Constantly Discover and Protect Sensitive Data for the GDPR

Posted by PDI Marketing Team

Published: July 27, 2021

The European Union's General Data Protection Regulation will come into effect May 25th, 2018. Companies are working to understand how the GDPR will affect them and how they can comply. Some companies will only need to tweak a few processes, while others are facing entire overhauls of their data processing and data security systems.

Discover what stands between you and GDPR compliance in our step-by-step guide > >

GDPR goes further than the Data Protection Act in encouraging companies to adopt privacy by design. Privacy by design is when data protection and customer privacy is built into every step of the data process, rather than thrown in as an after-thought.

When data security is a part of the entire process instead of the last step, the risk of a data breach plummets dramatically. Data can be more efficiently masked and de-identified, traced and protected.

This may sound like a complicated process, but it doesn't have to be. Informatica's Detect and Protect system is made of two tools that can discover, assess, de-identify, and protect all sensitive data within your company.

Sound too good to be true? It's not. Informatica focuses on creating integration solutions that mesh seamlessly with a company's entire database, rather than the traditional tag-on tools. Their Detect and Protect system is a top-tier solution, and it may just be the answer to your GDPR compliance initiative.

Informatica Detect and Protect – A Quick Peek

Informatica Detect and Protect pairs Secure@Source with Data Masking, giving you all the tools you need to ensure GDPR compliance.

Data Masking minimizes your sensitive data footprint with a combination of dynamic and persistent data masking. Dynamic Data Masking acts as a layer between sensitive data stores and unauthorized users, ensuring that only employees with the proper level of clearance can view sensitive data. Persistent Data Masking is used in development or testing environments. It is able to take sensitive data and create a high-quality data set that is robust enough to be utilized in testing environments and exposes no sensitive data.

Secure@Source uncovers and tracks sensitive data. This allows an organization to see if customer data is being used for the purpose it was intended. If customer data is being moved or replicated unnecessarily, Secure@Source will inform you, allowing you to minimize the spread of sensitive data.

Discover 3 steps to identifying and protecting your sensitive data for the GDPR > >

GDPR gives customers the right to be forgotten. When an individual requests their records be erased, Secure@Source can locate all places that the customer's information is stored so it may be erased. A second option uses Informatica Data Masking to remove all association between an individual and their data in the system.

This is merely a highlight of Informatica's Detect and Protect system. Read on for a deeper look into Secure@Source and Informatica Data Masking!

Secure@Source – Discover Sensitive Data and its Risk

Companies often consider identifying sensitive data security to be phase one of their GDPR compliance project. Once it's complete, they move on to phase two and data discovery is forgotten.

However, an annual assessment of the sensitive data in your company will be out of date eleven months of the year. And that's being generous. For some, a manual tracking system will be out of date the day after it's finalized.

Data changes too often to ever truly be 'complete.' This is especially true when dealing with sensitive data. A data breach can cost you revenue, customers, even your reputation.

Informatica Secure@Source is a dynamic data security tool that can keep up with dynamic data. It uncovers all sensitive data, assesses its risk, and keeps you up-to-date on the status of your data.

"We've probably never been in an age where there is so much processing of data… So to think of discovery as a one-time process as a foundation stone of GDPR is not accurate, is not good enough. We need to think of discovery as an ongoing, real-time process. We can't have a discovery system that is based on where the data used to be three months ago." – Paul Garstang, Data Security Leader EMEA*

Discovery is a great place to start, but Secure@Source goes one step further by assessing the risk of all sensitive data. It identifies high-risk data stores and locations, showing you the most vulnerable areas of your company.

Many factors come into play when determining risk. Secure@Source considers facts such as how many users can access sensitive data and how often they look at the data. You can click on each domain to access a list of all sensitive fields in the domain, letting you know exactly what type of information is where.

Once Secure@Source identifies where your sensitive data is, it will provide a list of users who have access to GDPR data within your company. The more people have access to sensitive data, the higher the risk of a breach.

This visibility allows you to determine which users have unnecessary access to sensitive data and to restrict unnecessary access. You will know exactly who has access to sensitive data today, not last week or three months ago.

With Secure@Source companies can better understand their data risks and react accordingly. Companies can decide for themselves which data is labeled 'sensitive,' giving them the ability to track certain types of data that are determined sensitive by the company. This can include more than GDPR-relevant data, such as software or classified projects.

The proliferation function in Secure@Source will map out your data and how it transfers between data domains. It can trace the replication of sensitive data and pinpoint any unprotected data. Secure@Source handles structured and semi-structured data, and there are plans for adding non-structured data processing capabilities in the future.

Informatica Data Masking - Secure Customer Information

Once sensitive data is classified and the high-risk areas have been identified, it is time to secure your data. Informatica Data Masking secures production, test, and development data by either dynamic or persistent data masking.

Informatica Data Masking has helped Cognizant, Bank of Dalian, and Transamerica protect their sensitive data, their customer relationships, and their reputation.

Persistent Data Masking

developers with a usable data set. In these cases, sensitive data is permanently changed.

Sensitive data is often used in testing environments because meaningful, high-quality data is necessary for accurate testing. However, this exposes sensitive data and increases the risk of a data breach.

Companies take this risk because poorly masked data is not robust enough to accurately test code. Using low-quality data for testing can result in non-functional code being released, which makes the risk of a data breach seem worth the cost.

However, GDPR has placed heavier restrictions on test data environments, banning this type of testing in certain circumstances.

Informatica Data Masking solves this conundrum by masking sensitive data in a way that produces high-quality data that is robust enough to be used in testing environments.

Persistent Data Masking can shuffle employee ID's or other identifying information, substitute names consistently throughout the data set, utilize a credit card technique that retains a validated credit card number while masking the sensitive numbers, and more. It can also change emails to reflect name changes that occur in the masked data set.

Dynamic Data Masking

For production data, sensitive data is masked when any unauthorized users attempt to access it. This allows Dynamic Data Masking to protect data with minimal impact. It acts as a filter between the data store and users without changing the data in the database.

Dynamic Data Masking captures all sensitive data and masks it depending on the admin level of the individual attempting to access the information. It applies different levels of masking based on which user is accessing it.

Individuals with top clearance are allowed to see the original sensitive data. Non-authorized individuals will only be able to view data that has been masked.

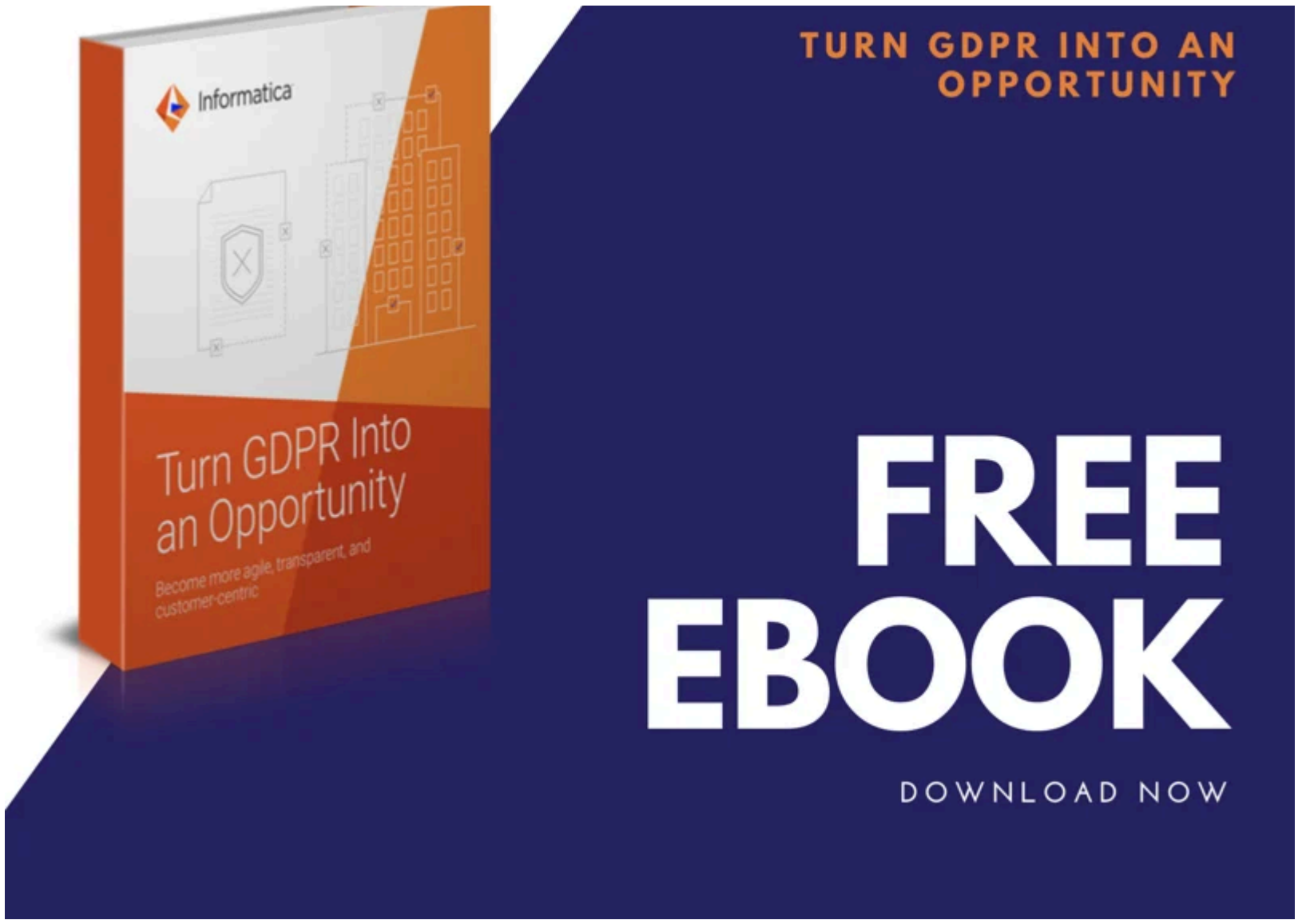
You can also create clearance levels in between, with some employees being granted access to view some pieces of the sensitive data but not others.

For instance, IT Administrators may need to know the type of information in a data set but do not need to see the full values. Informatica's Dynamic Data Masking can allow them to see part of the information but not all.

The rules applied by Dynamic Data Masking are flexible and customizable. Many different levels of clearance can be created, helping companies comply with GDPR and other security policies that are in place.

Dynamic Data Masking is robust enough to be used in real-time. Any time an employee attempts to access sensitive data, Dynamic Data Masking will look at their clearance level and protect the data with de-identification where necessary.

*Sourced: Brighttalk



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

[3 Steps to Identify and Protect Sensitive Data for the GDPR]

[Your Guide to Becoming CCPA Compliant]

[Master Data: A Strategic Asset for Your Business]