

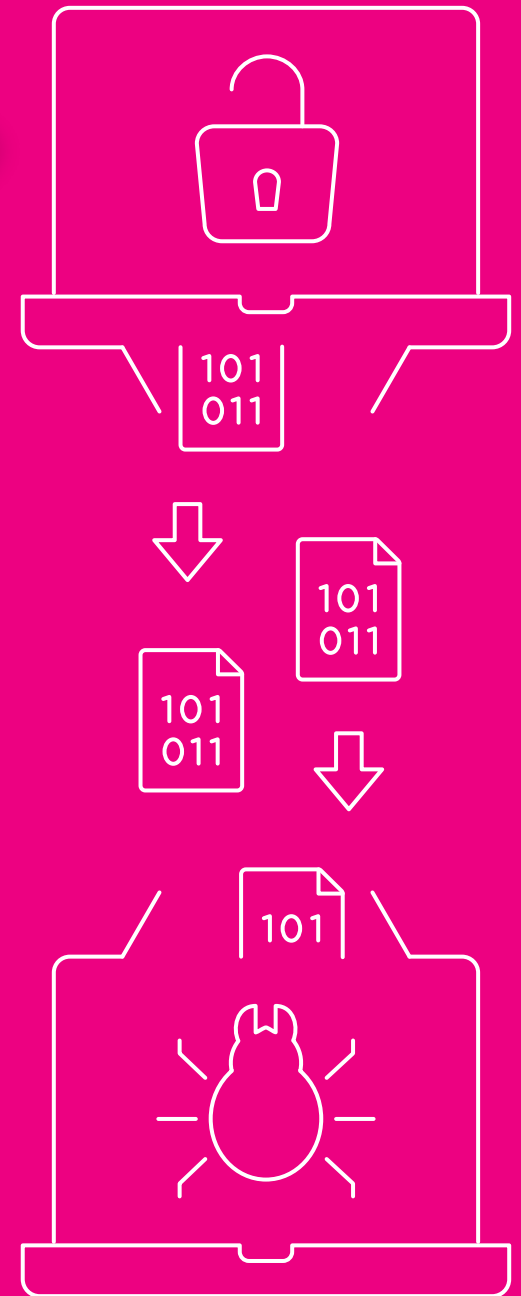
**THE MISSING PIECE
IN THE GDPR PUZZLE**



**DATA
GOVERNANCE**

Data breaches. Hacking. Cyber crime.

The sheer mention of these terms likely sends chills down your spine.



Today, people and businesses are generating data at a staggering pace.

And as data grows, so does the number of data breaches and “near misses” – security incidents that could have resulted in a severe data breach, but (thankfully) did not.

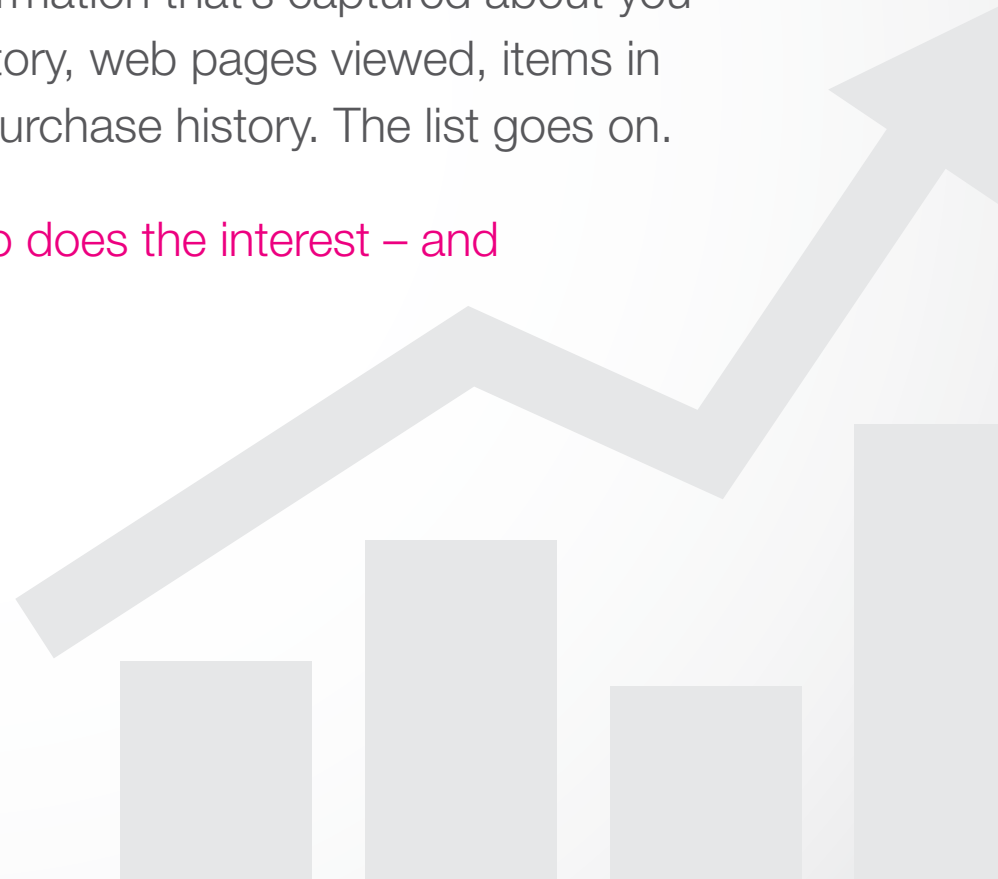


But here's the obvious dilemma.

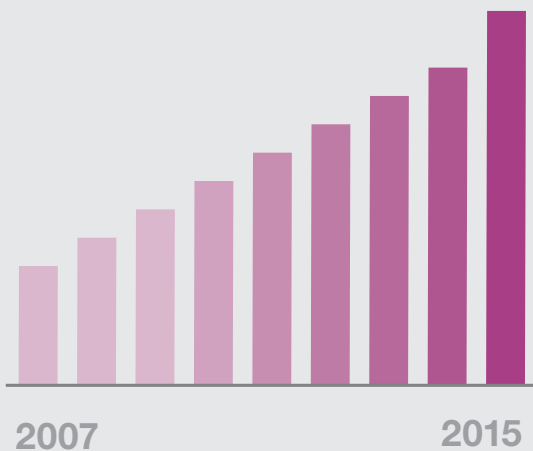
So much data, created so quickly, is difficult to control. And it's not just about the volume of data. It's also about the **value of the data** that's captured about you. Think about the data you intentionally enter online: your address, birthdate, credit card numbers, passwords, and more.

And then think about the OTHER information that's captured about you without you even noticing: search history, web pages viewed, items in your online shopping cart, and your purchase history. The list goes on.

And as the value of data increases, so does the interest – and sophistication – of the hackers.

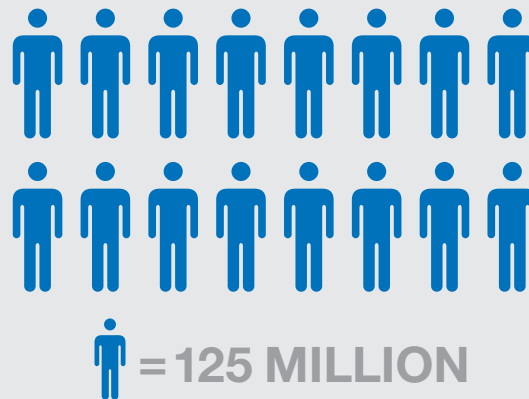


In 2015, hacking incidents reached a nine-year high.



Source: ITRC

Over two billion records were stolen in 2016 alone



Source: ZDNet, Nov. 2016

During the first half of 2016, there were 974 publicly disclosed data breaches, which led to the theft or loss of 554 million data records.



Source: Gemalto

And these numbers continue to grow.

IDC predicts that by 2020, data breaches will affect nearly **25%** of the world's population.





Financial gain

continues to be a principal motive for data breaches.

But have you thought about the signs of more ominous motives for stealing private, personal data such as forcing people or groups to change their behavior or embarrassing organizations, individuals, and even nations?

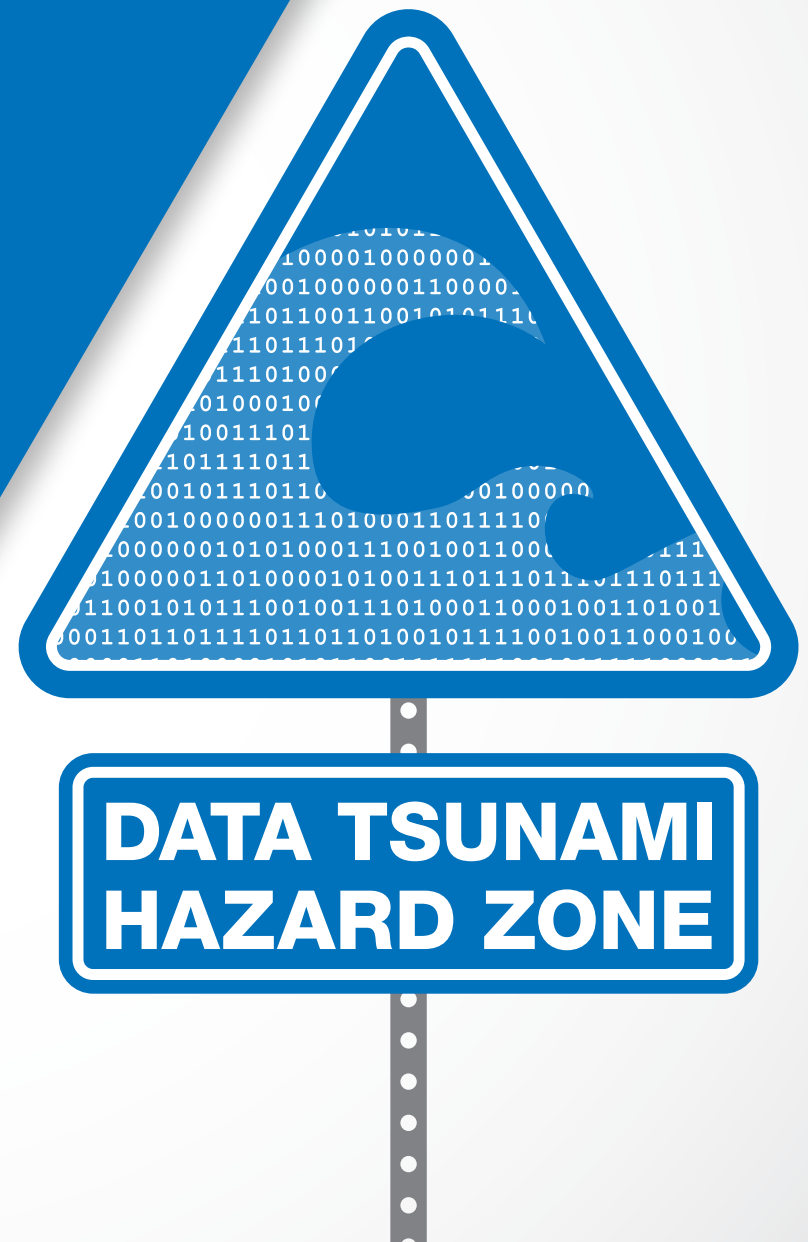
The global economy runs on data. But we need to ensure we are protecting the rights of citizens whose data makes the world go 'round. And by "we," we mean all businesses that collect, use, and store a person's personal information.


Sounds familiar, right?

There are inherent risks of the data tsunami. We hardly understand the data we have, let alone the unanticipated ways in which it could be used.

The bottom line:

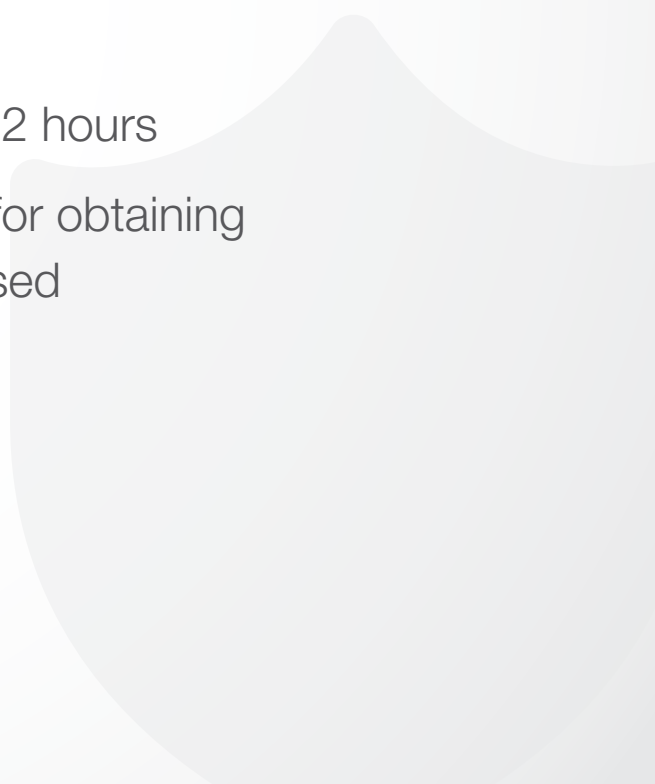
The digital age requires a new set of data rules.






In April 2016, The European Commission ratified **The General Data Protection Regulation (GDPR)**, which covers the capture, control, and consent to use personal information.

GDPR broadens the scope of personal privacy laws to protect the data rights of E.U. citizens.

- Individuals will have greater control of who has their data, and how it will be used
 - Organizations must report on data breaches within 72 hours
 - Organizations will be bound by more stringent rules for obtaining consent from individuals on how their data can be used
- 

Under the GDPR, it's clear that the responsibility of protecting the personal data of customers and prospects falls on the shoulders of your organization.





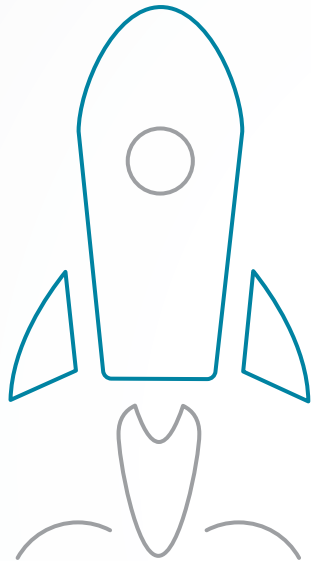
GDPR applies to personal data that resides anywhere within an organization.

Its impact will be felt by every area of the business. Web marketplaces, social network sites, search engines, and other Internet-based companies – as well as companies in the financial services sector, retail, consumer goods, communications and, of course, healthcare – are obvious targets for GDPR.

Today, this is an E.U. regulation. But think about your customers. Do they include E.U. citizens?

GDPR applies to any company, inside or outside the E.U., that offers goods and services to European citizens. It's likely your organization must comply with GDPR.



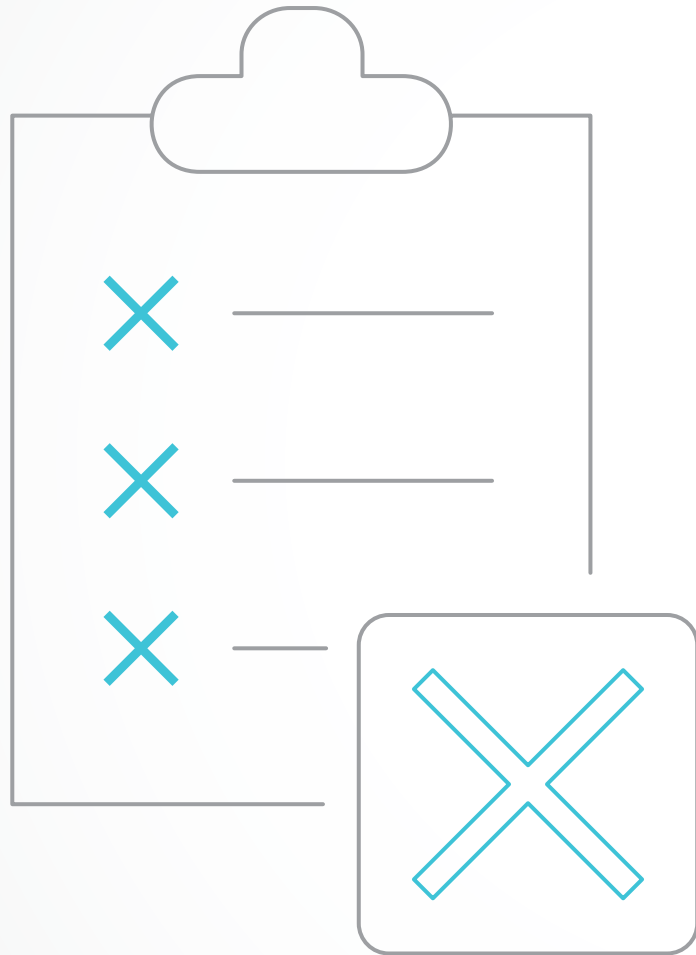


COMPLIANCE DAY

- 24 —
- 23 —
- 22 —

GDPR isn't something organizations can take lightly.

Organizations must be **100% compliant** from day one.



Regulators will issue significant fines for GDPR non-compliance: up to **2-4% of global revenue** for non-compliance.

DO THE MATH

A single violation could potentially put your company out of business.

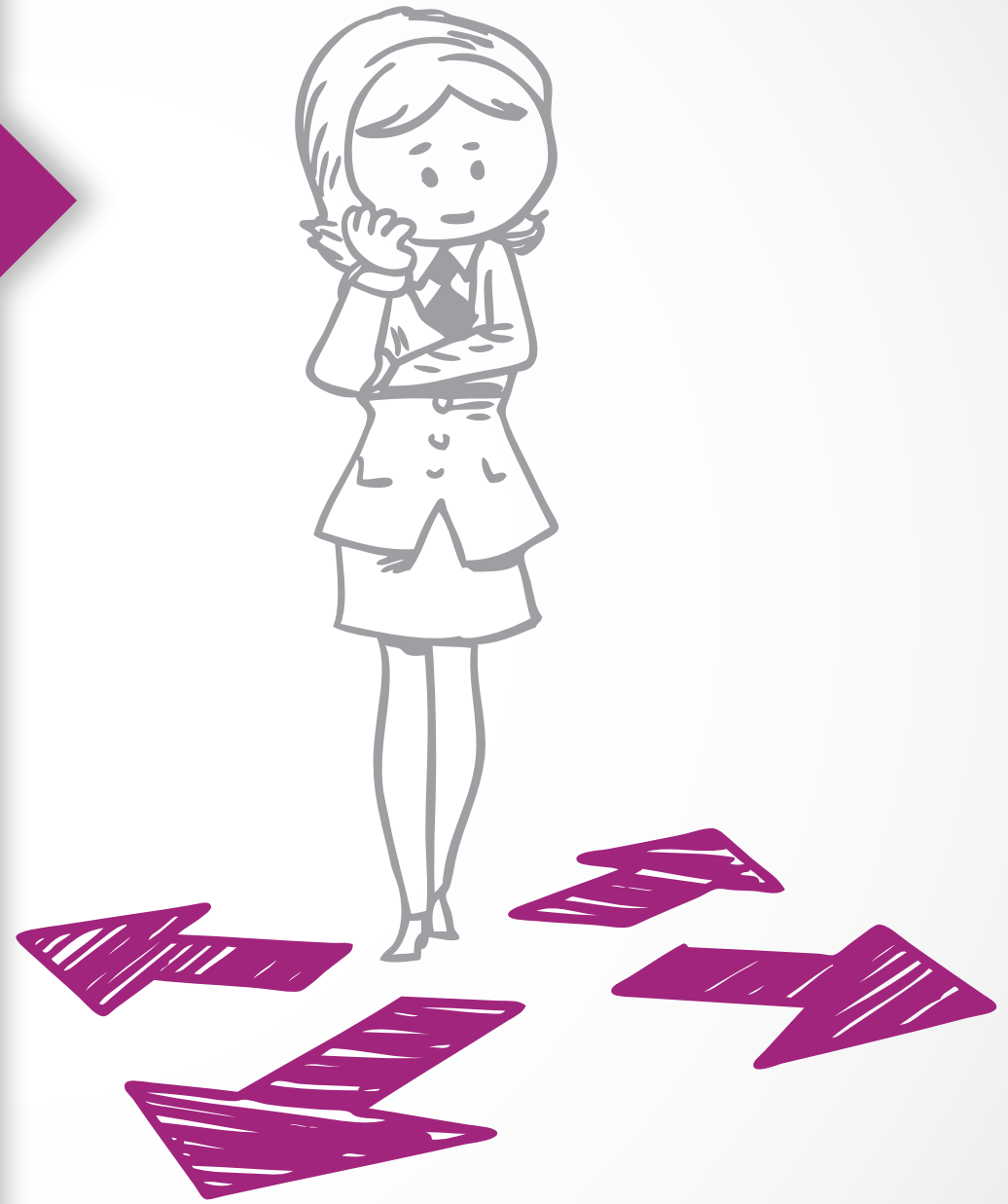
And depending on the infringement, the reputational damage from non-compliance may be long lasting, or even insurmountable. A simple 'we're sorry' will not suffice.

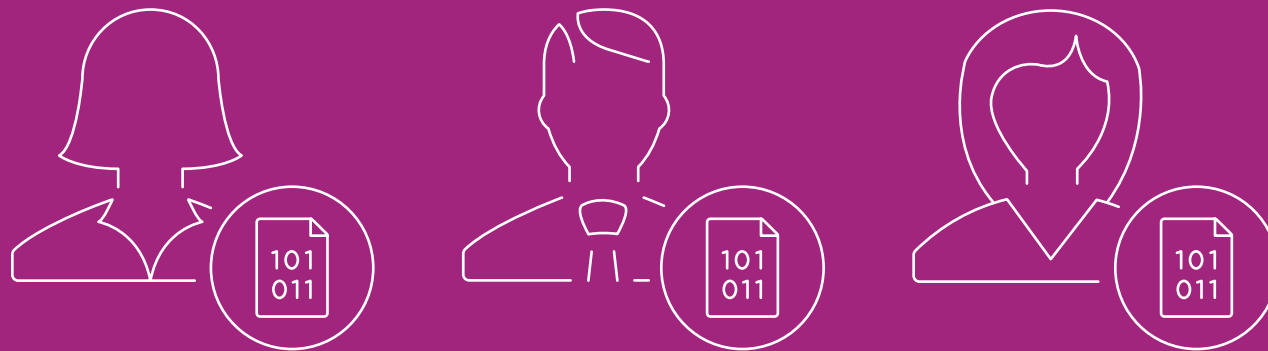
GDPR goes into effect

MAY 25, 2018

The countdown to compliance is on.

And while the GDPR regulation is clear on what needs to be done, many organizations are struggling with how to do it.





Protecting and securing data isn't about creating a veil of secrecy. It's about breaking down silos. It's about control. It's about making the data transparent, where necessary, across the organization.

After all, you can't protect what you don't know.

To ensure GDPR compliance, you must be able to **answer two critical questions** and show proof of your answers:

- Where is my data?
- Who is responsible for that data?



Classification
lies at the heart
of GDPR.

Identifying and
classifying your
data is the first step
toward answering
these questions.

For instance:

- What types of personally identifiable information do you have on file?
- Where is it located?
- What level of security is required?
- Who has access?
- How will the data be used?
- Do you have consent to use that data?

The ability to report on data is incredibly important when it comes to one of the biggest challenges posed by GDPR: breach notifications.

Under the regulation, companies must report certain data breaches no later than 72 hours following the occurrence. But in the absence of context, you simply can't provide answers to regulators' most critical questions.

And the inability to respond is costly. Remember those hefty fines mentioned earlier?



GDPR further complicates data protection by establishing far-reaching rules for how data is **managed, processed, and deleted.**



It's no longer just about finding data and making sure it's secure. It's about capturing the context of data and being able to prove everything is being done to protect the subject's data and the rights of the subject itself.



GDPR is a massive regulation. With 99 articles, where do you begin?

Data governance provides the path you need.

Data governance can serve as the underpinning of GDPR compliance.

It provides a framework for managing and defining enterprise-wide policies, business rules, and data assets to provide the necessary level of data protection and quality.

And data governance gives your data context. It provides the answers that you need to begin addressing the complex issues surrounding GDPR compliance.

If you can find the data and understand it, you can report on it. And that allows you to provide the evidence regulators require and helps to make your organization GDPR-ready.





Responsibility and **accountability**

are the hallmarks of good data governance. And they are critical to ensuring GDPR compliance.

That's why data governance and GDPR are a perfect pair.



Responsibility

Data protection must become a board-level discussion. The International Association of Privacy Professionals (IAPP) believes that companies will need to hire close to 75,000 data protection officers to meet the demands of GDPR.

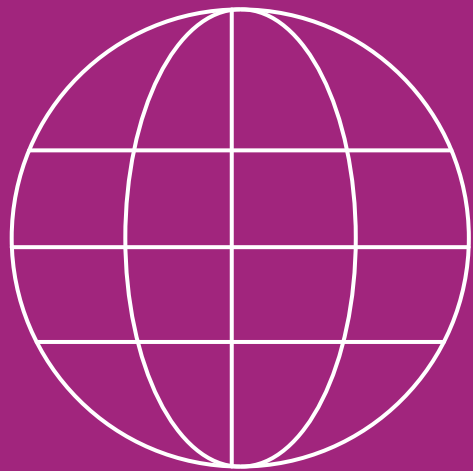


Action item:

Assign a chief data officer who oversees the establishment of the controls and processes necessary for data protection and privacy.

Accountability

True data governance is an enterprise-wide effort that establishes accountability through the organization. It breaks down silos and empowers data stewards to be accountable for owning the data – ensuring it is accurate, trustworthy, and accessible.



Action item:


Create a closed loop governance framework involving your entire organization to continuously assess risk, monitor gaps, and track progress.



GDPR has raised the stakes around data protection and data privacy.

With the promise of significant fines for compliance failures, the E.U. is signaling it is serious about compliance.

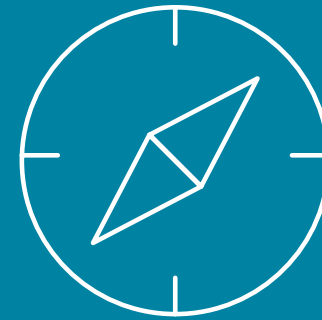
To comply with GDPR, you need a new approach and new tools for data protection and privacy. Manual approaches and spreadsheets won't cut it. Neither will another 'bolt-on' IT system. If you choose either of those routes, prepare to open the corporate checkbook to pay the penalties.



And when you consider the planning and budgeting, as well as the organizational and infrastructure changes that need to take place to ensure GDPR compliance, it's clear that preparing your organization to address and comply with GDPR can't be done overnight.

But despite the looming deadline, only a small percentage of companies have started to take steps to ensure compliance.



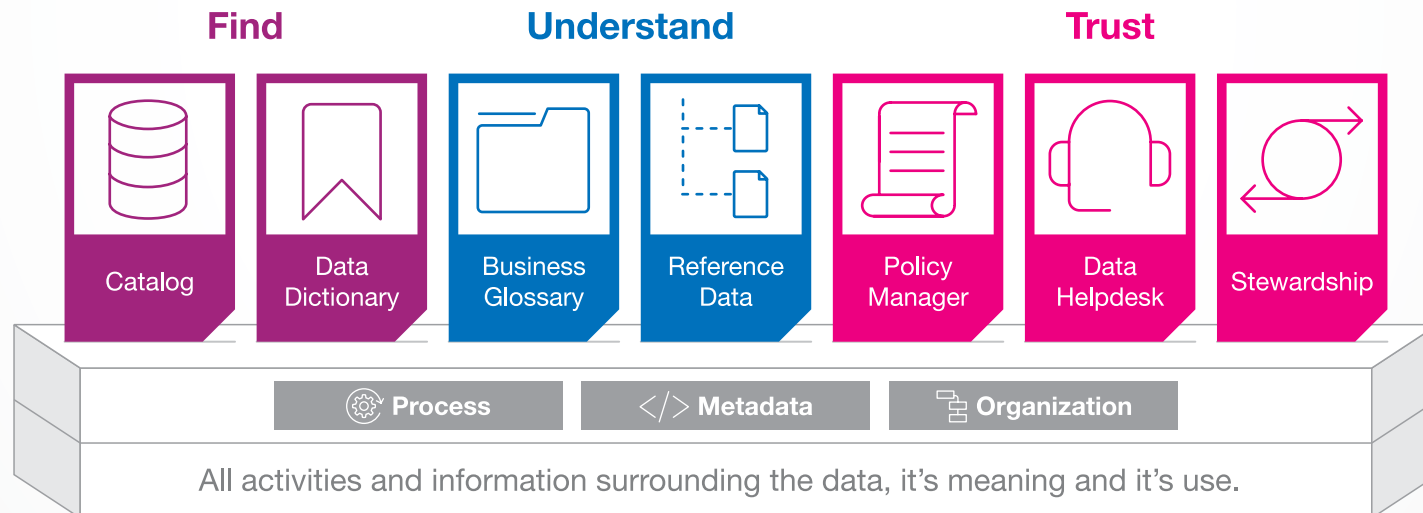


Navigating the requirements of GDPR is no small feat.

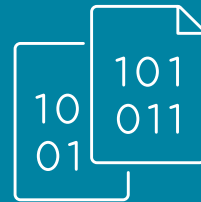
But you don't have to go it alone.

Collibra helps organizations prove that they are always doing the right thing with the data.

It is a platform for orchestrating the people, the policies, the data sharing agreements, the definitions - all activities and information surrounding the data, its meaning, and its use.



True data governance benefits organizations by providing the policies, controls, and workflows needed to:



Document data and show its lineage



Set appropriate policies (and enforce them)



Address roles and responsibilities of everyone that touches that data

Data governance can help ensure you're GDPR compliant.
But the clock is ticking.

MAY 25, 2018

Don't risk your bottom line. Or your reputation.



collibra™

collibra.com

info.collibra.com

Follow Us:
twitter.com/collibra