GDPR and the Data Dilemma

March 15, 2018 by Kon Leong

(garagestock/Shutterstock)

There's a data dilemma in the world today. To provide the best and most personalized services to clients and to get the best analytic insights, companies need more data than ever before. Yet to comply with ever-increasing privacy regulations, they need to shed excess data and limit its use.

Take the financial services industry. From SEC 17a-4 to FINRA, banks have been subject to data regulations for decades. SEC 17a-4 requires copies of certain communications be stored for five to seven years on WORM storage where it cannot be altered. It's a fairly straightforward requirement that improves review and audit capabilities with a singular goal: avoid fraud.

Yet this requirement entailed intensive restructuring of internal policies and systems. It has taken millions of dollars in fines for the industry to take notice and become satisfactorily compliant.

When the General Data Protection Regulation (GDPR) comes into full effect May 25, 2018, things will get even more complicated. The global privacy landscape will be irrevocably changed. With a regulation as complex and far-reaching as GDPR, organizations should learn from the past and arm themselves before multi-million euro fines — up 4 percent of global revenue — get doled out.

The Challenge

GDPR exists to protect the rights and freedoms of European "data subjects." It covers everything from data processing and transfer to organizational structure. When it comes to unstructured data, such as emails and files, there are three key requirements:

Portability. Data subjects have the right to access all data held about them by any organization. Organizations must be able to comprehensively locate and compile this data and provide it in a timely manner.

Erasure. Data must be erased when the controller ceases its approved use, the data subject removes consent or invokes Article 21 rights, or other regulated circumstances occur.

Consent. Data processing under GDPR must be "freely given, specific, informed and unambiguous." Personal information must be properly managed to ensure it is only processed for approved purposes.

While the capabilities needed to comply with these requirements are fundamentally similar to those required during the eDiscovery process, our research shows that 81 percent of organizations are not very confident they could identify and remediate employee data. Organizations need to expand these existing capabilities and turn them inwards to become fully compliant with GDPR.

The Unified Approach

SEARCH

Search...

RECENT NEWS

As Object Storage Booms, Analytics Issues Emerge
April 19, 2018

New Device Spots Quantum Particle 'Fingerprint'
April 18, 2018

Serverless Computing: Big Potential – with a Few 'If's'
April 17, 2018

VMware Sharpens Focus on Hybrid Cloud
April 17, 2018

DARPA Scales Its Electronics Effort
April 13, 2018

Point solutions won't cut it anymore. In fact, they are the source of the problem. How can someone control data and privacy within their organization if all of that data is in silos, scattered across the organization? This central control — a single point of access, if you will — is the lynchpin in finding an approach that goes beyond meeting any specific regulatory requirement and ensures privacy as GDPR requires: "by design and by default."

To comply with this and myriad other regulations, companies would be wise to implement comprehensive content indexing, minimization and collection processes. Together, these capabilities enable organizations to handle complicated subject access requests (SARs).

Think of all the elements involved in responding! When customers request that their data be deleted for instance, this applies to more than mailing lists and databases. It involves customer service chat or recordings, scanned contracts and anything else containing their personal information. Without a proactive governance system in place, it could take weeks to months to sift through the data – with no assurance that such a manual process is even defensible to regulators.

Now imagine responding to requests like this *every day*. As the number of data sources and management systems multiplies, so does the complexity of locating and acting upon the information they contain. Without a unified approach to information governance, it would be incredibly difficult — if not impossible — to efficiently comply, even just with SAR requests. And that's not the only concern.

The Analytics Era

From trawling social media sites to employing sentiment analysis on email, analytics are the backbone of many big business decisions. Since GDPR covers all personal data held on EU residents, businesses need to rethink how they manage the data they use. A single piece of data analyzed, even in composite, about someone who has requested that their information be deleted could result in previously unparalleled sanctions.

The lesson? Disparate data repositories are anathema to GDPR compliance. It's necessary that every department is acting upon the same source to ensure data, once deleted under GDPR, is deleted everywhere. Without a single point of access, it would be nigh impossible to ensure all enterprise data is processed, viewed and retained in a compliant way. The law doesn't care that human error is unfortunately inevitable, so it's time to employ information governance technologies — such as a centralized archive — to bridge the gap and ensure corporate data can be effectively analyzed and managed. After all, if you opened your inbox next May to hundreds of subject access requests, would you be prepared?

Kon Leong is president, CEO and co-founder of ZL Technologies.

Share this:

Tweet Share G+ reddit this!

Related

Pegasystems Introduces Pega GDPR Accelerator
April 10, 2018
In "Happening Now"

Dataguise Announces Four Steps Enterprises Can Take to Accelerate GDPR Compliance
August 9, 2017
In "Happening Now"

Got GDPR Anxiety? Here Are 3 Must-Do's
April 5, 2018
In "Government"

Categories: Financial Services, Security, Slider: Front Page, Slider: Security, Software
TAGS: cybersecurity, data security, GDPR, regulatory compliance

Add a Comment

Along These Lines

Got GDPR Anxiety? Here Are 3 Must-Do's

Cybersecurity: Defending the Defenseless OS

How to Prevent GDPR Mistakes

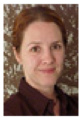
Attacks, Regs Driving Security Spending

CONTRIBUTORS

Doug Black
Managing Editor

John Russell
Editorial Director

George Leopold
Senior Editor


Tiffany Trader
Senior Editor

Alex Woodie
Contributing Editor

Steve Conway
IDC

UPCOMING EVENTS

Percona Live Open Source Database Conference
April 23

IP EXPO Manchester 2018
April 25 - April 26

GlobusWorld 2018
April 25 - April 26

Intelligence Analytics 2018
April 30 - May 2

BigIT Diverse 2018
May 8 - May 9

View All Events

Name *

Email *

Website

Your Comments

Add comment

□ Notify me of follow-up comments by email.

About EnterpriseTech | Contacts | Back to Top