6 STEPS FOR BETTER DATA RECOVERY UNDER GDPR

Compliance is a main priority for many executives. Financial services, insurers, government agencies and so many others must comply with regulations governing how they use and protect data. As more

data enters through more sources, you need to look at all of the angles to safeguard your clients and protect your brand integrity.

The General Data Protection Regulation (GDPR) is a major advancement in data protection law and will significantly impact your business. You should start preparing now to make sure that you are compliant when the law comes into effect next May. The regulation states that organizations must have a formal process in place to restore the availability of, and access to, personal data in ***a timely manner*** in the event of any physical or technical incident.

Does your organization have ability to locate all instances of personal data pertaining to a given data subject?

Are you prepared to recover data in a timely manner with proof that the information is accurate and the process is repeatable?

If you answered no, you are not alone.

94% of the CIOS in the United States say they have data that is affected and over 90% of them are worried about the impact it will have on their ability to process that data.[1] Organizations outside the EU are subject to the regulation and the penalties for non-compliance could be up to four percent of revenue or twenty million euros, whichever is greater.

The blueprint for GDPR data recovery

To meet the obligations of the GDPR, we suggest you consider these six steps for better data recoverability:

1. **Establish what you have.** Begin identifying where data is stored across multiple formats and applications, in different departments, divisions or subsidiaries. Any data associated with personally identifiable information (PII) that is gathered on a citizen of the EU needs to be located.
2. **Develop a detailed data recovery plan.** Define categories of potential breaches and a procedure for notifying citizens and authorities about personal data breaches in a timely manner (within 72 hours in most cases).
3. **Implement security techniques.** Explore techniques such as dynamic data masking, pseudonymization, and encryption of personal data to ensure data is disguised and is no longer personally identifiable.
4. **Remove single points of failure.** Your current state of compliance and disaster recovery (DR) plans may not account for data corruption or data loss. DR testing is extremely costly to repeat regularly to prove continued compliance. Your existing DR plan may not help comply with GDPR.
5. **Prove timeliness of recovery.** Develop and document your process to recover data and agree with IT and risk management teams on expected recovery times.
6. **Enforce testing and simulation.** Perform a recovery simulation and clearly document techniques. This will allow you to identify bottlenecks in the process, which if removed, would allow for even faster recovery of data.

We hope this helps you get started and thinking about how you can ensure compliance with GDPR. BMC has robust Recovery Solutions for both the Db2 and IMS platforms that will enable customers to meet GDPR requirements.

[1] http://resources.compuware.com/research-improved-gdpr-readiness-businesses-still-at-risk-of-non-compliance