3 Steps to Identify and Protect Sensitive Data for the GDPR

Posted by PDI Marketing Team

Published: July 27, 2021

Step 1. Identify Sensitive Data

Take the time to identity all sensitive data when starting your GDPR compliance project.

The Information Age has been marked by rapid technological advancements, but the security measures that keep those advancements in check have progressed in fits and starts. The European Union's General Data Protection Regulation is a comprehensive piece of legislation that seeks to increase the level of protection surrounding the information of EU citizens.

Every company that sells to citizens of the European Union must become GDPR compliant. This will be more exhaustive for some businesses than others, but the majority of companies will need to ramp up the security of their customer information to one degree or another. That means finding where all sensitive data is stored.

Before a business can build a fortress around customer data, they must know where it exists. It doesn't do any good to build a wall if you don't know where the boundaries should lie.

Discovering your company's sensitive data may sound like a simple endeavor, but anyone in IT knows it is not. Systems are complex and always changing. Data may be duplicated for testing environments or archived and promptly forgotten.

Companies need to know which data is relevant under the GDPR, which systems contain those types of data, and which databases have specific combinations of sensitive data that place them at a higher risk.

To make matters worse, identifying data is continuous job. If you identify all sensitive data today, congrats! That will change in a month, a week, even a day. New data is produced, a new test environment created… sensitive data is an ever-changing organism that requires constant tracking.

Ideally, a company should be able to see how data moves from system to system so they can identify where sensitive data originated. If sensitive data lies outside secured data bases, a company needs to be able to track how it got there.

designed by companies who focus on data security, and who produce tools that meet the highest standards of scrutiny. Such tools allow you to constantly track sensitive data.

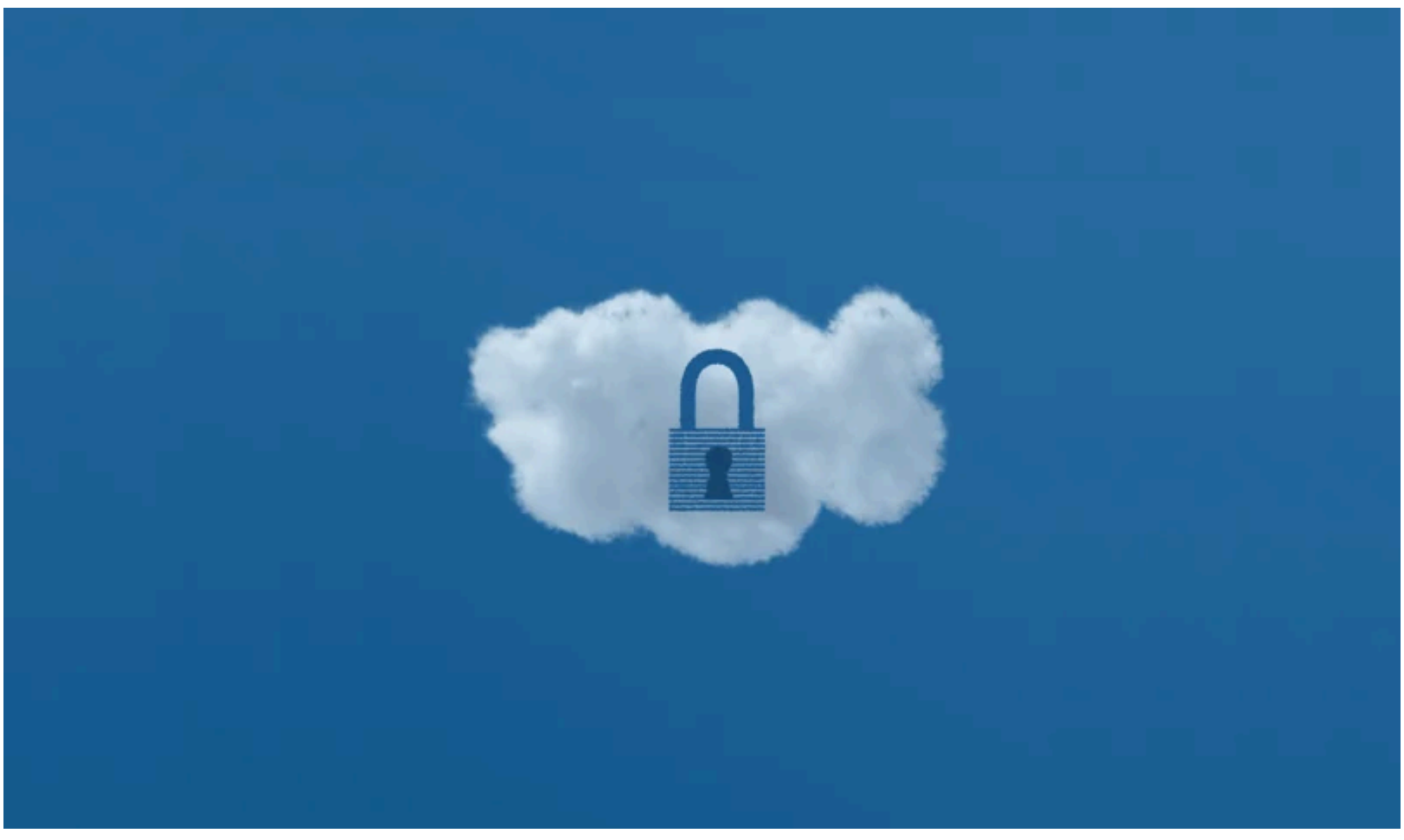
It may seem silly to buy a tool to help you map your own data. It's your company, your data...shouldn't you be able to figure out where everything is?

Perhaps an in-house project could find all sensitive information. But remember, identifying sensitive data and where it resides is going to become the foundation your GDPR compliance project. If this step is wrong, everything else could crumble. With fines up to 4 percent of an organization's annual global turnover, this isn't a chance you'll want to take.

A surprising number of companies choose to go with manual data-discovery projects, where sensitive data is tracked on paper or excel sheets. However, it is a major problem when an information manager asks to have a look at a company's sensitive data, and they pull out a spreadsheet with information that is months out of date.

This is why discovery tools are so beneficial. They are able to provide speedy insights into sensitive data and systems because they have a permanent connection to your data source. Data fluctuates by the second, and this can only be tracked when data discovery is as a continuous process.

There is also the issue of cloud to be considered. Jerry Irvine, CIO of Prescient Solutions, says the top cloud and data security issue that companies face is a "lack of understanding that they are already in the cloud and they should [be] protecting themselves accordingly."



Cloud storage and processing adds another dimension to the already sprawling issues of mapping out sensitive information. While cloud companies have their own GDPR standards to meet, it is ultimately up to you to make sure all sensitive data remains secure whether it is in your possession, in a cloud, or transferring in between. The right tool can do all that for you.

Instead of diverting your IT team's efforts, find a tool that is a good fit for your company. This will allow you to save the time you would have invested in trying to map your sensitive data in-house. Plus, as you move forward with your GDPR compliance project, you can be sure your data continues to be monitored.

Step 2. Assess and Respond to Data Risks

Data security can no longer be viewed simply as an IT problem. It is a business problem that affects all departments and the company's bottom line. Global spending on data security grew 7.6 percent last year, and shows no sign of stopping. The average U.S. company with over one thousand employees now spends over 15 million dollars a year fighting cybercrime.

Once you've uncovered your sensitive data, it's time to assess the risk. A good place to start are Privacy Impact Assessments (also known as Data Protection Impact Assessments), which are outlined in Article 35 of the GDPR. These assessments evaluate the impact of a company's processes on customer information. They should contain a description of processing operations including their necessity, proportionality, purpose, and the imposed "risks to the rights and freedoms of data subjects."

Privacy Impact Assessments are meant to identify data security problems so companies can address them before a breach occurs. This step should occur after you have located all sensitive data in your organization. You cannot examine the security of sensitive data if you don't know where it is.

A robust risk assessment identifies the following parts:

- The movement of sensitive data between departments and data siloes
- The volume of sensitive data your company stores and processes
- The liability cost of sensitive data
- The number of users who have access to sensitive data
- The physical location of sensitive data

Now that you have identified the weak spots in your security, create a plan to address them. When you know where your highest vulnerabilities lie, you are able to shape your security plan accordingly.

Discovering where your sensitive data is and how it moves is extremely valuable. Security plans built without this knowledge are not going to be as effective as plans tailored to deal with your company's specific weak points.

company's weaknesses.

Discover how to "Constantly Discover and Protect Sensitive Data for GDPR" in our next GDPR blog > >

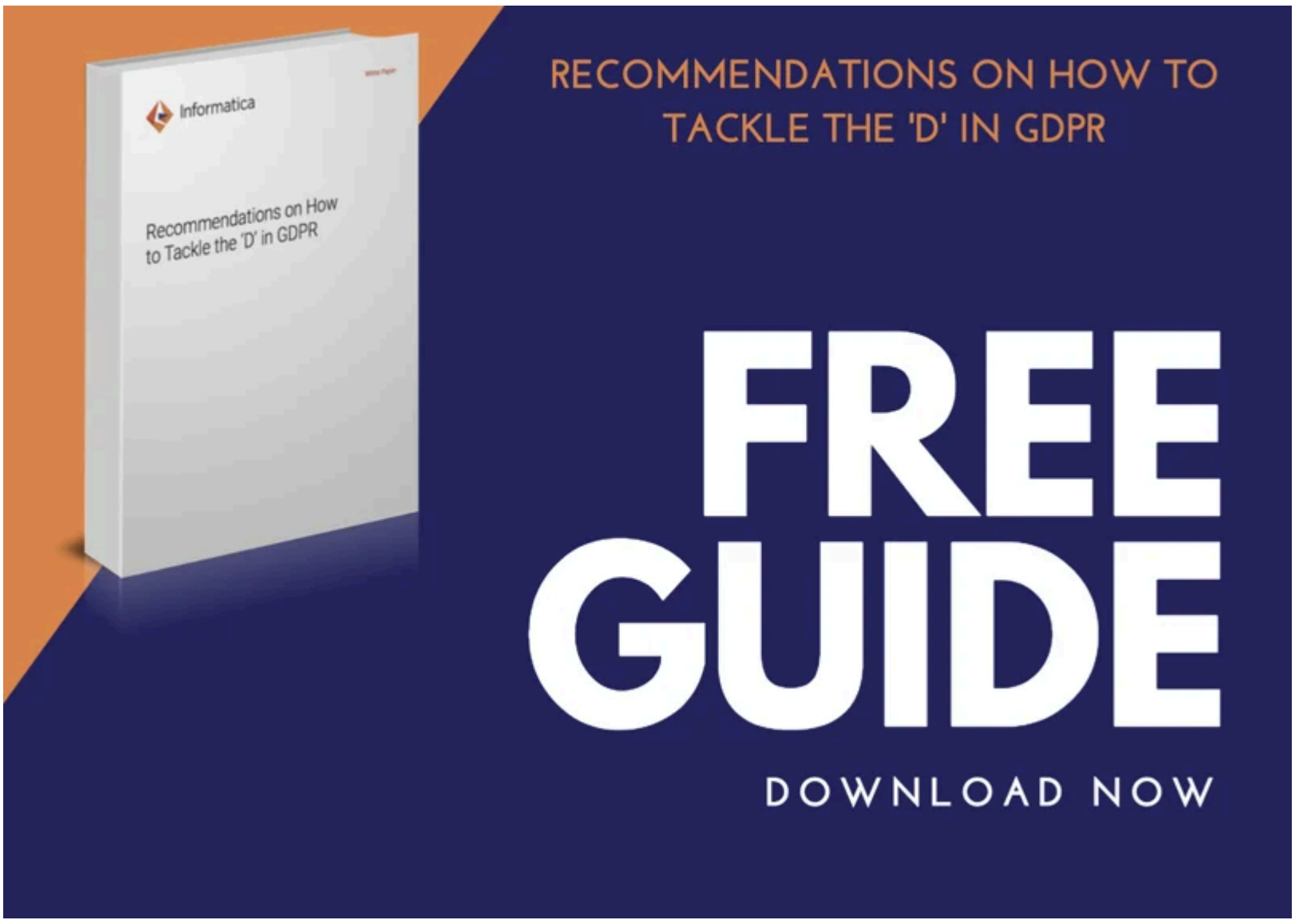
Step 3. Monitor Implemented Security Processes.

Continue to check in on your data security practices from time to time to make sure no weak points develop.

Once you've identified your sensitive data, assessed its risk, and updated the necessary data security measures, you are well on your way to being GDPR compliant. So, what happens after your compliance project is stamped complete?

Do not make the common mistake of deciding that data security is now complete. Many companies made this error after the Data Protection Act (DPA) of 1998 was implemented. They upped their security, became compliant, then placed data security on the back burner.

Do not forget how rapidly technology is changing. Once you become GDPR compliant, pick a date when you will reevaluate your company's data security. There's nothing wrong with being the company who continually examines and improves their data security. Become proactive rather than remaining reactive. Your customers will thank you for it.



Posted by PDI Marketing Team

Pacific Data Integrators Offers Unique Data Solutions Leveraging AI/ML, Large Language Models (Open AI: GPT-4, Meta: Llama2, Databricks: Dolly), Cloud, Data Management and Analytics Technologies, Helping Leading Organizations Solve Their Critical Business Challenges, Drive Data Driven Insights, Improve Decision-Making, and Achieve Business Objectives.

Submit your email below to book a consultation with PDI !*

SUBMIT

Share

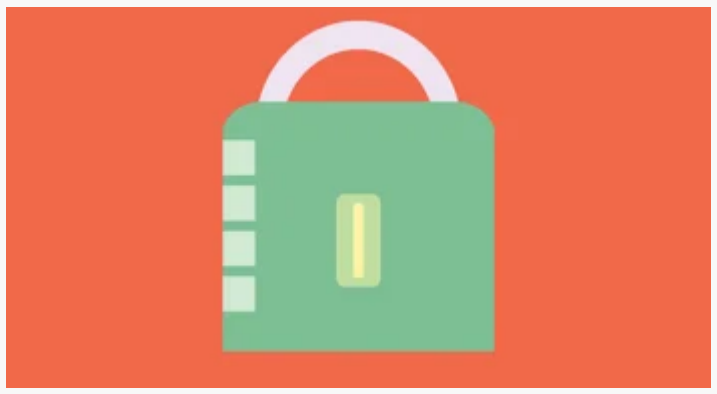
Share

Share

Related Articles

[Constantly Discover and Protect Sensitive Data for the GDPR]

[What is GDPR: Your 5 Minute Brief]



[Yes, GDPR Compliance is Worth the Cost]