GDPR and brand reputation: Five best- and worst-case scenarios

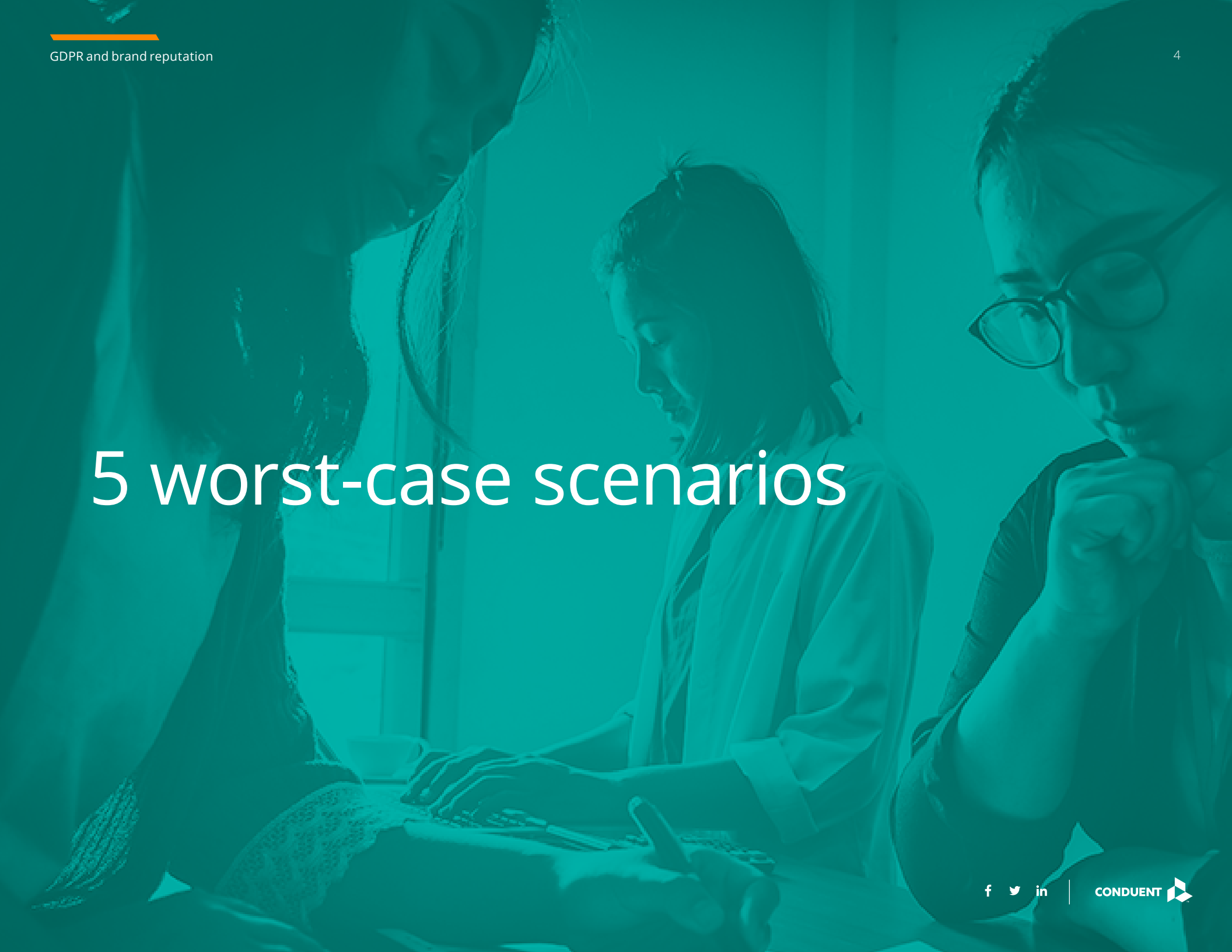
By Brian Clayton
Associate General Counsel and Chief Privacy Officer at Conduent

The European Union's General Data Protection Regulation — better known as GDPR — will impact businesses' brand reputation. GDPR presents an opportunity to forge a new level of trust between consumers and businesses.

Introduction to GDPR

GDPR is short for General Data Protection Regulation, a sweeping set of European Commission rules that are in force as of May 25, 2018. The regulations dictate how organizations handle customer data and data breaches, and give regulators the power to levy stiff fines for noncompliance. Though GDPR applies to European citizens, the rules will have an impact on companies worldwide.

Even for organizations that are well prepared, sustaining GDPR compliance will be an ongoing challenge. To bring home some of those challenges, we've outlined five potential worst-case scenarios. But after that, we'll look at five best-case scenarios — situations in which GDPR compliance will benefit brands and their relationships with consumers. Finally, we've listed five key questions your organization should be asking about GDPR.



5 worst-case scenarios

1 Confusion paralyzes your digital marketing and branding efforts.

GDPR requires companies keep a record of when each data subject consented to be part of their data processing. Do you have trustworthy records of when everyone on your marketing list explicitly agreed to receive email from you? If you aren't sure, you may find yourself in a bind as you try to navigate GDPR. Email marketers in particular will be in a tight spot if they lack accurate records of when each customer affirmatively opted in.

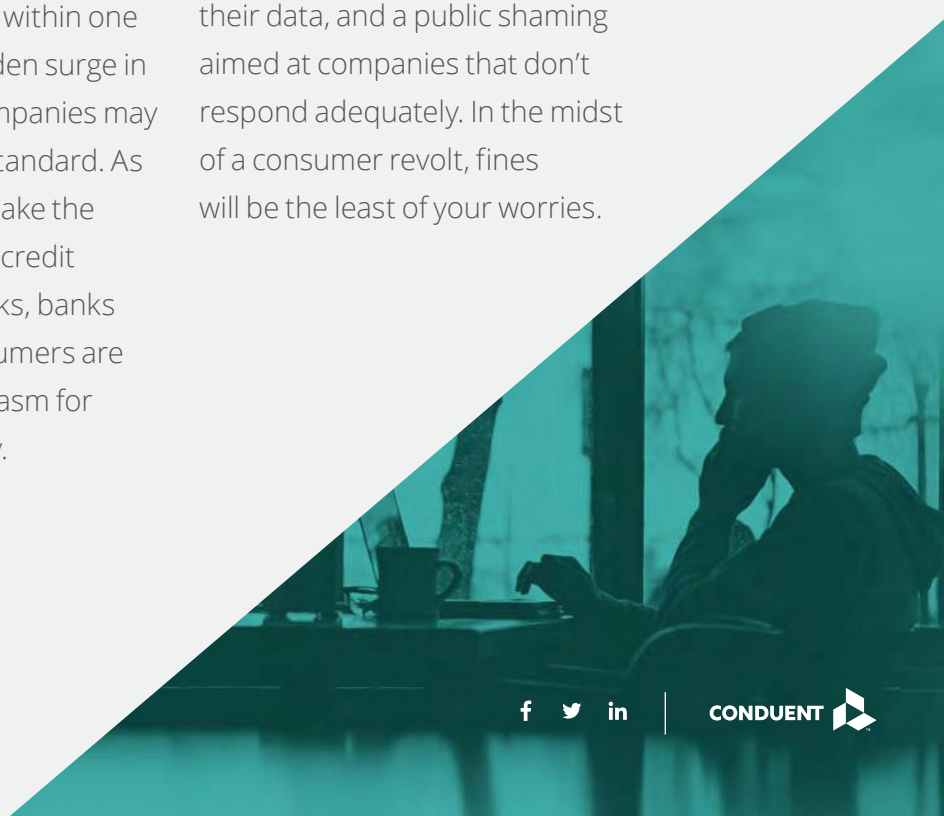
In this worst-case scenario, your organization might determine your sloppy data subject consent records pose too big of a risk — and your digital marketing efforts will grind to a screeching halt. Your customers will hear a single message from you: Silence.

Marketers will be in a tight spot if they lack accurate customer opt-in records.

2 Sluggish answers to customer inquiries lead to complaints, fines and damage to your brand.

Under GDPR, companies that hold personal data must provide a copy of an individual's data on request, free of charge. Companies owe consumers a response within one month. If there's a sudden surge in customer demand, companies may struggle to meet that standard. As major data breaches make the news — from retailers, credit bureaus, social networks, banks and on and on — consumers are showing a new enthusiasm for reclaiming their privacy.

It's easy to imagine a worst-case scenario — like a social media uproar — that provokes a flood of consumers to demand copies of their data, and a public shaming aimed at companies that don't respond adequately. In the midst of a consumer revolt, fines will be the least of your worries.

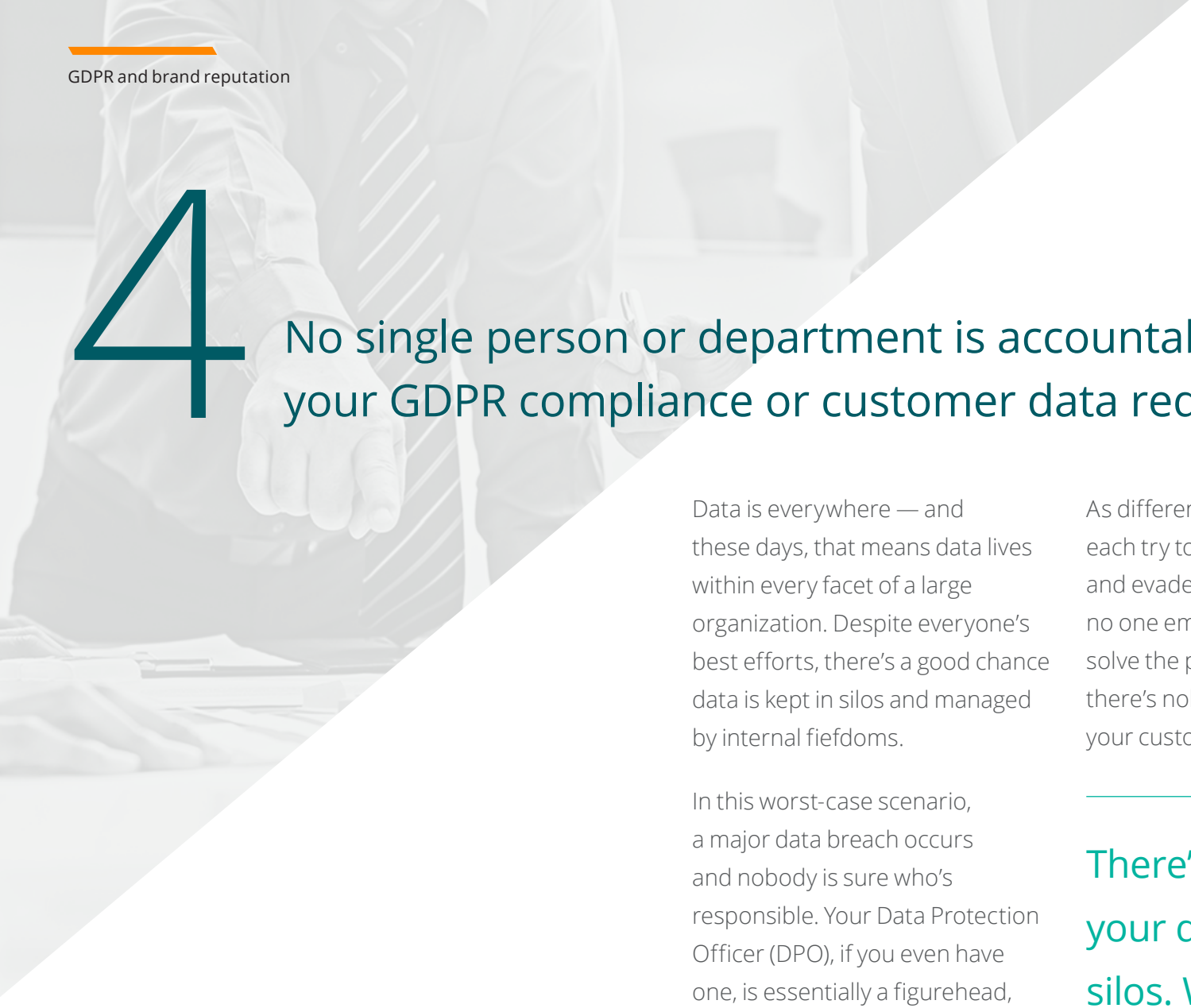


3 You lack a complete understanding of which third parties have copies of your customers' data — making it hard to comply with customer requests.

Let's take the previous worst-case scenarios another step. Imagine your customer data is in perfect order, and you have systems in place to deliver timely and courteous answers to customer data requests. But a partner you share data with suffers a massive breach in which data you collected was exposed. Even though it was no fault of your own, your customers won't accept a response that passes the buck to someone else.

On top of that, you will have to launch a time-consuming investigation to figure out exactly whose data was compromised and where else it might have been shared. You're on the hook and your brand will suffer damage.

If a partner you share data with suffers a breach, you'll need fast answers about what happened.



4 No single person or department is accountable for your GDPR compliance or customer data requests.

Data is everywhere — and these days, that means data lives within every facet of a large organization. Despite everyone's best efforts, there's a good chance data is kept in silos and managed by internal fiefdoms.

In this worst-case scenario, a major data breach occurs and nobody is sure who's responsible. Your Data Protection Officer (DPO), if you even have one, is essentially a figurehead, not informed or empowered to help. There's no playbook, so everyone is improvising.

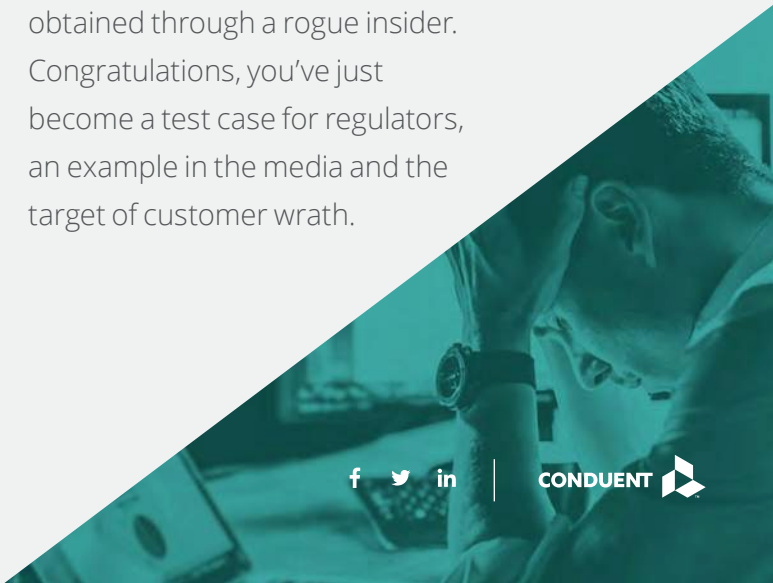
As different departments each try to protect themselves and evade responsibility, there's no one empowered to step up and solve the problem. Worst of all, there's nobody looking out for your customer.

There's a good chance your data is kept in internal silos. Who's responsible for all of it?

5 A data breach you never saw coming prompts a customer backlash, lost sales and a hefty fine.

Under the GDPR, most organizations are required to notify the European Commission within 72 hours of becoming aware of a security breach that "poses a risk to an individual's rights and freedoms." If your company happens to be a data processor, that 72-hour rule applies to every breach. And if the breach poses a "high risk" to the individuals affected, you have to tell every individual user too.

You can weave these rules into your own worst-case scenario. It might go something like this: You're notified that a purported list of your customers' personal information is for sale on the dark web. As you begin a mad 72-hour scramble to find out what happened, news of the breach appears in the press. The deadline passes and you still lack a conclusive response. Now hackers release the list and reveal that it is indeed your customer records, obtained through a rogue insider. Congratulations, you've just become a test case for regulators, an example in the media and the target of customer wrath.



And now:

5 best-case scenarios

1 Your customer data is sourced and safeguarded as a matter of practice, making GDPR compliance a breeze and helping you unlock new insights.

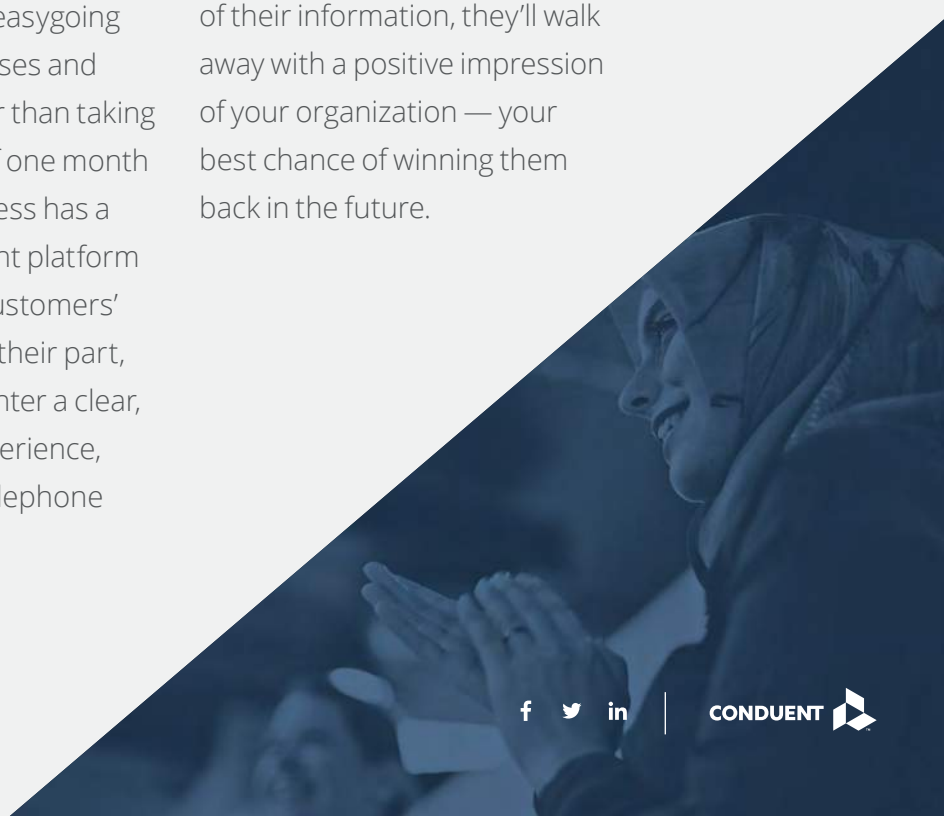
Now let's suppose you've taken the right steps to move your company into compliance with the GDPR, going beyond the bare minimum. As you onboard customers, you're offering them a variety of granular privacy options. You're asking customers what kinds of communication they want to receive.

Now, when it's time to communicate with your customers, you have insight into their individual interests and expectations — laying the foundation of a good customer relationship. And you'll experience fewer GDPR compliance issues.

As you onboard customers, you can offer them a variety of granular privacy options.

2 Your business delivers easy, self-serve portals for customer data inquires, with prompt response to data deletion requests.

Under the GDPR, citizens gain specific rights to request access to (and deletion of) their data at no cost. In the best-case scenario, these requests are an easygoing experience for businesses and customers alike. Rather than taking the GDPR-maximum of one month to respond, your business has a single data management platform and can service your customers' requests instantly. For their part, your customers encounter a clear, seamless and easy experience, whether it's a digital, telephone or multichannel interaction. You've demonstrated that you're a good steward of their data. Even when customers call to request deletion of their information, they'll walk away with a positive impression of your organization — your best chance of winning them back in the future.

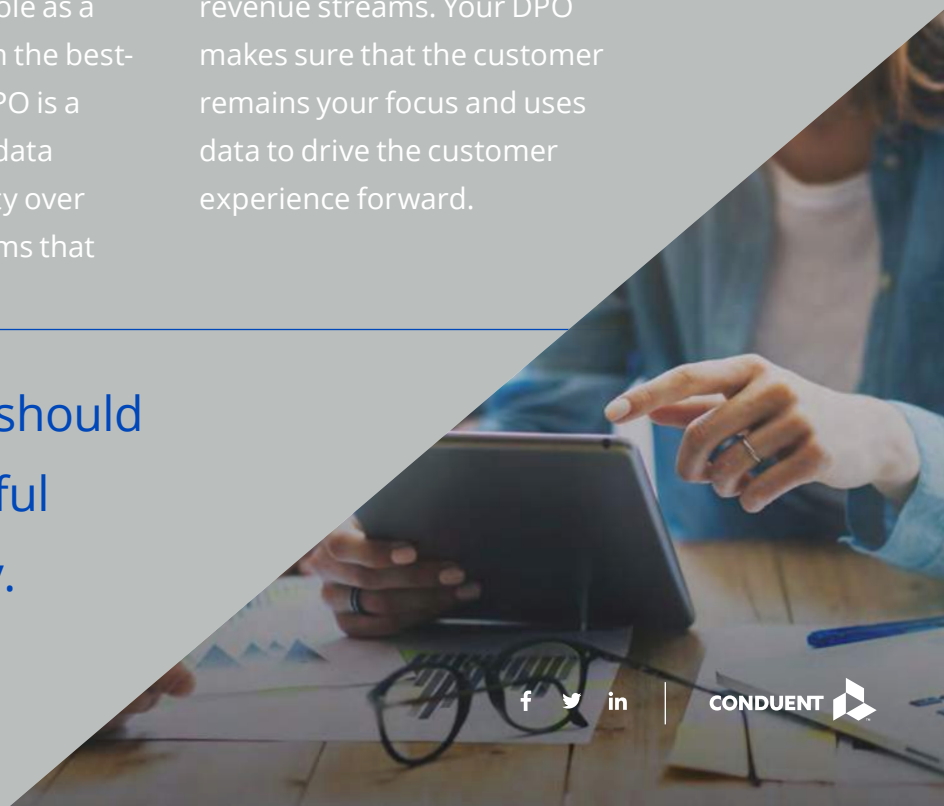


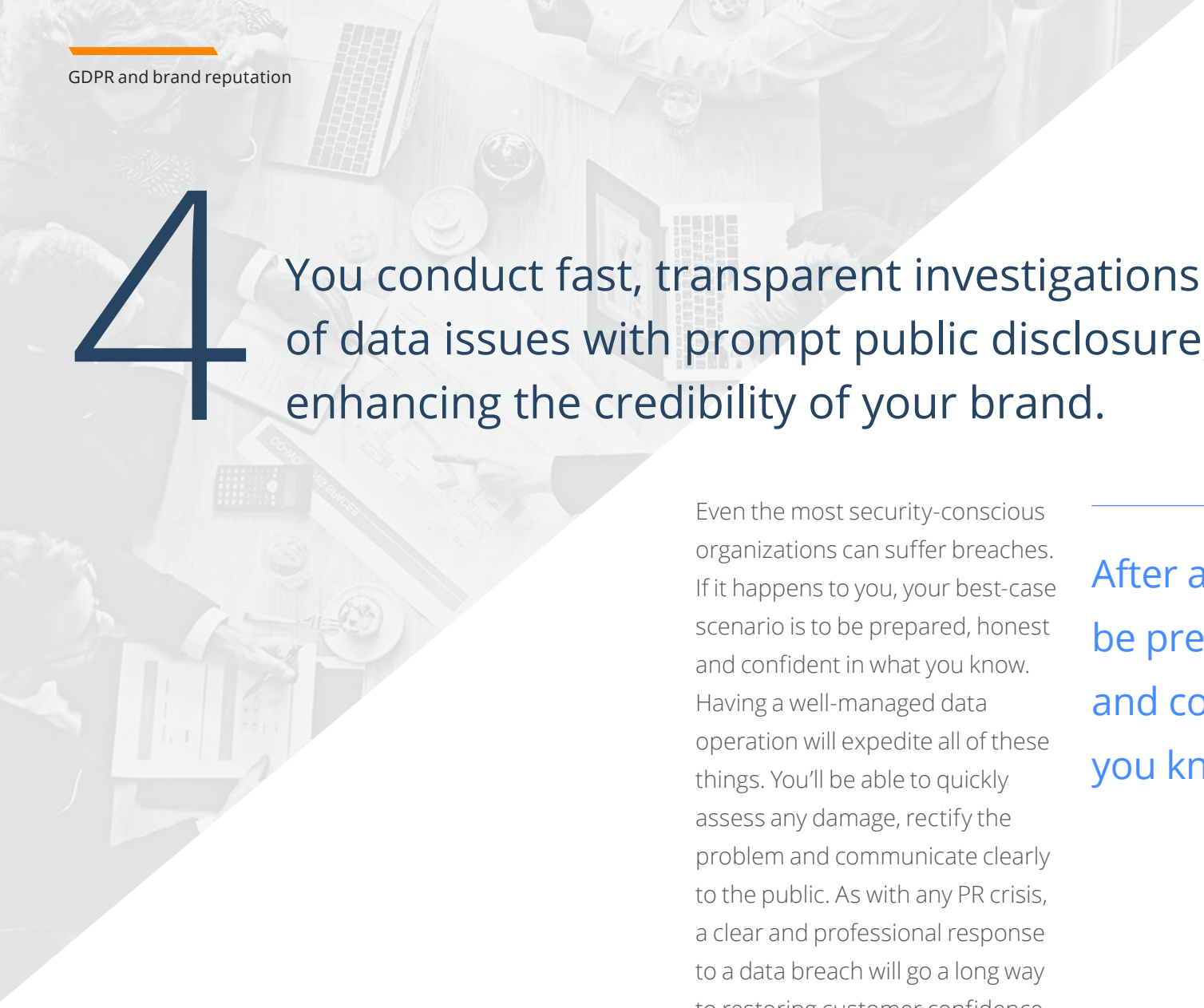
3

A Data Protection Officer oversees GDPR compliance and pursues ways to improve customer experiences.

The GDPR establishes conditions under which you must have a Data Protection Officer, or DPO. Some companies will no doubt treat the DPO role as a ceremonial title. But in the best-case scenario, your DPO is a forceful advocate for data security, with authority over your data and the teams that manage it. Your DPO is also looking into ways to break down silos within your organization and use your data to drive new revenue streams. Your DPO makes sure that the customer remains your focus and uses data to drive the customer experience forward.

A Data Protection Officer should be empowered as a forceful advocate for data security.





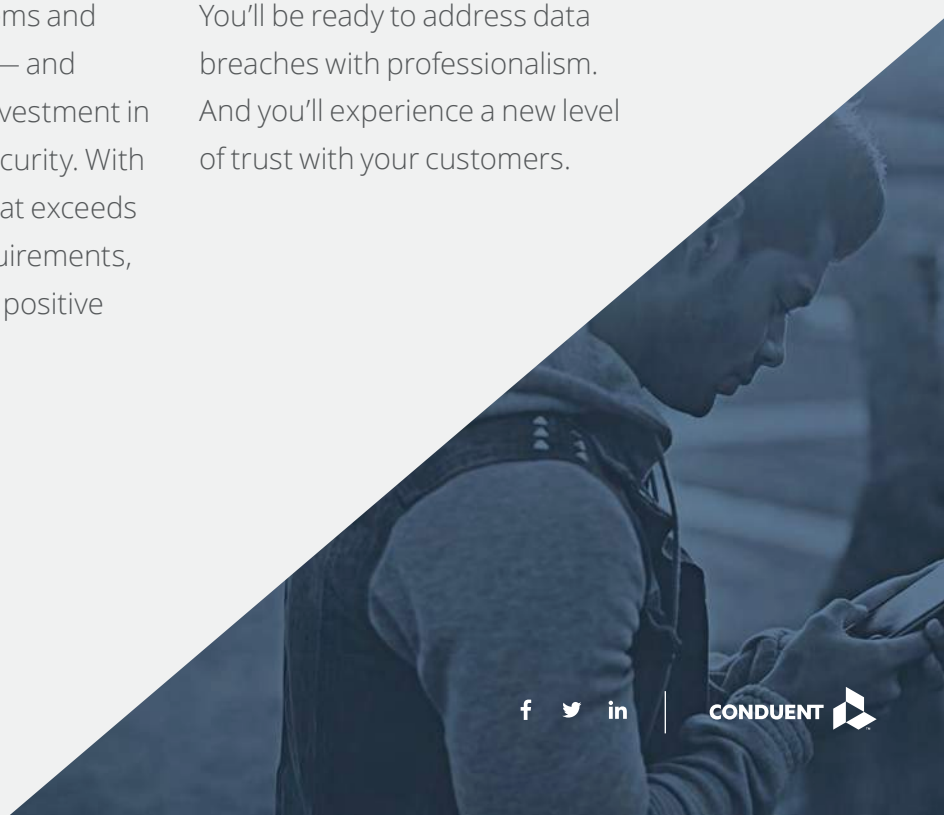
4 You conduct fast, transparent investigations of data issues with prompt public disclosure, enhancing the credibility of your brand.

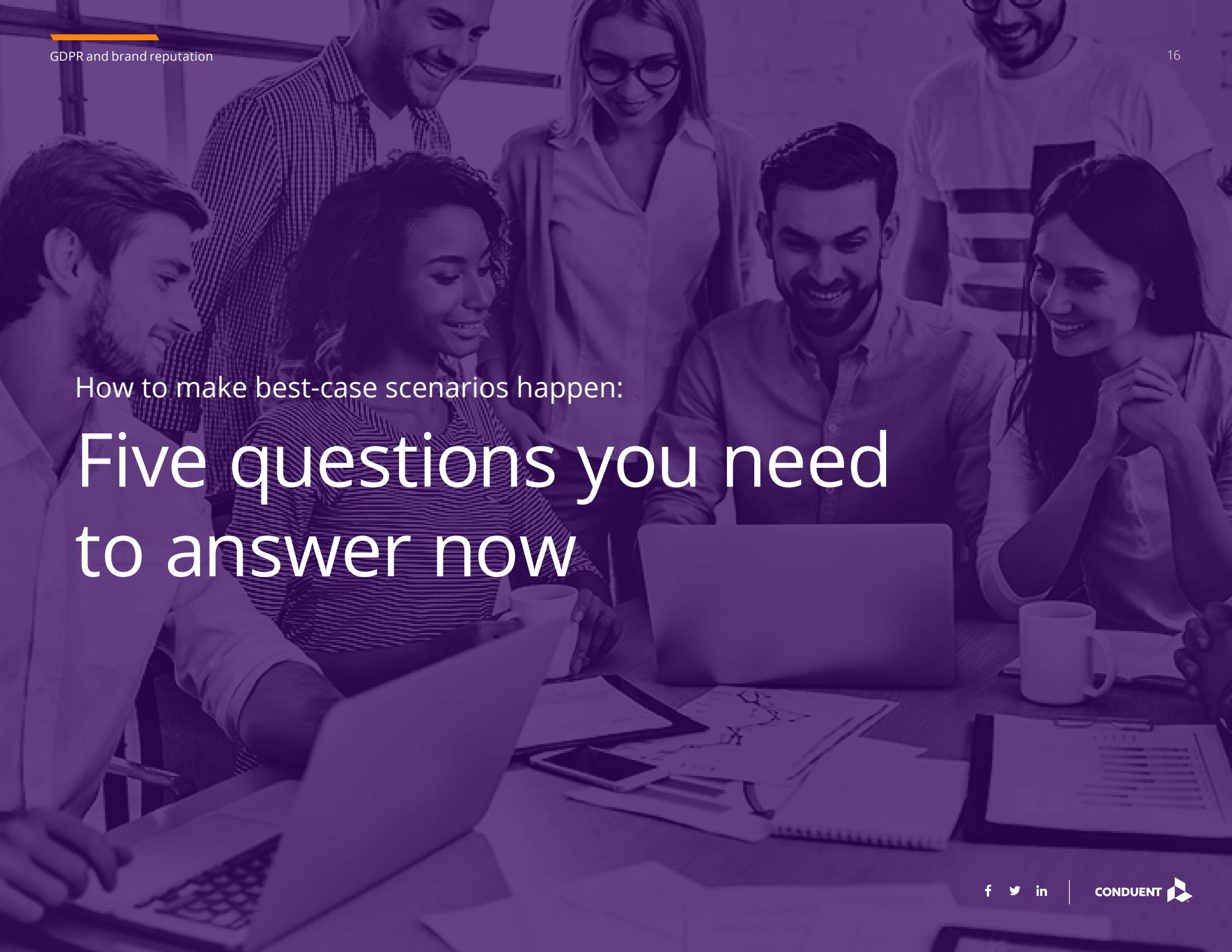
Even the most security-conscious organizations can suffer breaches. If it happens to you, your best-case scenario is to be prepared, honest and confident in what you know. Having a well-managed data operation will expedite all of these things. You'll be able to quickly assess any damage, rectify the problem and communicate clearly to the public. As with any PR crisis, a clear and professional response to a data breach will go a long way to restoring customer confidence in your brand.

After a data breach, be prepared, honest and confident in what you know.

5 You experience a renewed level of trust between you and your customer.

It may take years for the full implications of the GDPR to be understood. One immediate consequence is that it shines a light on your data systems and how you process data — and hopefully justifies an investment in improving customer security. With a GDPR plan in place that exceeds the bare minimum requirements, you'll experience other positive consequences. Your communication with customers will improve. You'll have cleaner customer data and be able to create better targeted messaging. You'll be ready to address data breaches with professionalism. And you'll experience a new level of trust with your customers.





How to make best-case scenarios happen:

Five questions you need to answer now

1

Who's your Data Protection Officer (and do you even need one)?

According to the European Commission, you need a DPO if your core activities involve processing sensitive data on a large scale, or involve large scale regular and systematic monitoring of individuals. Given the proliferation of online tracking, this likely covers most companies that conduct business on the internet. There's a good chance your company will need a DPO — who is it?

2

Which third parties have access to your data?

Even if your data is safeguarded, your data might routinely be in the hands of third parties such as marketing vendors or fulfillment partners. Know who they are and make sure you've negotiated a level of data protection and engagement that meets your highest standards.

3

Do you have protocols in place for Subject Access Requests?

Your customers have a right to see their data and request it be deleted. Make sure you have established channels for properly handling these inquiries. Having a single data system and proper GDPR training for your representatives will help accomplish this.

4

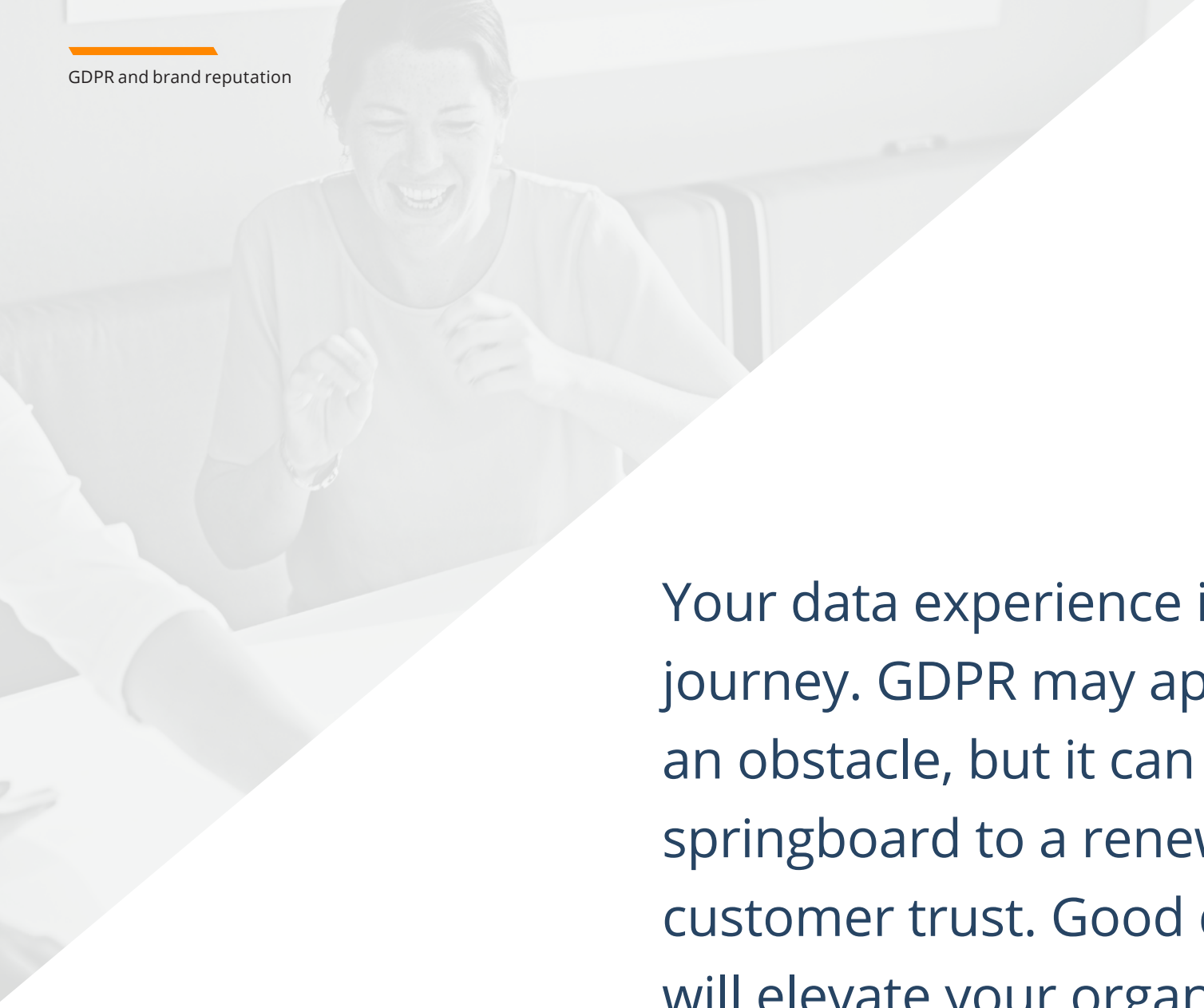
Do you have a response plan for disclosing data issues?

When you do encounter a breach, you must disclose it quickly. Avoid a mad scramble when this happens by being ready with a playbook and having assigned responsibilities. An inadequate response could cause serious harm to your business. The time to prepare is before it happens.

5

Do you have the right partners for your GDPR journey?

A partner can bring outside expertise and help you move from basic GDPR readiness to continuous GDPR compliance. Conduent's experts can help guide your organization through the regulations with a focus on customer experience and brand reputation.



Your data experience is an ongoing journey. GDPR may appear to be an obstacle, but it can also be a springboard to a renewed level of customer trust. Good data practices will elevate your organization.