collibra®

6 GDPR COMPLIANCE PITFALLS

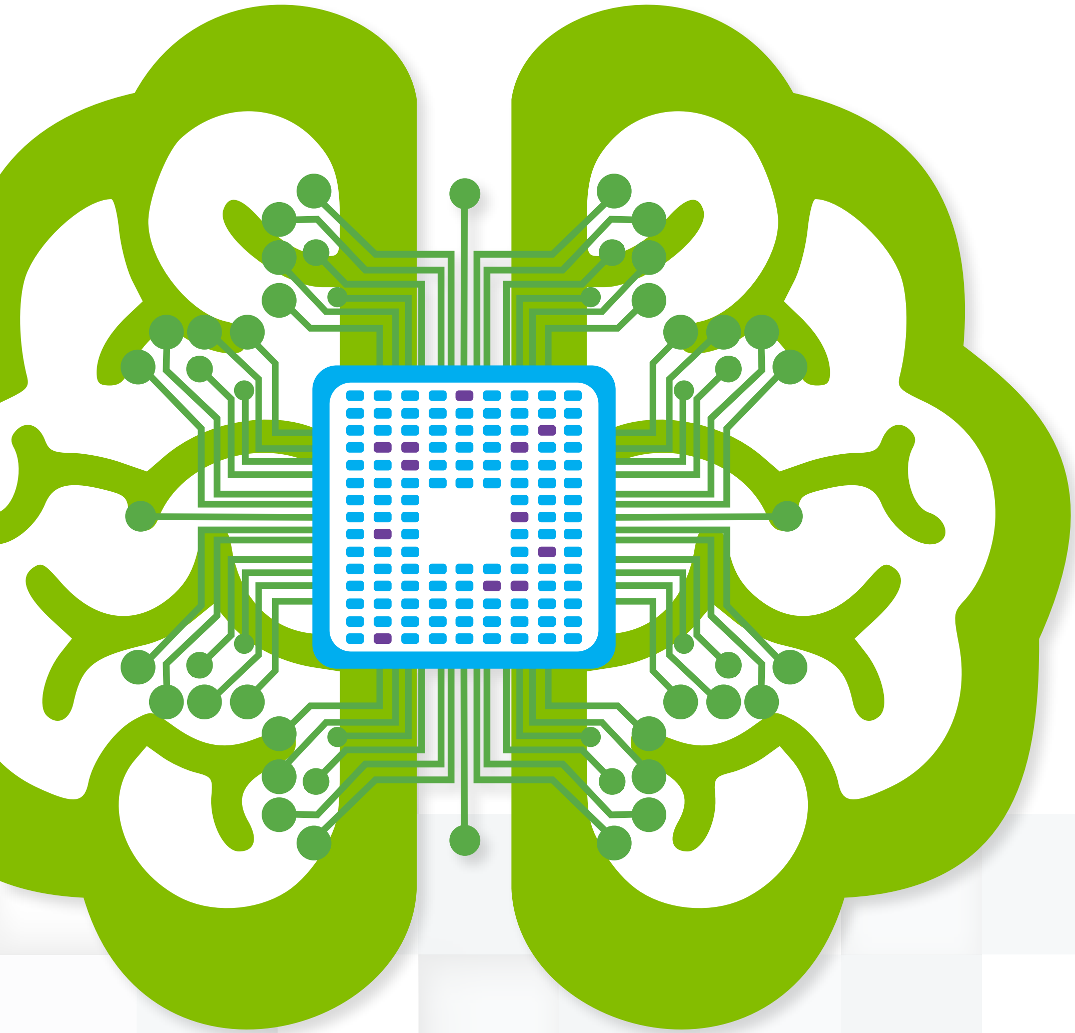
& How To Avoid Them

25 MAY 2018.

The date is likely on your calendar.
Flagged. In red.

This document is intended for general informational and educational purposes. It is not offered as and do not constitute legal advice or legal opinions. Use of any Collibra product or solution does not provide or ensure any legal or other compliance certification and does not ensure that the user will be in compliance with any laws, including GDPR or any other privacy laws.

And you're probably doing everything you can to make sure your organization is ready to comply with the **General Data Protection Compliance Regulation (GDPR)** when it goes into full effect next year.



But the GDPR 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.

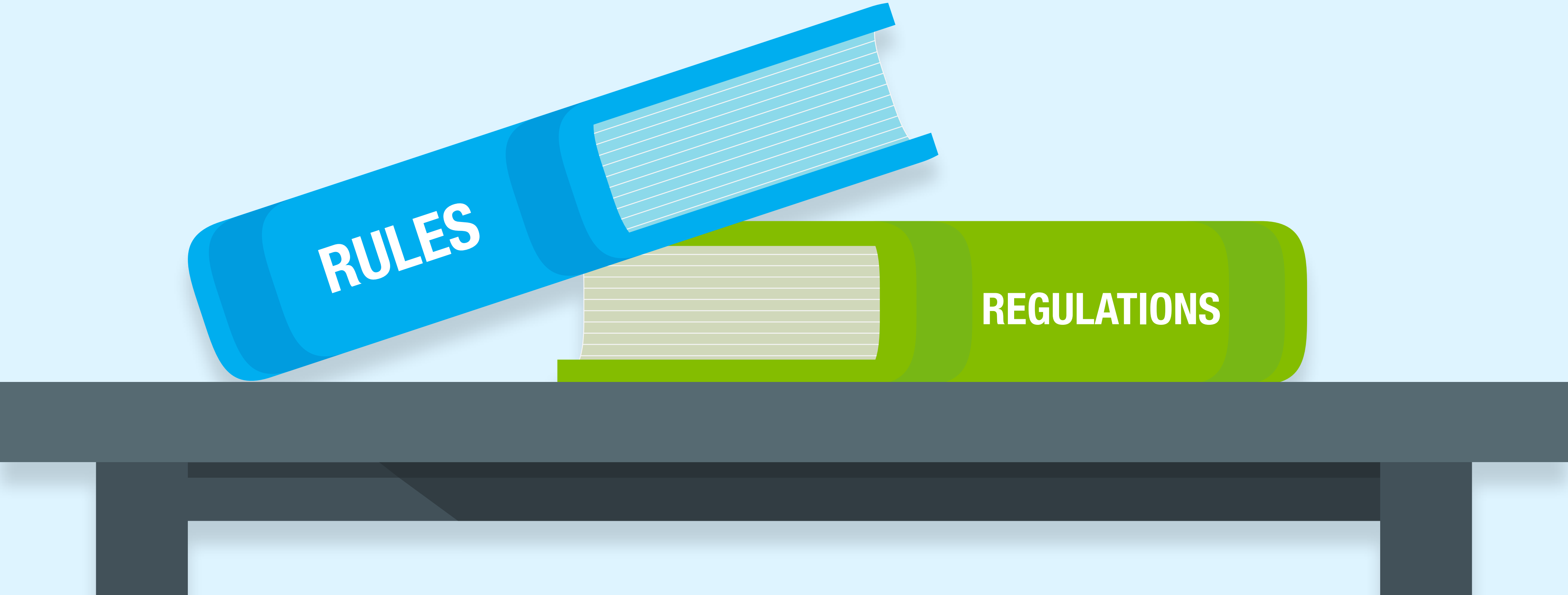
We've seen a lot of advice out there about how to implement a GDPR program to meet the impending deadline. But that hasn't stopped organizations of every size and shape from being derailed by unanticipated roadblocks that are wasting precious time and resources.

Don't let these **six pitfalls** derail your compliance efforts. Here are our suggestions for **how to avoid them.**

PITFALL #1

You haven’t engaged legal counsel.

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. With a compliance deadline less than a year away, launching a data privacy program without legal counsel in place is tempting, but foolhardy.



WHAT TO DO

Legal counsel isn't a luxury.

The GDPR is a robust piece of legislation, comprising 11 chapters, 99 articles, and 173 recitals. (Don't know what those are? There's a good argument for hiring legal counsel.)

An expert in data privacy law can help you understand the intent and impact of each of these provisions. And remember, how a financial institution stores and processes an individual's data will be different from how a healthcare organization carries out those activities. You also want to look for legal counsel with deep knowledge about your industry to help you understand how GDPR will affect your organization.

Implementing a comprehensive GDPR program involves different parts of the organization—each with competing interests. Legal counsel should be able to explain the nuances of GDPR to each business unit, prioritize which processes to tackle first, and resolve any disagreements.

We've seen organizations make some bad decisions about how to approach GDPR compliance. A legal professional dedicated to the project can help your implementation team strike the right balance between doing too much (losing sight of the regulation's essential requirements) and doing too little (exposing your organization to unnecessary risk).

PITFALL #2

You’re not looking at GDPR holistically.

Building data privacy and protection into your business processes touches every part of your organization. But many organizations are handing 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 stakeholders across the organization.

WHAT TO DO

Bring stakeholders together* and make sure every part of the organization understands its role.

Business managers will need to identify what data they use, where it lives, and how they use it.

Data teams will need to establish protocols to secure personal data and design governance processes so that privacy by design can be sustained beyond immediate deadlines.

IT will need to ensure the availability and resiliency of processing systems and services.

HR will need to hire additional resources, train employees in how to identify data flows, and help communicate new policies and procedures throughout the organization, in addition to reviewing and documenting their own data processing activities.

The C-Suite will need to take responsibility for the integrity of their organization's data and, ultimately, the success or failure of compliance.

*See Pitfall #1. Legal counsel is well-positioned for making sure the right stakeholders are engaged.

PITFALL #3

You haven't made an inventory of your business processes.

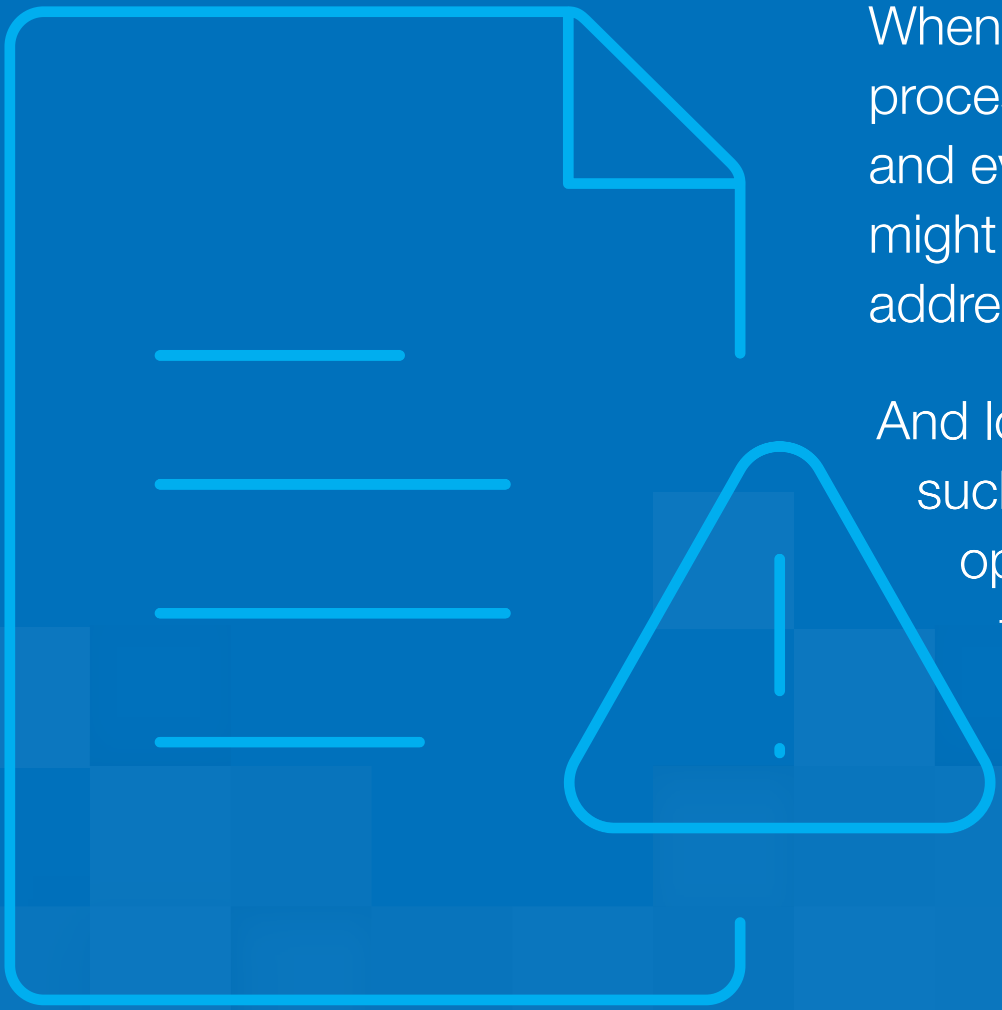
Understanding how your data moves across and beyond your organization is a critical component of GDPR, which will require organizations to maintain records of processing activities for any personal data handled by your organization. If your organization hasn't documented the kind of data you collect or process, if you don't understand where that data lives or how it is used, or if you can't identify who is responsible for that data or who has access to it, you have some work to do.

WHAT TO DO

Don't panic.

Begin by working with business units to identify business activities across the organization and the processes that support those activities. This typically involves questionnaires circulated to business units, business process discovery sessions, and process mapping. If you need to, engage a consultant who can help you accelerate these discussions.

And 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.

And look for tools and technologies such as out-of-the-box workflows, operating models, and dashboards that can be easily adapted to your business.

PITFALL #4

You are not accounting for shadow systems.

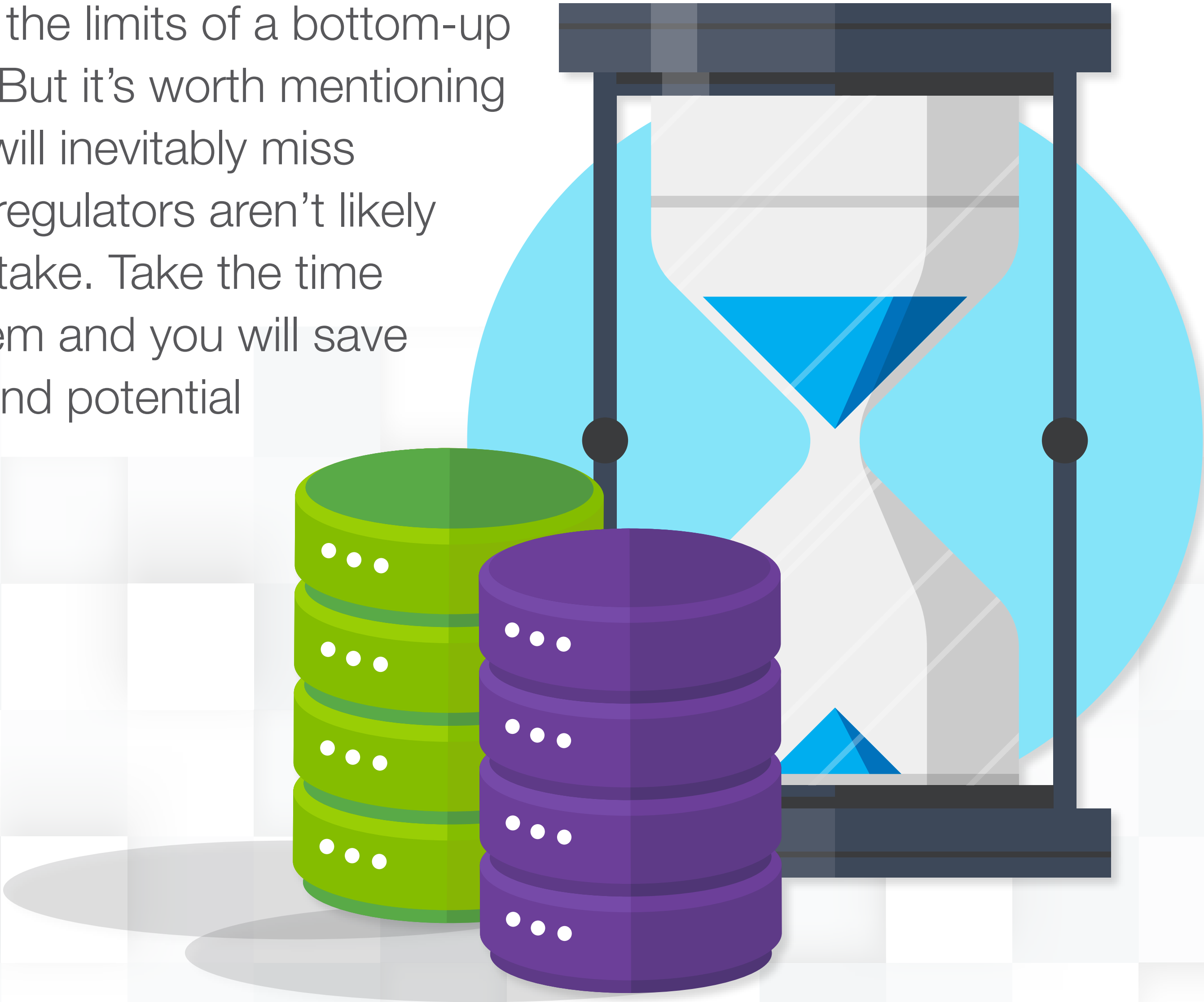
80%

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.

We warned you about the limits of a bottom-up approach in Pitfall #3. But it's worth mentioning again. 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.

And be sure to understand what makes these tools attractive to your users. Who knows – you may be able to offer a more compliant alternative that your users will actually want to use.

PITFALL #5

You rush to encrypt your data.

In response to an imminent GDPR deadline, a flurry of vendors are offering encryption services to help organizations 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!

But 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 encryption has its attractions, it is fundamentally a technical solution that does 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 will 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.

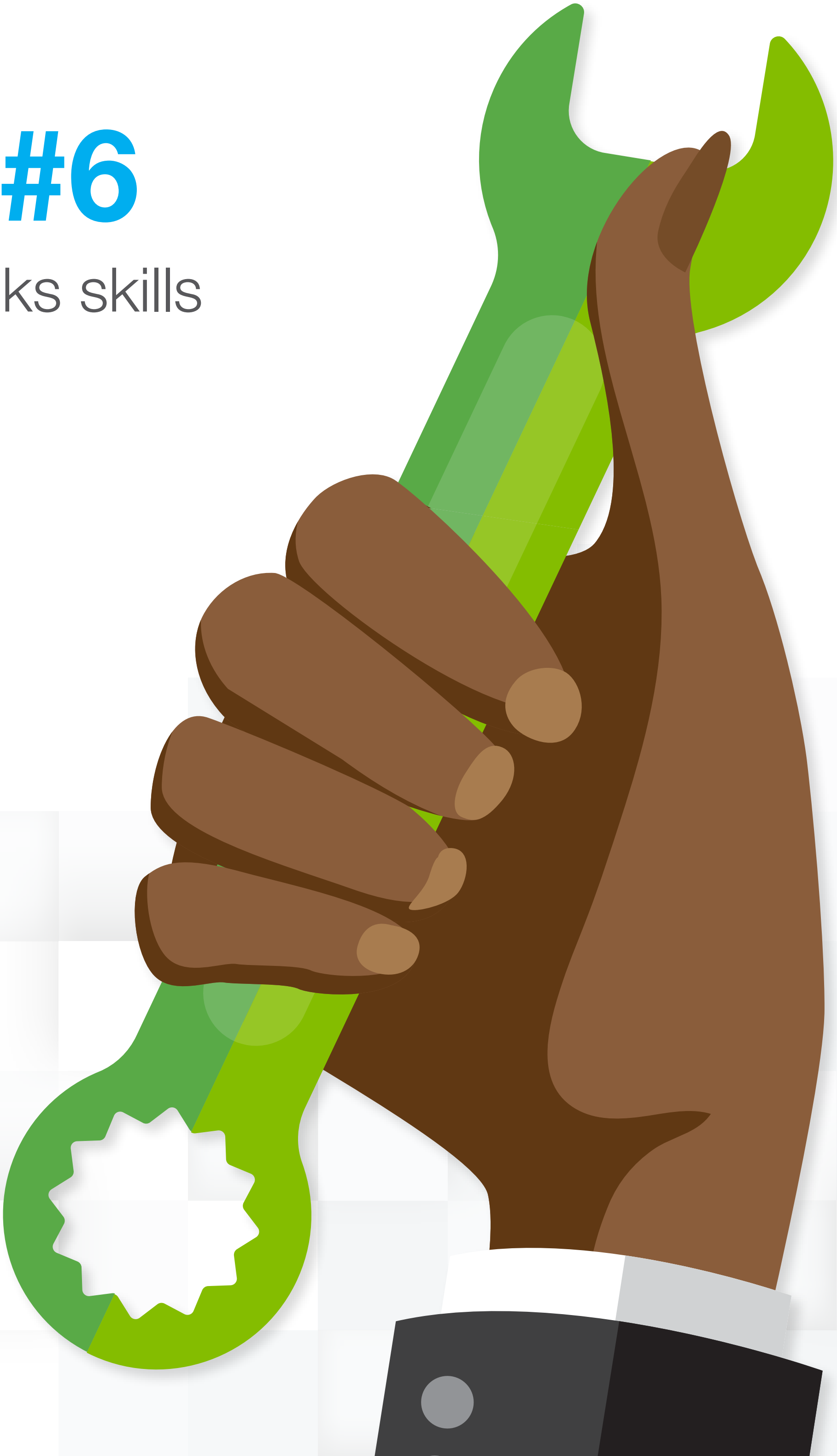
Put a framework into place that can help you understand what data you have, where it is, who is accountable for it, and the controls (including encryption) that are applied to it. A data governance framework will ensure that any new data your organization acquires will be accounted for (and secured, if necessary) based on your defined processes.

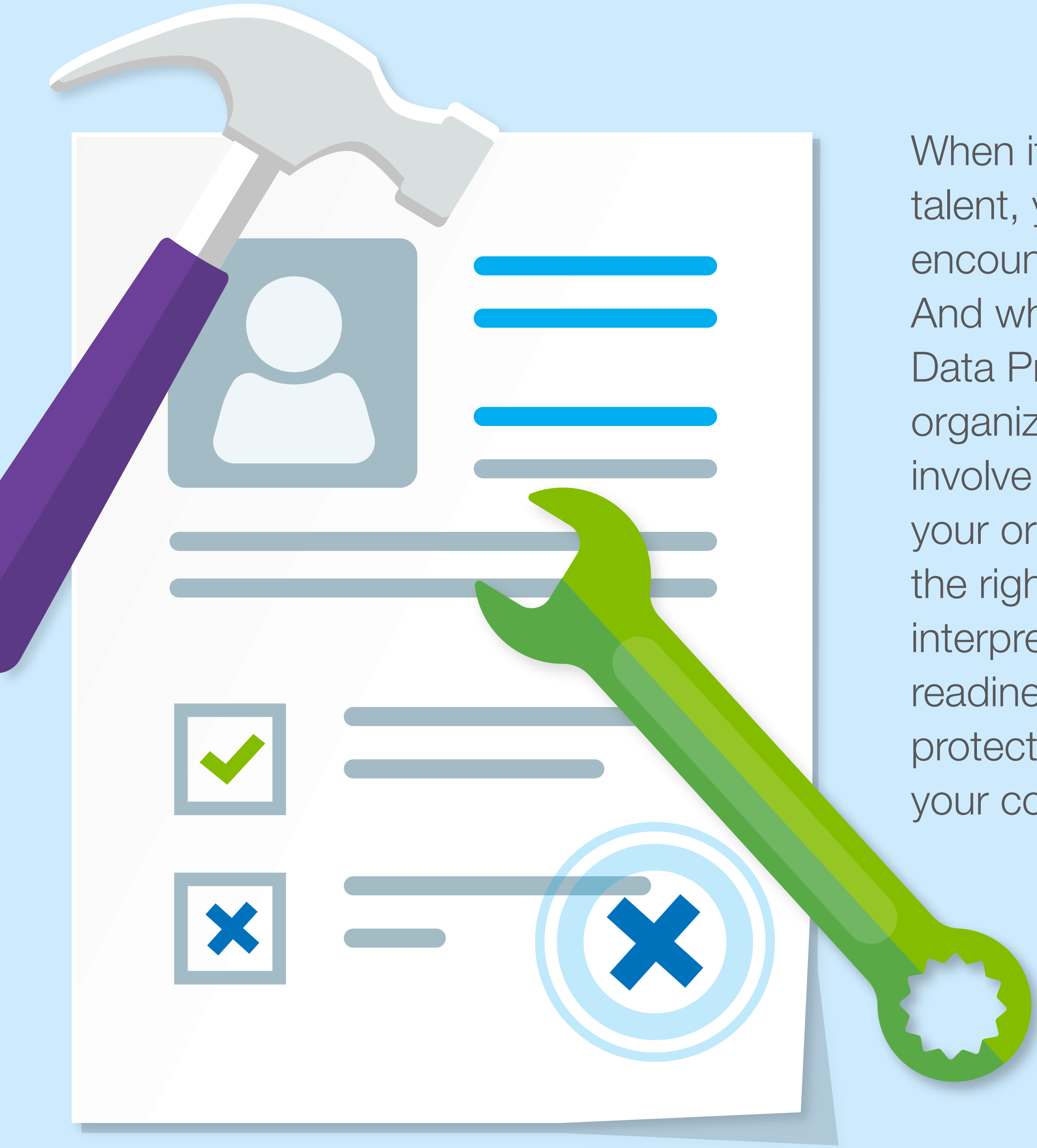
Involve the business to identify and prioritize what data needs to be addressed. Not all data will require the same level of control. You will likely want to start with customer data and then move on to assess employee data. Document how personal data is shared, both across your organization and beyond it, to build a data registry.

And focus your IT team on first 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.

PITFALL #6

Your organization lacks skills specific to GDPR.





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 will still need the right expertise on board to interpret regulations, assess your readiness, implement a data protection program, and monitor your compliance journey.

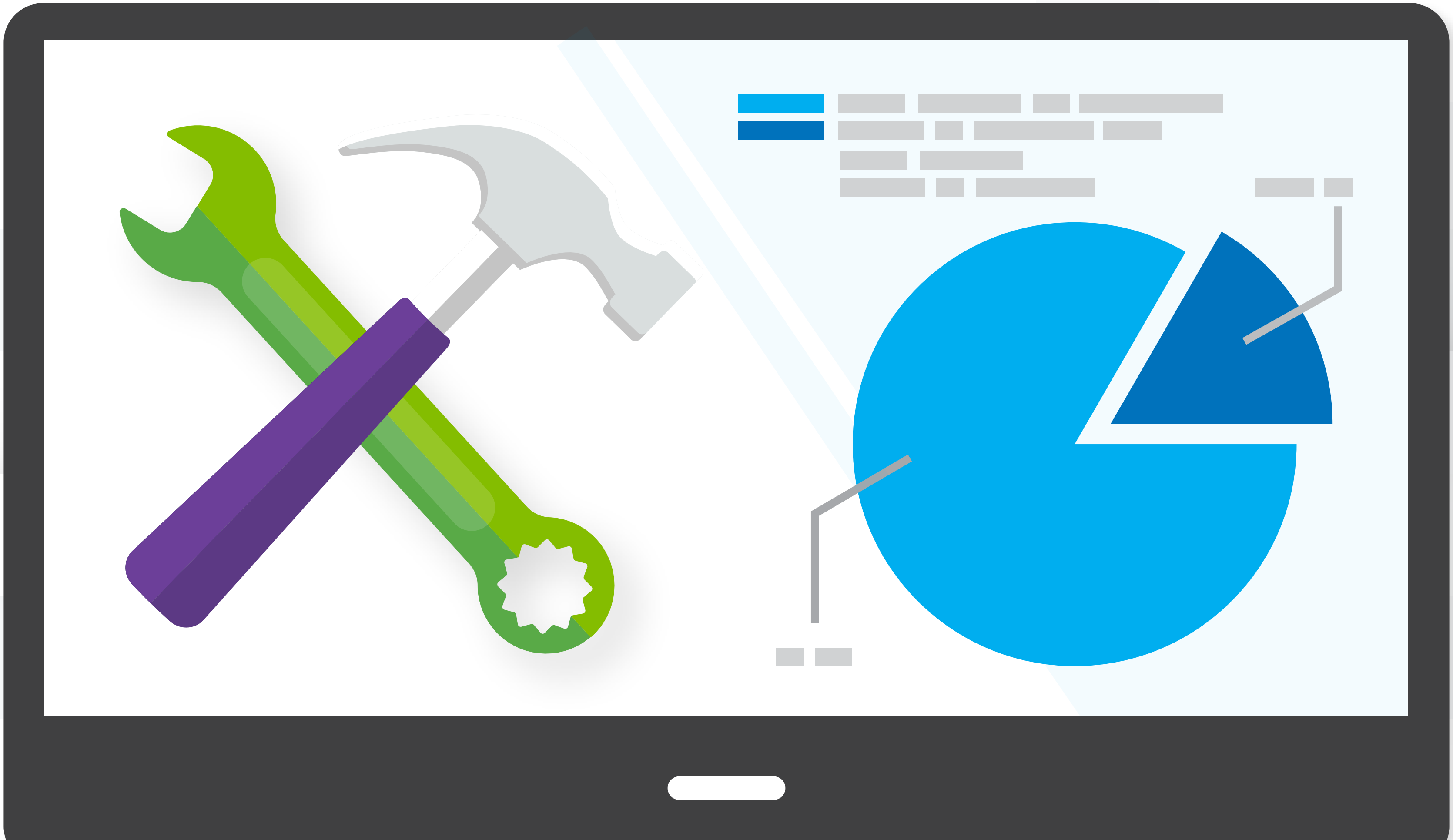
WHAT TO DO

Cultivate the talent you have.

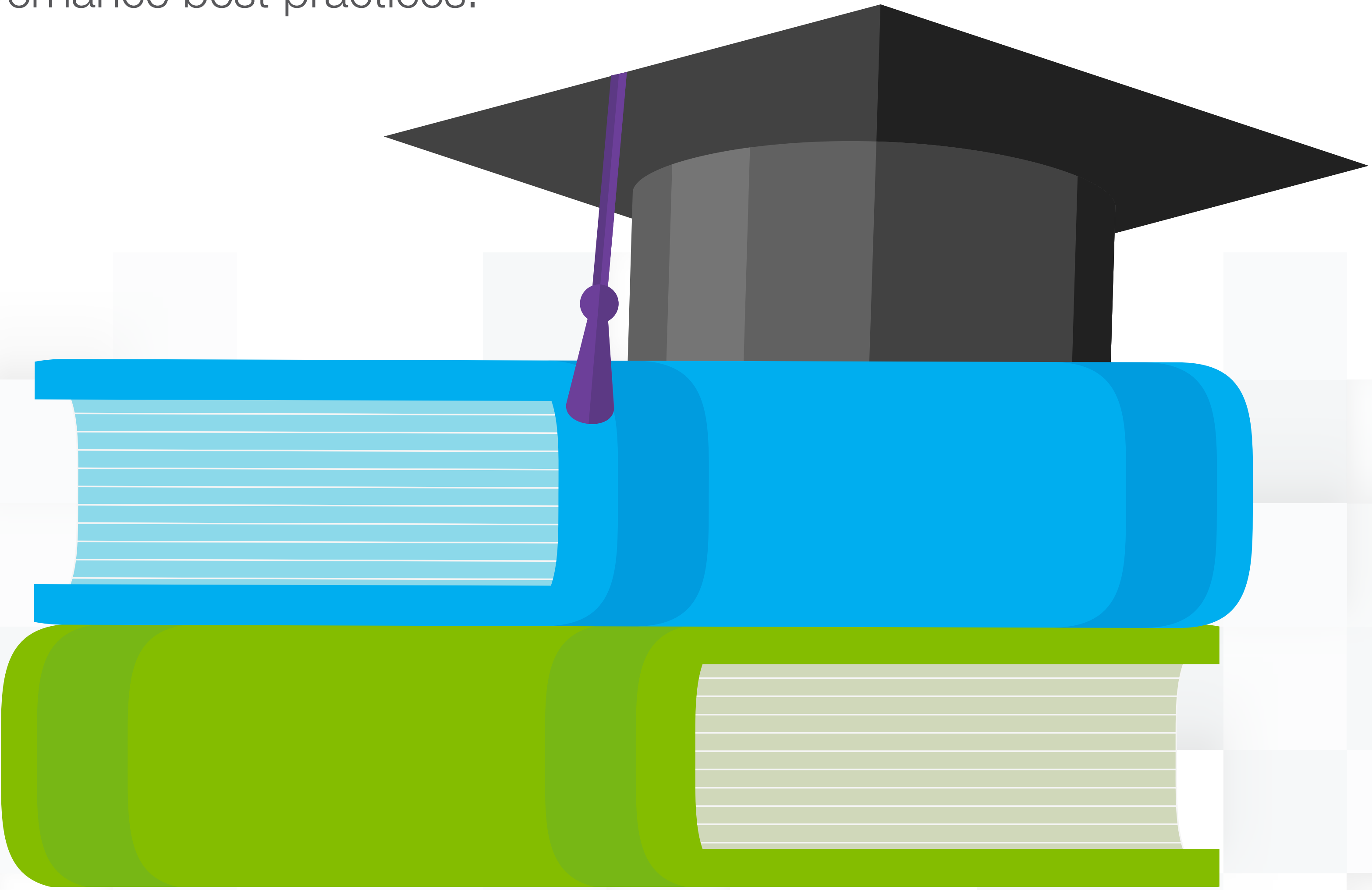
Hiring specialized talent can help, but your current employees are the people who know your business–and your data—best. Take the time to put a program in place to help users across the organization understand what GDPR is and how it will impact their functional roles. People in IT may see their responsibilities 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 implementation of a GDPR compliance program. 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.

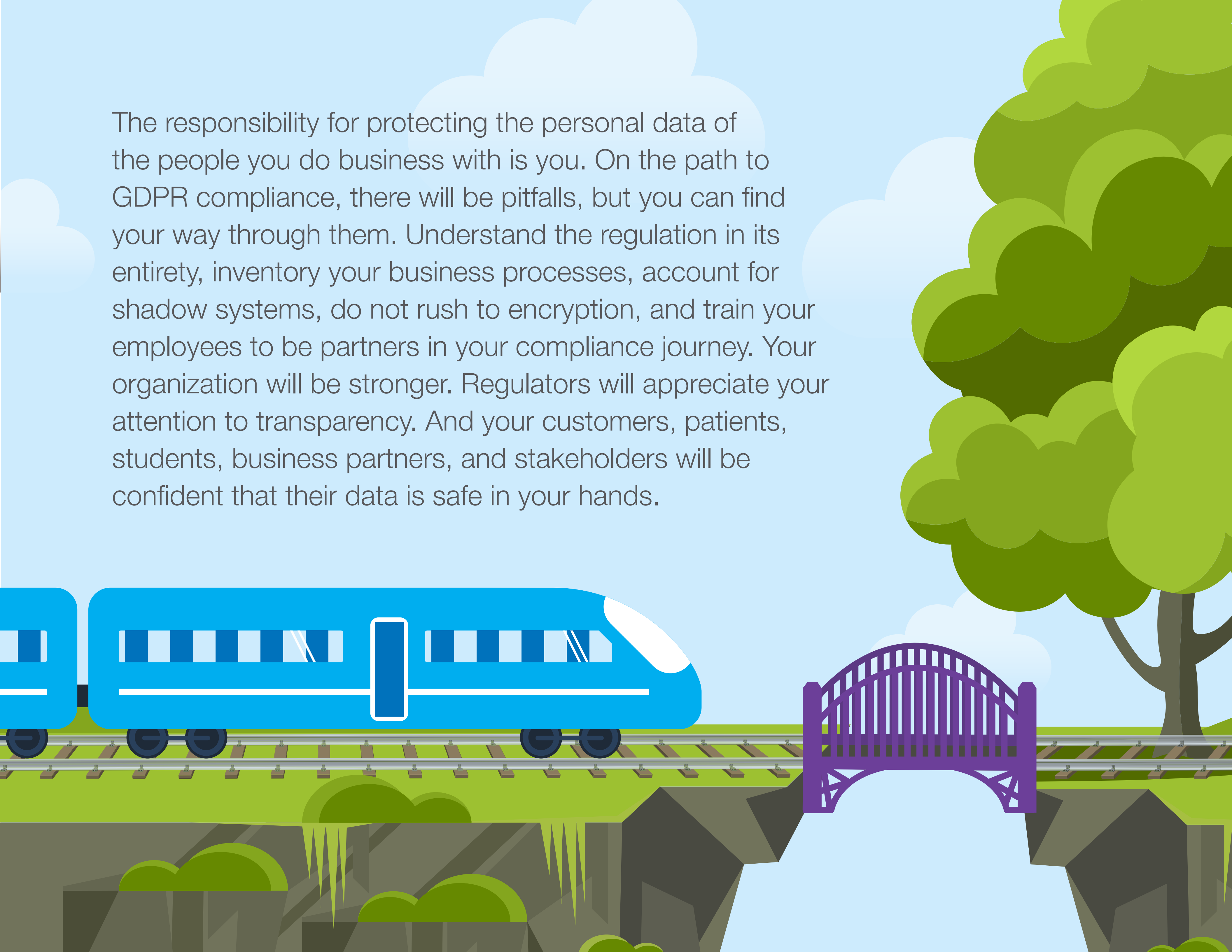
Train business users to recognize GDPR-related data flows. Taking the time to help business users understand your “privacy by design” philosophy and equipping them with the knowledge they need to identify appropriate data flows is worth the effort. Of course it will help you accelerate data mapping activities, but it will also create a foundation on which to build the kind of robust data protection program you need.



And 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.



The responsibility for protecting the personal data of the people you do business with is you. On the path to GDPR compliance, there will be pitfalls, but you can find your way through them. Understand the regulation in its entirety, 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, students, business partners, and stakeholders will be confident that their data is safe in your hands.



collibra®

collibra.com/gdpr

info@collibra.com

Follow Us:
twitter.com/collibra