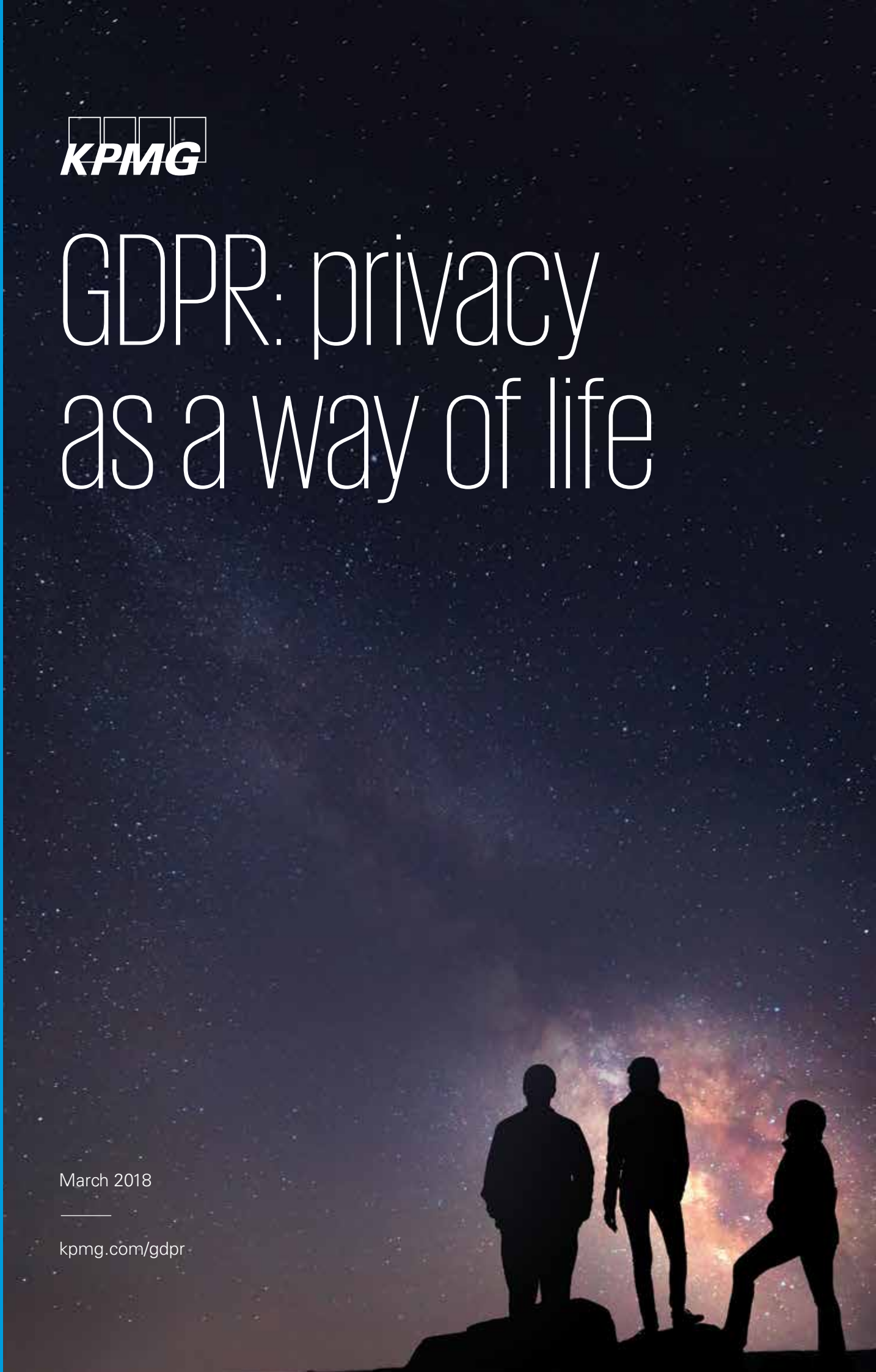
KPMG

GDPR: privacy as a way of life



March 2018

kpmg.com/gdpr

Nurturing a privacy-conscious culture

As the 25 May 2018 deadline for the General Data Protection Regulation (GDPR) looms ever closer, organizations of all sizes are busy getting their houses in order, in a bid to achieve compliance.

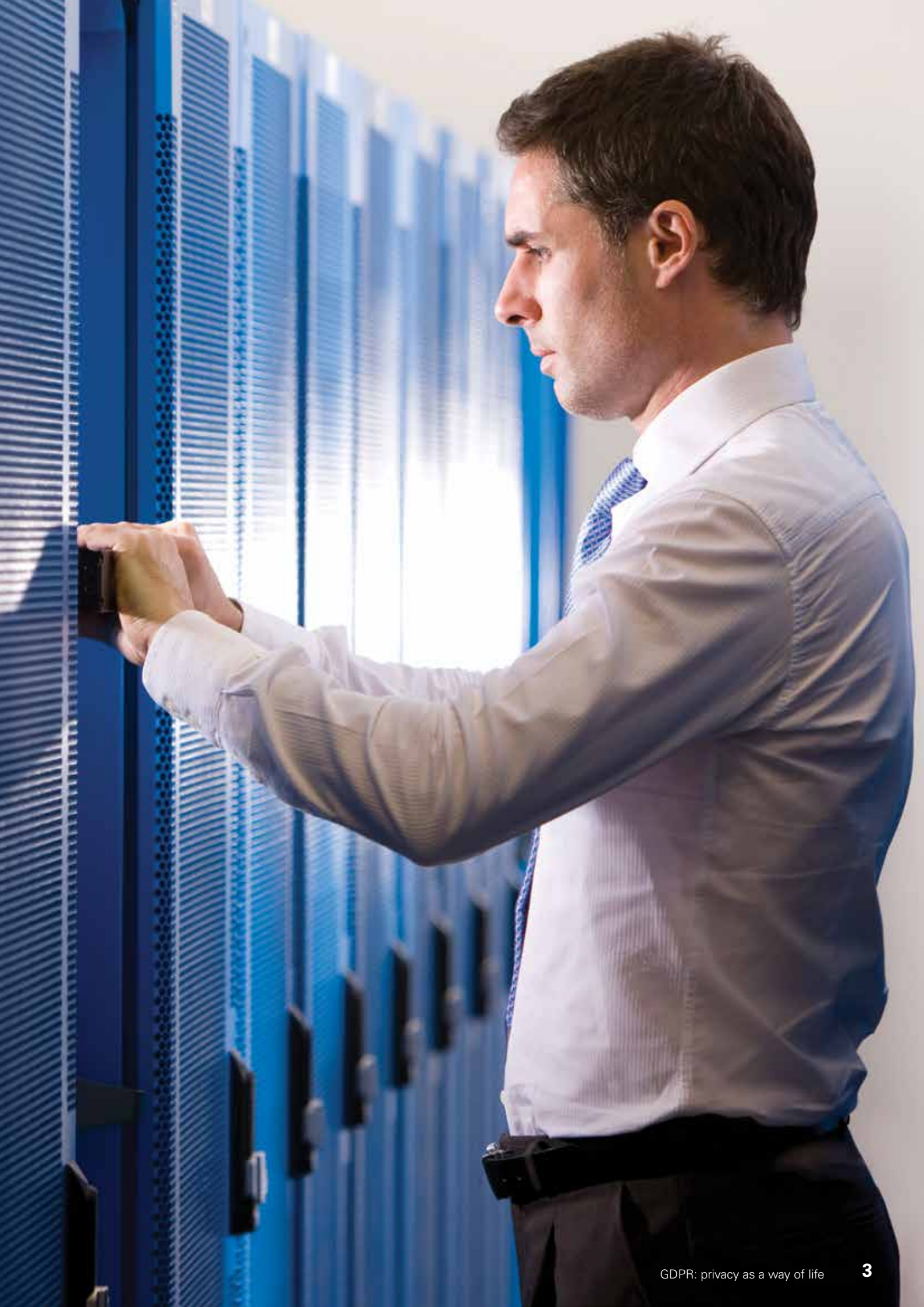
The GDPR affects organizations that deal with consumers and businesses in EU member states, and will transform the way that personal information is collected, stored, used, disclosed and disposed of.

While meeting regulatory obligations is a must, there is a danger of treating the GDPR as a one-off, 'tick the box' compliance activity, rather than a deliberate move towards a privacy-conscious culture, where transparency, citizens' rights and accountability become second nature to all employees.

In this brief paper we discuss five issues for you to consider, as you seek to make privacy an integral part of the way your organization does business.

> "There is a danger of treating the GDPR as a 'tick the box' compliance activity, rather than a deliberate move towards a culture where transparency, citizens' rights and accountability are second nature."

> "Viewing personal data as an asset opens the door to exciting, value-creating investments, accelerating a shift to simpler, less costly and more powerful data systems."



1. Put customers and employees at the heart of your privacy strategy

In the words of Elizabeth Denham, CEO of the UK Information Commissioner's Office, *"The biggest threat to organizations from the GDPR is not massive fines. It's about putting the consumer and citizen first."*[1] Much of what's been written about the GDPR centers on penalties. Although these have the potential to be severe (non-compliant firms can be fined up to 4 percent of turnover or 20 million Euros, whichever is greater), they should not be the driving force behind change. It's more important to begin to instill the right habits and behaviors, so that everyone in your organization appreciates customers' rights to privacy and choice.

In order to help build and cement trust, your business should make customers aware of what kinds of personal information you hold and how you use it, with transparency and accountability as your guiding principles. Customers are entitled to know what is being done with their personal information — and expect you to tell them. This means understanding the customer journey, and making privacy an essential feature of that journey — and an integral part of your wider business strategy.

And as you map the customer journey, it's the touchpoints that should receive the highest priority. These are the public-facing aspects of your business, like handling customer complaints and queries, or targeting individuals with personalized offers. In an omni-channel world, where customers interact via phone, apps, online chats, email and post, these touchpoints need to offer a consistent experience.

Touchpoints offer an ideal opportunity to showcase transparency, and to explain how you're using customers' personal data responsibly. By paying close attention to the quality and integrity of such interactions, you can present a positive picture of how your organization manages privacy, in the process enhancing your reputation with customers and employees, and reassuring regulators.

You may want to introduce incentives that encourage appropriate values and behavior. And you'll certainly want to nurture an environment where any risks and issues can be discussed openly, and processes challenged where necessary. Training and communications can help spread the word and equip employees with the skills and awareness of privacy issues.

2. Understand that data is an asset and a liability

As we've mentioned, the GDPR is not simply a static deadline. It's part of a journey towards better management and use of that most valuable resource: personal data.

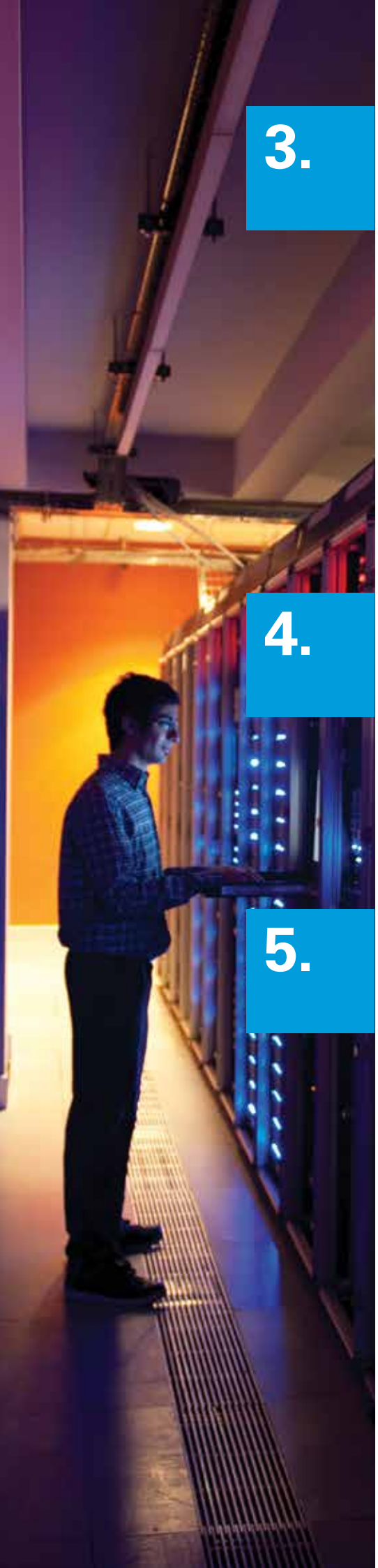
The potential liability of data derives not just from the clearly articulated GDPR penalties, but also from any loss of customer trust and brand and reputational damage resulting from a breach and/or unacceptable behavior.

On the flip side, viewing data as an asset opens the door to exciting investments that can create value: transforming the operational infrastructure and accelerating a wider and longer-term shift to simpler, less costly and more powerful data systems.

All of which should help enable your organization to not only gain more confidence in its privacy capabilities; but to also enhance other functions that depend heavily on customer data, like fraud detection, marketing and customer analytics.

You may also want to think about the skills you have within your organization. In addition to lawyers and compliance and risk professionals, you need access to technology and data experts who can help you embed the GDPR as part of your overall data strategy.

1 *GDPR — sorting the fact from the fiction,* Elizabeth Denham, CEO, Information Commissioner's Office, 9 August 2017.



3. Don't rush into major technology investments

In the push to be ready for the May deadline, it's tempting to believe that GDPR software solutions can ensure compliance. In reality though, without a clear privacy strategy and documented roadmap, and a pre-existing culture of transparency, technology may simply add more complexity — at considerable cost.

By concentrating on activities that will add value to your privacy efforts and by seeking advice from knowledgeable experts, you should have a better chance of making the right technology choices. Don't forget that GDPR preparation doesn't simply finish on 25 May 2018 — privacy regulations should continue to evolve, so avoid large investments today that may leave you with something that isn't fit for tomorrow.

Before considering which solutions to invest in, you must first get the basics right — starting with strong privacy governance. Once a simpler, more streamlined set of processes and roles are in place, you can then seek the appropriate applications to meet your needs and to help automate repeatable processes.

4. Be prepared for questions

Privacy is a hot topic and only likely to get hotter. Reputational damage — as a result of breaches or unethical activity — can be immense, and there is a small but growing community of journalists and other stakeholders that are eager to ask difficult questions. The answer is to be media ready at all times, with a well-briefed communications team and a senior, credible, privacy-aware spokesperson/people.

When dealing with customers, it's vital that all staff are fully trained and able to anticipate questions. It only takes one poor or uninformed response — especially where a customer has a good understanding of her/his rights — to create a negative experience, as well as an investigation.

5. Organizations located outside the EU

Any company dealing with data from EU data subjects needs to comply with the GDPR, and the globalization of business means that many organizations are likely to handle such data in some form — even if this means just one customer or employee. The GDPR impacts collection, use and disclosure of data, on a global scale, for organizations outside of the EU, which is likely to have considerable impact.

With today's international organizations typically involved in a complex web of subsidiaries and outsourced providers, the onus is on your data controller to ensure that every part of the value chain applies the same high standards of privacy. And it's not just about customers; employees in the EU also fall under the GDPR. Any financial, health and other sensitive, personal information needs to be handled in a way that meets the new standards. You will probably have to align any HR systems with relevant EU laws.

Some non-EU companies may lack strong relationships with and understanding of the various EU regulators, and may be uncertain about their stance. If an organization is from a country where privacy laws are relatively relaxed, and penalties are modest, then a possible non-compliance fine of up to 4 percent of turnover — in addition to the other powers given to privacy regulators — make the GDPR a daunting prospect. It's therefore essential to gain a good understanding of both local GDPR requirements and the various regulatory authorities across the EU that are responsible for enforcing it.

Privacy as a source of competitive advantage

Compliance deadlines inevitably focus the corporate mind. But in the case of the GDPR, any attempts to meet regulatory obligations should not be at the expense of a longer-term strategy that acknowledges privacy as a source of competitive advantage.

By considering how your organization can meet the needs of customers and employees, you can build a privacy-aware culture, and a governance infrastructure, which puts the right information at everyone's fingertips and consistently demonstrates transparency.

Key questions for Boards

- Who is in charge of privacy compliance? Are the right accountability and governance structures in place?
- Are we prepared to speak publicly and to our customers about how we manage their privacy?
- How do I know whether employees are taking an ethical stance towards privacy?
- Do we have a data strategy? Is it focused on what's best for the customer?
- Are we handling our key customer touch points efficiently and appropriately?
- What actions are we taking to nurture a privacy-aware culture to earn and retain our customers' trust?
- Do we view the GDPR as a one-off initiative? Or is it part of a proactive risk management approach, enabling us to put our customers at the center of everything we do?

"While the controller has ultimate accountability, the shift in liability for processors reinforces the need for controllers and processers to work closely together, to help maintain the privacy rights of data subjects in line with the GDPR."

KPMG member firms' privacy expertise

KPMG member firms' privacy professionals support clients around the globe in resolving complex privacy issues, from niche challenges specific to certain organizations to end-to-end privacy compliance programs in complex and highly regulated industries.

The KPMG privacy team has deep experience in helping organizations to address the challenges posed by privacy risk, with a structured and flexible approach to meet the needs of diverse organizations. The global reach of KPMG member firms helps to enable them to work effectively across multiple territories at a local level.

Areas where KPMG member firms are frequently engaged include:

Assess — Provide an independent assessment of current GDPR risk profile and how this compares to desired state

Design — Work with you to design a GDPR Compliance program to meet the requirements of the legislation

Strategy — Work with you to develop a pragmatic GDPR Privacy strategy and gain buy-in from Senior Management

Implement — Support the implementation of robust and sustainable GDPR processes, policies and controls to allow you to mitigate your Privacy risk

Operate — Provide ongoing support and advice to assist you in operating your GDPR control environment

Monitor — Support you in maintaining your GDPR Privacy control environment

Contacts

Mark Thompson
KPMG International
E: mark.thompson@kpmg.co.uk

Greg Bell
KPMG International
E: rgregbell@kpmg.com

Akhilesh Tuteja
KPMG International
E: atuteja@kpmg.com

Doron Rotman
KPMG in the US
E: drotman@kpmg.com

Koos Wolters
KPMG in the Netherlands
E: wolters.koos@kpmg.nl

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

Leandro Augusto Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Luca Boselli
KPMG in Italy
E: lboselli@kpmg.it

Gordon Archibald
KPMG in Australia
E: garchibald@kpmg.com.au

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

Ilya Shalenkov
KPMG in Russia
E: ishalenkov@kpmg.ru

Michael Falk
KPMG in Germany
E: mfalk@kpmg.com

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

Atsushi Taguchi
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

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

Dani Michaux
KPMG in Malaysia
E: danimichaux@kpmg.com.my

Sylvia Kingsmill
KPMG in Canada
E: skingsmill@kpmg.ca

Eric Muscat
KPMG in Malta
E: ericmuscat@kpmg.com.mt

Adrian Mizzi
KPMG in Malta
E: adrianmizzi@kpmg.com.mt

kpmg.com/socialmedia

Designed by Evalueserve.
Publication name: GDPR: privacy as a way of life
Publication number: 135313-G
Publication date: March 2018