CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | July 11, 2022

The Great Data Reset: How to Manage Risk Around Massive Data Growth

Tito Adeyemi
tadeyemi@veralocity.tech
(404) 450-1850

Dan Panitz, Esq.
dpanitz@veralocity.tech
(415) 999-4440
(203) 254-2927

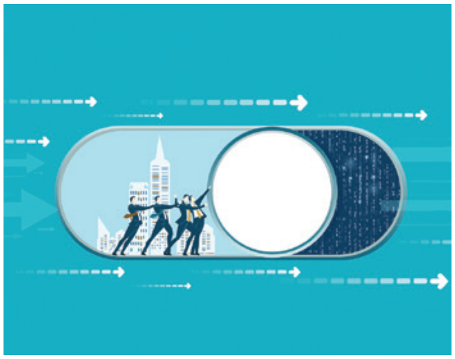
BY DAN PANITZ AND TITO ADEYEMI

One of the most prominent challenges facing global businesses today surrounds the deluge of massive data growth and the risk it presents to companies as the management issues of this data take shape. This risk comes in several major forms, including the legal/regulatory exposure from investigations and litigation, ongoing cybersecurity vulnerabilities and unsustainable increased spend on its storage.

According to Gartner Research, people generate 2.5 quintillion bytes of data (2.5 million TB) each day, with nearly 90% of all that data being created in the last two years alone. As a result, unstructured data (or data that is not arranged according to a preset data model or schema and therefore cannot be stored in a traditional relational database) is a major problem for 95% of businesses.

While data disposition is growing, it is vastly outpaced by creation of new data which companies consume, ingest and maintain within a vast array of disparate systems. These issues then compound when two companies merge or another is acquired, with the integration process which follow those trigger events frequently confronting large additional multiples of both new and legacy data. In short, the call to action for companies to focus on ongoing IT Asset Destruction (ITAD) is at our doorstep and won't go away without concerted, efficient and continual processes being implemented and refined to evolve with a company's data landscape.

What Is Data Beyond Its Legitimate Business Purpose (LBP)?



Credit: IRStone/Adobe Stock

As a guide to our growing laws in the United States, the purpose limitation principle of the General Data Protection Regulation (GDPR) requires that, when collecting personal data:

- There must be a clear expression to the data subject the purpose for the processing of a person's data from the outset;
- The purpose for the processing of a person's data must be set forth in privacy information provided to data subjects and must be documented as part of the business' record-keeping activities;
- The business must comply with your transparency obligations to inform data

subjects (individuals whose data the business is processing); and

- The business must make sure that if it ever intends to use data for any purpose other than what was originally specified, that further use is compatible with the original purpose or you get specific consent for the new purpose, i.e., lawful, fair, and transparent.

In 2018, the California Consumer Privacy Act (CCPA) extended consumer privacy protections to the internet, which remains the most comprehensive internet-focused data privacy legislation in the US with no federal law equivalent at this time.

Under the CCPA, consumers have a right to access through a data subject access request (DSAR) categories and specific pieces of personal information held by covered businesses. Businesses can't sell consumers' personal information without providing a web notice with a "clean and conspicuous link", giving them an opportunity to opt-out.

Like the GDPR, there is also a "right to delete" consumer personal information on demand (with limited exceptions). The CCPA also confers consumers a limited right of action to sue if they're the victim of a data breach with legislation in the works to broaden consumers' private right of action to sue on other grounds.

It is important to note the CCPA contains a very broad definition of personal information as: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This casts a wide definitional net and is similar to the GDPR's own expansive view of personal data.

If any of this strikes fear into company leadership and the fiduciary duties to their shareholders for the risk it presents to the business, we would argue responsible data, legal and corporate leader stewardship are not dead yet.

How Long Should a Business Hold Data?

The regulatory periods requiring a business to hold certain types of data vary but can be easily ascertained and applied. *From there, the general rule of thumb should be to maintain data for its LBP period and its applicable required regulatory or litigation hold period and not one day thereafter.* **By employing this approach, the immediate business impact will measurably reduce a company's litigation, regulatory and reputational risk while generating quantifiable data storage savings.** For the latter impact alone, we can easily track and report on USD savings in the seven and eight figures for many businesses. Done continually with active management, we are able to document and prove out very significant risk and spend reduction year-over-year.

To understand the nonexclusive risk spectrum for companies which maintain data beyond its applicable LBP, regulatory or legal hold period presents, we highlight the following:

- Data security, ransomware and virus risks (global ransomware damage costs reached $20 billion in 2021 — which is 57X more than it was in 2015, with an attack on businesses every 11 seconds in 2021, up from every 40 seconds in 2016)
- Noncompliance liability related to evolving regulations and law (eg., CCPA, GDPR, data breaches, etc.)
- Penetration vulnerability and data loss exposure of computer systems, platforms and application program interfaces (APIs)
- Litigation exposure — data which should have otherwise not been maintained beyond its LBP, now becomes discoverable and potentially increases existing and new claim liability

- Scope creep — When data is maintained in the cloud, costs accrue over time based on the size, duration and other characteristics of the workload. That means budgeting for and managing cloud resources is a constant ongoing process that requires unique tools, oversight and governance.

In the FTC's "Protecting Personal Information: A Guide for Business," the "Scale Down" principle was made: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. … If you have a legitimate need for the information, keep it only as long as it's necessary." While the writing was already on the proverbial wall, it has become clear today that nothing short of ITAD will adequately address the massive current and ever-increasing risk for businesses on their legal, regulatory and spend exposure in maintaining data beyond its LBP lifecycle.

A prime example for the need to continually monitor and remove data beyond its LBP is evident in a number of trigger events, such as those following integration of corporate acquisitions, which frequently involve duplicative systems/platforms, API vulnerabilities and other related exposures. From a litigation standpoint, we additionally observe the evaporation of the ability to successfully assert an "unduly burdensome" objection to a document production request when that data is readily available (versus the same having been properly destroyed post its regulatory/litigation hold period subject to an updated and enforced data retention and disposition schedule).

What Are Businesses Doing About This?

To combat the avalanche of new data and its associated risk, organizations need to undertake a revised assessment of existing data retention/disposition, security and information governance policies. All these policies must then be implemented, enforced, refined and tracked at regular intervals and upon key trigger events. Engaging organizations such as Veralocity for these purposes is generally the best first step as teams begin to re-assess data retention and disposition policies (which are well intentioned but rarely fully executed upon, quality controlled (QC'd) or enforced consistently).

Other trigger events for ITAD re-assessment and implementation include where retention policies may have become obsolete. This frequently occurs in situations where an organization adds a business line, sunsets software, acquires new software, or even increases the usage or storage of specific data types. This further evidences a call to action for corporate data retention/disposition, information governance and data security policies to become "living" documents which are updated and refined in implementation as the business and data landscape evolves. Information governance policies and their siblings should now not only cover changing data itself, but also data and technology events which encompasses the whole. Without these processes being actively managed, corporations face the equivalent of a perfect storm in a row boat.

Managing the Data Wave

To meet the exponential challenges from this massive data growth, the answer lies within tailored processes, subject matter experts (SMEs) and technology accelerators such as file analysis tools and managed services around related processes, combined with archiving solutions, and data disposition/destruction options. No magic here, but we need to determine and accomplish the following:

- Map where each type of data maintained lives, migrates and travels
- What are respective LBP, regulatory and legal hold requirements by data type
- Who are the business owner(s)/cost center(s) and use constituents for each of the aforementioned data types
- Apply the principal of least privilege (Access privileges for any user should be limited to resources essential for completion of assigned duties or functions, and nothing more)
- Tag, monitor and schedule end-of-LBP/related lifecycle ITAD for those respective data types
- Log, audit and report upon the above process inclusive of exceptions

This file analysis, data mapping, restriction of access and scheduling for destruction (as appropriate) exercise is not one-and-done, as mentioned above, but must be regularly revisited at the most appropriate periodic intervals and as the business and the data it manages evolves.

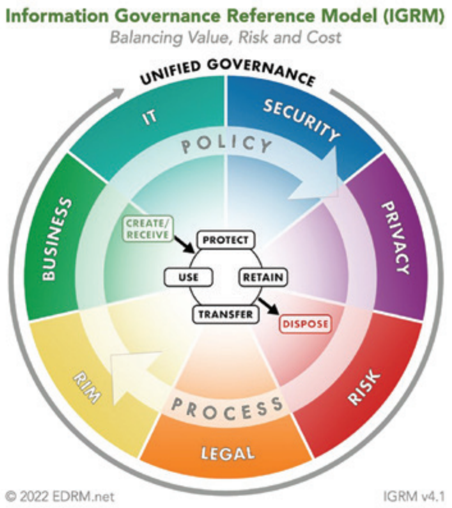
Next, we codify what we have identified to develop or revise right-sized retention/disposition, information governance and corresponding data security policies to that current assessment or state-of-the-state for the business. Don't forget to flag any upcoming changes to the business which are anticipated or experienced as they could conceivably affect these policies.

From there, our SMEs and value-add consultants can then tailor the right processes to address your current ITAD prospects, formulate the process to effectively implement that schedule, manage and administrate such deployment and track/refine the process from end-to-end with detailed key performance indicator (KPI) reporting on the specific business impact to risk reduction, cost avoidance, and savings achieved.

Next Steps

In a post 2020-2021 COVID world of massive and increasing waves of new data upon us, it is critical for companies to reduce their risk through ITAD and transform their data retention/disposition policies from the shelf to active management which mirror current business functions and data.

Like any good plan, the next step of action is implementation which becomes a solvable challenge achieved through an iterative process, the right consultants/SMEs and technology accelerators as appropriate. With the understanding that all successful initiatives to reduce risk begin with a conversation, we invite you to the same and stand ready to help.


Information Governance Reference Model (IGRM)
Balancing Value, Risk and Cost

© 2022 EDRM.net
IGRM v4.1

Dan Panitz, *Veralocity President and CEO, is an experienced attorney based in New York with more than 25 years of combined legal, technology and corporate advisory experience. Having worked with SEC Enforcement and NASD (now FINRA) Arbitration, Panitz also holds anti-bribery and corruption specialty certifications for the PRC, U.K. and the United States.*

Tito Adeyemi *is VP of Solutions Architecture for Veralocity. She served as Director of Infrastructure and Operations at Gartner, counseling leadership boards and business leaders on functional and operational best practices for data retention, e-discovery, file analysis, software, data management, GDPR, DSAR, backup and related processes.*