish rules that are fit for innovation, as the majority of these laws and regulations are technology-neutral

— cultivate a culture of data protection 'by design' — embedding protection into devices to ensure the safe and ethical use of new technologies and data-processing activities

— put individuals in control of their personal data by articulating important rights that give them greater powers to protect themselves.



"There is strength in numbers for collective redress. Under the current regulatory framework, a class-action lawsuit is much easier to file, and litigation funders are keen to provide the financial firepower to support them. Where class actions are upheld, the financial penalties only add to the existing regulatory and reputational damage to the affected organizations."

— Doron Rotman
Managing Director
KPMG in the US

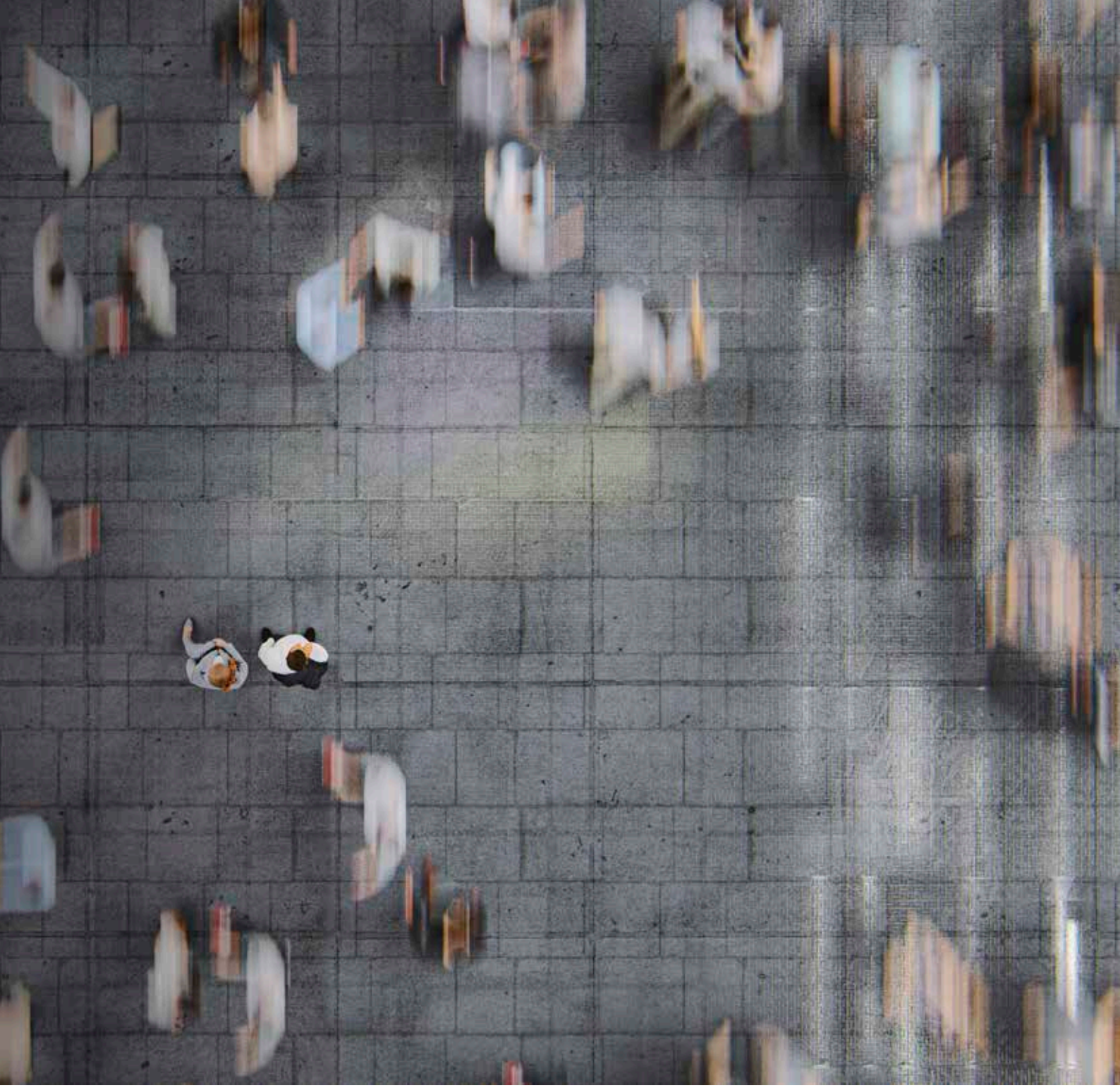
Regulations and penalties — on the rise

The GDPR has acted as a catalyst for change in the privacy regulatory framework at a global level, and several GDPR-aligned regulations have quickly followed suit, including the California Consumer Privacy Act, the Brazilian General Data Protection Law, India's Personal Data Protection Bill 2018, and the Thailand Personal Data Protection Act.

"Organizations need to understand that being just 'GDPR ready' is unlikely to meet all privacy obligations globally. We also have to consider the diverse cultural expectations of these different markets from a privacy perspective," says Michael Falk, Privacy Lead, KPMG in Germany.

With tighter privacy regulations on the rise, penalties are also increasing. Ten years ago, fines regarding data-protection breaches were in the low

[12] *The new imperative for corporate data responsibility,* KPMG LLP, 2020.



millions for security controls deemed weak. By contrast, in 2019, the US Federal Trade Commission approved a fine of roughly US$5 billion[13].

Meanwhile, since the GDPR's enactment, more than 100 cases of enforcement action were put forth with an imposed fines of over US$400 million since May 2018[14]. There has also been a significant surge in class-action lawsuits challenging the privacy and cybersecurity practices of some organizations, including their use of tracking and the loss of personal data.

"There is strength in numbers for collective redress," says Doron Rotman, Managing Director, KPMG in the US. "Under the current regulatory framework, a class-action lawsuit is much easier to file, and litigation funders are keen to provide the financial firepower to support them. Where class actions are upheld, the financial penalties only add to the existing regulatory and reputational damage to the affected organizations."

[13] *Press release*, Federal Trade Commission, July 24, 2019.
[14] *Global Privacy and Data Protection Enforcement Database*, IAPP, 2020.

Embracing trust as the new currency

So what is public and what is private in this challenging era of data use and the need to develop the perfect data compound? How can organizations wisely and strategically resolve the high-wire act they face: balancing data use to drive value and a competitive advantage versus the need to respect customer privacy, security concerns and the evolving regulatory environment, in the wake of the new reality?

75%

of consumers think that data protection should be embedded into digital devices 'by design,' and 58 percent said they would avoid storing data on a device that does not embed sufficient data-protection controls.

It should be abundantly clear by now to any business that misjudging consumer concerns or violating regulations risk not only significant financial penalties but also the harmful erosion of trust and reputation among their customers and markets.

"Expectations of customers are changing, and organizations need to understand these expectations to be successful," notes Atsushi Taguchi, Privacy Lead, KPMG in Japan. "As we saw in KPMG's *Consumer Loss Barometer* survey, for example, 75 percent of consumers think that data protection should be embedded into digital devices 'by design,' and 58 percent said they would avoid storing data on a device that does not embed sufficient data-protection controls."

In an era of heightened transparency and informed, empowered and connected consumers, the concept of trust has risen to a new level of prominence. No longer to be taken for granted, trust is fast emerging as a critical *prerequisite* to accessing and using valuable data and insights from consumers.[15] Winners in the race to maximize data's value and its impact on competitive advantage will strategically address and manage trust.

Data professionals hold the key

We believe that data-protection professionals will hold the key to success on this front. Data-protection professionals are ideally placed to put data protection and data ethics at the heart of a smart business strategy — ultimately helping to shape a digital economy in which personal data is exploited successfully while privacy and security rights are robustly upheld.

How can data-protection professionals help shape data-led businesses that successfully use data to achieve strategic business and growth objectives — and enhance competitive advantage — while sustaining trust and confidence in the organization?

The answer, in part, lies in creating a holistic data strategy that's designed to put data protection at the center of data-driven and insight-led businesses. Data strategies based on trust will act as a catalyst for change for the entire organization and inspire the business strategy as a whole.

KPMG's research report, *Me, my life, my wallet* revealed consumer anxiety about how user data could be accessed, used or abused online. Globally, just under three-quarters of consumers are concerned that their identity will be stolen, with 48 percent reporting 'high anxiety' over identify theft and a similar number (51 percent) reporting 'high anxiety' at the prospect of hacking of financial, medical or other personal information online.[16]

COVID-19 has forced customers down digital commerce channels, and therefore it is even more critical that data protection is at the heart of an organization's data strategy.

Data-protection professionals are uniquely qualified to support the organization in understanding the value that personal information — used correctly — can unlock, while effectively controlling, predicting and mitigating risk. An embedded strategic data strategy will include critical insights into

- the quality of existing data inventories and when or what type of new data needs to be captured
- whether existing and prospective customers trust the organization
- innovative practices for future implementation and trust enhancement.

Data-protection professionals will need to work closely with data analysts and modelers to validate whether the business has the right data structures in place to ensure data use remains appropriate and trustworthy throughout its lifecycle.

[15] *Me, myself, my wallet*, KPMG International, 2019.
[16] *The new imperative for corporate data responsibility*, KPMG LLP, 2020.

Embed trust across the enterprise

"Given the huge volumes of data collected, it's becoming increasingly challenging for businesses to keep track of personal information captured and the processing purposes that data subjects were notified of or consented to," says Orson Lucas, Privacy Co-Lead, KPMG in the US. "Since data is such a cross-functional asset that's collected, used, enhanced and analyzed by a multitude of teams throughout the organization, implementing a cross-functional target operating model that embeds trust and data protection across multiple touchpoints within the organization is fundamental to ensuring transformation efforts thrive."

Data-protection professionals can also bring a unique perspective to a company's board. Not only are they able to articulate how to exploit personal information, but they are also able to help convey the ROI that will be unlocked by striking the right balance between risk and reward. This balance will be of particular importance to boards as companies seek to recover efficiently from the pandemic.

Given the volume of sensitive or confidential personal data and the rapidly evolving nature of AI and machine learning tools powering data consumption and use, data-protection professionals may need to adapt how they approach their day-to-day jobs. Undertaking risk assessments from the outset, before a project or activity starts, and then relying on regular audits to understand risk mitigation in line with recommendations given, may no longer be sufficient.

Data-protection practitioners will also need to adopt cyclical processes for monitoring privacy and security risk and controls — continually reviewing and reassessing data-processing activities; conducting privacy, cyber and ethics impact assessments; and updating their inventory and notice as AI or machine learning solutions unlock new processing purposes.

> **"Since data is such a cross-functional asset that's collected, used, enhanced and analyzed by a multitude of teams throughout the organization, implementing a cross-functional target operating model that embeds trust and data protection across multiple touchpoints within the organization is fundamental to ensuring transformation efforts thrive."**
>
> **— Orson Lucas**
> Privacy Co-Lead
> KPMG in the US

Conclusion

As organizations navigate their way into the new reality and seek to capitalize on data and drive growth, particularly through new digital channels, they will need to remain mindful that commercialized data still belongs to their customers — who are entitled to access, rectify, restrict and possibly even erase sensitive or confidential information that's constantly being compiled, analyzed and shared.

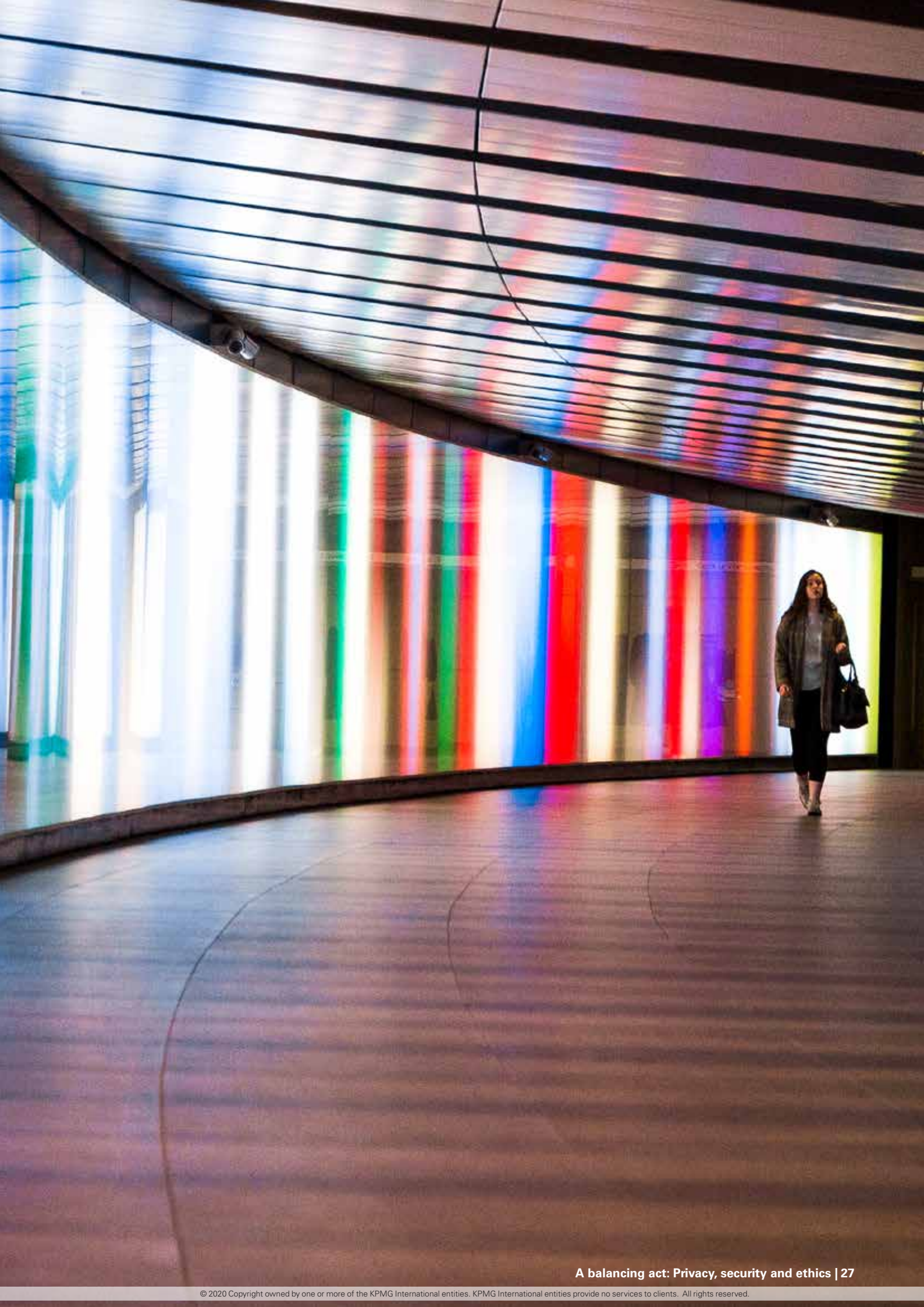
To protect and enhance customer trust while pursuing new value and advantages, businesses will need to design controls that acknowledge and facilitate the public's rights regarding data use. To help ensure businesses are 'formulating' the right data compound — producing healthy, sustainable results instead of a 'toxic mix' that could prove costly to brand trust and customer loyalty — organizations will need to

- support and define a data vision in which appropriate data use and protection is at the heart of data strategy and closely aligned to business objectives
- truly understand the challenges around creation or acquisition of data and the potential risks or rewards related to how well customer concerns and expectations are met
- understand the value data holds for your organization both now and in the future
- balance data consumption and commercialization — don't use the asset so much that you diminish its value.

"It's clear that to fully use personal information and translate it into positive business results, trust — in the form of data protection, security and ethics — must be built into business processes by default and embedded into an organization's culture, thought and behavior," says Mark Thompson, Global Privacy Lead, KPMG International. "The winners in the quest for a smart data compound that unlocks new competitive advantage will make privacy an integral part of the way they do business."

> **"The winners in the quest for a smart data compound that unlocks new competitive advantage will make privacy an integral part of the way they do business."**

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International



Contacts

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International
T: +1 416 777 8190
E: skingsmill@kpmg.ca

Walter Risi
KPMG in Argentina
T: +541143165843
E: wrisi@kpmg.com.ar

Matthew Quick
KPMG in Australia
T: +61 3 9288 6015
E: mquick@kpmg.com.au

Andreas Tomek
KPMG in Austria
T: +43 1 31332 3930
E: atomek@kpmg.at

Benny Bogaerts
KPMG in Belgium
T: +3238211893
E: bbogaerts@kpmg.com

Leandro Augusto M Antonio
KPMG in Brazil
T: +551139403740
E: lantonio@kpmg.com.br

Sylvia Kingsmill
KPMG in Canada
T: +1 416 777 8190
E: skingsmill@kpmg.ca

Tamara Agnic
KPMG in Chile
T: +56229971519
E: tagnic@kpmg.com

Henry Shek
KPMG in China
T: +85221438799
E: henry.shek@kpmg.com

Vincent Maret
KPMG in France
T: +33155682664
E: vmaret@kpmg.fr

Michael Falk
KPMG in Germany
T: +49 69 9587-3680
E: mfalk@kpmg.com

Mayuran Palanisamy
KPMG in India
T: +914439145000
E: mpalanisamy@kpmg.com

Dani Michaux
KPMG in Ireland
T: +35317004769
E: dani.michaux@kpmg.ie

Jonathan Brera
KPMG in Italy
T: +3902676431
E: jbrera@kpmg.it

Kenjiro Obora
KPMG in Japan
T: +81335485111
E: kenjiro.obora@jp.kpmg.com

Min Soo Kim
KPMG in Korea
T: +82221127010
E: mkim9@kr.kpmg.com

Rommel Garcia
KPMG in Mexico
T: +525552468789
E: rommelgarcia@kpmg.com.mx

Koos Wolters
KPMG in the Netherlands
T: +31206 564048
E: wolters.koos@kpmg.nl

Souella Cumming
KPMG in New Zealand
T: +6448164519
E: smcumming@kpmg.co.nz

John Anyanwu
KPMG in Nigeria
T: +2348039754061
E: john.anyanwu@ng.kpmg.com

Arne Helme
KPMG in Norway
T: +4740639507
E: arne.helme@kpmg.no

Glenn Tjon
KPMG in Panama
T: +5072080700
E: gtjon@kpmg.com

Imelda Corros
KPMG in the Philippines
T: +6328857000
E: icorros@kpmg.com

Krzysztof Radziwon
KPMG in Poland
T: +48225281137
E: kradziwon@kpmg.pl

Mihai Gabriel Tanase
KPMG in Romania
T: +40372377785
E: mtanase@kpmg.com

Andrey Lepekhin
KPMG in Russia
T: +74959374444 x14239
E: alepekhin@kpmg.ru

Daryl Pereira
KPMG in Singapore
T: +6564118116
E: darylpereira@kpmg.com.sg

Javier Aznar Garcia
KPMG in Spain
T: +34914563430
E: jaznar@kpmg.es

Peter Lind
KPMG in Sweden
T: +46 8 7239967
E: peter.lind@kpmg.se

Thomas Bolliger
KPMG in Switzerland
T: +41 58 249 28 13
E: tbolliger@kpmg.com

Jason Y.T. Hsieh
KPMG in Taiwan
T: +886281016666 x 07989
E: jasonhsieh@kpmg.com.tw

Chris Saunders
KPMG in Thailand
T: +6626772359
E: csaunders2@kpmg.co.th

Maliha Rashid
KPMG in the United Arab Emirates
E: mrashid5@kpmg.com

Rodrigo Ribeiro
KPMG in Uruguay
T: +59829024546
E: rribeiro@kpmg.com

Doron M Rotman
KPMG in the USA
T: +1 408 367 7607
E: drotman@kpmg.com

Orson Lucas
KPMG in the USA
T: +1 813 301 2025
E: olucas@kpmg.com

Will Nguyen
KPMG in Vietnam and Cambodia
T: +84 28 38219266-8770
E: williamnguyen@kpmg.com.vn

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: A balancing act: Privacy, security and ethics | Publication number: 136701-G | Publication date: November 2020