ARE YOU READY FOR A POST-GDPR WORLD?

collibra®

25 MAY 2018.

Some organizations celebrated with cakes. Some organizations (quite a few, according to some estimates) have punted. And some organizations are biting their nails anticipating a flood of requests from customers who want to see—and possibly delete—their data.

The General Data Protection Regulation (GDPR), which went into effect at the end of May, 2018, is a complex regulation, designed to shift how we think about data protection. Broad in scope, the regulation expands what counts as personal data and grants new rights to individual data subjects. And the regulation applies to any organization, in or out of the EU, processing data on EU data subjects.

Whether you're celebrating, in denial, or just holding your breath, GDPR is here to stay. That means organizations everywhere are rethinking how to manage business processes. For some, that means implementing new ways to protect personal data and manage consent.

Other organizations are working to build transparency into how they are using their data, and building processes to help them respond knowledgeably to consumer inquiries or report data breaches quickly.

Larger organizations have been examining their supply chains to ensure that partners and other stakeholders are complying with the new regulation.

We can't predict how well organizations will meet these new challenges, but we do know this: understanding how your data moves across your organization, who has access to it, and what controls are being applied to it will be fundamental to your privacy efforts now and in the future.

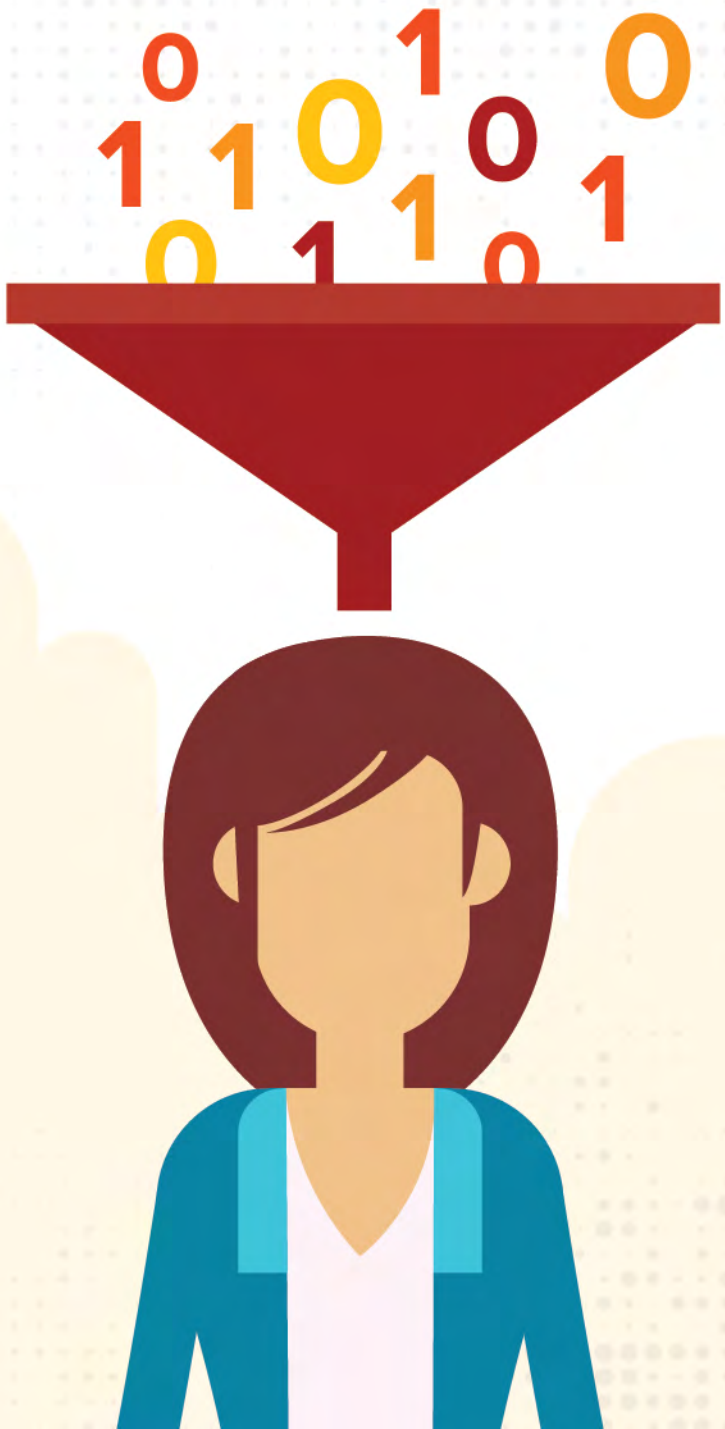
Organizations are discovering that GDPR is changing how they manage and process data.

Here are six ways to stay ahead of the game.

1

PREPARE TO HANDLE AN INFLUX OF DATA REQUESTS

GDPR is, first and foremost, a compliance regulation. While GDPR tosses around phrases like the "pseudonymization of data" (we'll get to that later), its intent is to assure that organizations like yours provide individuals with more control over their personal data.

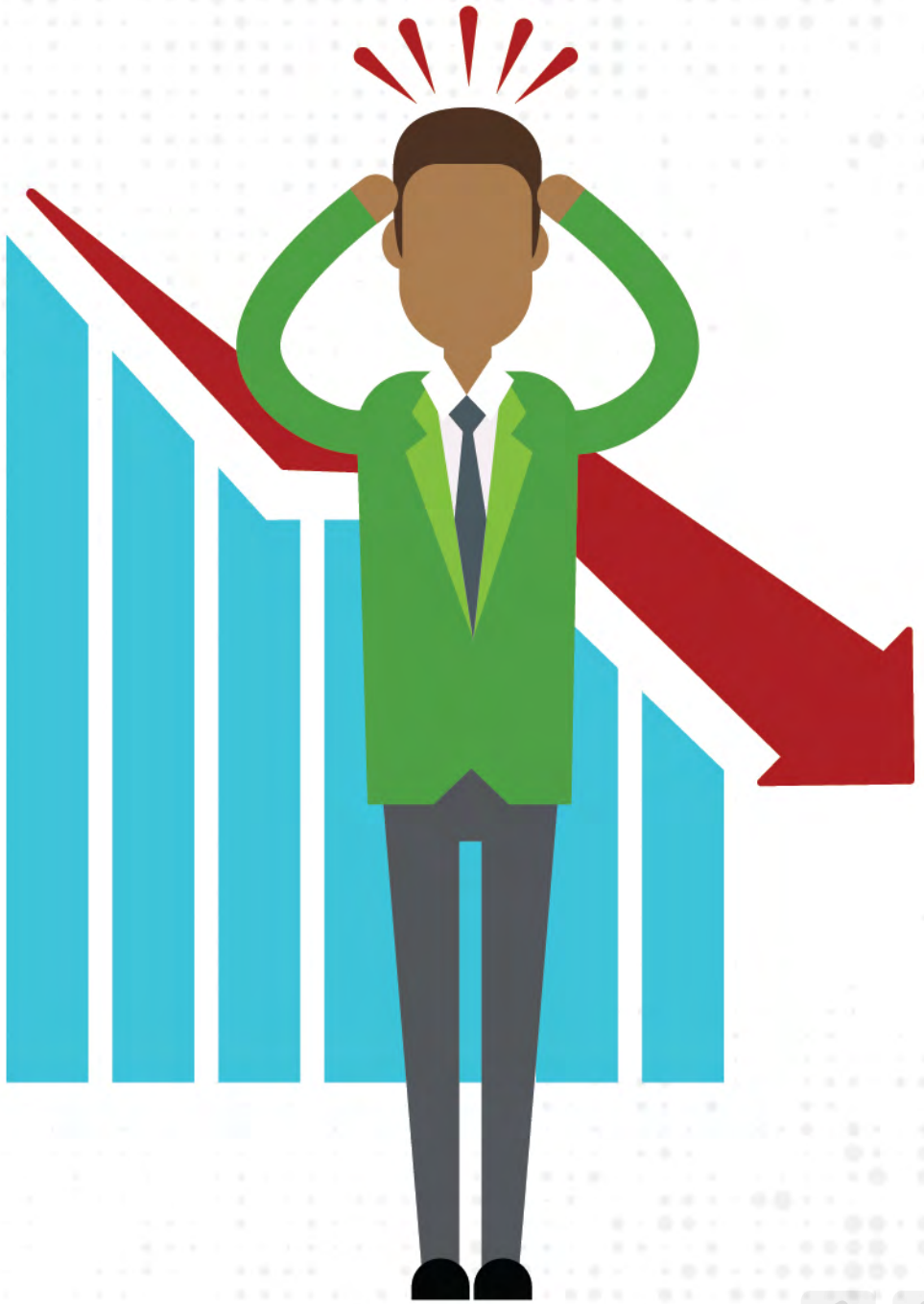


That intent is expressed in a set of complex new rules about data privacy, including consent, access, portability, erasure, notification of breach, and more. Penalties for non-compliance can be significant.

Because GDPR redefines the rights of the data subject, requests for information is likely to be on the rise. Some customers might simply want to test the waters, others might legitimately want to curtail their digital footprint, still others will file requests as political protest.

According to the IAPP, data portability, the right to be forgotten, and gathering consent are among the most difficult processes for data privacy professionals to master. GDPR puts all of these processes front and center.

Indeed, without the proper controls in place, some organizations will experience a short-term dip in productivity as they rush to respond to requests from data subjects.



WHAT TO DO:

Put the data subject front and center.

- Make sure you have processes in place to allow data subjects to easily access their own data.
- You should also make sure you can delete or update data quickly upon request.
- Can you halt processing activities when an individual challenges the accuracy of their data or objects to it for other reasons?
- Can you easily transfer their data to another organization or data controller?
- Finally, make sure you have created simple ways to communicate how you're handling these requests.

2

EXPECT YOUR PRIVACY EFFORTS TO REACH ACROSS THE ORGANIZATION

Building data privacy and protection into your business processes touches every part of your organization. But many organizations have handed off their data privacy needs to IT or information security teams. While both provide critical support for any data privacy program you implement, the GDPR isn't just about identifying and securing data. Rather, "privacy by design" requires the full participation of everyone in your organization, as well as its partners and other stakeholders.

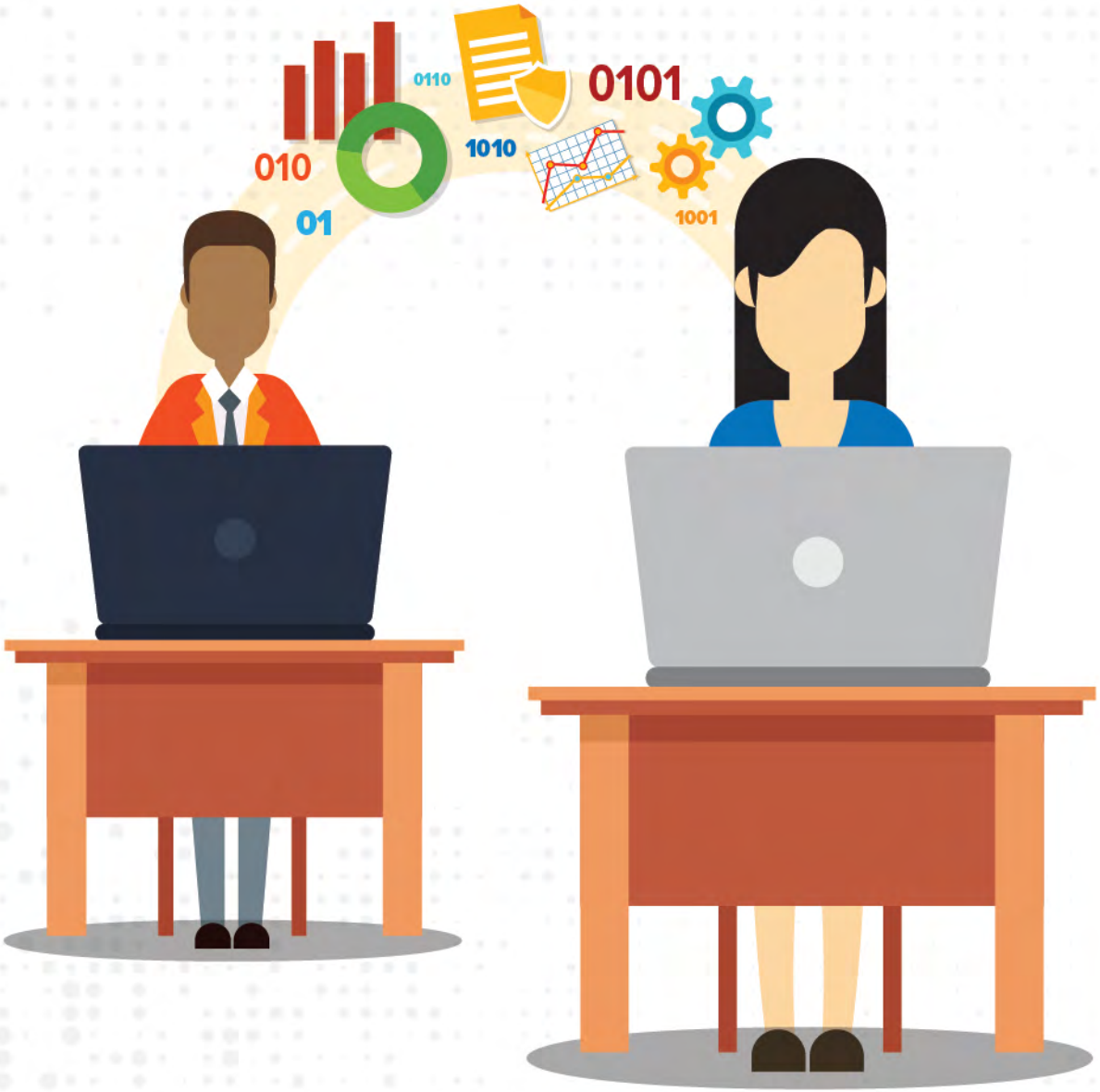
WHAT TO DO: Make sure every part of the organization understands its role.

- Business managers should continue to identify what data they use, where it lives, and how they use it.
- Data teams will need to design governance processes that support privacy by design, and establish protocols for gathering and passing consent information throughout the supply chain.
- As privacy demands shift, organizations should periodically reassess the availability and resiliency of processing systems and services.
- If you have hired additional resources, HR should continue employee training and communicate new policies and procedures throughout the organization.
- The C-Suite will need to take responsibility for the integrity of their organization's data and, ultimately, the success or failure of compliance.

3

BE ABLE TO DEMONSTRATE COMPLIANCE

Accountability is a key provision of GDPR. Its key indicator? Organizations that are able to demonstrate compliance. There are several ways to demonstrate your compliance with GDPR, such as written policies, impact assessments, and certification schemes. While these are important elements, forward-thinking organizations are taking a ‘data protection by design and default’ approach and putting data protection measures in place across their data processing operations.



Understanding how your data moves across and beyond your organization is a critical component of GDPR, which will require organizations to maintain records of processing activities for any personal data handled by your organization. Organizations should document the kind of data they collect or process, understand where that data lives and how it is used, and identify who is responsible for that data or who has access to it.

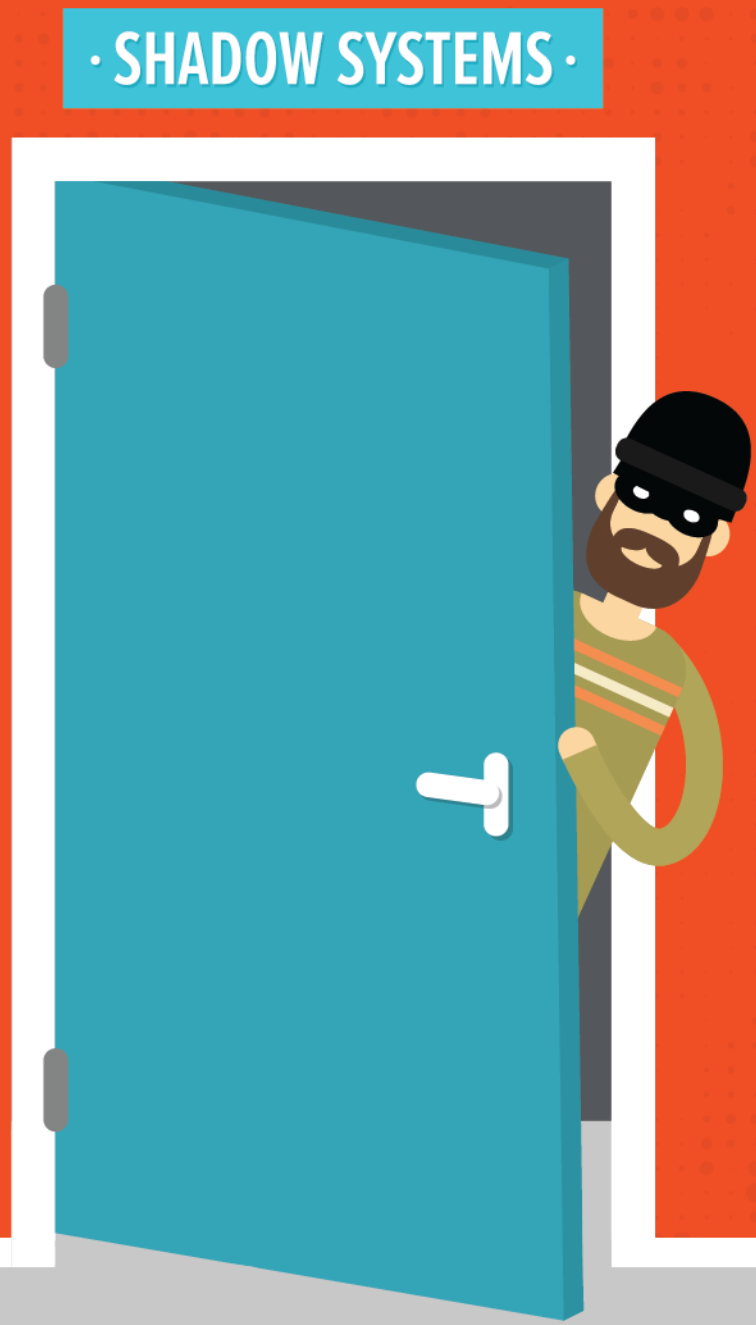
WHAT TO DO: Make privacy by design everybody's business

- Work with business units across the organization to identify business activities and the processes that support those activities. This typically involves questionnaires circulated to business units, business process discovery sessions, and process mapping. If you haven't yet done this, consider engaging a consultant who can help you accelerate these discussions.
- Do not rely solely on a "bottom-up" approach that begins with data discovery, data scanning, and data ingestion. Yes, techniques like these can help you uncover data; however, they will not actually capture the kind of information regulators are looking for—how that data is being processed and managed.
- When documenting business processes, be sure to understand and evaluate the risks a data subject might be exposed to so that you can address those risks appropriately.
- Look for tools and technologies such as out-of-the-box workflows, operating models, and dashboards that can be easily adapted to your business.

4

BE SURE TO ACCOUNT FOR SHADOW SYSTEMS

More than 80% of IT professionals say their end users have implemented unauthorized cloud services and other software in their organizations. Rogue systems like these have always been a problem (some sales person somewhere still has ACT loaded on his laptop), but it's a problem that's exploded with the consumerization of IT, BYOD programs, and the rise of cloud technologies.



WHAT TO DO: Assess, evaluate, and negotiate.

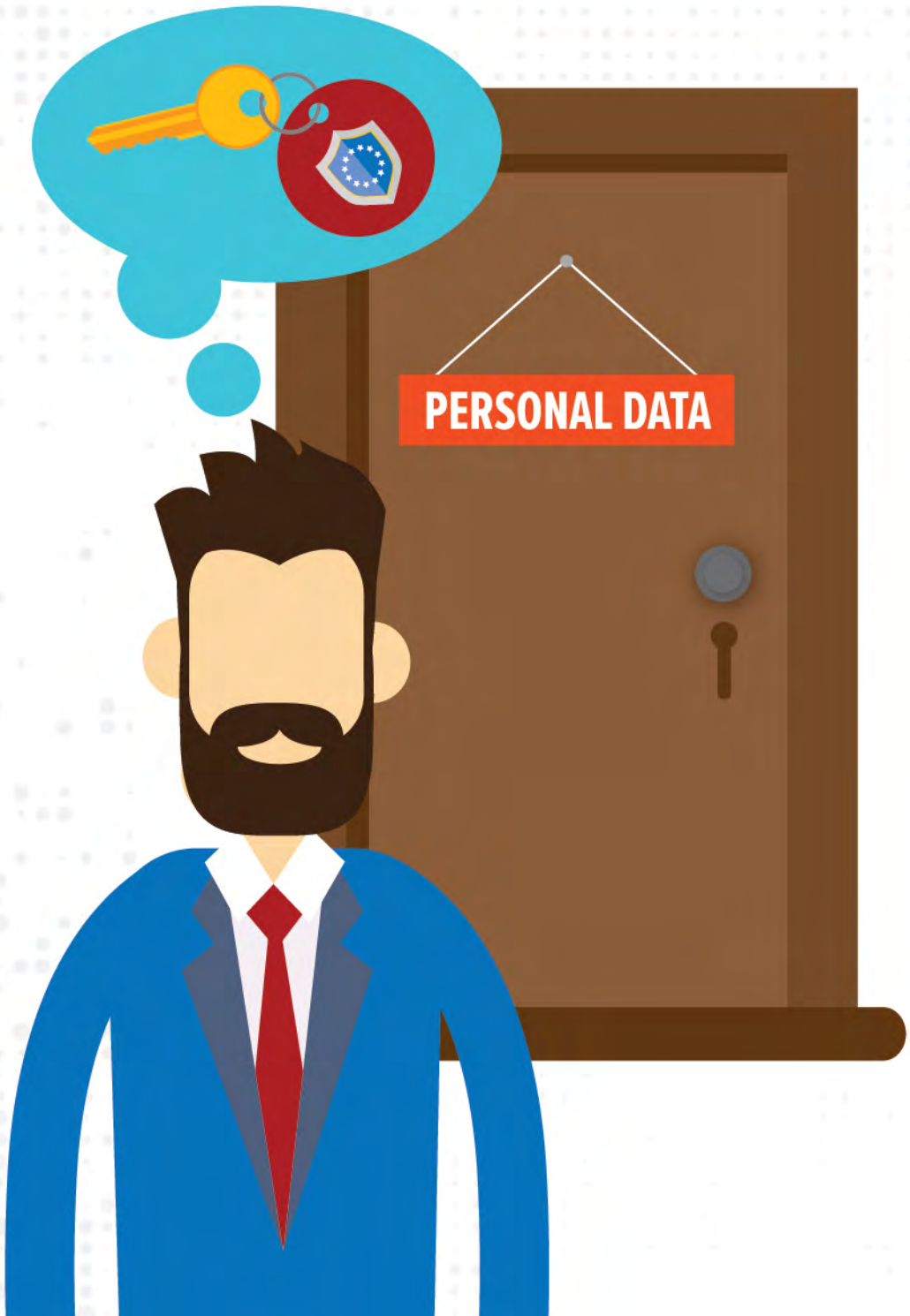
- Data scanning will inevitably miss shadow systems, but regulators aren't likely to make the same mistake. Take the time now to account for them and you will save yourself a lot of pain (and potential fines) down the road.
- Sit down with users from across the business to discover what tools they use and why. This can certainly be incorporated into your business process discovery activities—but a separate face-to-face might be more effective. No one likes to give up the tools they think they need to do their jobs.
- Understand what makes these tools attractive to your users. You may be able to offer a more compliant alternative that your users will actually want to use.
- Look for tools and technologies such as out-of-the-box workflows, operating models, and dashboards that can be easily adapted to your business.

5

DON'T RELY ON THE EASY OUT

Have you been seeing a lot of cookie notifications popping up on the web pages you visit? We have too. It's a trend. Because they don't want to hold (and be responsible for) data, some organizations are sending more and more unencrypted data back to the browser so that it's presented in every new session. That allows them to gather your consent in one simple "hey, we cookie!" message.

At the other end of the spectrum are organizations who have embraced encryption wholeheartedly in order to anonymize the personal data that they control or process. The rush to encryption is understandable. One solution to solve complex data protection needs? Sign us up!



Neither solution will be viable in the long term. “We use cookies!” will likely not meet GDPR accountability standards. And while encryption can be a valuable tool, it’s not, in and of itself, a complete solution. Encryption, essentially, protects your data from those who have no business touching it.

But data needs to be used to be valuable. So while both of these solutions have their attractions, they are both technical solutions that do not address the human factor—how to control access in a way that protects personal data while providing legitimate data users with the information they need to do their jobs.

WHAT TO DO: Data governance is key.

- To successfully comply with GDPR, you need more than technical solutions. You need to understand how personal data is being handled across your organization—and that requires an end-to-end understanding of how data is captured, transformed, held, and destroyed.
- You should have a framework in place that can help you understand what data you have, where it is, who is accountable for it, and the controls (including encryption) that are applied to it. A data governance framework will ensure that any new data your organization acquires will be accounted for (and secured, if necessary) based on your defined processes.
- Involve the business to identify and prioritize what data needs to be addressed. Not all data will require the same level of control. You have likely started with customer data; it's now time to move on to assess employee data. Document how personal data is shared, both across your organization and beyond it, to build a data registry.
- IT should focus first on securing systems. Consider working with a security partner to anonymize, pseudononymize, encrypt, or delete the appropriate data you've identified across the business and technical landscape.

6

KEEP YOUR TALENT POOL STRONG

When it comes to hiring data talent, you've likely already encountered some difficulties. And while GDPR mandates a Data Protection Officer only for organizations whose core activities involve processing personal data, your organization still needs the right expertise. You should hire policy experts who can interpret regulations as they are applied and interpreted. You should have data privacy champions who can assess your organizational readiness and monitor your compliance journey. And you should have visionaries who can prepare your organization for new data privacy standards, protocols, and regulations.

WHAT TO DO: Cultivate the talent you have.

- Hiring specialized talent can help, but your current employees are the people who know your business–and your data—best. Take the time to put a program in place to help users across the organization understand data privacy and how it will impact their functional roles. People in IT may see their responsibilities shift. People in marketing will likely be asked to put new protocols around consent into place. Help people manage change and your implementation will proceed a lot more smoothly.
- Identify roles and structures already in place that you can use to accelerate data privacy protocols. Look to your data governance framework to identify data processes and the people responsible for them. If you don't have a governance program in place, consider implementing one as you dig into your data. Accountability and security begin with good stewardship
- Train business users to recognize privacy-related data flows. Taking the time to help business users understand your privacy by design philosophy and equipping them with the knowledge they need to identify appropriate data flows is worth the effort. Of course it will help you accelerate data mapping activities, but it will also create a foundation on which to build the kind of robust data protection program you need.
- Take advantage of resources such as Collibra University, a free, self-paced online learning platform and data governance certification program for people interested in data governance best practices.

Businesses will have to continue focusing on vendor and partner networks to ensure additions fall within a compliance scheme. And employees, who continue to pose the biggest cybersecurity risk for companies, will need special attention and training.

The responsibility for protecting the personal data of the people you do business with lies with you. understand data privacy regulations that will impact your business, now and in the future. Inventory your business processes, account for shadow systems, do not rush to encryption, and train your employees to be partners in your compliance journey.

Your organization will be stronger. Regulators will appreciate your attention to transparency. And your customers, patients, business partners, and stakeholders will be confident that their data is safe in your hands.

collibra®